

Decentralized Cellular Networks

Towards Blockchain Enabled Cellular
Overlays

Author: Steven Platt

TESI DOCTORAL UPF / year 2021

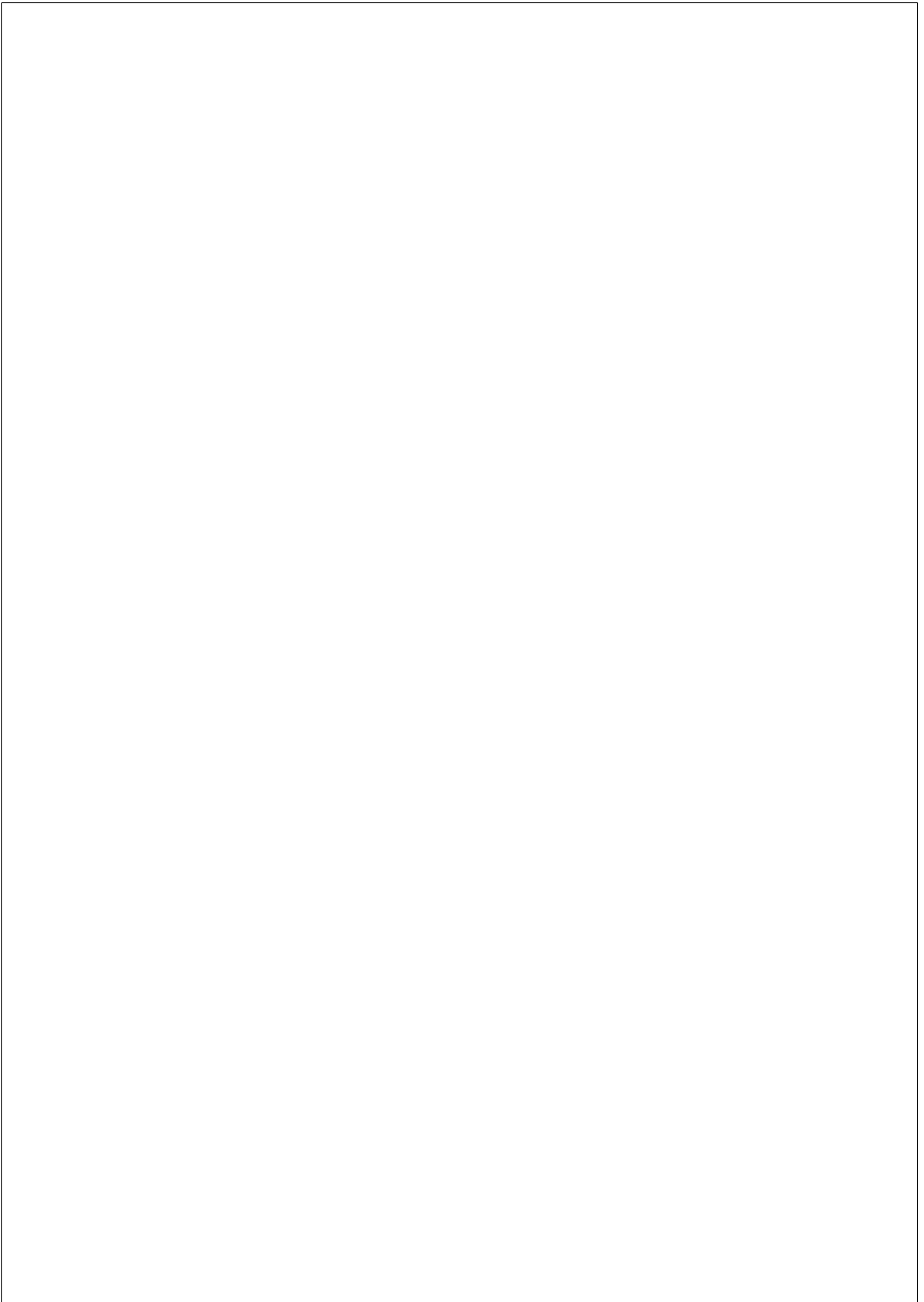
THESIS SUPERVISOR

Miquel Oliver

Department of Information and Communications
Technologies



To Gülhan, my better half. We did it.



Acknowledgements

I would like to thank my supervisor Dr. Miquel Oliver, for his foresight in selecting this novel path for wireless research, and for providing the autonomy and guidance to undertake this investigation. I would also like to thank my lab mate, Fabio Della Valle for giving me a partner to toil along with during the PhD journey, and for adding a relaxed perspective to give balance to the extra pressure I often put on myself. To the broader UPF community, the faculty and administration, I would like to say thank you. Specifically, I would like to thank Dr. Boris Bellalta for his teachings in the year prior to the PhD journey, and his specific work in organizing the Wireless Communications Masters diploma. It was the initial reason I chose to attend UPF. Among the broader research community, I would like to thank the Centre Tecnologic de Telecomunicacions de Catalunya, specially Luis Sanabria-Russo for being a willing research collaborator, and whose passing mention that *“blockchain is just like any other network function”*, turned out to be the pivot point of my entire PhD research. To all the friends I’ve made in the beautiful city of Barcelona, specifically, my Volley Circus volleyball team - thank you, I will never forget how we won *one* game. I will also never forget Veronica Moreno, who welcomed me enthusiastically, forced me to practice my spanish, and on a few especially tough days, listened and reminded me everything would be ok - 2 years later, your *“buenos dias”* post-it note is still attached to my iMac display. To my Dad and Stepmom, thank you for a lifetime of support and for my first PC, all good things can be traced back to playing *SkiFree* on Windows 3.1. A final thank you goes to my partner Gülhan who has given support, stability, patience and love every day of the PhD journey. You truly are my better half.



Abstract

This thesis undertakes an investigation into the fit and utility of blockchain technologies within cellular networks. The core of this writing is a new 5G core network blockchain designed to be compatible with, and paired as storage for 3GPP-compliant virtual network functions. Compatibility of the blockchain design is delivered by inheriting a number of behaviors from wireless network operation, including a CSMA/CD mechanism of congestion control; a first for a blockchain design. At the carrier level, a deployment model compatible with ETSI General Autonomous Network Architecture is presented to enable decentralized service overlays. At the network edge, a novel model of transition learning allows fluid roaming of user-equipment across network boundaries. At the conclusion, the theory is combined, to reveal a model of decentralized overlays, which at the user equipment, functions in a manner similar to FM radio. A network channel radio of sorts for decentralized cellular access.

Resum

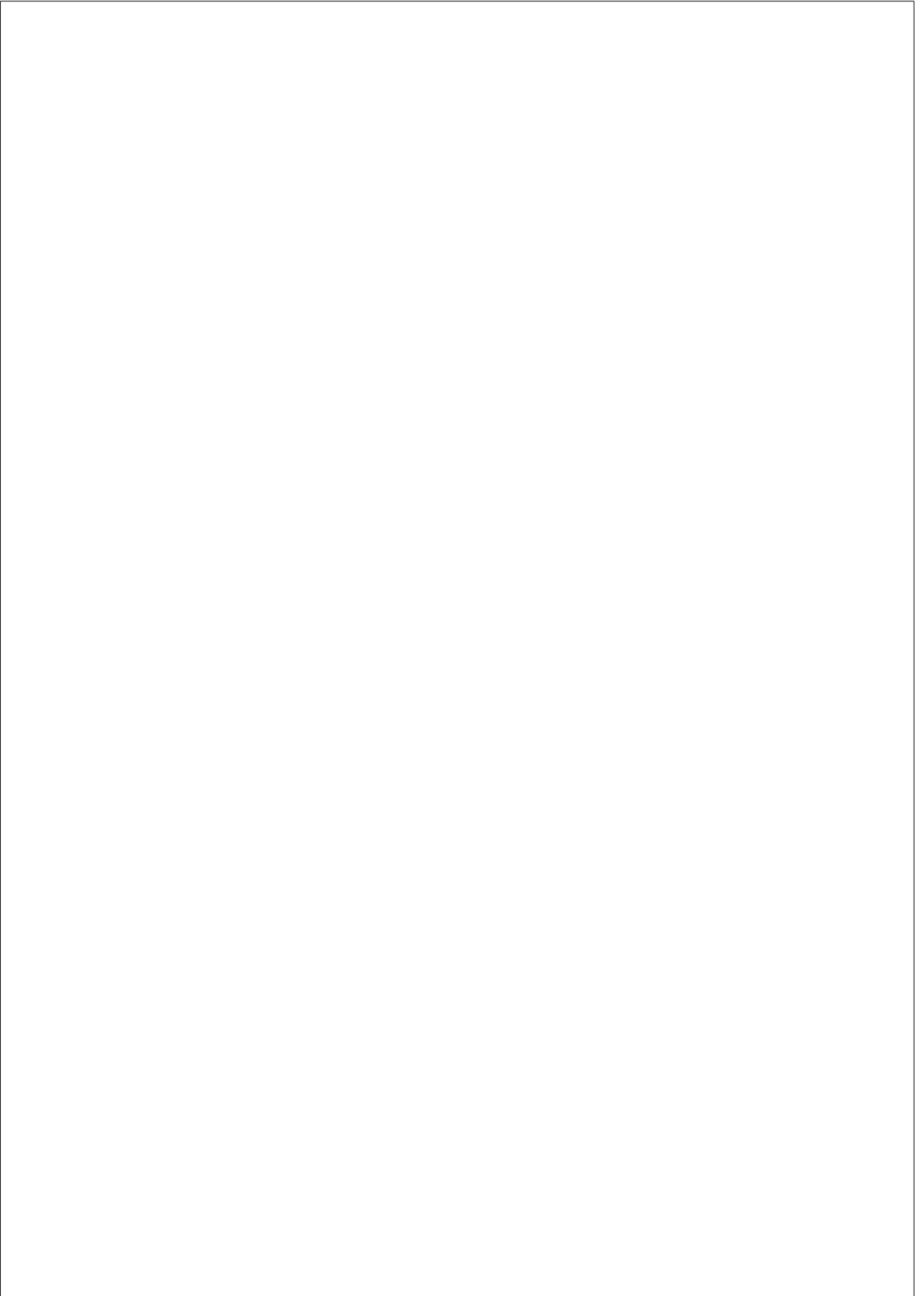
Aquesta tesi realitza una investigació sobre l'ús i l'adptabilitat de les tecnologies blockchain en xarxes cel·lulars. El nucli d'aquest treball és una nova blockchain basada en la xarxa 5G dissenyada per ser compatible i utilitzada com a emmagatzematge per a la funció de xarxa virtual compatible amb 3GPP. La compatibilitat del disseny de la blockchain s'ofereix adoptant diversos comportaments de l'operació de xarxa sense fils, inclos un mecanisme CSMA/CD de control de congestió; la primera vegada que s'utilitza per a un disseny de blockchain. A nivell de transport, es presenta un model de desplegament compatible amb l'arquitectura general de xarxes autonomes ETSI per permetre superposicions de serveis descentralitzats. A la capa de xarxa, presentem un nou model de "transition learning" que facilita una itinerància fluida de l'equip d'usuari a través dels límits de la xarxa. Per acabar, la part teòrica es combina per revelar un model de capes superposades descentralitzades, on l'equip de l'usuari funciona de manera similar una radio FM. Un canal de radio amb accés descentralitzat.

Contents

List of figures	xvi
List of tables	xvii
1 BACKGROUND	7
1.1 Secondary Access Networks	7
1.1.1 Bluetooth Technology	8
1.1.2 Television White Space Networks	9
1.1.3 Cellular Overlay Networks	11
1.2 Distributed Ledger Technologies	13
1.2.1 Composition of Modern Blockchain	18
1.2.2 Evolution Potentials of Blockchain	25
1.2.3 Blockchain Potentials in Wireless	28
2 TOWARDS BLOCKCHAIN IN WIRELESS	39
2.1 The TCP-Air Interworking Model	39
2.1.1 Introduction	40
2.1.2 State of the Art	41
2.1.3 TCP-Air Model In Detail	43
2.1.4 Sample Use Case: Vehicle Networks	47
2.1.5 Discussion	49
3 BUILDING A BLOCKCHAIN PROTOTYPE	57
3.1 Experiment: Decentralized Access Control	57
3.1.1 Introduction	57

3.1.2	Bitcoin and Ethereum: Blockchain for Currency and Contract	58
3.1.3	Self-Organizing Networks	60
3.1.4	Blockchain For Self-Organizing Networks	62
3.1.5	Discussion	69
4	THE CONTE TEMPORAL BLOCKCHAIN	73
4.1	Introduction	74
4.1.1	Enabling Lifecycle Control	75
4.2	Blockchain Unbundling	77
4.2.1	Unbundling of Currency	80
4.2.2	Unbundling of Contract	81
4.3	Federated Byzantine Agreement	83
4.3.1	Replacing Fault Tolerance with Quorum	85
4.4	The Conte Blockchain Protocol	86
4.4.1	Block Structure and Storage	88
4.4.2	Transaction and Protocol Messages	90
4.5	Handling Transmission Contention	94
4.6	Performance and Scalability	97
4.7	Deploying Conte as a Network Function	101
4.7.1	Evolving Alongside a Cloud Native Core	109
4.7.2	Carrier Security Model	109
4.8	Discussion	110
5	DECENTRALIZING CELLULAR OVERLAYS	117
5.1	Introduction	118
5.1.1	Contributions	119
5.2	Background and Related Work	119
5.2.1	ETSI Autonomic Networking	121
5.2.2	The Decentralized 5G Use Case	123
5.2.3	CoNTe: A Blockchain for 5G	127
5.3	Combining Blockchain and ETSI GANA	133
5.3.1	ETSI MANO Carrier Architecture	133
5.3.2	ETSI GANA Overlay Design	136

5.4	Evaluation	140
5.4.1	Performance Under Network Delay	140
5.4.2	Performance Under Varying Block Sizes	141
5.5	Discussion	148
6	ENHANCING MOBILE-CONTROLLED HANDOFF	155
6.1	Introduction	156
6.2	Background and Related Research	157
6.2.1	Cellular Mobility Management	157
6.2.2	Blockchain Network Decentralization	159
6.2.3	Learning Applications and Limitations	160
6.3	Transition Learning System Design	164
6.4	Evaluation	169
6.5	Discussion	175
7	CONCLUSIONS	183
7.1	Future Research	186
A	THE CONTE CSMA/CD ALGORITHM	187
B	RETIRED RESEARCH PATHS	189
B.1	BSAFE.Network Consortium	189
B.2	University of Cape Town Research Stay	190
B.3	Blockchain For Pandemic Response	190
B.3.1	Introduction	191
B.3.2	Pandemic Surveillance Prior to Blockchain	192
B.3.3	Blockchain For Digital Contact Tracing	194
B.3.4	Blockchain For Electronic Medical Records	197
B.3.5	Blockchain For Vaccine Supply Chain	198
B.3.6	Discussion	200
B.4	Spectrum Protocol	201



List of Figures

1.1	TVWS base station, client, and database flows.	10
1.2	Distributed Hash Table data structure.	15
1.3	Directed Acyclic Graph data structure.	16
1.4	Block Lattice data structure.	17
1.5	Blockchain data structure.	18
1.6	Connectivity level required to preventing forking in the Ripple Network [24].	23
1.7	IOTA graph structure and two block verification [25]. . .	24
1.8	IOTA network 51% double spending attack [25].	25
1.9	Blockchain Composability.	27
2.1	The modified Host Identity and port pairing applied with Host.	42
2.2	Bitcoin blockchain structure.	43
2.3	Air interface peering through direct supplication.	46
2.4	Layer interaction model of TCP-Air.	50
3.1	SON Architectures.	61
3.2	Redes separation of concensus and application code. . .	62
3.3	Forward hash linking in Blockchain Data Structure [10].	66
3.4	New node registration using the Postman utility and Re- des JSON API.	67
3.5	Issuing a new block using the Postman utility and Redes JSON API.	69

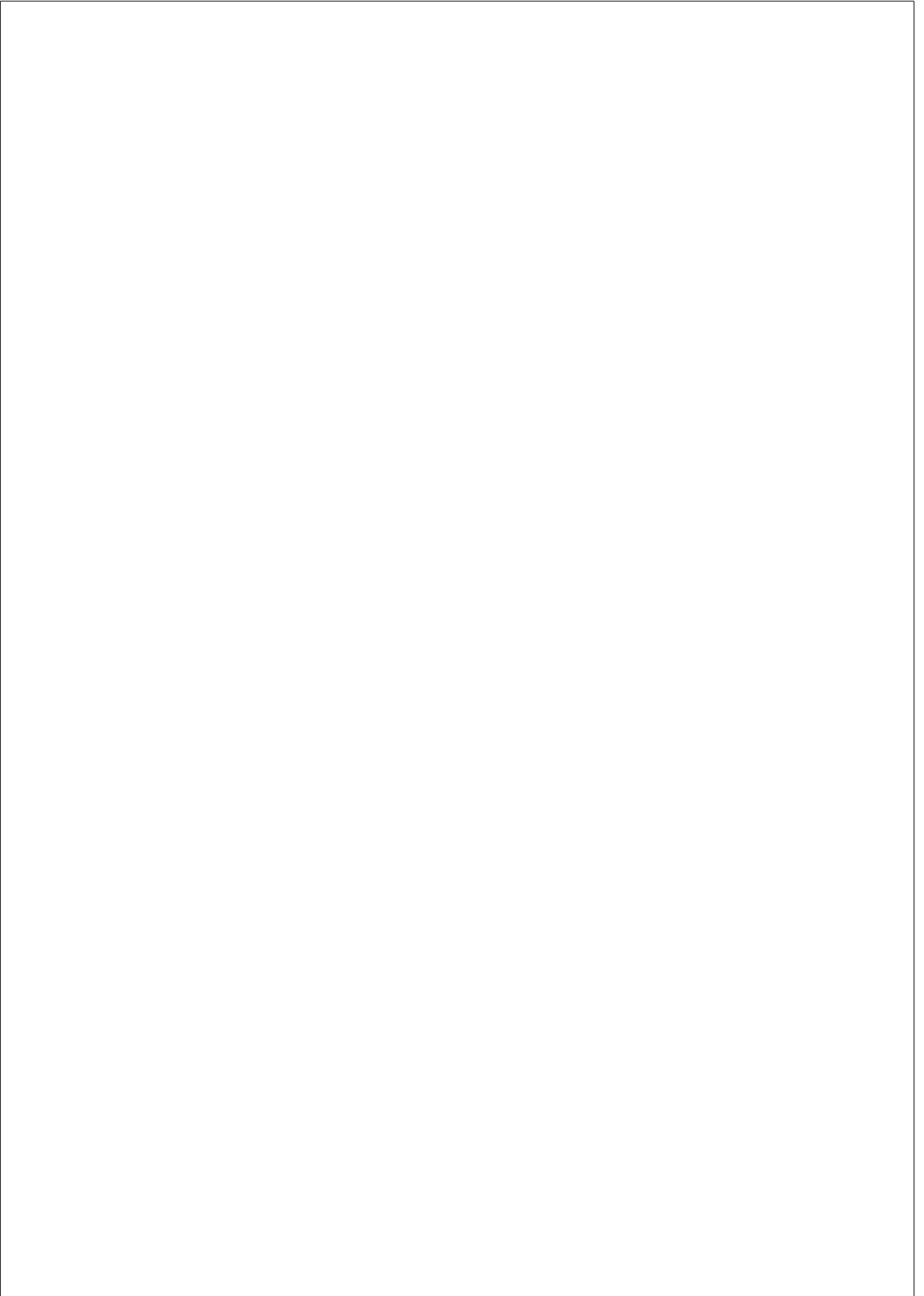
4.1	A logical representation of 5G network functions, with a single function (AUSF) being decentralized by using Conte blockchain storage.	83
4.2	Two quorum slices, intersecting at nodes $\{v_5, v_6\}$	87
4.3	Two quorum slices intersecting at nodes $\{v_2, v_4, v_5, v_6, v_8\}$	87
4.4	Example of multiple network function-specific blockchains running across operators.	90
4.5	Conte Single Round Block Commit.	93
4.6	Block throughput performance of Conte at 1,500 km node distances and maximum hops to graph edge of 10.	99
4.7	Network efficiency of Conte at 1,500 km node distances and maximum hops to graph edge of 10.	100
4.8	Block throughput performance of Conte at 15,000 km node distances and maximum hops to graph edge of 10.	102
4.9	Network efficiency of Conte at 15,000 km node distances and maximum hops to graph edge of 10.	103
4.10	Block throughput of Conte at 1,500 km node distances and maximum hops to graph edge of 50.	104
4.11	Network efficiency of Conte at 1,500 km node distances and maximum hops to graph edge of 50.	105
4.12	Block throughput of Conte at 15,000 km node distances and maximum hops to graph edge of 50.	106
4.13	Network efficiency of Conte at 15,000 km node distances and maximum hops to graph edge of 50.	107
4.14	ETSI NFV MANO Architecture: highlighting slices’ reference points and manager in an integrated NFV MANO model [36].	108
5.1	Summary representation of the 4 levels of the ETSI GANA model [30]	123
5.2	Quorum slices that intersect with nodes $\{v_5, v_6\}$	130
5.3	Quorum slices that intersect with nodes $\{v_2, v_4, v_5, v_6, v_8\}$	130

5.4	Messaging flow during a “hidden node” event; peers operating the CoNTE blockchain will resequence blocks to maintain linear record consistency.	132
5.5	Individual CoNTE blockchains (microchains) replace traditional virtual storage for individual network functions within the ETSI MANO architecture [33]	134
5.6	Decentralized 5G service overlay, using the ETSI GANA model - instantiated atop a ETSI MANO architecture. . .	138
5.7	CoNTE simulation topology shown at 1,500 km.	141
5.8	CoNTE blockchain throughput scaling at 1,500 km. . . .	142
5.9	CoNTE blockchain throughput scaling at 15,000 km. . .	143
5.10	CoNTE blockchain throughput scaling at varying block sizes and distance of 15,000 km.	146
6.1	Example transitions based on RSSI received at the UE. .	159
6.2	Example networks operating individually decentralized network functions [8].	160
6.3	2-D Markov Chain model with North [N], South [S], East [E], and West [W] transitions.	163
6.4	Handoff override decision process	166
6.5	The simulation environment using a 10-step random walk and static base station allocations.	168
6.6	Network allocation distribution over 2,000 rounds (Default Environment).	170
6.7	Allocation map of Scenario 1 (Default Environment). . .	170
6.8	Average allocation performance over 2,000 rounds using transition learning (Default Environment).	171
6.9	Monte Carlo sample of a single random walk round. Allocations marked “0” are unexplored states. (Default Environment).	171
6.10	Allocation map of Scenario 2 (Sector Load).	172
6.11	Monte Carlo sample of a single random walk round. Allocations marked “0” are unexplored states. (Sector Load).	172

6.12	Average allocation performance over 2,000 rounds using transition learning (Sector Load).	173
6.13	Network allocation distribution over 2,000 rounds (Sector Load).	173
B.1	An example SEIR model, accounting for asymptomatic spread, and spread originating from travel. Adapted with permission from [6].	193
B.2	The BeepTrace COVID-19 tracking framework. Adapted with permission from [11].	196
B.3	The Spectrum Protocol login page.	203
B.4	The Spectrum Protocol main dashboard. On the main dashboard, active contracts with corresponding frequency bands as well as recent activity are displayed.	203
B.5	The peer nodes page displaying core networks (by IP) and the sharing contracts they are connected to.	204
B.6	Adding a new network core into the Spectrum Protocol platform.	204
B.7	The map page was intended to show the physical location of base stations and their calculated coverages.	205
B.8	A benchmark tool was planned for the Spectrum Protocol dashboard as an easy way to run scripted load tests.	205

List of Tables

1.1	TVWS channel availability for the five largest population centers in the United States.	9
1.2	Comparison of TVWS (698Mhz) spectrum range.	11
2.1	TCP-Air model layers. <i>*table is not inclusive of all possible model layer functions.</i>	44
3.1	Comparison of Bitcoin, Ethereum, and Redes Blockchains [10].	63
4.1	Comparison of selected blockchain distributed ledger systems.	77
5.1	Comparison of blockchian configurations [7]	133
5.2	Comparison of total data transmission for Ethereum and the CoNTe blockchain with 30 kbit and 1,000 kbit block sizes.	144
5.3	Comparison of total data transmission for Bitcoin and the CoNTe blockchain with 3,000,000 kbit and 7,112,000 kbit block sizes.	147
6.1	Scenario 1 simulation results	169
6.2	Scenario 2 simulation results	169



Introduction

It is the ultimate goal of this research, to investigate blockchain design based on wireless network function and behavior that delivers capabilities not possible using the isolated network designs of today.

The proposed system would allow devices to scan or tune to available spectrum channels in a universally compatible way. The blockchain at the core of the research is named ”CoNTe”. Investigation of this solution was split into three core areas of research questions.

Research Question 1: Blockchain Tuning

How can blockchain technology be tuned for use in massively scaled network environments?

Existing blockchain systems have multiple features that impact how well or poor they perform in a given application. Considering the incentives, and dependencies of existing designs, it is important to investigate how the behavior of these systems can be tuned to better perform in wireless network environments. These behaviors can relate to consensus, topology formation, block size, network synchronization, fault tolerance, or additional unknown factors. The goal here is to investigate in what combinations and scale can these behaviors can be tuned to allow a blockchain design that is uniquely performant in 5G and beyond network use.

Research Question 2: Shared Spectrum Access

In what ways can blockchain assist in network discovery and access control that are compatible across existing and future open access and licensed spectrum bands?

With an assumed blockchain that scales and is performant, how can the traits of distributed consensus and coordination be used to assist in network discovery, channel selection, and access controls, across open access and licensed spectrum bands? Because there is incumbent access in certain bands, a deeper investigation is needed to understand in what ways access controls can be packaged so as to remain highly compatible.

Research Question 3: Device Identity

In what ways can a network identity be created, maintained, and shared, for unknown or unassociated devices?

Research question 2 intentionally does not clarify where or how identity is established, it instead relies on existing mechanics of identity and investigates how to support these using blockchain functions to achieve identity interworking and access across networks. Question 3 investigates how the device identity itself can be constructed in ways that allows handling unknown or previously unassociated devices. If resolved, it would allow a form of autonomous access without a formal network trust. The goal is for these devices to “just work” where there is a shared coverage, in a manner similar to terrestrial broadcast radio. This form of identity without trust is a showcase benefit of integrating blockchain into the 5G network core.

Thesis Structure

This thesis is presented as a compendium of research articles investigating the utility of blockchain technologies in wireless networks. Chapter 1 provides a general background, covering the systems and technologies which served as a starting point for this work. Chapter 2 proposes a framework for blockchain deployment in wireless networks. Chapter 3 details an

early blockchain prototype for federating device access. Chapter 4 is the core of this thesis and provides the final design of a new blockchain protocol named CoNTE. Chapter 5 extends the theory to show optimizations done to the CoNTE protocol, as well as provides a standards-complaint model of deployment. To provide context for the potential implications of CoNTE, chapter 6 covers impacts on user equipment, presenting an extension of existing mobile-controlled handoff mechanics to allow higher autonomy in device mobility. Chapter 7 concludes the line of research, summarizing the research findings, and identifies potential paths for further research. A number of appendices are included at the end of this document. This additional material covers research and activities which were not completed, or otherwise not included with the main research line.

Research Contributions

The material presented in this thesis extends the current body of knowledge and provides the following major research contributions:

1. **5G specific blockchain:** The utility of blockchain immutability and decentralized control are investigated from a wireless network perspective. From this, we propose a new blockchain protocol, that is standards compliant with existing cellular architecture.
2. **Decentralized cellular overlays:** What are the implications of a decentralized cellular network? What does this deployment look like? To understand this, we present a deployment model for decentralized wireless overlay services, and in doing so, provide an early reference for the general decomposition and decentralization of future networks.
3. **Carrier-agnostic device mobility:** To take advantage of decentralized connectivity, we present a method of enhanced mobile-controlled handoff that increases the capability of existing devices to roam autonomously across newly decentralized access overlays.

Publications

During the process of investigation, this research has produced the following publications:

1. Platt, S., Oliver, M. A Distributed Ledger-Enabled Interworking Model for the Wireless Air Interface, 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 402-407, doi: 10.1109/WF-IoT.2019.8767349.
2. Platt, S., Oliver, M. Towards Blockchain for Decentralized Self-Organizing Wireless Networks, 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 2019, pp. 1-5.
3. Platt, S., Sanabria-Russo, L., Oliver, M. CoNTe: A Core Network Temporal Blockchain for 5G. *Sensors* 2020, 20, 5281.
4. Platt, S., Oliver, M. Decentralizing Future Networks: Combining Blockchain and ETSI Generic Autonomic Networking Architecture, *IEEE Transactions on Network and Services Management*, Submitted - Under Review, June 2021.
5. Platt, S., Demirel, B., Oliver, M. Using Transition Learning to Enhance Mobile-Controlled Handoff In Decentralized Future Networks, *IEEE Globecom*, Submitted - Under Review, June 2021.
6. Della Valle, F., Platt, S., Oliver, M., Review of Blockchain for Pandemic Surveillance and COVID-19 Response, *Electronics*, Submitted - Under Review, June 2021.

Standardization Activities: IEEE P2677

To aid in the reproducibility of results and general utility of this research, all programming completed to carry out experiments has been documented and shared with open access through Github ¹. Beyond the sharing of

¹<https://github.com/stevenplatt>

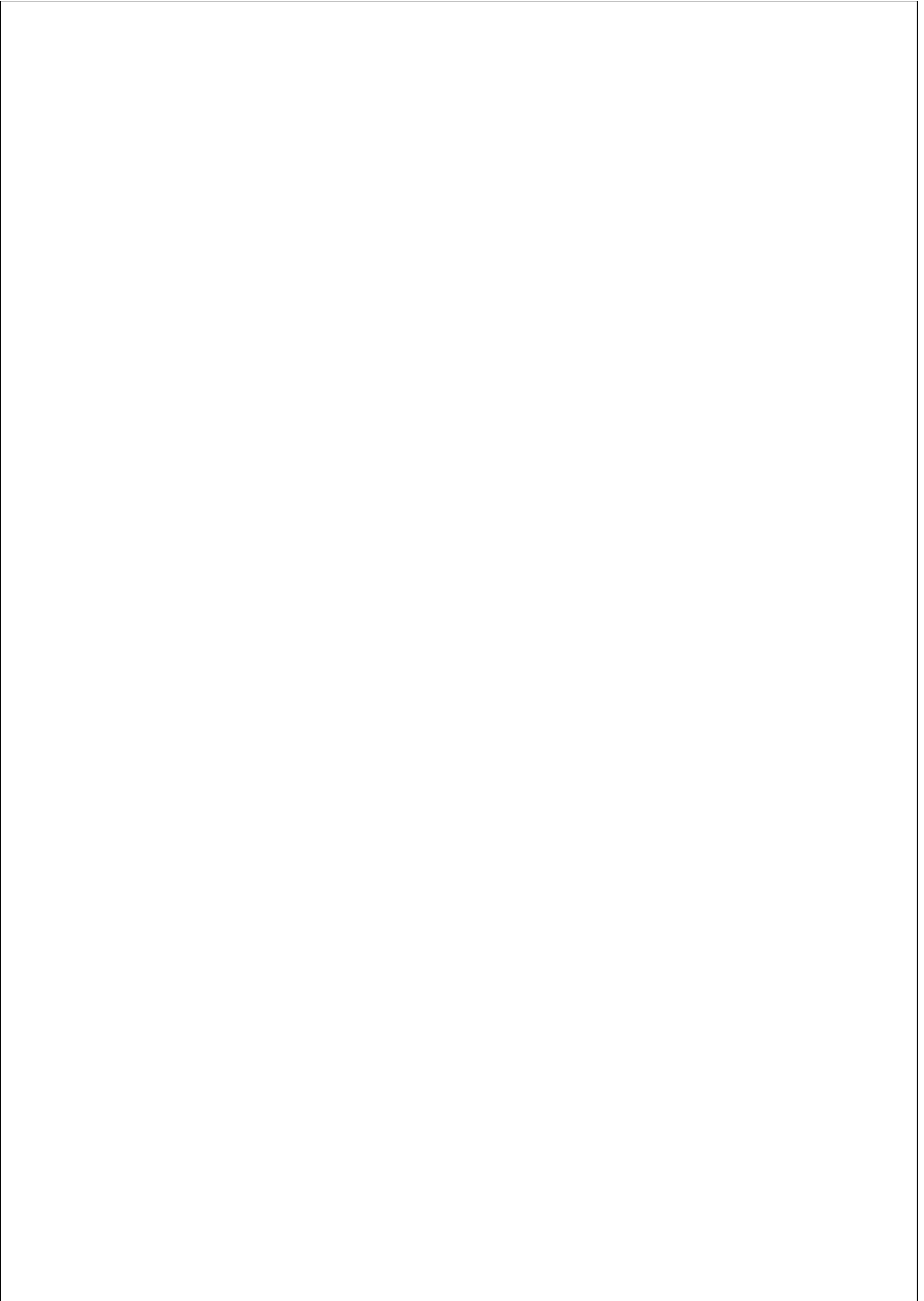
programming code, findings from this research were also shared with the IEEE Standards Association, through participation in the IEEE P2677 (Blockchain-based Omnidirectional Pandemic/epidemic Surveillance) working standard. Details of the working standard are provided below.

IEEE P2677 aims to provide a framework for the systems, devices, applications, and services which may be used to collect data for the purpose of pandemic surveillance. The project places a focus on privacy, transparency, and efficiency, and is planned to include a number of specific sub-standards:

- IEEE P2677.10 Access to Personal Data
- IEEE P2677.11 Access to Telecommunications Data
- IEEE P2677.12 Access to Transportation Data
- IEEE P2677.20 Requirements for Blockchain Infrastructure
- IEEE P2677.21 Requirements for P2P² Storage Infrastructure
- IEEE P2677.22 Requirements for Grid Computing Infrastructure
- IEEE P2677.30 Personal Application Programming Interface
- IEEE P2677.31 Healthcare Application Programming Interface
- IEEE P2677.32 Government Application Programming Interface

At the time of writing, the IEEE P2677 is still a working standard and has not yet moved into draft phase. The work of this research contributed most directly to IEEE P2677.11, which intends to provide a framework for the access, sharing, and use of telecommunications data such as position and mobility during pandemic events. The author of this thesis currently serves as project lead for this sub-standard.

²Peer-to-Peer



Chapter 1

BACKGROUND

1.1 Secondary Access Networks

To understand the intended application of this research we propose starting with network access models. Within the whole of wireless network access, we propose there can be a broad grouping into three categories: open access, licensed access, and secondary user.

Within open access models, are systems which impose no restriction to the access of wireless spectrum, or are otherwise operated license-free. The most common of these systems is 802.11-based WiFi, operating in spectrum bands that include 2.4Ghz, 5Ghz, 6Ghz, and 60Ghz. This category also includes wide area networks such as LoRa (Long Range), which operate license-free in lower frequency bands including 433Mhz and 868Mhz in Europe, 915Mhz in the United States, and 923Mhz in Asia [1].

Licensed access models are those of a typical cellular network, which requires a license for operation in designated frequency bands. Also in this category are networks deployed via satellite and for military application [2]. For cellular deployment, frequency bands allocated to this access model vary across region and cellular network generation, but are utilized as low as 600Mhz in certain 4G and 5G deployments, and is allocated as high as 39Ghz for higher capacity 5G designs [2]. Research already un-

derway is planned to extend this access yet higher spectrum ranges, with terahertz deployments expected for networks designated as 6G [2].

A hybrid of the previously mentioned models, we term as *secondary access*. A secondary access network is one in which a primary user or incumbent has a license or right of first use, and unused or underutilised spectrum is then made available to secondary users. Within this access model, these networks can be either unmanaged (bluetooth), or managed (television white space networks and cellular network overlays).

1.1.1 Bluetooth Technology

With bluetooth standards, the spectrum range that is being shared is fixed, allowing for simpler hardware support and compatibility. Today, Bluetooth is on its fifth revision and because of its standardization, all versions of bluetooth standard have remained backward compatible with bluetooth devices using versions prior, dating back to its original implementation.

The original bluetooth standards pre-date current 5Ghz spectrum networks and specify the use of the crowded 2.4Ghz internationally standardized ISM bands. Because this spectrum space is shared with consumer WiFi, bluetooth was designed to make secondary use of the channels already used by WiFi, through the use of frequency hopping spread spectrum (FHSS) [3]. FHSS works by dividing the larger ISM frequency band into smaller channels, or carriers. Devices connecting to each other hop between these channels using a pattern that is established as part of initial communication, based on predicted noise, channel occupation, or a number of other algorithms. A secondary feature of note for bluetooth, is how it forms topologies consisting of a master and multiple possible slave devices. This allows a master device to synchronize and communicate with additional devices more efficiently, and form mesh topologies, while still accessing the ISM band opportunistically.

As FHSS has matured, a second use case for sensor networks has further modified and applied these mechanics with protocols using time slotted channel hopping (TSCH) as described in the IEEE 802.15.4 standard, which underpins ZigBee and Thread smart home standards [4]. Systems

Location	Population	Available Channels	Available Spectrum
New York	19,006,798	2	12MHz
Los Angeles	17,786,419	0	0MHz
Chicago	9,785,747	10	60MHz
Boston	7,514,759	9	54MHz
Philadelphia	6,385,461	7	42MHz

Table 1.1: TVWS channel availability for the five largest population centers in the United States.

operating under the IEEE 802.15.4 standard also make use of additional longer range frequency bands near the 900Mhz spectrum space.

1.1.2 Television White Space Networks

In the most simple usage, White Space refers to portions of allocated spectrum that are unoccupied. In real world application, it is the portion of spectrum that has been allocated to a licensee - but is either unused or underused. The largest weakness of TVWS systems is that the frequency and amount of available white space varied between countries and even within country regions, which has made creating radio hardware that works across available spectrum space difficult, compared to standards such as bluetooth. This unreliability of channel access and bandwidth has been a large factor in lack of adoption, even after new spectrum bands are made available for use. Table 1.1 highlights the nonstandard nature of share spectrum by detailing TVWS channel availability across the five largest US population centers.

The IEEE formalized standards and technologies for TVWS communications in 2004, as IEEE 802.22. It defined TVWS as spectrum residing in the 54 to 862 MHz range. The Media Access Control (MAC) layer of the 802.22 standard relies on the use of cognitive radios for dynamic spectrum sensing in a model similar to our planned Channel Radio [5].

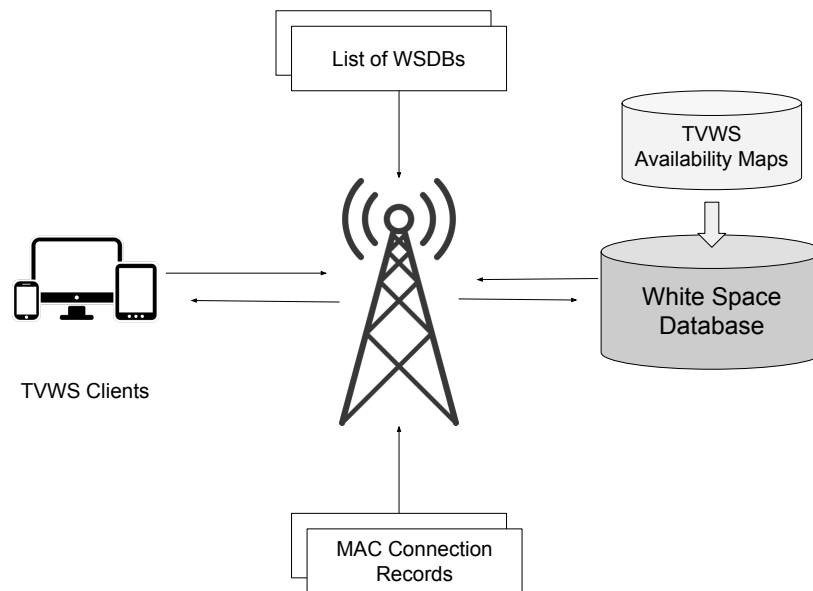


Figure 1.1: TVWS base station, client, and database flows.

Supplementing cognitive radios to resolve response time and cost concerns; Television White Space Databases (also referred to as a Geolocation Database or WSDB) has been tested and certified as a method to store and communicate known spectrum usage from licensed operators. Later in 2010, the United States updated its rules for TVWS use to make the use of a cognitive radio optional [6]. The flow of TVWS spectrum access requests using a white space database are shown in figure 1.1.

Use of TVWS spectrum was initially appealing for its targeting of lower frequency bands, allowing macro cells with wider coverage. Table 1.2 shows the number of cells required to cover 100 square kilometers in a non-line-of-sight deployment for networks in TV White Space 700MHz; compared to 2.4Ghz and 5.8Ghz network bands [6]. However, more than a decade after IEEE standardization, there are only seven known hard-

Frequency	Cell Radius	Path Loss at 4,380 m	Site Count
698Mhz	1,989 m	130 dB	10
2,400Mhz	955 m	144 dB	43
5,800Mhz	565 m	154 dB	121

Table 1.2: Comparison of TVWS (698Mhz) spectrum range.

ware vendors supporting TVWS technologies. These commercial hardware vendors are: 6Harmonics, Adaptrum, Carlson Wireless, KTS, Innonet, Redline Systems, and Metric Communications Corporation. Perhaps more importantly, there are only two vendors supporting a client radio (6Harmonic and Carlson Wireless), and only one which produces hardware in all four network categories (Carlson Wireless).

1.1.3 Cellular Overlay Networks

Cellular network overlays are perhaps the most recent interpretation of secondary user access. With a cellular network overlay, the network is partitioned virtually to allow dynamic allocation and configuration of network resources. A common use case for this type of network partitioning is the Mobile Virtual Network Operator (MVNO) business model. In MVNO deployment, network resources are partitioned and allocated, to an extent that an entire cellular carrier can operate under a secondary user access model in which the underlying network infrastructure which may be owned by another Mobile Network Operator (MNO) [7].

Cellular network overlays carry a benefit in that they are enabled by a number of technologies which are requisite in 5G and beyond cellular deployments:

- *Software Defined Networking*: The general decoupling of control traffic from core data to create what is often termed as a *control plane* and *data plane* [8]. Separating traffic in this way allows flexibility in deciding where processing and routing controls are placed

in the network. For example, the centralization of routing decisions to a datacenter, or the offloading of data processing to lower-cost commodity hardware [9]. Software defined networking technologies can be deployed to both wired and wireless networks.

- *Software Defined Radio*: Software defined radio inherits software defined networking principles and applied them specifically to the radio interface of wireless networks. In a software defined radio application, signal processing functions are allowed to be offloaded from physical antenna resources, allowing reconfiguration and the ability to centralize control [10]. As with software defined networking, in application, this allows wireless radio and antenna resources to be deployed using commodity hardware.
- *Network Function Virtualization*: Network function virtualization targets the isolation and abstraction of network operations at a functional level rather than an individual hardware resource level. Because abstraction occurs at a higher level, network function virtualization also covers abstraction of operations and algorithms existing entirely in software, such as accounting, authorization, and mobility management [11].
- *Network Slicing*: Combining the previously mentioned mechanics of abstraction, service providers are able to deliver an end-to-end wireless connectivity (overlay), built atop groupings of heterogeneous and commodity infrastructures underneath. These underlying infrastructures can be delivered by a single provider, or in the case of an MVNO, stitched together from a number of providers for redundancy [7].

Technologies in these categories can be deployed individually or in tandem depending on performance targets, use case targets, desired business model, or the general availability of the enabling infrastructure. This research inherits the structures and mechanics that enable cellular overlay networks and extends the current body of work by introducing mechanics of decentralization using blockchain, a distributed ledger technology.

1.2 Distributed Ledger Technologies

At its heart, a blockchain system is designed to store data. In this function, a blockchain system is a database system. One deployed with storage that is made immutable. Before a blockchain system is deployed in an application, it can be considered as competing with traditional databases for storing that same data.

As a technology in early development, it remains difficult to place blockchain into context for wireless design. To date, early research has focused primarily on individual use cases in part to simplify the network context. This framing however does not fully acknowledge heterogeneity in wireless networks, or the rapidly expanding variety of blockchain designs. To understand blockchains' fit with native network operations, we must first acknowledge its data structure, inherited behaviors, and position it relative to alternatives that also functionally serve as distributed ledgers. Viewing blockchain in this format provides a more durable understanding as to the long-term functional fit of the blockchain structure while additionally highlighting areas that may conflict with the format and behavior of networks in 5G and beyond.

In tandem with the development of blockchain, alternative ledger structures have been produced, or evolved to address known limitations, or provide specific focus for behaviors that were secondary or underdeveloped in blockchain. Research has identified a "trilemma" within these systems, noting that at best, they may perform well on only two of three axis: decentralization, scalability, and security [12]. In the context of this trilemma, we can deduce, for example, that a data structure adopted for high scalability and decentralization traits, makes tradeoffs in security, making it less suitable for network access control. Or conversely a ledger structure with high inherent security and high decentralization will do so at the expense of scalability - resulting in limited compatibility for network intelligence operations such as the handling of streaming data. The following section provides a representative sample of ledger data structures beyond blockchain, detailing the behaviors inherent to each corresponding data structure. The data structures include: Distributed Hash

Table, Directed Acyclic Graph, and Block Lattice, and finally Blockchain.

Distributed Hash Table

Distributed hash tables (DHT) operate as a peer-to-peer network layer for storing data. DHT systems operate by spreading data among peers in a network, with a cryptographic function being used to either randomly select, or select in a set distribution, which peers store the data. Like a traditional database, DHT systems function as a key value store where a lookup is required to gain a list of nodes which store the file(s) being requested [13]. It is the oldest distributed ledger design presented here, having underpinned early internet file sharing applications including versions of BitTorrent. Because the selection of nodes which store data is distributed, data stored in distributed hash tables is highly decentralized with high throughput, making it well suited for 5G and beyond applications relying on hyper density, including data caching and edge compute. DHT systems may store multiple copies of a file or segment files to further enhance these traits. Devices participating in a distributed hash table system can join and leave the system at any time, allowing long term compatibility in dynamic and multi-tiered topologies where network access may be on-demand or temporary.

Negative areas of impact for DHT systems are in transparency and security. The selection process of storage nodes as participant numbers are changing makes it difficult to audit activity or trends in deployment. Security is reduced in the system overall, by a possibility that modified, malicious, or duplicate data records can be added and shared - although partial mitigation is possible using hashed message digests such as MD5 values to improve trust of records distributed. Figure 1.2 shows a representation of the distributed hash table data structure.

Directed Acyclic Graph

Directed Acyclic Graph (DAG) structures such as IOTA [14] modify the linked hashing of data to use a graph structure that allows it to expand exponentially. IOTA achieves this by allowing data blocks to be added by

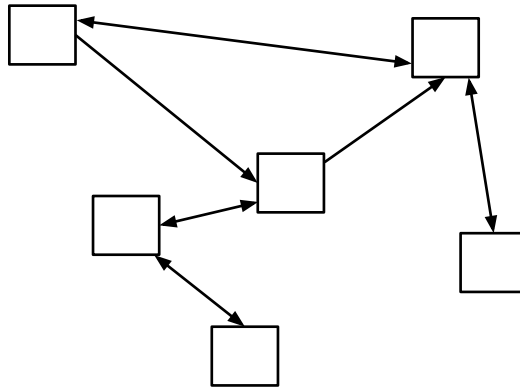


Figure 1.2: Distributed Hash Table data structure.

validating only two edge blocks (tips) selected at random which forms its graph structure. Decentralization in this format is high due to the linear effort of block contribution tied to the forward hashing from two previous graph tips. This native behavior of high throughput allows DAG structures to easily handle streaming network data, of the kind required for high level network intelligence (AI) systems that power high levels of autonomy in next generation designs.

Having a low barrier of participation conversely creates circumstances that can result in restricted availability as increases in block volume also increases storage usage and the probability that nodes in a network cannot update local records and remain current as new blocks arrive. A second limitation inherited in DAG-based distributed ledgers is the finality of the data stored in its blocks. Because block truthfulness is weighted by the number of forward validations from a graph tip, the state of the data in DAG structures is probabilistic rather than deterministic as certainty increases with each forward block, giving the system moderate levels of security. A consensus mechanism that enforces determinism as seen in certain blockchains is not possible in graph structures, based on current research - making the systems a poor fit for rule-based operations, such as spectrum sharing policy which relies on binary "allowed" or "not al-

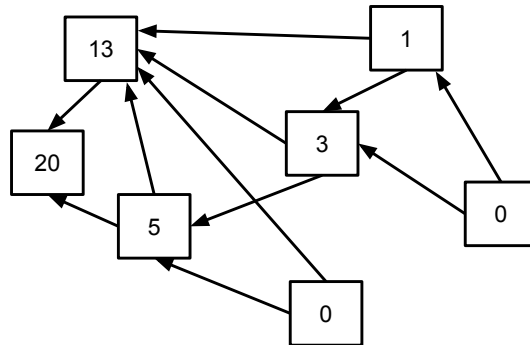


Figure 1.3: Directed Acyclic Graph data structure.

lowed” states. Figure 1.3 shows a representation of the directed acyclic graph data structure.

Block Lattice

At the time of writing, block lattice structures are early in development, with the earliest block lattice cryptographic construction being outlined by Miklos Ajit in 1996 [15]. Modern lattice structure, such as QLC Chain [16] focus on the reduction of storage requirements compared to blockchain, which stores an ever-expanding block history. Rather than a single monolithic history that is stored and maintained at each node, block lattice platforms require participants to only store their personal ledger, with each block of data having a corresponding block stored in the ledger of the device or system on the other end of the interaction. These records become immutable as independent nodes complete further interactions, effectively spreading or sharding dependencies and storage within the wider environment. The transactions tie together in mutual dependency, the ledgers of peer nodes which expands over time, creating its mesh or lattice structure.

Block lattice structures have further benefit in that they potentially simplify consensus mechanisms, as consensus on balance and block state

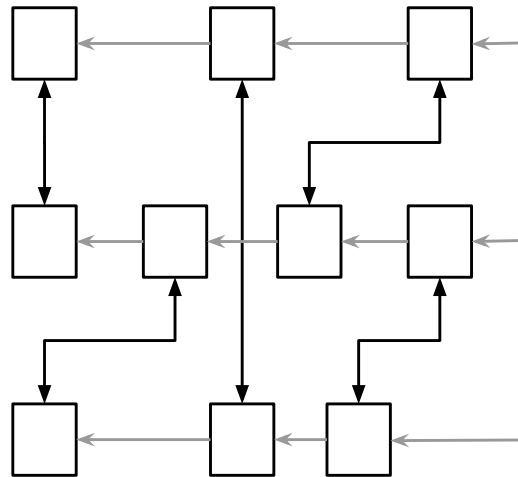


Figure 1.4: Block Lattice data structure.

is only required between peers participating in an interaction - presenting an attractive alternative to Proof-of-Work implementations relying on hash power, or BFT consensus which encounters higher bandwidth use under multiple rounds of peer confirmation. The lack of unified history and isolated nature of transactions makes lattice structure highly compatible with operations existing exclusively device-to-device, such as the payments and user data exchange in hyper dense environments at the expense of higher-level network infrastructure use. Figure 1.4 shows a representation of the block lattice data structure.

Blockchain

Unlike previously mentioned ledger structures which gain flexibility through modification and fragmentation of the underlying hashed-linked storage, blockchain allows little manipulation of its base structure outside of consensus model and block size. All nodes participating in blockchain systems must agree on the state of each block added, and the sequence of added blocks - regardless of who authors or ultimate users of the data

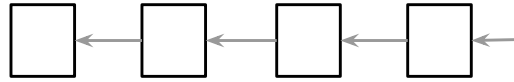


Figure 1.5: Blockchain data structure.

inside of blocks. This rigid chain structure guarantees a record that is always identical for all nodes in the system, making it especially well-suited to policy-based operations demanding high transparency and auditability, including software defined radio, roaming in hyper mobility, and expanded spectrum resource sharing. By modifying the algorithms for achieving consensus, blockchain systems can be manipulated to process higher transaction volumes, improve security or control resource usage by allowing nodes to keep full (full-node) or partial (light-node) states [17]. Deploying such modification however, shows consensus latency in blockchain under best case scenarios, are reduced to reach 1 second, confirming that blockchain structure remains incompatible with operations at μ -second scale, such as real-time radio resource control and dynamic accesses not set on a semi-permanent basis. Figure 1.5 shows a representation of the blockchain data structure.

1.2.1 Composition of Modern Blockchain

Recent taxonomy identifies some of these configuration components as [18]:

- Block proposal model
- Fault tolerance model
- Network accessibility model
- Network communication model

- Network timing model
- Transaction finality model

These configurations are usually dictated by the chosen consensus model being used, but it is also possible to deploy additional algorithms in a blockchain design, which augment or modify the individual behaviors. The following section reviews the consensus and configurations of a selection of distributed ledger projects, which include: *Bitcoin*, *Ethereum*, *Ripple*, and *IOTA* projects.

Bitcoin

Today Bitcoin is the most well known application of blockchain technology, but also the oldest and simplest technical implementation in popular use. The original Bitcoin whitepaper was published in 2008, and detailed the design of a digital currency system that removed the need of a trusted third party for the verification of transactions [19]. The system did this using a peer-to-peer distribution of a universal ledger.

- *Consensus and Fault Tolerance*: Bitcoin’s ledger is designed as a never ending chain structure, where new data being added to the chain requires combining the timestamp of the last transaction, along with a hash of the new data being appended to the ledger. The resulting aggregate hash gives the ledger its chain structure, and is seen as immutable and highly secure, as a recomputation of all subsequent work is required in order to modify old transactions on the chain [20][21][22]. The later ubiquity of Bitcoin helped popularize the terms Blockchain and Distributed Ledger.

To aid in decentralization, Bitcoin allows nodes or participants to join and leave the network at any time, with all transaction data sent as broadcast. After data is broadcast, computers in the network compete to find a hash of the block data that is smaller than a threshold size set for the entire network. Because the result of hashing is pseudo-random, it is believed that every computer in the network

of equal computing power has an equal chance of being first to find the correct hash. The equality created through the pseudo-random hash function also makes the network able to remain secure as long as a simple majority, or 51% of the network are acting in good faith. To provide incentive for doing the difficult computation work, machines participating in the network are issued a reward in the form of Bitcoin, for finding and broadcasting the first successful hash. These reward payments are covered by transaction fees charged to users wishing to add blocks to Bitcoins' chain. Because this hash value can be verified by others in the network - this process of consensus is named "Proof of Work". A primary side effect of the race condition created through POW consensus, is that power used for all unsuccessful hashes is considered wasted, making the system highly resource inefficient. A secondary behavior and weakness of using the POW consensus model is that it makes financial incentive in the form of block rewards and transaction fees, native to the operation of the system.

- *Use Cases and Current Research:* Bitcoin was originally designed as a digital currency, and remains in this structure today. The organization supporting Bitcoin positions it as a digital bank and offers developer documentation in support of sending and receiving transactions. While it is possible to build large applications that integrate the use of the Bitcoin ledger, these interaction is limited to the sending and receiving of the Bitcoin digital currency, and limited to the binary state of spent or unspent, a limitation later addressed in the development of the Ethereum blockchain.

Ethereum

While Bitcoin itself was designed as a digital currency, the blockchain structure of its underpinning ledger can be applied for most any application where high trust without direct ownership or relationship is desired. Ethereum was developed for this purpose and designed to allow building general purpose applications atop its blockchain structure. Ethereum does

this mostly through extending the block data to allow storage of application code, written in Ethereum's own "Solidity" programming language. State changes occurring from the application code are also written to the blockchain and made permanent. This behavior has made Ethereum popular not only for application development, but as a platform for contracts - or code that executes on when pre-set conditions are met.

- *Consensus and Fault Tolerance:* The Ethereum network carries over the POW consensus method proven with Bitcoin. This includes the process of hashing data, and broadcast communications, as well as the resulting power consumption and 51% fault tolerance. Similar to the Bitcoin network, incentive is provided by awarding payment to the first user completing a valid hash. Reward and transaction fee payments in the network are made using its native digital currency, "Ether".
- *Use Cases and Current Research:* A new class of applications developed atop the Ethereum blockchain are increasingly termed as "Web3", indicating a belief that the next generation of internet development will exist in this decentralized architecture. Filecoin [23] is an example of such a Web3 class application. Filecoin is a decentralized network storage platform. Built on top of a distributed ledger; the Filecoin system allows users to pay for storage of data on the network or earn payment through hosting the files of others. Files stored in the Filecoin network use data sharding and peer-to-peer distribution to ensure file contents cannot be read by network participants not directly owning the file.

Ripple

Another project extending from the currency conventions set with Bitcoin is the Ripple network, formed in 2012. As with Bitcoin, Ripple operates using its own native crypto currency: XRP. Ripple is not content to be a universal platform, but is purpose designed to handle bank transfer settlements in a manner faster, and lower cost than the incumbent SWIFT

settlement platform used globally by banks today [24]. Unlike the Bitcoin and Ethereum projects, Ripple is a for-profit company. Among early adopters of the Ripple platform are American Express, Santander Bank, and MoneyGram. The novelty of the Ripple platform is its method of consensus, which differs from Bitcoin and Ethereum and is based on Practical Byzantine Fault Tolerance which allows it to handle network segmentation and higher transaction throughput - without relying on mining for collective compute derived security.

- *Consensus and Fault Tolerance*: Ripple was among the first large blockchain networks to utilize the Practical Byzantine Fault consensus method. In its default state, PBFT can successfully form consensus, while withstanding up to 33% faulty or malicious nodes [35]. Ripple further tunes this measure for lower latency and improved transaction speeds, by reducing overall fault tolerance to 20% faulty or malicious nodes [24]. In this new structure, Ripple is able to allow smaller segmentation of network participants, so long as 20% of nodes in a segment are shared in another segment. Doing so guarantees that consensus does not conflict between any network segments since the final state achieved in a segment would require agreement from some portion of these shared nodes in order to reach 81% quorum. This 20% shared node structure is represented in figure 1.6.
- *Current Research*: As a for-profit company, the Ripple platform is closed source. The company does not publish or otherwise make public a research roadmap. At the time of writing, due to its performance and computer characteristics, the PBFT consensus algorithms used by Ripple and other networks, has been targeted for possible Chanel Chain use.

IOTA

IOTA is the newest project included in this section, and does not use a blockchain data structure as a basis for its chain. IOTA instead uses an

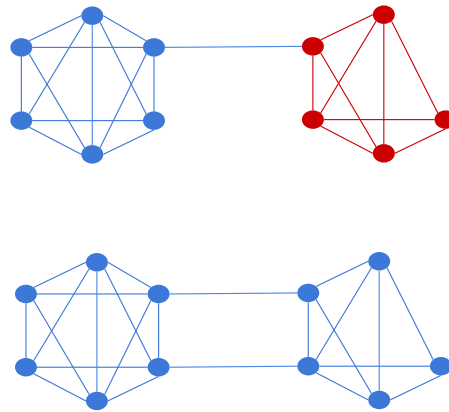


Figure 1.6: Connectivity level required to preventing forking in the Ripple Network [24].

acyclic graph structure, which the IOTA team refers to as the “tangle”; this allows the total system to have much higher transaction throughput, compared to traditional blockchain systems. The developers of IOTA position the project as a solution for the large volumes of data produced by the internet of things applications and systems. Similar to other ledger systems, IOTA has its own digital currency (also named IOTA) and is structured as a financial ledger at its core, with the most common use of the system being to buy and sell the data generated from IoT devices.

- *Consensus and Fault Tolerance:* Because transactions are stored in a graph, the forward hashing and proof of previous transactions are carried in a pseudo-random branching, where each new block added to the graph ledger, is added only after verifying two randomly selected previous transactions [25]. Figure 1.7 shows the graph structure of the IOTA tangle.

Each block in the IOTA graph receives a weighting equaling the cumulative verifications it has received - accounting for the verifi-

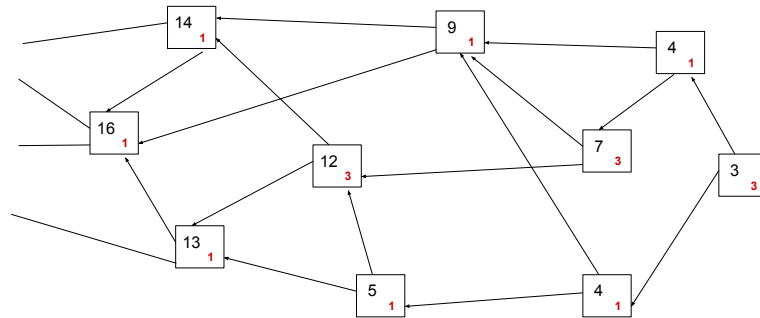


Figure 1.7: IOTA graph structure and two block verification [25].

cations received by all forward blocks branched from it [25]. This means that as time passes, the random verification process increases the weighting and truthfulness of past blocks - but there is never a final state of consensus achieved. This lack of formal consensus is still a point of contention for the IOTA project. A majority of early academic research for the project was focused on the pseudo-random process of past block verifications and mathematical proofs to explain the security of the system. In the official whitepaper, titled "The Tangle", author Sergui Popov conceded that due to the lack of finality in the system state, it is still possible to post fraudulent blocks and have them adopted, so long as an attacker has a majority of compute power and does a manual validation of their own block, rather than following the pseudo-random block verification use by the rest of the network. Because of this, fault tolerance in the network is 51%, matching that of Bitcoin. A visualization of such 51% attack is shown in figure 1.8.

- *Current Research:* Research and development for the IOTA project is tied more closely to university research than other projects, and the team maintains a research roadmap at the project site. Because IOTA does not have a proven method of locking state or developing

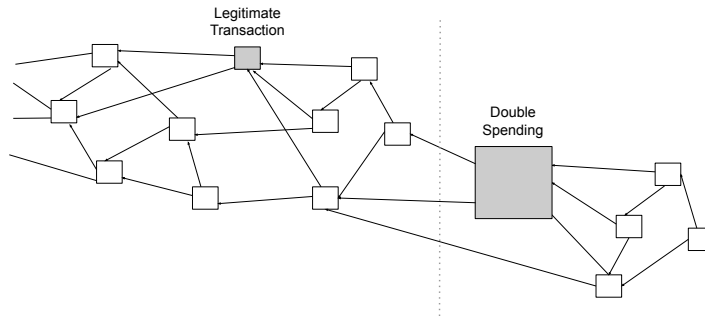


Figure 1.8: IOTA network 51% double spending attack [25].

distributed consensus - the network deploys a centralized server, named the "coordinator" that has the ability to lock and roll back the state of the network if required. Removal of this coordinator role is currently the largest research effort for the project. At the time of writing, the site also lists spam prevention, economic incentive, attack analysis, and other items as research interests [26].

1.2.2 Evolution Potentials of Blockchain

To our knowledge, the origins of blockchain began with cryptographers Haber and Stornetta who in 1991 published research titled "How to time stamp a digital document" in the Journal of Cryptography [27]. The problem being addressed in research was how to handle authenticity as increasing amounts of records were existent only in digital form and at the time, lacking verifiability. This early system lacked however the decentralized consensus methods later popularized with Bitcoin, an evolution that was made in order to allow the preexisting blockchain structure to function in a permissionless manner as digital currency. As with Bitcoin, the blockchain structure is expected to further evolve increasing its compatibility in network application. The following section outlines three areas where the blockchain structure is evolving in ways that will further its compatibility with wireless designs, these areas are: *increased*

composability, de-emphasizing of incentive model, and independent code execution.

- *Increased Composability:* The size and resource usage of modern blockchains preclude them from full participation among low power or resource constrained network systems. This is shown in network research such as [28], which require a separation of network operation as a result of using proxy devices able to run intensive proof-of-work calculations, or which having enough storage to retain the entirety of a monolithic ledgers’ history. A natural progression in this scenario is to implement an alternative consensus model, or compression scheme to tune chain operation for the environment, rather than modifying the network structure to suit the chain. For example, if a universal record such as currency balance is not being mandated, it is further possible to form and retire chains for individual network operations as the shared data reaches the end of its useful life. Composability of this type is not possible for the most popular blockchain systems, such as Ethereum, which are delivered as an all-or-nothing design which may bundle behaviors that are superfluous or an active detriment in network environments. This awareness bring pressure to the necessity of tuning or composing the functions of the blockchain which impact its performance in the desired application, these include but are not limited to, abilities to modify block size, consensus model, and block timing (Figure 1.9).
- *De-Emphasizing of Incentive Model:* As a system demonstrated to support contract execution, several experiments have investigated the use of blockchain to incentivize behavior desired in network environment, such as resource sharing. Maksymyuk et al for example, propose a spectrum sharing solution which identifies spectrum owners, infrastructure owners, ISP, and end users as independent participants in a dynamic market driven by the nash equilibrium game theory [29]. In the Maksymyuk model, end users make digital currency payments to infrastructure (base station) operators, who in

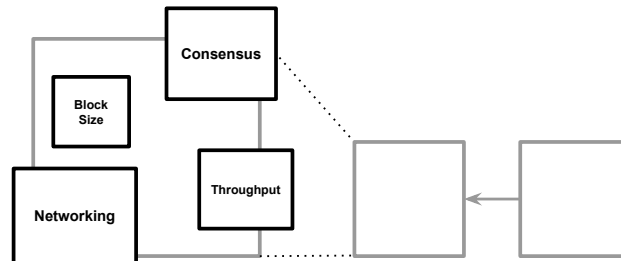


Figure 1.9: Blockchain Composability.

turn, pay for dynamic spectrum access to incumbents and regulators, while also paying for ISP backhaul services to carry traffic to the wider internet. The nash equilibrium model behaves similarly to other existing blockchain models built atop currency incentive; in network context however, it assumes a level of parity in the distribution of infrastructure, demand, and incentive that is uncommon in production markets. As deployed in network context, current blockchain incentive models are functionally similar to existing research into "neutral carrier" models, which abstract individual carrier businesses and to date have not gained wide market adoption [30].

To best fit existing incentives of network environment, blockchain must be evolved to be inclusive of competing operational incentives such as resource management, network investment levels, and demand growth which may be uneven among equivalent providers. Early research by Haber and Stornetta offers a possible path forward to highlight blockchain predating digital currency, in this format, the focus is on the latent utility of verifiable shared data instead of currency and contract incentive [27]. As sharing of limited resources such as spectrum increase in the evolution to 6G, it possible that the higher utility is served through the sharing of context and data, such as tower location and channel occupation - which are required for functional operation for everyone - decoupling any

awareness of economic model from the chain.

- *Independant Code Execution*: Unlike ledger structures such as distributed hash table, blockchain is a rigidly time ordered structure by nature of its linear forward hashing. The general speed of code execution tied to the contribution of blocks will be inversely proportional and dependent on block consensus time. This means that a blockchain deployment seeing an increase in block contributions, will also see a corresponding decrease in how quickly those blocks, and corresponding information can be processed; all else remaining unchanged.

In systems such as Ethereum, where end-to-end operations occur within its own virtual machine - Impacts of block additions can be partially controlled by charging a digital currency fee proportional with delay imputed on the system. This type of control however is difficult to replicate in network environments, where creating an API or software representation for the unbounded number of machine operations in heterogeneous networks is impractical. Within networks of an identical generation; configuration for antenna geometry, sectoring, deployment density, backhaul capacity, and algorithms therein can differ, conflict, or be upgraded over time. Pointing again to a general benefit of limiting blockchain deployment, to decentralization of data. Unbinding blockchain data storage from code execution such as smart contracts can partially mitigate the original risk and related overhead tied to block delay.

1.2.3 Blockchain Potentials in Wireless

With an awareness of the behavior and performance of blockchain structure, it is confirmed that blockchain works best for network policy and record keeping that is set on a semi-permanent basis. Deploying blockchain in this context allows full realization of its utility as a system of accounting and storage, that can be shared among peer networks which have a mutual incentive to coordinate - but are otherwise competitors or lack a

formal trust. The following section extends this behavior relationship to identify three specific use cases utilizing blockchain as secure, auditable, and decentralized storage in a way that enhances network operation even when deployed in a competing network operator context.

- *Software Defined Networking*: 6G networks will add additional network dimensions to support a new mix of infrastructures ranging of satellite constellations to marine infrastructures for support of new services deployed to space and sea. This adds further complexity and heterogeneity in both the network core and radio access layers. Beyond the increase in service heterogeneity, the use of terahertz frequency bands increases energy usage, requiring additional configurability to operate network hardware efficiently. Network softwarization built on network function virtualization, software defined radio, and general network slicing technique matured in 5G will be extended to support these additional network dimensions. As network infrastructure is increasingly abstracted and replaced with application-controlled architectures in 6G, use of blockchain allows more direct coordination for Mobile Network Operators (MNO) and subscribing Mobile Virtual Network Operators (MVNO) to share and coordinate configuration due to differences in services and customers on either side. Blockchain-powered policy orchestration also increases security and transparency in Distributed Antenna Array (DAS) systems deployed to regulated environments such as light rail tunnels, sport venues, high rise towers and other increasingly specialized shared infrastructures where deployment is restricted or multiple operators are otherwise required to be multi-tenant [31].
- *Spectrum Sharing*: In 2016 the Federal Communications Commission (FCC) in the United States, deployed a 3-tier sharing model for the 3.5Ghz citizens broadcast radio service (CBRS) bands in the country. The three tiers policy identifies incumbent rights for military applications, secondary rights for opportunistic access of approved parties, and a third tier for open access in a smaller sub-

set of the airspace with medium access controls matching that of Wi-Fi [32]. In tandem with recent policy changes, research has begun formal investigation into blockchain technologies support for spectrum operations, following statements by the FCC acknowledging that existing rules and technologies for spectrum sharing had become antiquated, highlighting blockchain as a potential path towards this goal as networks move to 6G [12]. As a peer-to-peer system, blockchain provides a desirable method of accounting for spectrum sharing operations as it allows verifiable record keeping among unmanaged peer operators who lack a formal trust.

Deploying blockchain for spectrum sharing has a secondary benefit in that it allows networks to achieve a proactive awareness on a macro scale of networks operating in its coverage zone. The ability to share spectrum, while maintaining coverage and providing service level guarantees has been a barrier to deployment of commercial service on top of shared spectrum. In 6G, this proactive awareness, combined with software-controlled radio policy; network providers can dimension or tune 6G spatially multiplexed MIMO behaviors to maintain cell-less coverage, even as additional networks operate in the shared airspace - providing access consistency in a manner not possible today with independent cognitive radio or brute force approaches [33].

- *Public Utility Services:* As device density increases, there is also an increasing of public infrastructures such as hyper high-speed rail and sensors that become network enabled in non-commercial contexts, such as for the deployment of safety services. Public infrastructure often span municipality, region, and country boundaries. For a number of countries, there are restrictions placed on deploying municipal cellular networks [30], and there remains no natural path of coverage for these systems that are not considered commercial services or the domain of private operators.

With blockchain, it is possible in this scenario, to deploy a registry of public utility services, such as vehicles in road networks, that are

allowed specific connectivity. To date this has been complicated by limitations of IP address mobility across network boundaries, but that complication will be resolved through the transitional period to IPv6 during the deployment of 5G. In 2016, version 2 of the IETF Host Identity Protocol (HIP) standard [34] abstracts the IPv6 address, by placing a “host identity” between the network and higher-level internet layers of the TCP/IP stack. Combining this evolution of identity with securely shared blockchain registries allows public utility wireless services that can take advantage of fluid access *across* networks as IPv6 addressing becomes native in 6G. Combining mobile network identity with blockchain decentralized secure storage allows these new classes of access to be regulated at the spectrum block, country, or region level - without tying them to individual carriers coverage who in isolation may not have market incentive to extend coverage, or otherwise allow access.



Bibliography

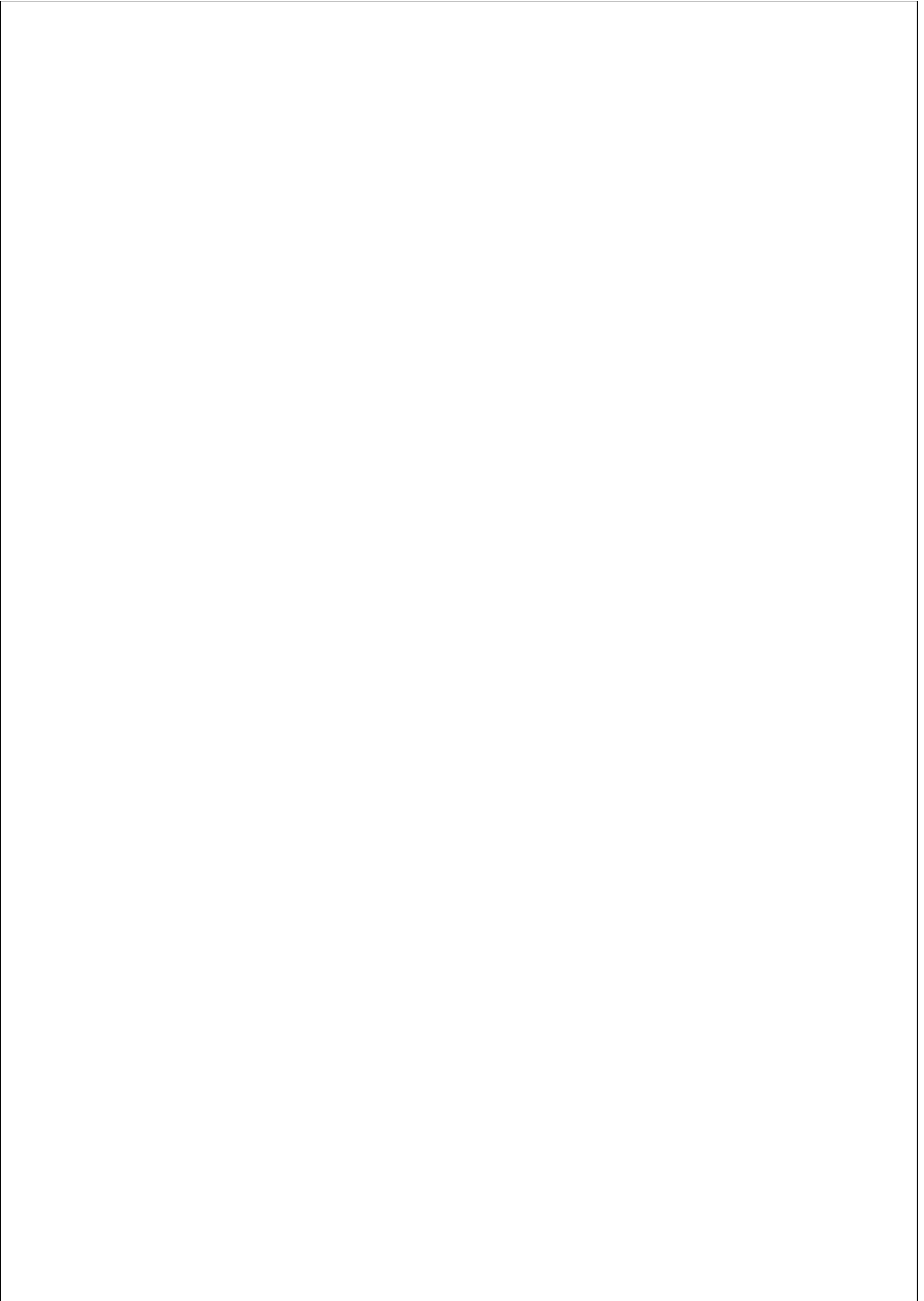
- [1] Sanchez-Iborra, R., Sanchez-Gomez, J., Ballesta-Vinas, J., Cano, M. D., & Skarmeta, A. F. (2018). Performance evaluation of lora considering scenario conditions. *Sensors (Switzerland)*. <https://doi.org/10.3390/s18030772>.
- [2] Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., Karagiannidis, G. K., & Fan, P. (2019). 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. *IEEE Vehicular Technology Magazine*, 14(3), 28-41. <https://doi.org/10.1109/mvt.2019.2921208>
- [3] Specification of the Bluetooth System. Core, Version 5.1. [Online]. Available: <http://www.bluetooth.com>.
- [4] Du, P., & Roussos, G. (2012). Adaptive time slotted channel hopping for wireless sensor networks. 2012 4th Computer Science and Electronic Engineering Conference, CEEC 2012 - Conference Proceedings, 29-34. <https://doi.org/10.1109/CEEC.2012.6375374>
- [5] Khan, M. W., Zeeshan, M., & Shahzad, K. (2019). On Performance Analysis of IEEE 802.22 PHY for Cognitive Radio based Smart Grid Communications. 2018 IEEE International Smart Cities Conference, ISC2 2018, 1-4. <https://doi.org/10.1109/ISC2.2018.8656948>.
- [6] Boonyeon K., Maengjoo L. (2014) Opportunities and Challenges of Using TV White Spaces - A Comparative Analysis of Approaches among U.S.A., U.K., and S. Korea.

- [7] U. Ofcom, The Office of Communications, Infrastructure report 2014. ofcom’s second full analysis of the uk’s communications infrastructure. Ofcom, The Office of Communications, UK., Tech. Rep., 2014.
- [8] Hu, F., Hao, Q., and Bao, K. A survey on software-defined network and openflow: from concept to implementation, *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 4, pp. 2181-2206, 2014.
- [9] Richart, M., Baliosian, J., Serrat, J., & Gorricho, J. L. (2016). Resource Slicing in Virtual Wireless Networks: A Survey. *IEEE Transactions on Network and Service Management*, 13(3), 462-476. <https://doi.org/10.1109/TNSM.2016.2597295>
- [10] Hadzialic, M., Dosenovic, B., Dzaferagic, M., and Musovic, J. Cloud-ran: innovative radio access network architecture, in *ELMAR, 2013 55th International Symposium. IEEE*, 2013, pp. 115-120.
- [11] Hawilo, H., Shami, A., Mirahmadi, M., and Asal, R. Nfv: state of the art, challenges, and implementation in next generation mobile networks (vepc), *Network, IEEE*, vol. 28, no. 6, pp. 18-26, 2014.
- [12] Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2019). A Survey on the Scalability of Blockchain Systems. *IEEE Networks Magazine*, 166-173. DOI: 10.1109/MNET.001.1800290.
- [13] Chalaemwongwan, N., & Kurutach, W. (2018). State of the art and challenges facing consensus protocols on blockchain. *International Conference on Information Networking*, 2018-January, 957-962. <https://doi.org/10.1109/ICOIN.2018.8343266>.
- [14] Popov, S. (2018). The Tangle v1.4.3, 1-28. [Online] Available: <https://www.iota.org/research/academic-papers>. Accessed on: Oct 2, 2019.
- [15] Ajtai, M. 1996. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the twenty-eighth annual ACM*

- symposium on Theory of Computing (STOC '96). ACM, New York, NY, USA, 99-108. DOI: <https://doi.org/10.1145/237814.237838>.
- [16] Li, C. A., & Zhao, C. (n.d.). A Multidimensional Block Lattice Public Chain with Smart Contract Support for Network-as-a-Service. [Online] Available: <https://whitepaper.io/document/238/qlcchain-yellowpaper>. Accessed on: Nov 2, 2019
- [17] Vukoli, M. (2017). Rethinking Permissioned Blockchains [Extended Abstract]. IBM Research, 3-7. <https://doi.org/10.1145/3055518.3055526>.
- [18] Nijssse, J., & Litchfield, A. (2020). A Taxonomy of Blockchain Consensus Methods. *Cryptography*, 4(32), 1-15. <https://doi.org/10.3390/cryptography4040032>
- [19] Nakamoto. S. (2016). Bitcoin: A Peer-to-Peer Electronic Cash System. 1-9. <https://doi.org/10.1007/s10838-008-9062-0>
- [20] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on Blockchain technology? - A systematic review. *PLoS ONE*, 11(10), 1-27. <https://doi.org/10.1371/journal.pone.0163477>
- [21] Skwarek, V. (2017). Blockchains as security-enabler for industrial IoT-applications. *Asia Pacific Journal of Innovation and Entrepreneurship*, 11(3), 301-311. <https://doi.org/10.1108/APJIE-12-2017-035>
- [22] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*. <https://doi.org/10.1016/j.future.2017.08.020>
- [23] Benet, J., & Greco, N. (2018). Filecoin: A Decentralized Storage Network. *Protocol Labs*, 1-36. <https://doi.org/10.1088/1126-6708/2007/08/019>

- [24] Schwartz, D., Youngs, N., & Britto, A. (2014). The Ripple Protocol Consensus Algorithm.
- [25] Popov, S. (2018). IOTA whitepaper v1.4.3, 1-28. https://iota.org/IOTA_Whitepaper.pdf.
- [26] IOTA Foundation. Academic Papers. <https://www.iota.org/research/academic-papers>.
- [27] Stornetta, W. S., & Haber, S. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology*, 3(2), 99-111. <https://doi.org/10.1002/pssb.201300062>.
- [28] Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184-1195. <https://doi.org/10.1109/JIOT.2018.2812239>.
- [29] Maksymyuk, T., Gazda, J., Han, L., & Jo, M. (2019). Blockchain-based intelligent network management for 5g and beyond. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings, 36-39. <https://doi.org/10.1109/AIACT.2019.8847762>.
- [30] Infante, J., Oliver, M., & Maciñ, C. (n.d.). Wi-Fi Neutral Operator: Promoting cooperation for network and service growth. ITS Conference on Regional Economic Development, Pontevedra, Spain, 07/2005.
- [31] You, X. H., Wang, D. M., Sheng, B., Gao, X. Q., Zhao, X. S., & Chen, M. (2010). Cooperative distributed antenna systems for mobile communications. *IEEE Wireless Communications*. <https://doi.org/10.1109/MWC.2010.5490977>
- [32] Zhang, Z. et al. (2019). 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. *IEEE Vehicular Technology Magazine*, 14(3), 28-41. <https://doi.org/10.1109/mvt.2019.2921208>.

- [33] Medeisis, A., & Minervini, L. F. (2013). Stalling innovation of Cognitive Radio: The case for a dedicated frequency band. *Telecommunications Policy*. <https://doi.org/10.1016/j.telpol.2012.07.001>
- [34] Internet Engineering Task Force (IETF). (2015). Host Identity Protocol Version 2 (HIPv2). [Online] Available: <https://tools.ietf.org/html/rfc7401>. Accessed on: Nov 19, 2019.
- [35] Lamport, Leslie, Robert Shostak, & Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4.3 (1982): 382-401.



Chapter 2

TOWARDS BLOCKCHAIN IN WIRELESS

2.1 The TCP-Air Interworking Model

While direct allocation of spectrum and evolved medium access protocols provide a base for ubiquitous wireless connectivity, the existing TCP/IP and OSI models were designed for wired networks and do not address open interconnection of air interfaces. Without an interworking model for the air interface, existing network designs continue to tie wireless medium access to that of the backhaul provider for ownership of access and identity trust, resulting in limitations on functionality and coverage.

In this paper¹, we propose a novel solution to access ownership and identity trust by extending the TCP network standard, under a new model we propose, named TCP-Air which integrates distributed ledger technologies directly at the air interface. Further, we present two use cases of the TCP-Air model, demonstrating applications not feasible under existing permissioned-access network designs.

¹Platt, S., Oliver, M. A Distributed Ledger-Enabled Interworking Model for the Wireless Air Interface, 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 402-407, doi: 10.1109/WF-IoT.2019.8767349.

2.1.1 Introduction

Today, wireless networks continue to be treated as permissioned gateways of access to a wired backhaul network, rather than an independent environment - leading to gaps in coverage and access. To address these shortcomings, TCP-extending protocols such as Ad Hoc On-Demand Distance Vector (AODV), and Optimized Link State Routing (OLSR) were introduced as part of the mobile ad-hoc networks paradigm (MANETS). These designs have since failed to gain market adoption [1], [2], in part due to a failure to address the structure of permissioning network access, required ahead of ad-hoc routing.

In this paper, we propose a novel interworking model for the wireless air interface, built upon distributed ledger technologies, named “TCP-Air”. The proposed framework splits interworking functions of the air interface into four model layers, able to operate wholly independent of the wired network functions underneath. The layers, as defined are: Application, Identity, and Spectrum, atop a base layer defined as Ledger - effectively substituting transport functions which bind the air interface and backhaul today. The main contributions of the proposed model are:

- *Mobility*: TCP-Air allows full abstraction of air interface functions from those of a wired backhaul, enabling mobility independent of physical layers underneath.
- *Security*: Using Identity-Based Networking, and immutable ledger distribution, TCP-Air enables higher security, associated to a device identity carried between networks.
- *Permissionless Access*: By combining the additional context of device behaviour, TCP-Air enables autonomous access of physical devices, resolving limitations of existing permissioned network access.

The remaining data of this paper is organized in the following sections. Section II provides information of the state of the art, provid-

ing context of recent research into Identity-Based Networking, and Distributed Ledger technologies which informed the TCP-Air design. Section III defines the proposed TCP-Air interworking model and details its four component layers: Application, Identity, Spectrum, and Ledger. Section IV details TCP-Air in generalized application, detailing two use cases designed under the model. In Section V we discuss the limitations and implications of the proposed framework, and in Section VI we provide a summary of the papers contributions and planned direction for further research.

2.1.2 State of the Art

Identity-Based Networking

Under TCP/IP, the IP address serves dual purpose, as both the machine identity, and a basis for routing to a device in a network. While designed for universality, the IP address introduces security vulnerabilities, because the address itself is not backed by anything verifiable and can be easily spoofed.

In 2015, the IETF adopted draft RFC 7401 [3] for the creation of the Host Identity protocol (HIP). This protocol intends to insert an identity mechanism between the network and transport layers of TCP/IP, effectively isolating the two functions of the IP address, while retaining backwards and forwards compatibility. HIP achieves this by replacing existing “IP Address + Port” routing used at the higher layers of TCP/IP, with a new “Host Identity + Port” pairing (figure 2.1) generated using a Diffie-Hellman method of public key exchange [3]. Under Diffie-Hellman, two communicating parties exchange cryptographic public keys in order to form a shared private key without requiring a prior trust. Because this new identity is verifiable, a network implementing HIP is significantly more secure against man-in-the-middle and DDoS style attacks, which exploit the unverifiability of a traditional IP address [3]. Placing identity as the centre of network design in this manner often referred to as “Identity-Based Networking”.

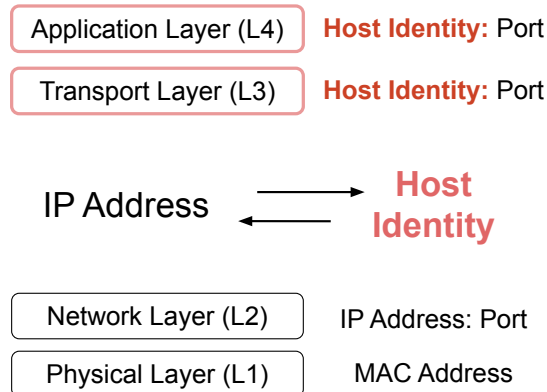


Figure 2.1: The modified Host Identity and port pairing applied with Host.

Distributed Ledger and Web3

The original Bitcoin whitepaper was published in 2008, and detailed the design of a digital currency system that removed the need of a trusted third party for the verification of transactions [4]. The system did this using a peer-to-peer distribution of a universal ledger. Bitcoin’s ledger is designed as a never ending chain structure, where new data being added to the chain requires combining the timestamp of the last transaction, along with a hash of the new data being appended to the ledger (figure 2.2). The resulting aggregate hash gives the ledger its chain structure, and is seen as immutable and highly secure, as a recomputation of all subsequent work is required in order to modify old transactions on the chain [5][6][7]. The later ubiquity of Bitcoin helped popularized the terms Blockchain and Distributed Ledger.

While Bitcoin itself was designed as a digital currency, the blockchain structure of its underpinning ledger has been applied in a number of applications requiring high trust without direct ownership. This class of applications are increasingly termed as “Web3” indicating a belief that the next generation of internet development will exist in this decentralized model.

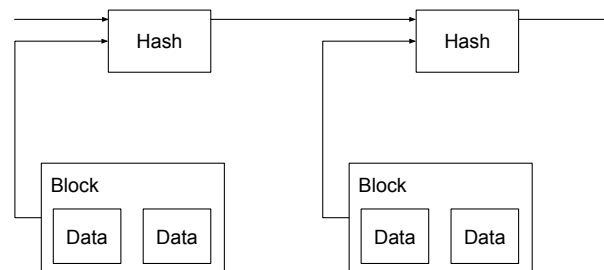


Figure 2.2: Bitcoin blockchain structure.

Filecoin [8] is an example of such Web3 class application. Filecoin is a decentralized network storage platform. Built on top of a distributed ledger; the Filecoin system allows users to pay for storage of data on the network or earn payment through hosting the files of others. Files stored in the Filecoin network use data sharding and peer-to-peer distribution to ensuring file contents cannot be read by network participants not directly owning the file.

2.1.3 TCP-Air Model In Detail

TCP-Air is an abstract model designed to provide a framework for direct interworking of the wireless air interface by combining existing TCP/IP and wireless medium access functions, with new services provided through host identity and distributed ledger technologies.

Similar to the TCP/IP and OSI model, TCP-Air is modelled using a layered architecture [9], with each interconnecting system being composed of subsystems, where equivalent subsystems exist in the same layer of the model and interactions occur only between subsystems at adjacent layers.

In total, the TCP-Air model is consisting of four layers, they are: Application, Identity, Spectrum, and Ledger.

TCP-Air is not designed as a replacement for the existing TCP/IP standard, rather as a parallel model, in a relationship similar to that of

TCP/IP and the OSI model, while being purpose built to enable coordination among unmanaged air interface networks. The following sections provide detail on the function of each layer of the TCP-Air model (table 2.1).

TCP-Air Model Layers		
<i>Layer Number</i>	<i>Layer Name</i>	<i>Layer Function*</i>
4	Application	Internet Protocol, User Interface
3	Identity	Host Identity, Profiling, Access and Authorization
2	Spectrum	Spectrum Addressing, Wireless Medium Access, Spectrum Sensing, Peer Supplication, Ledger Termination, TCP/IP Termination
1	Ledger	Block Store, Route Store, Block Distribution, Block Cache, Chain Connection, Chain Management, Accounting

Table 2.1: TCP-Air model layers. **table is not inclusive of all possible model layer functions.*

Definitions

- *Air Interface*: The radio managing interconnection between access points and other physical devices, which use air as the transport medium.
- *Peer*: Two air interfaces which have the ability to bi-directional exchange data using air as the transport medium.
- *Supplication*: The registration of an access point as client to another access point.

- *Block*: A single unit of storage for data written to a ledger.
- *Chain*: The total of block data, which has been cryptographically linked. (a chain of blocks).
- *Ledger*: The aggregate of block storage, chained and distributed throughout a network. (distributed ledger).
- *Route*: The stored path to an air interface peer within separately managed networks that is connected through federation.

Application Layer: The application layer handles peer-to-peer and client-server communications for applications and services using Internet Protocol (IP), as well as surfacing data for user interaction. Services provided are:

- *Internet Protocol*: Handling of communications between peer protocols functioning in the Internet Protocol suite, including, but not limited to: HTTP, FTP, DNS, SSL, IMAP, NTP, SIP, and SMTP.
- *User Interface*: Handling of data presentation, and manipulation for services allowing end-user exposure or interaction.

Identity Layer: Execution of identity and authentication functions within the TCP-Air model. Services provided are:

- *Host Identity*: Assignment of host identity for routing and termination of application, network, and chain connections. Correlation of cryptographic identity, hardware address, and/or IP address.
- *Profiling*: Correlation of traffic patterns, access patterns, mobility patterns, and physical device attributes.
- *Access and Authorization*: The identity layer is responsible for granting and revoking access to network, spectrum, and chain resources.

Spectrum Layer: The spectrum layer handles all functions to enable connection within wireless spectrum. Services provided are:

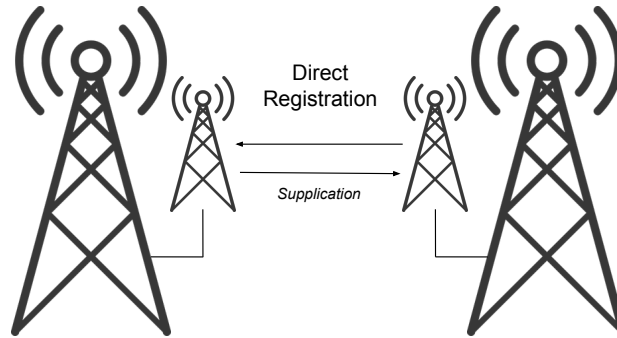


Figure 2.3: Air interface peering through direct supplication.

- *Spectrum Addressing*: Legacy MAC and IP addressing of physical devices accessing a given air interface.
- *Wireless Medium Access*: Wireless channel assignment, power, flow, and transmission controls, beam-forming, contention resolution, and quality of service.
- *Spectrum Sensing*: Scanning of compatible air channels and surrounding devices [10].
- *Peer Supplication*: Registering as supplicant to unmanaged air interface peers. Routing and peering of data outside a given air interface (figure 2.3).
- *Ledger Termination*: The spectrum layer handles routing and delivery of data and connection to the ledger layer for immutable storage [11].
- *TCP/IP Termination*: Routing and termination of data, and connection to the broader internet.

Ledger Layer: The ledger layer is the communications path of the TCP-Air model and provides abstraction from the routing and topology of

a wired backhaul. The ledger layer enables seamless mobility, and higher security [6], through the syncing, caching, and distribution of network permissions among participating air interface termination points [11][12]. Services provided are:

- *Block Store*: Assignment, hashing, and storage of data onto chains.
- *Route Store*: Recording of air interfaces, network routes, peer air interface routes, and/or cryptographic identity data for physical devices transacting on a given chain.c) *Block Distribution*: Peer-to-Peer propagation of block data among air interface termination points, transacting on a given chain.
- *Block Cache*: Temporary storage of chain data with highest probability of near-term access.
- *Chain Connection*: Connectivity between physical endpoints accessing the same service whose permissions are distributed on the ledger layer.
- *Chain Management*: Management of network participation. Orchestration of chain functions, including contracts.
- *Accounting*: Immutable storage of physical device access and behavior profile data.

2.1.4 Sample Use Case: Vehicle Networks

Despite the maturity of ITS [13][14] and vehicle network research [15], there has not been developed consensus for handling permissioned network access in a manner that enables global coverage. For this reason, a vehicle network example is chosen to demonstrate the resolution of coverage limitations through adoption of a TCP-Air model design.

Network Design

The design assumes random distribution of roadside units on a road network spanning multiple municipalities. Each municipality operates independently, without a trust to authorize vehicles arriving from outside of its zone. Figure 2.4 shows the interaction among model layer functions. The layer functions are:

- *Application Layer*: To demonstrate expanded coverage, the application in this example is the general internet. No restriction is placed on routing in this design.
- *Identity Layer*: Access to the network is granted autonomously. To establish identity in the trustless environment, a host identity is created for each vehicle. This identity serves both as an aggregation point for behavior data, and as an abstraction for routing as vehicle IP addressing changes in network handoff between municipalities. With an identity abstracted from network ownership, a profile is created to learn devices with mobility patterns matching that of the road network - determined by patterns of roadside unit adjacency, distribution and variation of speed. A final filter of hardware address (MAC) is applied to remove devices which are not produced by known vehicle manufacturers. The resulting host identity profile is set on an expiry, to allow pruning of retired vehicles and restrict anomalous vehicles, not matching established identity histories and patterns of behavior.
- *Spectrum Layer*: Utilizing spectrum scanning [10], the network reports device adjacencies. Through RSSI-based network localization [16][17], vehicle speed and direction are deduced. As the TCP termination point, and the layer handling medium access, an open SSID is broadcast with its default VLAN utilizing a null route. Vehicles learned and authorized by network behavior profiling are automatically placed into a routed VLAN to the broader internet.
- *Ledger Layer*: Rules governing access to the vehicle network are

stored as a smart contract on a single ledger chain [18]. The same chain stores vehicle behavior, host identity, and access authorizations. Data stored on the chain is immutable and propagated among participating roadside units in the multi-municipality network. Additional chains may be added to the ledger, for future services, such as safety and hazard notifications, without managed network access or identity trust [11][12].

Further Implementation

Through reuse of layer functions presented in our vehicle network example, the extended functionality of wireless emergency location services is possible. This additional use case is presented as a high-level proposal, to add further context for TCP-Air use as a generalized model.

- *Wireless Emergency Location Services*: Under government regulation, regions such as Europe and the United States require the inclusion of accurate location data with calls placed to emergency services from wireless networks [19]. In cellular networks, this is implemented using network localization among neighboring towers. A limitation of this implementation is introduced by elevation within buildings, due to refraction and reflection experienced among signals used to calculate location. For extending network functionality, to include accurate elevation, we propose use of access federation functions within the TCP-Air model among 802.11 access points within the building environment. In this design, further localization among 802.11 access points allow deduction of floor level, through the awareness and sorting of access point signal adjacency at a given building address.

2.1.5 Discussion

Implementation of functions described in the model are based on several assumptions.

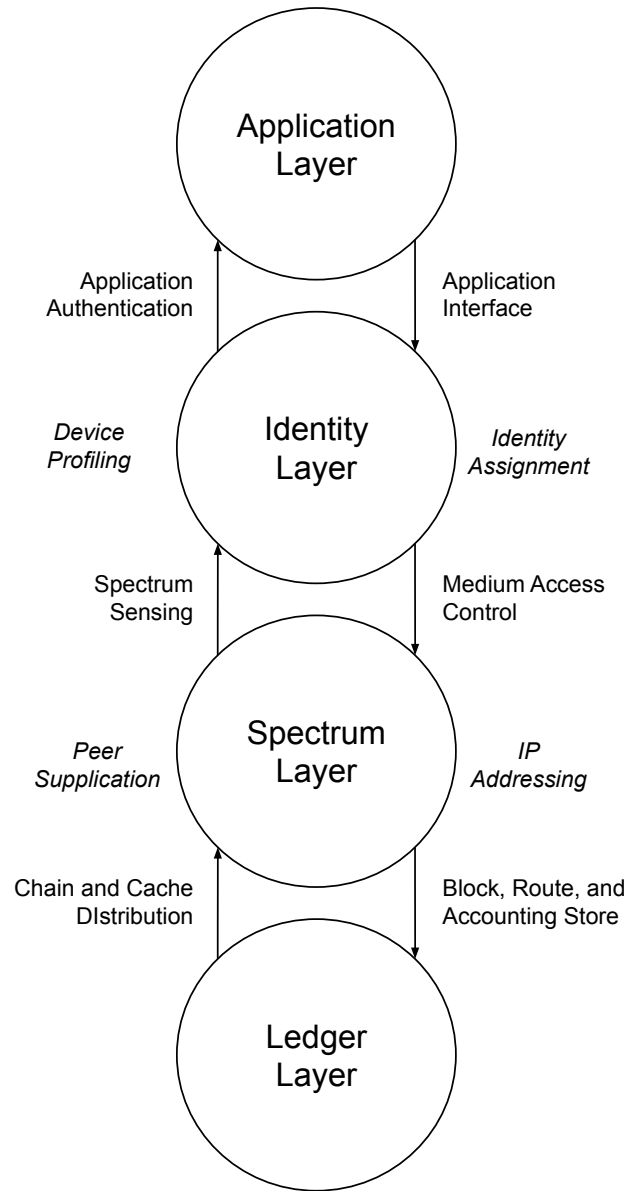


Figure 2.4: Layer interaction model of TCP-Air.

Equal network participation and traffic distribution

When connecting unmanaged networks, there arises a possibility of asymmetry within network traffic, for example: disproportionality due to network size, device numbers, or physical device distribution. In our example of federated coverage among municipalities, it is possible that a municipality hosting an urban hub has a network density exceeding the capacity of peer networks. It is possible to program balance into such traffic distribution, through routing modification, caching of interactions, quality of services measures, or smart contract functions programmed within the ledger. Such mechanisms of system-wide resource management require further research.

Scalability of the distributed ledger

There are many variations of ledge implementation, each with unique benefits and dependencies. The model as presented does not make an explicit choice of ledger technology, rather it amalgamates existing ledger technologies to prevent association or inheritance of characteristics existing in any single ledger. This limits specificity within the example designs, but opens an area of further research and resolution of which performance measures of distributed ledgers best suite a network infrastructure environment [20].

No association between physical device profile and user identity

Examples provided for TCP-Air implementation, enable permissionless access built on identity profiling. Because the system uses spectrum scanning of the ambient environment, there is no implicit ability to opt in or out of detection. Further, the profile data is collected over time and made immutable through its storage within a distributed ledger. Although profile data is collected and correlated based on physical device behaviours, the extent to which these devices can be associated to unique users may invoke additional privacy restriction on such model functions. As a base,

the model assumes no association between physical device and user identity.

In this paper we identify the structure of permissioned network access and trust of identity, as characteristics which have prevented direct interworking of air interface networks. To address these limitation, we propose a new interworking model, named TCP-Air, combining existing function of wireless networks, with two new interworking layers handling identity and immutable storage on a distributed ledger. Additionally, the paper outlines two example deployments under the model, which enables permissionless network access and fluid mobility to create a pervasive vehicle network infrastructure, as well as enhanced functionality for wireless emergency location services. For future work, we are interested to investigate specific implementations of the ledger base layer protocols, to examine performance and scalability within a live environment implementation.

Bibliography

- [1] Conti, M., & Giordano, S. (2014). Mobile ad hoc networking: Milestones, challenges, and new research directions. *IEEE Communications Magazine*, 52(1), 85-96. <https://doi.org/10.1109/MCOM.2014.6710069>.
- [2] Bruno, R., Conti, M., & Gregori, E. (2005). Mesh networks: Commodity multihop ad hoc networks. *IEEE Communications Magazine*, 43(3), 123-131. <https://doi.org/10.1109/MCOM.2005.1404606>.
- [3] Internet Engineering Task Force. IETF Host Identity Protocol RFC: <https://tools.ietf.org/html/rfc7401>.
- [4] Satoshi Nakamoto. (2016). Bitcoin: A Peer-to-Peer Electronic Cash System, 1-9. <https://doi.org/10.1007/s10838-008-9062-0>. 2016.
- [5] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on Blockchain technology? - A systematic review. *PLoS ONE*, 11(10), 1-27. <https://doi.org/10.1371/journal.pone.0163477>.
- [6] Skwarek, V. (2017). Blockchains as security-enabler for industrial IoT applications. *Asia Pacific Journal of Innovation and Entrepreneurship*, 11(3), 301-311. <https://doi.org/10.1108/APJIE-12-2017-035>.

- [7] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*. <https://doi.org/10.1016/j.future.2017.08.020>.
- [8] Benet, J., & Greco, N. (2018). Filecoin: A Decentralized Storage Network. Protocol Labs, 1-36. <https://doi.org/10.1088/1126-6708/2007/08/019>.
- [9] ITU-T. (1994). X.200: Open Systems Interconnection - Model and Notation, 4, 23. Retrieved from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items.
- [10] Kismet Wireless Sniffer: <https://www.kismetwireless.net/>.
- [11] Polyzos, G. C., & Fotiou, N. (2017). Blockchain-assisted information distribution for the internet of things. *Proceedings - 2017 IEEE International Conference on Information Reuse and Integration, IRI 2017, 2017-January*, 75-78. <https://doi.org/10.1109/IRI.2017.83>.
- [12] Leiba, O., Yitzchak, Y., Bitton, R., Nadler, A., & Shabtai, A. (2018). Incentivized Delivery Network of IoT Software Updates Based on Trustless Proof-of-Distribution. *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018*, 29-39. <https://doi.org/10.1109/EuroSPW.2018.00011>.
- [13] ETSI TR 102 638, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions, V1.1.1, 2009.
- [14] [14] ITU-R M.1890, Intelligent Transport Systems - Guidelines and objectives, 2011.
- [15] 3GPP Release 15: <http://www.3gpp.org/release-15>.
- [16] Ranta-Aho, K. Performance of 3GPP Rel-9 LTE positioning methods, in *Proc. 2nd Invitational Workshop Opportunistic RF Localization Next Generation Wireless Devices*, Jun. 2010, pp. 1-5.

- [17] Shang, Y., Ruml, W., Zhang, Y., and Fromherz, M. Localization from mere connectivity, in Proc. Mobile Ad Hoc Netw. Comput. (MobilHoc), 2003, pp. 201-212.
- [18] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303. <https://doi.org/10.1109/ACCESS.2016.2566339>.
- [19] EU Single Market Rule 112: <https://ec.europa.eu/digital-single-market/en/eu-rules-112>.
- [20] Karafiloski, E. and Mishev, A. Blockchain solutions for big data challenges: A literature review, IEEE EUROCON 2017 -17th International Conference on Smart Technologies, 2017, pp. 763-768, doi: 10.1109/EUROCON.2017.8011213.



Chapter 3

BUILDING A BLOCKCHAIN PROTOTYPE

3.1 Experiment: Decentralized Access Control

Distributed consensus mechanisms have been widely researched and made popular with a number of blockchain-based token applications, such as Bitcoin, and Ethereum. Although these general-purpose platforms have matured for scale and security, they are designed for human incentive and continue to require currency reward and contract functions that are not requisite in machine communications. Redes Chain is a new blockchain, built to support fully decentralized self-organization in wireless networks - without a cryptocurrency or contract dependency.

3.1.1 Introduction

Initially popularized through application in digital currency, distributed ledger technologies (DLT) are now seeing wider adoption as a path for extending peer-to-peer design and security to the broader internet. To allow open participation, a number of DLT designs deploy computationally expensive cryptography paired with digital currency reward [1], creating a format optimized for human incentive and trust that is a less natural

fit for machines. Although popular applications of blockchain including Bitcoin and Ethereum, tie blockchain to a digital currency function - it is important to note that blockchain as a data structure has no native association to digital currency. It is this isolated application of the blockchain data structure, and its ability to support distributed consensus, that is the focus of this research.

The ability to form consensus among equal peers has a number of implications in networks research - but we propose its most natural application is that of decentralizing self-organization functions in wireless networks - systems which by design are dependent on coordination and context sharing among network participants.

In the following sections of this paper¹, we detail the use cases and limitations of existing cryptocurrency-based blockchain ecosystems Bitcoin and Ethereum. We then define the broader Self Organizing Network use case - presenting a new model, built atop blockchain, that is wholly decentralized. Next, we present Redes Chain - a new blockchain prototype, designed for machine communications and to allow the decentralization of self-organization functions in wireless networks. Finally, the Redes blockchain prototype is demonstrated through a proof-of-concept deployment handling access federation among independent 802.11 networks.

3.1.2 Bitcoin and Ethereum: Blockchain for Currency and Contract

Today Bitcoin is the most well-known application of blockchain technology, but also the oldest and simplest technical implementation in popular use. The original Bitcoin whitepaper was published in 2008, and detailed the design of a digital currency system that removed the need for a trusted third party for the verification of transactions [1]. In being designed as a digital currency, the Bitcoin ledger structure can be simplified as a state

¹Platt, S., Oliver, M. Towards Blockchain for Decentralized Self-Organizing Wireless Networks, 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1-5, doi: 10.1109/GCWkshps45667.2019.9024426.

transition system; with the current state represented as the total ownership of all digital coins at a moment in time, and the state transitions represented by the movement of these coins, or payments made between users in the network.

To aid in decentralization, Bitcoin is designed as a permissionless network, allowing nodes or participants to join and leave the network at any time - with all transaction data sent as broadcast. After data is broadcast, computers in the network compete to find a hash of the block data that is smaller than a threshold size or difficulty set for the entire network. The hash difficulty of the bitcoin network is a composite function of its block throughput target and the combined hash power of the total network (3.1). At the time of writing, hash difficulty is adjusted so as to keep block creation constant at roughly one block every ten minutes [2].

$$\text{hash difficulty} = f(\text{block throughput target}(\text{network hash power})) \quad (3.1)$$

Because the result of hashing is pseudo-random, it is believed that every computer in the network of equal computing power, has an equal chance of being first to find the correct hash [3]. The equality created through the pseudo-random hash function also makes the network able to remain secure as long as a simple majority, or 51% of the network are acting in good faith, but results in a number of required hashes that is a further composite function of the previously mentioned hash difficulty, and the number of pending blocks being added in the network (3.2).

$$\text{required hashes} = f(\text{hash difficulty}(\text{pending blocks})) \quad (3.2)$$

To provide incentive for doing the difficult computation work, machines participating in the network are issued a reward in the form of Bitcoin, for finding and broadcasting the first hash successfully. These reward payments are covered by transaction fees charged to users wishing

to add blocks to Bitcoins' chain. Because this hash value can be verified by others in the network - this process of consensus is named "Proof of Work" (POW). A primary side effect of the race condition created through POW consensus, is that power used for all unsuccessful hashes is considered wasted, making the system highly resource inefficient. A secondary behavior and weakness of using the POW consensus model is that it makes financial incentive in the form of block rewards and transaction fees, native to the operation of the system.

In 2013, Vitalik Buterin published the Ethereum whitepaper, seeking to expand the functions of Bitcoin - into a general purpose compute platform. The Ethereum blockchain included a more complex block structure that allowed storing logic which executes only when preset conditions are met. This new block structure allowed the creation of contracts, but retained Bitcoin's permissionless format, POW consensus, and block rewards [3]. Programmed into the contract support of Ethereum, is the ability to create a secondary digital currency token, pegged to the value of Ethereum's own digital currency, Ether. These tokens are referred to as ERC-20, and in effect, allow a white labelling of the core Ether token, while retaining compatibility with the broader ecosystem of Ethereum smart contracts [4]. A number of network systems have been built on top of the Ethereum blockchain, but in doing so, these systems must inherit Ethereum's contract structure, with peer-to-peer payments at the core. An example of such system is Privatix Network, a VPN service allowing peer-to-peer payment for bandwidth used while hosting VPN connections [5].

3.1.3 Self-Organizing Networks

To address concerns of increasing complexity in cellular networks, the 3GPP completed work to formally define Self Organizing Network (SON) functions in tandem with the development of the LTE cellular standard. SON functions today are formed in one of three designs: centralized, distributed, and hybrid [6]. In a centralized design, resource management and air interface coordination algorithms are processed by a central con-

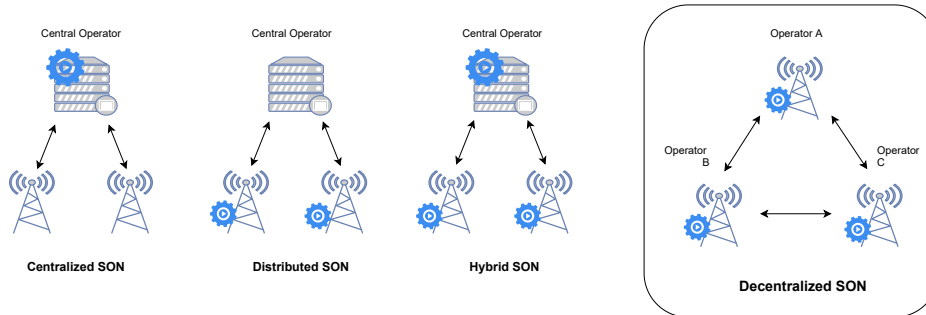


Figure 3.1: SON Architectures.

troller. With a distributed model, these algorithms are run at the network edge. Finally, a hybrid model employs a combination of the former two [6]. It is important to note that although a distributed model allows algorithms to run at the network edge, these controls remains limited to coordination within a single operator environment, often relying on S2 interface connections to a carrier core in cellular deployment, or a hub controller in 802.11x networks for compatible hardware actuation and control [7].

With a target to reduce manual administration by automating routine configurations in cellular networks; the SON standards developed by the 3GPP eventually included provisions for energy savings, handover optimization, automatic neighbor relation management, and load balancing [7]. Today these cellular-centric SON operations have also been extended to Wi-Fi and other air interface networks which benefit from the enhanced environment knowledge and distributed coordination capability that SON provides [8]. The Redes blockchain proof of concept, presents a new fourth model of wireless SON functionality, built in a fully decentralized context, allowing wider coordination among isolated networks that do not share controller or S2 interface connectivity (figure 3.1).

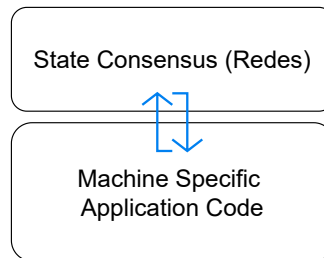


Figure 3.2: Redes separation of consensus and application code.

3.1.4 Blockchain For Self-Organizing Networks

The Redes blockchain is structured as a permissioned chain and does not attempt to enforce code execution commitments in the form of smart contracts as with Ethereum. The Redes proof of concept as presented, deploys blockchain in its more basic form - as a decentralized data store for network specific state data. With Redes, data storage and hardware specific actuation and control operate separately (figure 3.2). Structuring the chain in this way allows the benefits of developing distributed consensus while leaving code execution control with individual network operators who can optimize for various combinations of hardware in their environment. The Redes blockchain is unique in that it assumes inherent value for the data itself, demonstrated through examples such as spectrum sharing facilities, where a wider environment context is required for optimal network function [9].

System Requirements

The Redes blockchain is written in the Python programming language, for hardware isolation, and portability across infrastructure. Using Python version three for the construction of Redes also allowed the use of Python libraries and micro-frameworks - including Flask and SQLite for full web server and database functions in a compact package suitable for embedded systems use. Since it is not intended as a one-size application plat-

form, or a digital currency, Redes can strip out dependencies that would require a full Linux operating system or more robust database systems as seen in larger Ethereum, and Bitcoin derived projects [4]. In current form, the Redes Blockchain code utilizing less than 20kb of disk space in isolation, and can be installed on feature restricted embedded operating systems, such as the “Busy Box” Unix operating system, or any platform supporting Python version three.

	Bitcoin	Ethereum	Redes
Consensus	Proof-of-Work	Proof-of-Work	Proof-of-Signature
Participation	Permissionless	Permissionless	Permissioned
Language	C++	Go, C++, Rust	Python
Currency	Bitcoin	Ether	-
Contract Support	Partial	Full	-

Table 3.1: Comparison of Bitcoin, Ethereum, and Redes Blockchains [10].

API, Block Format, and Consensus

Making use of the Python “Flask” micro-framework, Redes includes its own API with 6 initial functions: register a node, remove a node, trigger consensus, issue a transaction, create a block, and request the longest chain. Testing functionality and interacting with the underlying ledger is done through calls to these 6 API’s.

Although the API format is consistent with other blockchain projects, the larger change is the format of the ledger blocks themselves. The block fields in Redes do not include provisions for currency or account balance as in Bitcoin and Ethereum. These are replaced with “mac address” and an “action” field for SON control of network access in the proof of concept use (3.3). Table 3.1 shows a high-level comparison of Bitcoin, Ethereum, and the new Redes blockchain.

```
def new_transaction(self, sender, recipient, mac, action)      (3.3)
```

As a permissioned system, the “register a node” API allows initial registration of peers in the Redes network. Only known peers are allowed to participate in synchronization, with its registered node IP serving as signature in synchronization requests. This IP whitelisting gives Redes its proof-of-signature consensus name. Network synchronization is handled by either an API request to “request the longest chain” for requesting the chain of a single peer, or through the “trigger consensus” API, which notifies all known peers to request the chains of their known peers. Algorithm 1 shows the pseudocode each node uses to reach consensus, based on the longest valid chain received after a request to the trigger consensus API.

Algorithm 1: Pseudocode for Modified Consensus

Data: chain, chain.length, max.length

Result: form consensus using longest chain

initialization

while *conflict = true* **do**

 // verify longest chain

for all neighbors

 requests.get(https://[node]/chain)

if *response = !null* **then**

 new_length = response.length

 new_chain = response.chain

if *new_length > chain.length & last_block.hash = self.hash(last_block)* **then**

 // accept longest chain

 length = new_length

 chain = new_chain

 process_son(block)

end

end

end

For this research, each node issuing a transaction, was required to hash the block itself, and after, trigger consensus on the network in order to remove the compute race condition present in Bitcoin and Ethereum. Before a node accepts the transaction, the proof is still validated before the updated chain record is accepted. Integrity and consensus of state formed in the chain is still assumed valid, as any modification or corruption of previous block data changes and invalidates the hash result achieved by network nodes when the proof is checked (figure 3.3) [10].

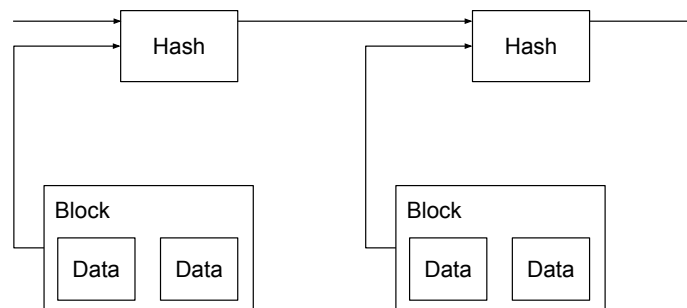


Figure 3.3: Forward hash linking in Blockchain Data Structure [10].

Decentralized Network Access Control Use Case

To test initial function of the Redes blockchain prototype, a testbed was devised, consisting of 3 802.11 capable wireless access points running the OpenWRT operating system, and installed inside VirtualBox. Running Redes within an installation of OpenWRT, the combined system, inclusive of the operating system, web server, and database - totals less than 60Mb for the VirtualBox disk image. Other specifications for the OpenWRT hosts are 1 virtual CPU core and 256Mb of RAM. The target of the testbed was to prove an early application of Redes state consensus, combined with local application control to execute the decentralized SON function of network access control among the otherwise isolated wireless access points.

Beginning with the base OpenWRT image, the three systems had all dependencies installed, then set to run the Redes blockchain. After this initial validation, the Redes blockchain API was validated using the "Postman" API testing application. All nodes were registered with each other, using the "register a node" API function, to allow syncing and writing the Redes blockchain (figure 3.4). Each OpenWRT system then issued "create a block" transactions to the Redes JSON API interface, with a value filled for "mac" and an additional "action" field, signaling a device should be "allowed" or "denied" network access (figure 3.5). In total, validation

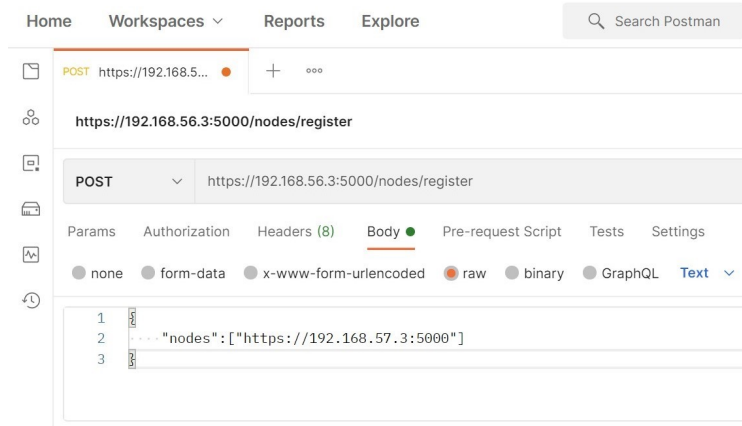


Figure 3.4: New node registration using the Postman utility and Redes JSON API.

of the 6 API functions was successful, proving that the desired data was stored in the chain and consensus based on the longest chain could be formed - although network access was not yet tied to information stored in the chain.

A final test from the testbed required pairing local code execution with the Redes state consensus, allowing the OpenWRT systems to issue system commands to add and remove devices from its local firewall configuration - in turn permitting access to the previously isolated wireless networks (Algorithm 2).

Running the updated Redes code successfully allowed adding new blocks, forming consensus based on the longest valid chain, and finally adding the new devices to local firewall rules, demonstrating a decentralized SON use case of federating access controls to the additional OpenWRT devices operating the Redes blockchain.

Algorithm 2: Pseudocode for OpenWRT SON Execution

Data: block, block.devicemac, block.deviceaction

Result: OpenWRT local code execution

initialization

while *block = true* **do**

 process block

if *deviceaction = add* **then**

 openwrt subprocess.call('add firewall rule [devicemac]')

 openwrt subprocess.call('set

 firewall.rule[-1].target=accept')

 openwrt subprocess.call('set firewall.rule[-1].proto=tcp

 udp icmp')

 openwrt subprocess.call('set firewall.rule[-1].src=lan')

 openwrt subprocess.call('set

 firewall.rule[-1].src_mac=[devicemac]')

 openwrt subprocess.call('commit and reload')

end

if *deviceaction = remove* **then**

 openwrt subprocess.call('delete firewall rule

 [devicemac]')

 openwrt subprocess.call('commit and reload')

end

end

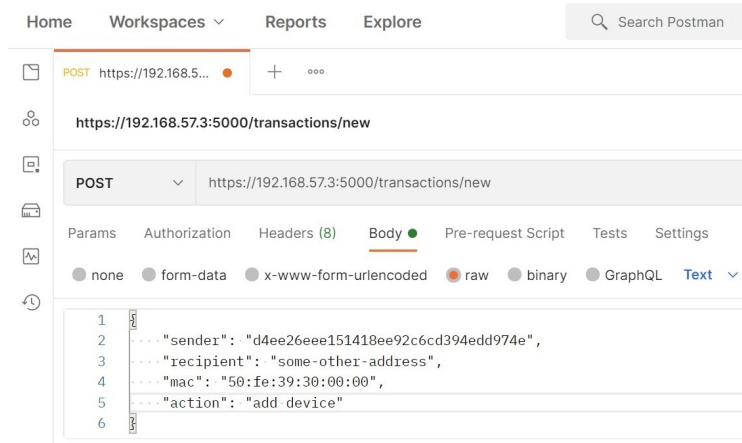


Figure 3.5: Issuing a new block using the Postman utility and Redes JSON API.

3.1.5 Discussion

In this research, we outline popular applications of the blockchain data structure and the limitations tied to its currency and contract use. Next, we outline the need for application specific blockchain technologies, presenting our SON use case where execution of code differs among nodes, and value is derived from the blockchain data itself, rather than a cryptocurrency token. Finally, we detail and demonstrate the Redes blockchain, a new blockchain we’ve developed which uses a proof-of-signature consensus to reduce hash power requirements and handle a single decentralized SON function of federating access controls among otherwise isolated 802.11 networks. Redes validates a path for use-case specific blockchain, rather than use of existing chain ecosystems for machine communications in our SON specific use case. The testbed delivers a basic permissioned blockchain that can be used to share and action data, while consuming less resources by removing the compute race condition inherent to Bitcoin and Ethereum POW; replacing it with a proof-of-signature consensus better suited to permissioned network environments. In present form, the proof-of-signature consensus does not include provisions to handle

malicious or malfunctioning nodes, and as a result, it is understood to be vulnerable to forking originating from block timing and/or forging of transactions using spoofed IP addresses as signature. Future research for Redes will focus on development of its security and consensus model, including but not limited to controls for block timing and collisions, implementation of cryptographic key signatures, and support of additional wireless SON functions, such as neighbor discovery, power control, and wireless channel selection.

Bibliography

- [1] Nakamoto, S. (2016). Bitcoin: A Peer-to-Peer Electronic Cash System, 1-9. <https://doi.org/10.1007/s10838-008-9062-0>. 2016.
- [2] Andreas M. Antonopoulos. 2014. Mastering Bitcoin: Unlocking Digital Crypto-Currencies (1st ed.). O’Reilly Media, Inc..
- [3] Feller, W. An introduction to probability theory and its applications. O’Reilly Media, Inc. 1957.
- [4] Buterin, V. A next-generation smart contract and decentralized Application Platform (White Paper). GitHub, 223. <https://github.com/ethereum/wiki/wiki/White-Paper>. Accessed 23/05/2019.
- [5] Privatix Network. Privatix Network. 2018. <https://privatix.io/>. Accessed 23/10/2018.
- [6] Nohrborg, M. 2019. Self organizing networks. <https://www.3gpp.org/technologies/keywords-acronyms/105-son>. Accessed 23/05/2019.
- [7] Ramiro, J., Hamied, K. Self organizing networks; self planning, self optimization, and self healing for GSM, UMTS, and LTE networks. O’Reilly Media, Inc. 2012.
- [8] Qualcomm Technologies, Inc. 2019. Qualcomm Wi-Fi SON and distributed networking.

<https://www.qualcomm.com/solutions/networking/features/wi-fi-son>. Accessed 1/5/2019.

- [9] Oliver, M., & Majumder, S. (2019). Motivation for TV white space: An explorative study on Africa for achieving the rural broadband gap. In The 2nd Europe - Middle East - North African Regional Conference of the International Telecommunications Society: Leveraging Technologies For Growth, February 18-21, 2019, Aswan, Egypt.
- [10] Chalaemwongwan, N., Kurutach, W. 2018. State of the art and challenges facing consensus protocols on blockchain. International Conference on Information Networking, 2018-January, 957-962. <https://doi.org/10.1109/ICOIN.2018.8343266>.

Chapter 4

THE CONTE TEMPORAL BLOCKCHAIN

Virtual Network Functions allow the effective separation between hardware and network functionality, a strong paradigm shift from previously tightly integrated monolithic, vendor, and technology dependent deployments. In this virtualized paradigm, all aspects of network operations can be made to deploy on demand, dynamically scale, as well as be shared and interworked in ways that mirror behaviors of general cloud computing. To date, although seeing rising demand, distributed ledger technology remains largely incompatible in such elastic deployments, by its nature as functioning as an immutable record store. This paper¹ focuses on the structural incompatibility of current blockchain designs and proposes a novel, temporal blockchain design built atop federated byzantine agreement, which has the ability to dynamically scale and be packaged as a Virtual Network Function (VNF) for the 5G Core.

¹Platt, S., Sanabria-Russo, L., Oliver, M. CoNTE: A Core Network Temporal Blockchain for 5G. *Sensors* 2020, 20, 5281. <https://doi.org/10.3390/s20185281>.

4.1 Introduction

Unlike alternative distributed ledger structures, such as Block Lattice [1], Directed Acyclic Graph [2], and Distributed Hash Tables [3], which gain flexibility through modification or fragmentation of the underlying hashed-linked storage; blockchain allows little manipulation of its base structure outside of consensus model and block size. This rigid chain structure guarantees auditability, making it especially well-suited to policy-based operations demanding transparency and coordination among unmanaged network peers. For example, in events of natural disaster, or widespread infrastructure failure, having access to a trusted, secure, and decentralized data store, can be extended to allow infrastructure coordination, such as network slice allocation and other decentralised cyber-physical control, delivering neutral carrier emergency services to endpoints who would not otherwise be known subscribers.

Understanding that blockchain has the structural capability to allow for coordination among infrastructure peers, recent research has moved to focus on how to fit such coordination within existing and popular blockchain mechanics and, as a result, places incentive mechanics as core and requisite to operation. These range from shared infrastructure deployment of a virtual LoRaWAN network [4], resource management in neutral carrier [5], and 5G small cell deployment [6], as well as macro-level spectrum trading and management [7]. Beyond these, bespoke wireless network-specific forks of Ethereum have also been deployed to handle coordination of mesh infrastructure and last mile connectivity [8, 9]. Underneath each of these is a limitation that is imposed by using a linear forward-hashed blockchain system that includes currency operations; they cannot be easily fragmented, since, by nature, currency transactions rely on the preceding balance recorded in perpetuity.

An inability to split up or retire ledger history has a secondary effect of reducing compatibility with the latest 5G and beyond network designs, which rely on virtual network functions with temporal/limited lifecycles and the ability to not only scale up, but also scale down. As network infrastructure is increasingly abstracted and replaced with software-

defined platforms for 5G and beyond generations of deployment, use of blockchain allows for sharing and coordination in ways both known and unknown, and this shows further need for blockchain that is generalized and made widely compatible with cellular design. One way of doing this is returning blockchain to the function of “dumb” storage and, in doing so, allow all cellular operations that store data, to make use of its decentralizing and immutable nature. On the path to generalizability in cellular deployment, it is important to recognize limitation in blockchain as a data structure, in that it is linear storage and, as such, does not scale in applications, where transactions have potential to be highly bursty, or expand exponentially, such as at the network edge. Recognizing this, and further time-bounds of edge operation, we target application of blockchain at the cellular core.

4.1.1 Enabling Lifecycle Control

In order to address concern of its monolithic structure and unbounded resource use, Ethereum has progressed through investigating a number of methods to scale down and make modular its monolithic blockchain, including horizontal data sharding [10], and state channels [11], as well as a full migration away from its original proof-of-work consensus, to a less compute intense implementation of proof-of-stake, named Casper, allowing for compute complexity of (O^2) [12]. In each case, although more efficient, total storage remains unbounded, and without lifecycle, so the original difficulty to wholly package the system for temporal network function use remains. Further blockchain systems have focused on efforts to scale, but make no allowance for temporal use. Tendermint provides for scaling up and down by implementing federation in consensus that creates smaller clusters of consensus that overlap to guarantee a minimum byzantine fault tolerance [13]. These smaller clusters of consensus allow for controlled network segmentation and isolation, but lose the ability to deploy permissionless, as network topology and membership must be known to enforce its consensus cluster overlap for fault tolerance. The Stellar project is structurally similar to Tendermint, but it does not guaran-

tee fault tolerance [14]. This federated model of consensus that removes fault tolerance but still guarantees safety and liveness was named Federated Byzantine Agreement and first appeared with Stellar. Removing the guarantee of fault tolerance has the added benefit of allowing the consensus model to be used permissionless, but, because Stellar also includes a native currency, its ledger is monolithic and cannot be made temporal, so long as any participant carries a balance or need to transact on a previous history. In each of these systems, a work around for perpetual storage, and to assign a lifecycle terminus, is to use the systems in private deployment. In this model, a smaller group of participants can deploy ledgers for a single use and retire the ledger when that use is complete. However, in private deployment, these systems again lose any ability to function permissionless and, instead, behave in a manner similar to the permissioned and enterprise focused Hyperledger Sawtooth [15]. Table 4.1 provides an overview and comparison of these systems, as well as *Conte*, a new blockchain system presented in this research. To the authors knowledge, we present the first permissionless blockchain which achieves the following properties:

- *Lifecycle Control*: Participants create single use chains that are immutable while being updated, and can be retired when no longer in use. By removing currency and contract functions, the remaining data storage function does not play a role in forward balance history, nor is it required for ledger security.
- *Network Function Compatibility*: As a data store, the blockchain is made agnostic to use case; combining this with lifecycle control allows for the system to be used for temporal 5G virtual network functions.

This research diverges from currency and contract focused research in two important ways; first, a deliberate focus is placed on blockchain use solely as secure, decentralized storage, rather than a mechanism of direct policy and incentive control; second, cellular design was given priority, with the goal of packaging blockchain to accommodate cellular operations rather than the inverse. This second goal, meaning to package

	Consensus	Compute Complexity	Model	Currency	Temporal
Ethereum [12]	Proof of Stake	$O(n)$	Permissionless	Yes	No
Tendermint [13]	BFT	$O(n)$	Permissioned	Yes	No
Hyperledger Sawtooth [15]	PBFT	$O(n^2)$	Permissioned	No	Yes
Stellar [14]	FBA	$O(n^2)$	Permissionless	Yes	No
Conte	FBA	$O(n)$	Permissionless	No	Yes

Table 4.1: Comparison of selected blockchain distributed ledger systems.

blockchain as a standard virtual network function, one that can be scaled up, down, deploy, and to retire-allowing orchestration and lifecycle management, fitting 3GPP 5G Core [16], and Common API Framework [17] designs. To achieve this, a wholly new blockchain design is required. This research presents this design, which we name *Conte*.

The following research is split into six parts. The first provides an overview of the modular structure of the 5G cellular core, and presents areas where blockchain can be matured in order to improve its general compatibility by moving to a format as temporal general storage, rather than more prescriptive currency and contract designs. The second section details the consensus model used in Conte (Federated Byzantine Agreement), its safety, liveliness, and intentional omission of fault tolerance controls. Following these are details of our proposed Conte blockchain protocol, its block structure, protocol messages, and algorithmic complexity. The fourth section explains how Conte handles congestion and flow control, while a fifth section returns us to our initial cellular core context, to detail how Conte can be deployed as stand-alone temporal storage, or bundled as storage underpinning existing virtual network functions in real-world environments. Finally a conclusion is provided as a closing to the research, declaring potential improvements identified and planned future research directions.

4.2 Blockchain Unbundling

Early blockchain research has focused largely on individual use cases and, as a by-product, makes a toy example of the wider cellular network dependencies. However, this framing does not fully acknowledge the hetero-

generality of wireless networks whose hardware is modified and upgraded over time; for example, the coordination of Mobile Network Operators (MNO) and subscribing Mobile Virtual Network Operators (MVNO), where blockchain can ensure the verifiability of data, but each carrier operates its own diverging, and possibly competing services. A given MVNO may even utilize infrastructures across multiple MNO's and, in this case, a level of compatibility, optionality, and generalizability of blockchain application would be desired.

When the 3GPP specification for 5G networks was released in 2018 [16], it explained its architecture as being comprised of many Network Service Functions (NSF) to support Network Function Virtualization (NFV) and Software Defined Networking (SDN) paradigms. It achieves this through modularity, separating hardware infrastructure into Control Plane (CP) and User Plane (UP) functions that are temporal, independently scalable, and loosely coupled to prevent structural dependencies when possible. Eighteen total service functions are identified within the "Architecture Reference Model" section of the 3GPP specification, and they are listed below:

- *Authentication Server Function (AUSF)*
- *Access and Mobility Management Function (AMF)*
- *Data Network (DN)*
- *Unstructured Data Storage Function (UDSF)*
- *Network Exposure Function (NEF)*
- *Network Repository Function (NRF)*
- *Network Slice Selection Function (NSSF)*
- *Policy Control Function (PCF)*
- *Session Management Function (SMF)*
- *Unified Data Management (UDM)*

- *Unified Data Repository (UDR)*
- *User Plane Function (UPF)*
- *Application Function (AF)*
- *User Equipment (UE)*
- *(Radio) Access Network ((R)AN)*
- *5G-Equipment Identity Register (5G-EIR)*
- *Security Edge Protection Proxy (SEPP)*
- *Network Data Analytics Function (NWDAF)*

Today, there are two dominant paths of blockchain development. Either a bespoke chain can be created for the intended purpose, or a monolithic, single purpose chain may be deployed. Bitcoin contributed to the early work of Haber and Stornetta [18] in proving a system that could remain secure while being public [19]. As a digital currency, it was designed to be decentralized and permissionless; two traits not requisite in the original Haber and Stornetta digital notary use. To achieve this however, Bitcoin deploys resource intensive Proof-of-Work (POW) consensus that imposes throughput constraint and is difficult to deploy to resource constrained network environments, such as IoT. This conflict is manifested in examples, such as [20] and [21], which require the deployment of proxy devices that are able to run resource intensive POW calculations, or store the entirety of a public ledgers history, which is then referenced by appendage devices through an informal star topology. Taken in isolation, this full and light node separation can be understood as a symptom of the research relying on the POW variant of the Ethereum blockchain—but, in a macro perspective, represent a risk in network environments where the design and traits of a given blockchain evolve independently and potentially in conflict with wireless network design. An existing example evolution includes the introduction of Ethereum state

channels, which impacts the auditability of data that would otherwise be stored in the main ledger [22].

Adopting a general use blockchain, such as Ethereum presents risk in that it lacks modularity of consensus, currency, contract, or other behaviors of operation. In Ethereum's case, this means adopting behaviors to support a POW permissionless security model backed by currency functions which may be superfluous or even detrimental to the intended cellular network use. For example, if a universal record such as currency balance is not being mandated, it is then possible to form and retire chains for individual network operations as the shared data reaches the end of its useful life. Modularity of this type is not possible for the most popular blockchain systems, such as Ethereum.

4.2.1 Unbundling of Currency

The ability to use currency payment and reward in POW blockchains to incentivize behavior desired in network environments, such as resource sharing, was an early focus in cellular use. Taking a specific example, Maksymyuk et al. propose a spectrum sharing solution that identifies spectrum owners, infrastructure owners, ISP, and end users as independent participants in a dynamic market driven by the Nash equilibrium in game theory [23]. In the Maksymyuk model, end users make digital currency payments to infrastructure (base station) operators, who, in turn, pay for dynamic spectrum access to incumbents and regulators, while also paying for ISP backhaul services to carry traffic to the wider internet [23]. For specific controls relating to spectrum sharing operations, the research proposes a game theoretical scenario, where each operator has equal currency to use for spectrum access and it is incentivized not to overuse resources, as they would lose access once their balance reaches zero. The balance is only regained in this case, by supplying access to competing providers in a model that is designed for reaching Nash equilibrium of serving and receiving access. Although Nash equilibrium format is novel, it is, however, an example of a currency model that assumes a balance of infrastructure and customer that is difficult to guarantee in

production networks. Another concern of the model is that it does not account for operations in congestion and peak demand scenarios where all of the participants have competing incentives to consume access, risk service disruption, or total service outage.

To best fit existing mechanics of network environment, blockchain must be evolved to function under competing operational incentives, such as resource management, network investment levels, and demand growth, which may be uneven among equivalent providers. One way of servicing this structure is through the sharing of context and data, such as tower location and channel occupation—which are required for functional operation of everyone—decoupling any awareness of economic model from the chain. Conte fully removes currency, for generalized network use.

4.2.2 Unbundling of Contract

Blockchain is a rigidly time ordered structure by nature of its linear forward hashing. The general speed of code execution tied to the contribution of blocks will be inversely proportional and dependent on block consensus time. This means that a blockchain deployment seeing an increase in block contributions will also see a corresponding decrease in how quickly those blocks and corresponding information can be processed; all else remaining unchanged. In systems, such as Ethereum, where end-to-end operations occur within its own virtual machine-behavior controls again fall back to currency incentive, where impacts of block additions can be partially controlled by charging a digital currency fee proportional with delay being imputed on the system [24].

Modern networks are built using an unbounded variety of hardware configurations and radio resource management algorithms. Within networks of an identical generation, configuration for antenna geometry, sectoring, deployment density, backhaul capacity, and algorithms deployed to maintain quality and coverage can differ and conflict among networks and be further modified in time. Contractual code execution assumes a level of heterogeneity and coordination that does not fit with existing or expected future network design. Contracts cannot easily account

for all possible transitions in heterogeneous networks or multiple operators. The latency of contract checks and block propagation cannot be completed at sub-millisecond scale, as required for time varied channel conditions/controls. It is possible to modify the algorithms for achieving consensus to get around these limitations. Blockchain systems can be manipulated to process higher transaction volumes, or also control resource usage by allowing for nodes to keep full (full-node) or partial (light-node) states [25]. Deploying such modification however, shows consensus latency in blockchain under best case scenarios, are reduced to one second [26]. This present scalability limitation reveals blockchain structure as largely incompatible with operations at μ -second scale at the network edge, such as real-time radio resource control and dynamic accesses not set on a semi-permanent basis. This again reveals a general benefit of limiting blockchain deployment to the decentralization of data. In part to mitigate known limitations of contract execution and corresponding cyber-physical control bound by block delay, Conte fully removes the function of contracts for generalized network use. In doing so, network operators can still share data in an immutable, decentralized record, while also independently updating and swapping out systems of cyber-physical control over time. The integration of Conte within a 5G system assumes a Cloud-Native 5G Core, whose composing functions/services (e.g., AUSF, NEF, etc.) are exposed via well-defined APIs (e.g., CAPIF, ETSI NFV IFA 013, etc.) under the Mobile Network Operator’s (MNO) policies. Conte operates as the Unstructured Data Service Function, making it not specific to any single network function, but rather it is agnostic storage that can be accessed and used by any network function, as defined by the previously mentioned 3GPP 5G Architecture Reference Model. This allows a network to decentralize storage and accounting for all or just a smaller subset of network functions. Figure 4.1 shows a logical example, where only a single network function (AUSF) uses the Conte blockchain for its storage, while all other functions retain an unmodified design.

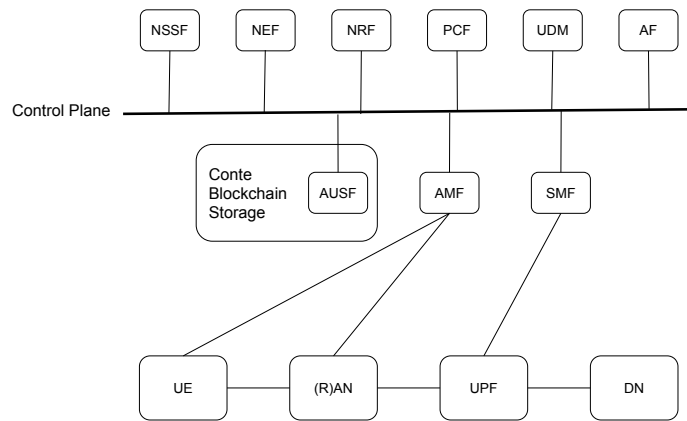


Figure 4.1: A logical representation of 5G network functions, with a single function (AUSF) being decentralized by using Conte blockchain storage.

4.3 Federated Byzantine Agreement

A consensus model must be deployed that functions in this mode of operation to make a blockchain that is temporal. The following section details how the Conte blockchain maintains safety, while removing currency and contract mechanics from its design.

When compared to permissionless consensus models, such as Bitcoins Proof-of-Work (POW), classic Byzantine Fault Tolerant (BFT) algorithms have been favored for permissioned or consortia deployments due to its lower resource consumption achieved in exchange for a reduced and adjustable fault tolerance, commonly set as low as 20% for environments consisting of known peers [13]. However, BFT models, in turn, carry risk in lacking the standardization and interworking required of heterogeneous network deployment. A more recent approach extended for this research is the FBA model, which balances the permissionless decentralization of POW, with the lowered resource use of BFT consensus.

Conte handles consensus while using a modified implementation of

the Federated Byzantine Agreements (FBA) structure first introduced with the Stellar Consensus Protocol [14]. FBA functions by dividing networks into smaller clusters of interlinked consensus, aptly named “slices”. Partitioning the network into slices in this manner allows for deploying BFT agreements at internet scale, while making the trade-off of slower consensus speed. Functionally, these slices behave in a manner similar to network subnetting, eliminating traffic storms formed during broadcast consensus in existing Byzantine Fault Tolerant (BFT) algorithms and, at a macro level, allows for consensus to mirror the unbounded peer-wise model of backbone internet, with nodes spanning consensus slices, functioning as gateway.

Modern blockchain consensus algorithms are characterized on the three matrices of safety, liveness, and fault-tolerance. The FLP Impossibility Theorem states that any asynchronous consensus mechanism can only guarantee and choose two among the three [27]. Extending from this, FBA diverges from Classic BFT consensus in being asynchronous and, consequently, foregoes guarantees of fault tolerance. An example BFT consensus algorithm guaranteeing 25% fault tolerance uses an $n \geq 3f + 1$ security model, with total nodes N , faulty nodes $f \in N$, and $n = \{ x \in N \mid x \notin f \}$. For such a guarantee to function, classic BFT algorithms must, at minimum, operate in partial-synchrony, often using a global stabilization time (GST) to end voting, and with a known registry of nodes N in order to reliably identify f nodes at a given time T [28, 29].

Through choosing safety and liveness over fault tolerance in its core algorithm, Conte does not need to restrict participation or incentivize behavior among unmanaged nodes in order to reach agreement. In this manner, it functions in a manner mirroring internet backbone peering; where connectivity is piecemeal, extending unbounded in all directions, and changing in time-based on trust relationships not managed by the blockchain itself. In this structure, Conte offers an ideal starting point, allowing for blockchain connectivity to be locally managed under existing infrastructure paradigms (as temporal virtualized network functions), while safely settling and distributing finalized blocks among unmanaged and heterogeneous networks. For this research, we define safety and live-

liness as:

- Safety: nodes operating a Conte blockchain enjoy safety if node outputs are consistent, with no two nodes committing a conflicting values for the same block.
- Liveness: nodes operating a Conte blockchain enjoy liveness if they are able to reach consensus on new blocks without the participation of failed or malicious nodes.

4.3.1 Replacing Fault Tolerance with Quorum

Consensus in FBA’s operates on a structure known as a quorum slice. A quorum slice is a grouping of network peers whose pairwise peering is symmetric. Transposed to wireless network context, a quorum slice could consist of all tier-1 mobile network operators (MNO) of a region, who all peer with each other. Within a quorum slice, block additions may be considered final, after a threshold amount of peers confirm the block. However, this functionality on its own does not consist a federation. To form a federation, quorum slices are intended to intersect, such that nodes operating in multiple quorum slices function as relay, extending consensus to the wider network of intersecting slices. In the 5G core network context, this would occur when some portion of regional MNO’s within a quorum slice, also peer with MNO’s or another region, or internationally. Federated Byzantine Agreement Systems (FBAS) and Quorum are formally defined as [14]:

- Federated Byzantine Agreement Systems: a federated Byzantine agreement system, or FBAS, is a pair $\langle V, Q \rangle$ comprising a set of nodes V and a quorum function $Q : V \Rightarrow 2^{2^V} \setminus \{\emptyset\}$ specifying one or more quorum slices for each node, where a node belongs to all of its own quorum slices-i.e., $\forall v \in V, \forall q \in Q(v), v \in q$. (Note that 2^x denotes a powerset of X .)

- **Quorum:** a set of nodes $U \subseteq V$ in FBAS $\langle V, Q \rangle$ is a quorum iff $U \neq \emptyset$ and U contains a slice for each member-i.e., $\forall v \in U, \exists q \in Q(v)$, such that $q \subseteq U$.

A quorum is a set of nodes that sets the threshold or reaching agreement, and it may be larger than a single quorum slice. Consider figure 4.2, which shows two clusters of nodes, each participating in a single quorum slice with symmetric pair-wise connection. Assuming that 100% confirmation is required, node v_5 can reach agreement with confirmations from peers $\{v_1, v_2, v_3, v_4, v_6\}$; however, since node v_6 has additional peers $\{v_7, v_8, v_9, v_{10}\}$, they must also agree to the update before it is accepted; therefore, v_4 must agree to an update from v_8 , etc.

Figure 4.2 represents a worse case scenario of federated agreement. In this example, the pairwise relationship of v_5 and v_6 represent a single point of failure in reaching consensus. Systems, such as Ripple [30], compensate for this by enforcing, at all times, a minimum connectivity between federated nodes \geq its maximum fault tolerance (and in turn, making it Byzantine Fault Tolerant). However, doing this again imposes the centralizing requirement of recording and enforcing connectivity among known participants-precluding unmanaged permissionless operation. FBA, as deployed in Conte, instead makes an alternate scenario possible, in which consensus resilience increases as additional unmanaged pair-wise relationships are formed elsewhere in the network-in a manner mirroring that of global internet (figure 4.3).

4.4 The Conte Blockchain Protocol

Conte operates permissionless, without an explicit membership or validator set; each block, however, is signed using the public key of the submitting node and is by design, not anonymous. Each block update is assigned an incrementing index number, such that only one block can be valid at a given index position, with each node able to independently confirm block sequencing against its local set (its local blockchain). Block submissions

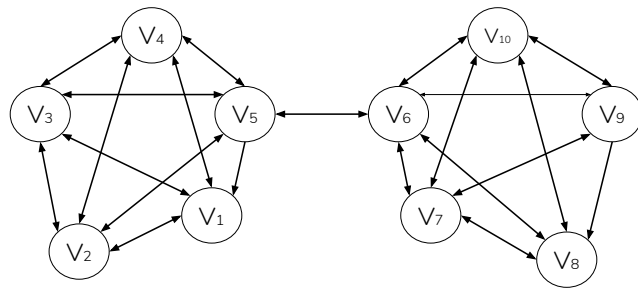


Figure 4.2: Two quorum slices, intersecting at nodes $\{v_5, v_6\}$.

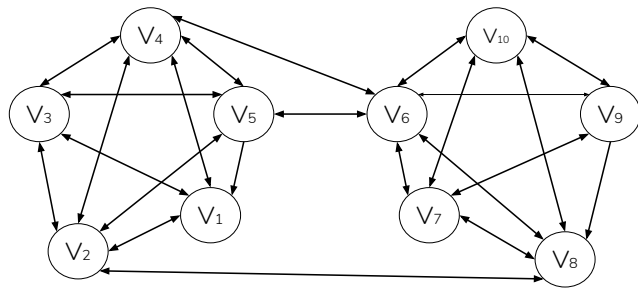


Figure 4.3: Two quorum slices intersecting at nodes $\{v_2, v_4, v_5, v_6, v_8\}$.

are then forward propagated until reaching a graph edge, where edge nodes begin a ripple effect through the back-propagation of an acknowledgment for a given block vote [30]. Blocks that are settled in consensus are then added to local blockchains using SHA-256 encryption. Because Conte is intended to operate with an unknown number of peers, there are no leader election processes, or transaction batching as done in Byzantine Fault Tolerant blockchain systems, such as Facebook’s Libra [29]. Rather, any participating node can submit a block at any time, relying on congestion control measures borrowed from medium access controls in IEEE 802.11 networks (carrier sensing multiple access with collision detection (CSMA/CD)). Exponential back-off timers [31] within Conte allow peers to send a negative acknowledgment, triggering a cool down period for a proposing node if receiving blocks out of order, or with conflicting index values to those received from disjoint peers; the details of this mechanism are provided later in the paper. Conte further combines these network behaviors with novel federated byzantine agreement consensus, which establishes finality without traditional fault-tolerance, to allow its temporal network function deployment, while also not sacrificing consensus safety.

4.4.1 Block Structure and Storage

Blocks within Conte are composed of three parts; the block header, a list of transactions, and the previous block hash. Rather than a bespoke programming language and contract syntax, Conte flattens and standardizes possible operations to aid in interworking between networks, in a similar manner to IP packet structure. Each transaction is atomic and contains all of the information required for processing operations of the specific network function for which it is deployed, while also adhering to a single global format containing the sections below.

- **Contract ID:** a globally unique integer value, serving as the identity of an Federated Byzantine Agreement (FBA).
- **Contract Name:** a non-unique string value, serving as a human readable name for a given FBA.

- **Message Signature:** the cryptographic signature, or public key of the network node proposing a transaction.
- **Function:** a rigidly defined struct value-defined as standard for each network function. An example struct being: [NF Name]; [Operation]. In the AUSF use case, this would designate: [AUSF]; [authorize], [AUSF]; [revoke], or others standard operations of the chains’ designated network function.
- **Message Body:** an array value containing the core transaction data. In the example AUSF use case, this is the 5G Globally Unique Temporary Identifier (the 5G subscriber ID).
- **Index Number:** an incrementing integer value, designating a records position in the hashed chain.

Conte is structured to allow a node to participate in multiple independent chains simultaneously. Rather than a monolith chain that grows in perpetuity, Conte intends new chains to be created, run in parallel, and retired after serving an intended purpose. This managed lifecycle can be months, years, or an indeterminate amount of time; partner networks may, for example, share subscriber data to grant access in cases of natural disaster. Because Conte requires full agreement to settle consensus, meaning that all peers of a given node must provide block confirmation before a block is considered to be final; there is no risk of fork and no increase of security through increasing the ledger length in perpetuity. This paradigm facilitates the negotiation of software upgrades among smaller subsets of peers for individual chains, and also with consideration to the expectation that network data is real-time data, whose value trends towards zero in time.

Because the Conte blockchain stores living network data, it is important to allow a mechanism to prune or optimize storage. This is done in two ways; during an initial sync or in ongoing pruning. Returning to our example scenario of authorization, let us assume a network requirement where devices must be reauthorized every 90 days through a transaction

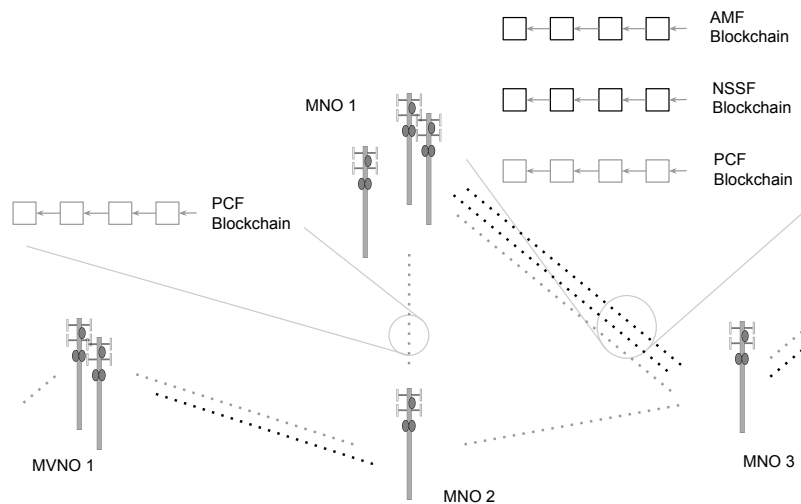


Figure 4.4: Example of multiple network function-specific blockchains running across operators.

renewing its permissions. Assuming that each network has an external record retention policy and mechanisms of network logging, this effectively places a 90-day expiry on the utility of transactions in the chain. In a scenario such as this, a node requesting to sync can do so by requesting all transactions from N date, rather than an entire chain growing in perpetuity. Because the chain length is not a mechanism of security, as in Ethereum, or assisting in reaching finality as in IOTA, the chain can be partially synced in this manner without risking safety of ongoing consensus, as defined by the intended use of the single chain, or microchain (figure 4.4).

4.4.2 Transaction and Protocol Messages

Joining consensus on a Conte blockchain occurs by configuring a peer and mutually validating identity through exchange of public keys. In ad-

dition to public key exchange, a peering request arrives with either a genesis block, containing a randomly generated contract ID, or a request to sync, containing the contract ID of an existing chain that is the target of synchronization. It is assumed that 5G core networks are connected pairwise, rather than fully peer-to-peer. Structuring consensus in this way allows it to function when networks are operating peer-to-peer, but also when sensitive infrastructure is siloed behind firewalls and strict route controls.

Nodes may also proxy or pass block proposals while using NEF operations, in compliance with 3GPP 5G design. Conte exposes secure RESTful APIs for protocol messaging between nodes, including GET and POST operations. Protocol messages include: peer, sync, propose, acknowledge, negative acknowledge, commit, and prune.

- Peer: initialize connection to new contract peer.
- Sync: after initial connection, or during conflicting commits, a node can request to sync transactions. This sync includes a check to confirm a known peer with the longest change, and a verification of new blocks by re-hashing them using the SHA-256 algorithm.
- Propose: issue a new transaction. A new block can be proposed by any member of the network. The block must be signed with a cryptographic key to validate identity. Each block is sent as unicast to all peers of a given node, which forwards the proposal, until reaching nodes at the graph edge. For bandwidth efficiency, a node may delay block proposal, until it has multiple transactions to submit-in which case, these may be bundled into a single block. A node is considered a graph edge after receiving the same proposed block from all its known peers.
- Acknowledge: provides confirmation of acceptance of new transaction blocks. Once a proposed block is received, its header, body, and signature data is validated and an acknowledgment is returned. A node must receive an acknowledgment for each forwarded block

proposal, before propagating back its own aggregate acknowledgment. Nodes receiving invalid blocks, competing blocks with the same index value, or out of sequence blocks send a negative acknowledgment, aborting consensus.

- **Negative Acknowledge:** deny confirmation of blocks in case of conflicting block data, such as index position, aggregate hash, or message signature.
- **Commit:** a final notification that a block is committed locally by a proposing node, signaling that remaining nodes handling consensus as clear to add the block into their respective local chains. Conte ensures that no two nodes store different blocks with the same index value, by aborting consensus when encountering conflicting data or error. In states where acknowledgment is received from all peers, the block is committed to the local chain and a final commit message is issued to peers (figure 4.5), who commit the block in their local chain and propagate the commit forward toward edge nodes.
- **Prune:** nodes that fail to reach consensus may initiate a request to prune from peer lists, any peer which has failed to respond to three consecutive proposals. Prune requests forward propagate in a manner that is similar to a propose message, with the full network reaching consensus to prune the peer. A negative acknowledgment may be sent if the target peer is responsive elsewhere in the network.

Because Conte requires full confirmation in order to reach finality in a manner that is similar to TCP error correction, a given message is repeated if an expected response is not received within a given timeout, until a pruning state is triggered. Algorithm 3 shows simplified pseudo-code of Conte message functions.

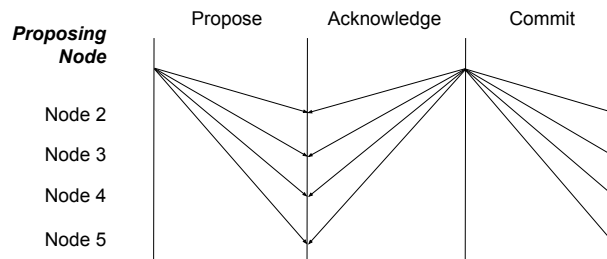


Figure 4.5: Conte Single Round Block Commit.

Algorithm 3: Conte messages for node $v \in q$

Function Message (*type, localIndex, key*) :

```

msg.index ← localIndex
           // peer, sync, propose, or prune
msg.type ← type
msg.peer ← peer
msg.signature ← key
    
```

return msg

Function Response (*type, msg.index, key*) :

```

msg ← Message(type, peer, key)
     // acknowledge or negative acknowledge
msg.response ← type
msg.peer ← peer
msg.signature ← key
    
```

return msg

Function Commit:

```

ackv ← msgv
ack.index ← msg.index
quorum ← quorumACK(ack.index, {msg.signature | v ∈ q})
    
```

return quorum

4.5 Handling Transmission Contention

As an asynchronous system without a static resource allocation, additional controls are needed in order to handle contention in transmissions. In addition to time-to-live limits on transactions, Conte handles conflict in the network using a binary exponential back-off mechanism, mirroring that of CSMA/CD in WiFi networks. The channel sensing in this case is the monitoring of the directly connected peered network interfaces for the transaction traffic of peer nodes. Under the CSMA/CD model [31], a transmitting node must wait some minimum sensing period in order to confirm the transmission medium is idle. In practice, if the transmission medium is not idle, then the node selects a random back-off duration, in seconds (contention window), and counts down. This back-off is chosen uniformly in the range $[0, 2^i W_0 - 1]$, where i is the number of times a node has attempted to issue the transaction (back-off stage), initialized at 0, and W_0 is the minimum sensing period [32]. If a node receives subsequent transactions during the sensing period, it pauses its countdown, and continues decrementing once the transmission medium is clear. After transmitting successfully, i is reset to 0. A maximum m number of re-transmissions attempts i is also set, to apply a bound for maintaining liveness. Again, matching the behavior of CSMA/CD, a node makes two attempts at the maximum back-off stage, before considering the block a failed transmission. This mechanism of congestion control is chosen, as it represents a worst case scenario in which only directly connected peers are known-with no visibility beyond, as opposed to Reno, Tahoe, and other congestion control algorithms available directly in TCP, which require maintaining a route table that eventually extends to includes all graph hosts. A summary pseudocode of Conte consensus, inclusive of back-off timing, is provided in Algorithm 4.

Algorithm 4: Conte *Consensus* for node $v \in q$

```

for  $msg.index \leftarrow 1,2,3,\dots$  do
    Propose State
    wait for minimum sensing period:  $W_i \leftarrow \{W_{iv} \mid 0\}$ 
    newBlock  $\leftarrow$  msg
    multicast newBlock

    Acknowledge State
    wait for newBlock from peer:  $v \in q$ 
    wait for minimum sensing period:  $W_i \leftarrow \{W_{iv} \mid 0\}$ 

    if  $newBlock.msg.index > localIndex$  then
        | send response:  $msg \leftarrow \{msg.response \mid ack\}$ 
    else
        | send response:  $msg \leftarrow \{msg.response \mid negative\ ack\}$ 

    Commit State
    As proposer:
    wait for peer response:  $quorum \leftarrow \{msg.response \mid$ 
         $ack(\forall v \in q)\}$ 

    for  $msg.response = negative\ acknowledgement$  do
        | send message:  $msg.type \leftarrow sync$ 
    if  $no\ msg.response$  then
        | unicast newBlock:  $msg.peer \leftarrow \forall v \in q(\notin quorum)$ 
    else
        | send commit:  $quorum \leftarrow quorumACK(ack.index, \{$ 
             $msg.signature \mid \forall v \in q\})$ 

    As peer:
    wait for quorum from proposer( $msg.index$ )
    
```

The CSMA/CD model provides four contention probabilities that can

be represented as a two-dimensional Markov chain with one step transition probabilities, as explained in [32] with possible states represented where t in our case is a block retransmission attempt, and s is the sensing period. These Markov transition probabilities are represented as (1), where P_w is the contention probability of the transmission medium, W_0 is the minimum sensing period length, $W_i = 2^i W_0$ is the sensing period length at a given block attempt i , and $i = m$ at the maximum retransmission attempt:

$$\left\{ \begin{array}{l} P\{t, s|t, s+1\} = 1, \quad s \in (0, W_i - 2) \quad t \in (0, m+1) \\ P\{0, s|t, 0\} = \frac{1-P_w}{W_0}, \quad s \in (0, W_0 - 1) \quad t \in (0, m+1) \\ P\{t, s|t-1, 0\} = \frac{P_w}{W_j}, \quad s \in (0, W_i - 1) \quad t \in (1, m+1) \\ P\{0, s|m+1, 0\} = \frac{P_w}{W_0}, \quad s \in (0, W_m - 1) \end{array} \right. \quad (4.1)$$

In descending order, these probabilities (1) are the transition probability of going from idle to successful transmission; the second representing the transition probability after successful transmission of having a subsequent successful transmission; the third represents the transition probability after an unsuccessful transmissions, in which the contention window W_0 is doubled, as defined by $[0, 2^i W_0 - 1]$; the last equation represents the transition probability after a fully failed transmission in which the contention window resets to 0. Letting an expired timer (or closed contention window) be represented as $b_{t,0}$, accounting for the distribution of Markov transition probabilities, the probability of a node sending a block in any 1 second time period τ_w is represented as (2):

$$\tau_w = \sum_{t=0}^{m+1} b_{t,0} = \frac{2}{W_0 \left(\frac{(1-(2P_w)^{m+1})(1-P_w)+2^m(P_w^{m+1}-P_w^{m+2})(1-2P_w)}{(1-2P_w)(1-P_w^{m+2})} \right) + 1} \quad (4.2)$$

A given node can only listen to the transmission medium of its connecting peers within a single quorum slice and, consequently, nodes on disjoint slices are occluded. To compensate for this, it is assumed that the binary exponential back-off is triggered either by listening directly on the transmission medium, or by a known peer sending a negative acknowledgment on a transaction, as done in cases when it has already received a superseding transaction time stamp or index position from elsewhere in the network.

4.6 Performance and Scalability

Because Conte does not deploy topology constraint, it is valid to represent its network scalability as a model of congestion control, where the performance bounds of the total system are held by link propagation and block contribution rate. Two simulations were implemented in Python in order to model the scalability of Conte CSMA/CD congestion control. In the first simulation, peer nodes were placed equidistant at 1,500 km apart, roughly the distance between the cities of Barcelona and Berlin. For the second simulation, peer nodes are set an order of magnitude further at 15,000 km, representing the equivalent distance between Los Angeles and Singapore. These two distances allow for evaluating Conte under both regional and global network delay.

All other parameters were set identical, with link speed of all nodes at 1 Gbps and block size at 1,500 bits. Because of the randomness introduced through retransmissions using a binary exponential back-off, each simulation was run ten times, with the results taken as the average. The simulations were run in two sets, one with node sizes ranging between two and 10 peers, and a second with node sizes that range between 10 and 50 peers. It is important to note that node sizes do not represent the absolute number of possible network participants, rather the maximum number of peer hops between the network graphs furthest edges, to present a worst case. As a system designed for policy orchestration at the

cellular core, the first simulation set with a node maximum value of 10 is representative of cloud native deployment, where regional data center and points-of-presence (POP) locations potentially house carrier cores. The second set with node sizes reaching 50 represents an outlier scenario of possible network loops or misconfiguration. Conte simulation code is available online and it has been open-sourced [33].

The first simulations that are depicted in figures 4.6 and 4.7 shows total block throughput and network efficiency for three rates of block contribution: one block per hour, one block per minute, and one block per second. Simulating block contribution at orders of magnitude is done to reflect a wide range of update frequencies possible across 5G core network functions. At 1,500 km, block throughput scales up to handle network updates at rates as fast as 1 block per second without significant degradation. Network efficiency, measured as the percent of packets transmitted successfully as compared to total packets, reduces as low as 69% at this peak load. At 1,500 km, both block throughput and network efficiency scale linearly at rates below one block per second.

At 15,000 km, figures 4.8 and 4.9 shows the performance roll off as a result of the additional network delay. In this simulation, as delay increases an order of magnitude, block contribution capacity drops correspondingly, with the network only able to scale to 1 block per minute without significant degradation. Network efficiency above this rate falls as low as 50%, with the additional overhead of retransmissions causing sustained reductions in block throughput beyond four graph hops at the one block per second rate. The one block per second contributed rate also shows how the system degrades under abnormally large network delays.

Increasing node sizes to 50 at 1,500 km, figures 4.10 and 4.11 show marginal impact at block rates of one per hour, while network efficiency begins to fall sooner, seeing reductions at the 1 block per minute transmission rate that was previously little impacted at smaller node sizes. It is important to note that overall throughput does continue to improve, and remains above the peak of the initial simulation set which capped node sizes at 10. With one block per second rates at 1,500 km, we see the system become overwhelmed with block throughput dropping sharply,

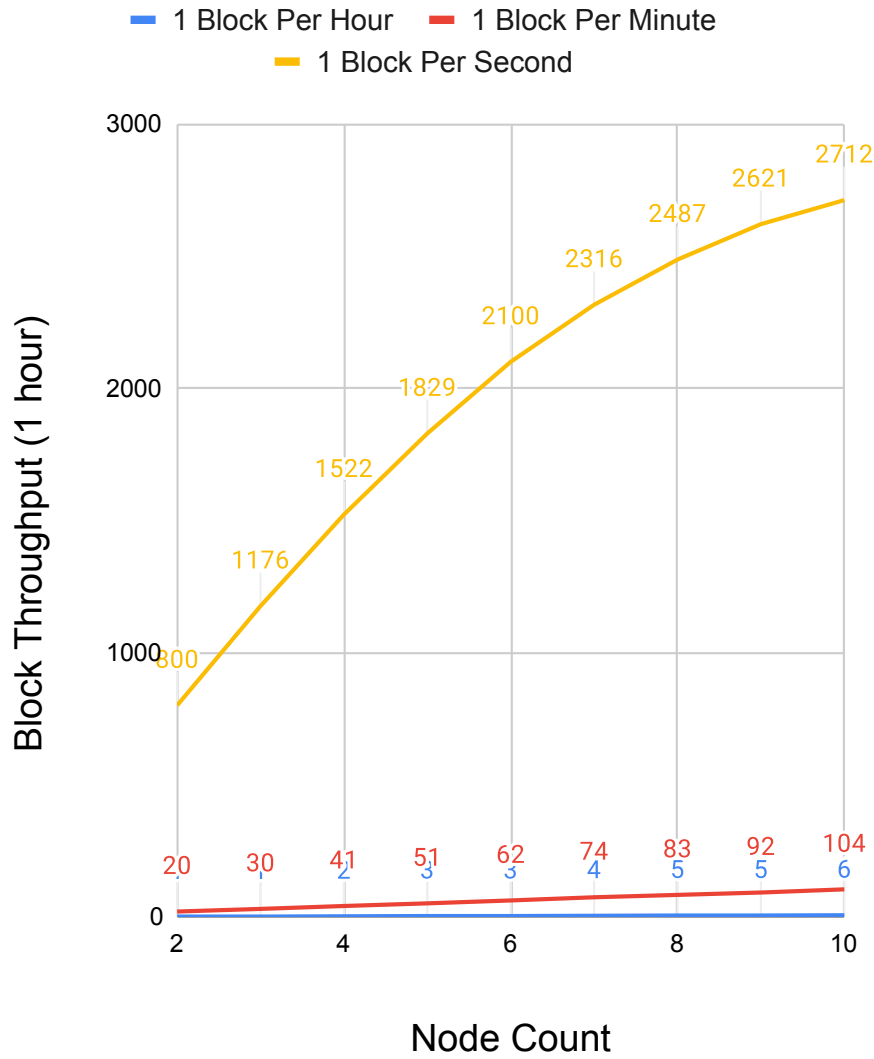


Figure 4.6: Block throughput performance of Conte at 1,500 km node distances and maximum hops to graph edge of 10.

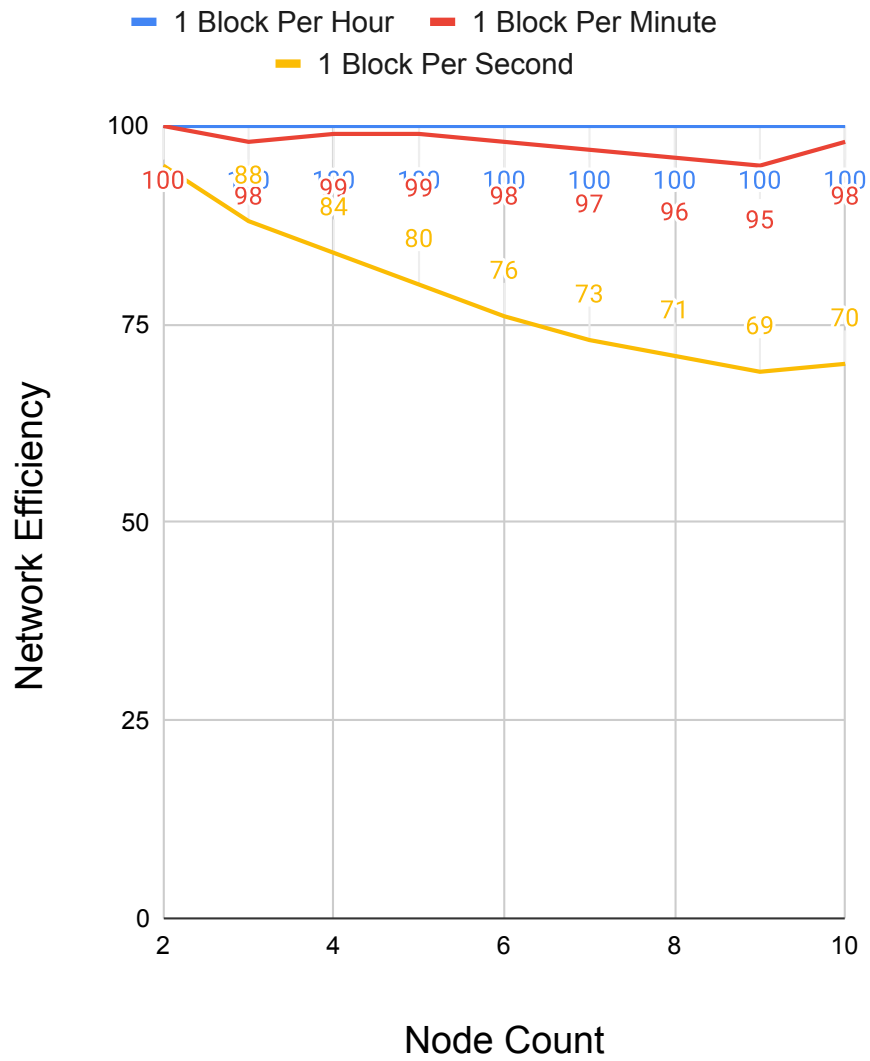


Figure 4.7: Network efficiency of Conte at 1,500 km node distances and maximum hops to graph edge of 10.

having a throughput rate at 50 nodes that is below that of a system having only three in the first simulation.

Simulation results at 15,000 km figures 4.12 and 4.13 exhibit similar behavior and continue a downward trend already present at smaller node sizes. An interesting behavior we can see in aggregate is that network efficiency measures do not drop to levels suggested by the raw block throughput numbers. This can be explained by the CSMA/CD algorithm implementation being assigned a maximum retransmission attempt value of 10. Network efficiency as reflected here, does not consider a packet dropped, until it has already attempted transmission 10 times. Adjusting this maximum retransmission attempts also has potential to impact performance, but this is outside the scope of this writing.

4.7 Deploying Conte as a Network Function

Conte is intended to be packaged as standalone temporal storage, or inside of other Virtual Network Functions (VNF) within an operators' Network Functions Virtualization Infrastructure (NFVI). Delivering a Conte node to the 5G core network is relatively straightforward thanks to virtualization technology. 5G adopts virtualization approaches commonplace in cloud data centers to realize virtual network functions (VNF), as opposed to relying on traditional network functions with a tight coupling between software and hardware, as mentioned previously. VNFs, or more generally, a Virtual Function (VF) can be thought of as a block of functionality running within a virtualization container (e.g., Virtual Machine, containers), which can then be connected together via Virtual Links (VL) and Software Defined Networks (SDN) to provide a service (e.g., 5G Core). In 5G, the way VF is described, deployed, managed, and destroyed has been defined by the ETSI NFV group [34]. Furthermore, resource and service isolation in multi-service multi-tenant environments is achieved via the concept of 3GPP Network Slices, which effectively treats a collection of VFs as a single administrative entity, allowing for administrators to scale VFs individually, destroy or create multi-VF services [35].

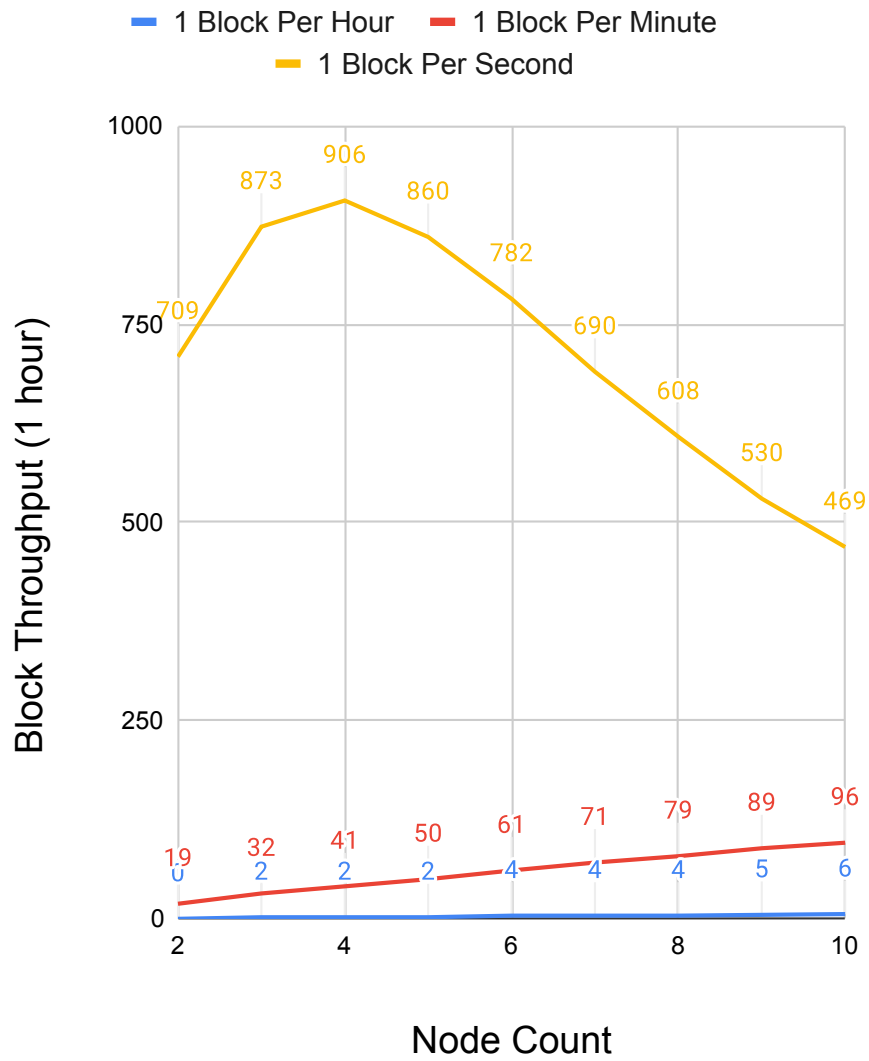


Figure 4.8: Block throughput performance of Conte at 15,000 km node distances and maximum hops to graph edge of 10.

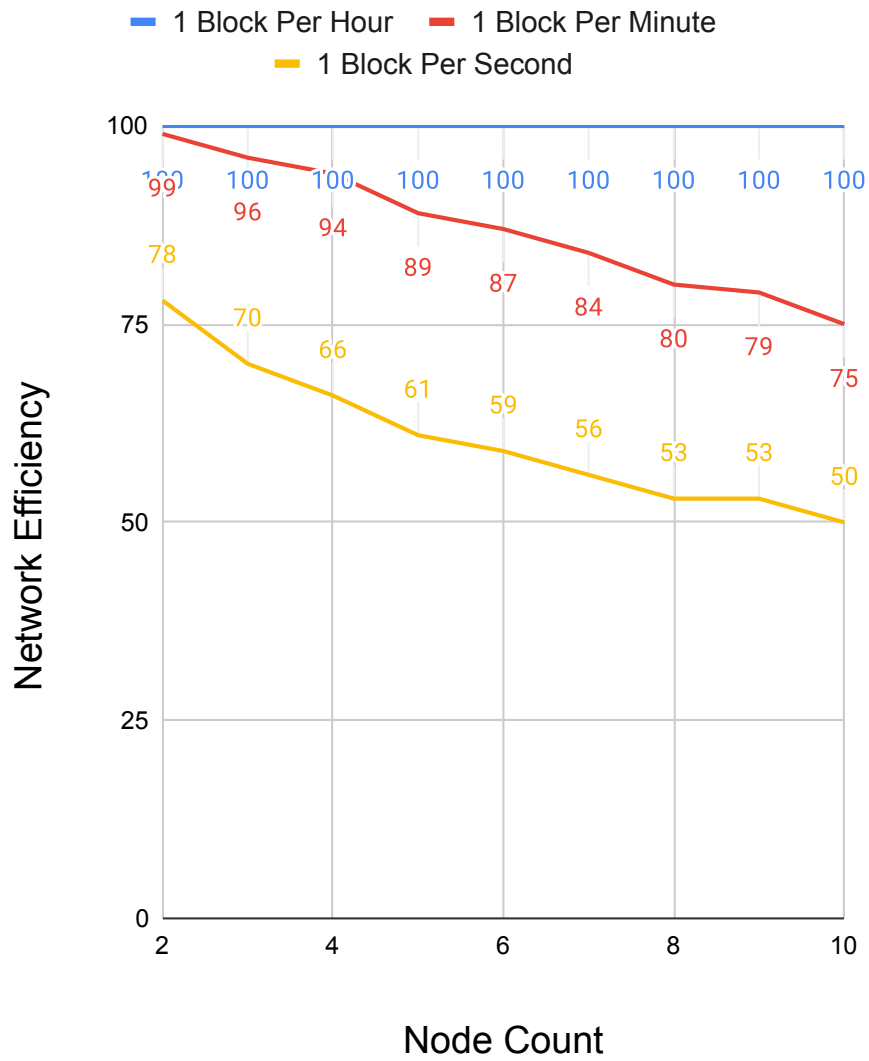


Figure 4.9: Network efficiency of Conte at 15,000 km node distances and maximum hops to graph edge of 10.

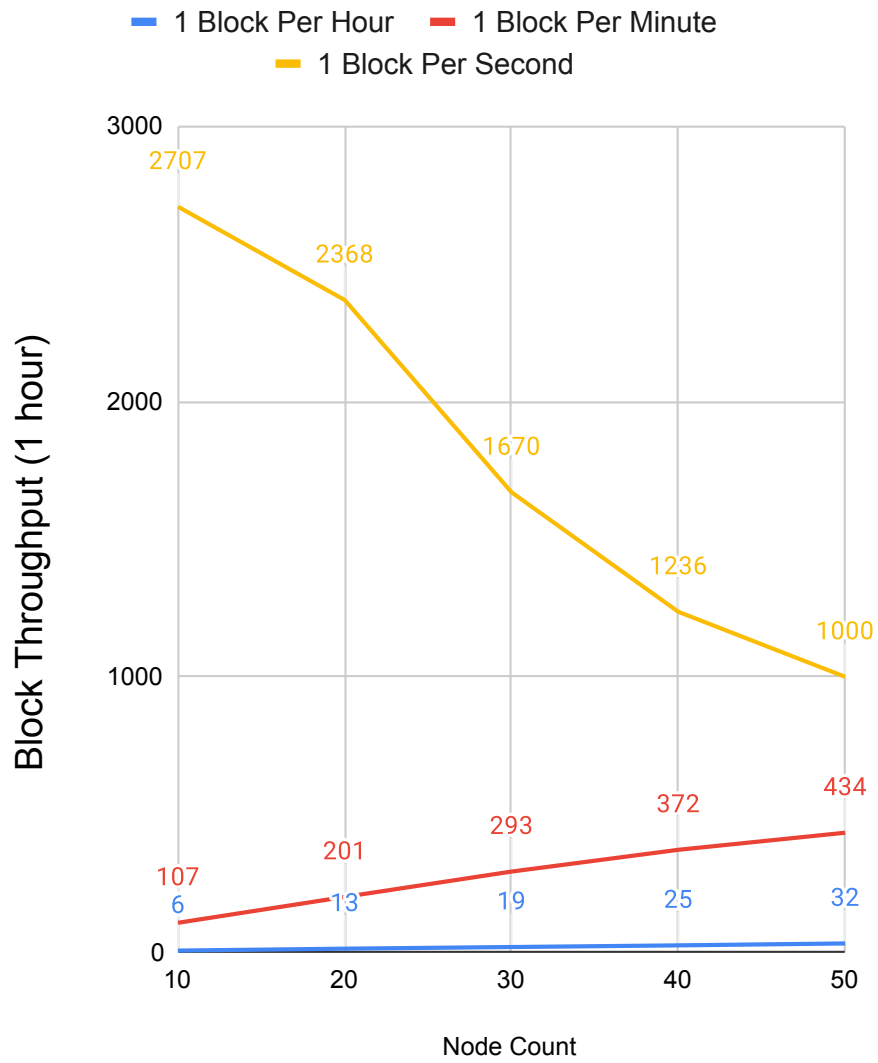


Figure 4.10: Block throughput of Conte at 1,500 km node distances and maximum hops to graph edge of 50.

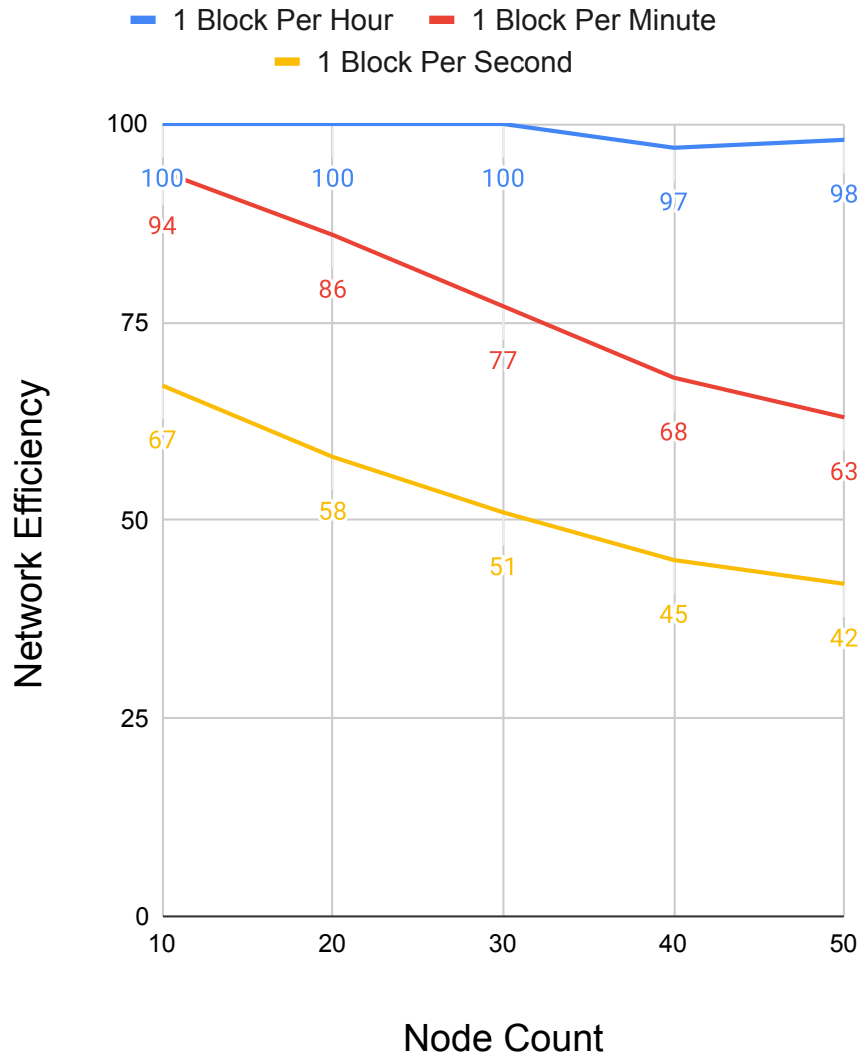


Figure 4.11: Network efficiency of Conte at 1,500 km node distances and maximum hops to graph edge of 50.

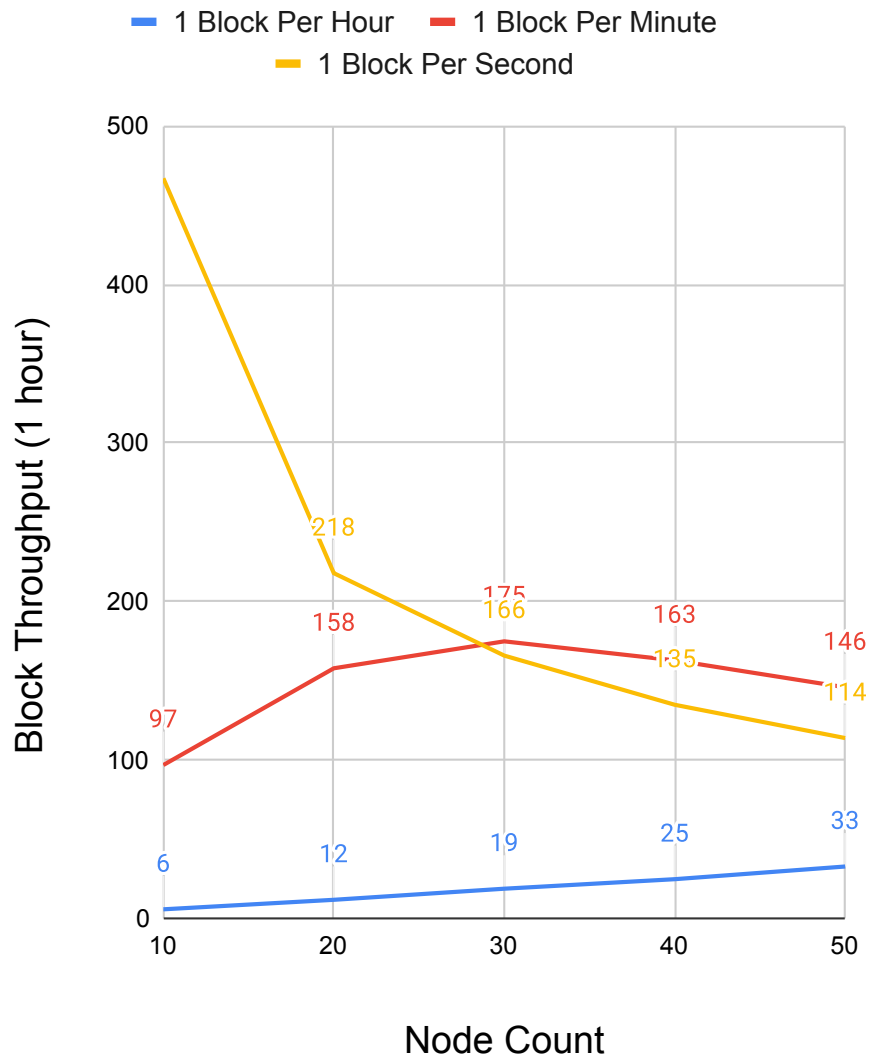


Figure 4.12: Block throughput of Conte at 15,000 km node distances and maximum hops to graph edge of 50.

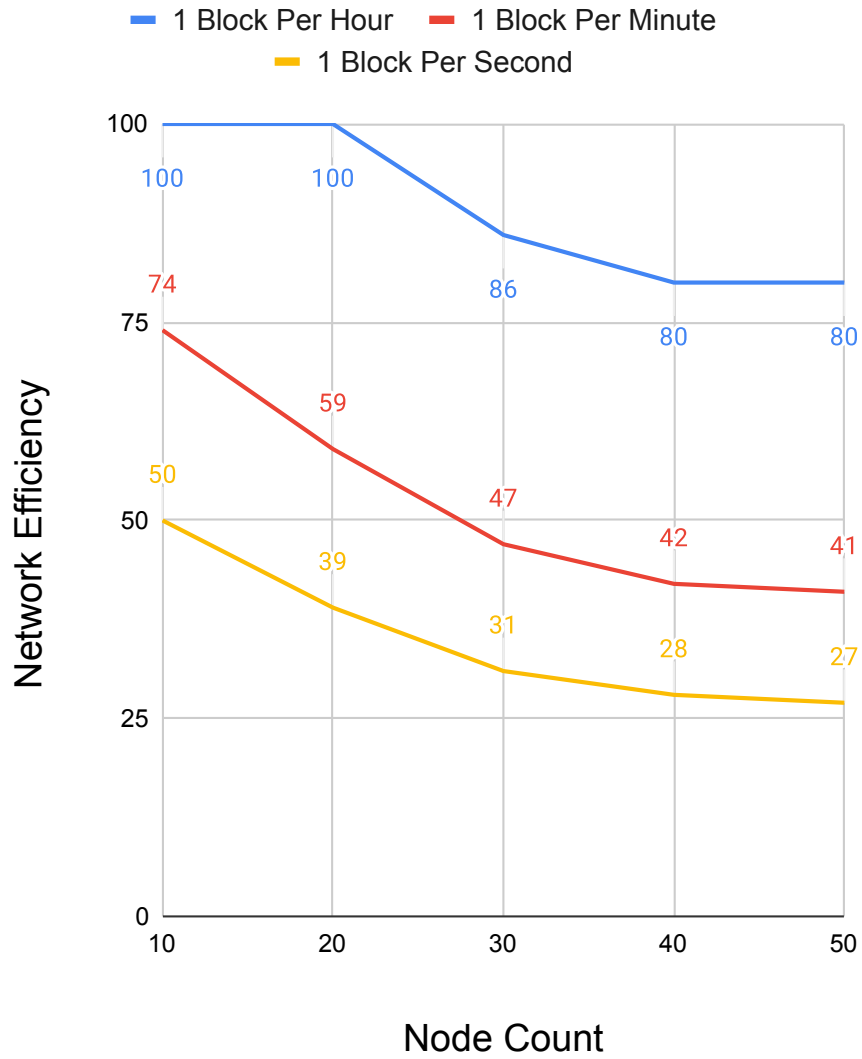


Figure 4.13: Network efficiency of Conte at 15,000 km node distances and maximum hops to graph edge of 50.

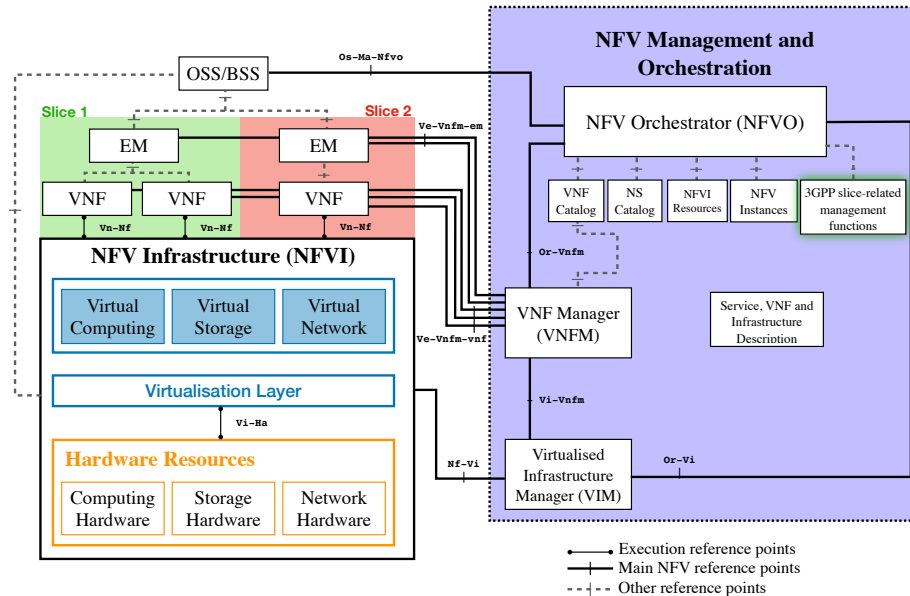


Figure 4.14: ETSI NFV MANO Architecture: highlighting slices’ reference points and manager in an integrated NFV MANO model [36].

Conte can be deployed as a VNF in an operators’ Network Functions Virtualization Infrastructure (NFVI). An example architecture of such deployment is provided in figure 4.14. In figure 4.14, the standard NFV Management and Orchestration (MANO) architecture is displayed, including reference points that enable communication among its components [36]. Moreover, two example slices (labeled Slice 1, and Slice 2) are displayed to describe how VNF’s share an underlying NFVI, which also allows communication among slices via Virtual Networks.

From the architecture proposed in figure 4.14, Conte orchestration on operator’s NFVIs can be realised as a separate slice (e.g., to isolate life cycle management operations), or as an additional VNF within 5G Core Network slice (or equivalent).

4.7.1 Evolving Alongside a Cloud Native Core

In order to achieve the advertised dynamicity and reconfigurability of the 5G core (e.g., placing UPF at the network edge), its implementation is expected to evolve towards stateless micro services [37]. Such micro services can be considered equivalent to VF, albeit often referred to as Container Network Functions (CNF), because they are implemented within lightweight virtualization containers (e.g., Docker containers). Such move towards micro services would allow a new set of functionalities (e.g., rolling updates, roll-back), and capabilities (e.g., placement of functions at resource-constrained devices at the edge, admit automation), while increasing performance when compared to VNF due to container’s reduced virtualization overhead.

Conte may be deployed as cloud-native application (i.e., a collection of micro services inside Docker containers) on top of a Platform as a Service (PaaS) provided by the operator, e.g., following ETSI NFV IFA 029 recommendations [38]. Such a PaaS may hold a Container Infrastructure Service (CIS) instance configured with a NFV MANO-compatible Container Orchestration Engine (COE, e.g., Kubernetes, OpenShift). Such a CIS will then support a cloud-native Conte, as well as expose network resources to reach the operator’s 5G core.

4.7.2 Carrier Security Model

Conte is permissionless, but not trustless. A limitation of the proposed Conte architecture is that it does not enforce any specific security model for the chain itself; an approach differing from blockchains designed to handle byzantine faults (BFT/PBFT) or incent network behavior through currency reward (POW). This model allows for decoupling currency and code execution from the underlying immutable storage and decentralized consensus of the blockchain, at the expense of security in isolation. This modified format is what allows Conte to achieve a 3GPP 5G Architecture compliant design.

By not directly enforcing security within the chain, Conte inherits SDN rules, and other security measures that are specified in 3GPP’s Com-

mon API Framework (CAPIF) [17] to guarantee secure and interoperable access to 5G Core functions (e.g., NEF)-both internally and across carriers. Beyond 3GPP-defined CAPIF controls, it is still possible for a peer carrier to broadcast malicious or misconfigured updates, making Conte vulnerable to update poisoning in a manner similar to BGP route poisoning. For this reason, it is assumed that a carrier operates Conte blockchains only with trusted peers. As peering expands, Conte remains permissionless in membership, but it does not support a trustless model.

4.8 Discussion

Recently, blockchain and other distributed ledger systems have received increased attention as a means of augmenting cellular networks. Using existing systems, such as Ethereum and Bitcoin, however, requires accepting both a monolithic, never-ending ledger structure, as well as currency and contract models that are not a native fit in existing cellular design. This paper introduces and details a new blockchain protocol, named Conte, designed with a temporal structure, more suitable for expiring data and as storage backing native network function with a known lifecycle terminus, fitting within 3GPP and ETSI defined 5G dynamic function design. The Conte design that is presented in this research is permissionless, decentralized, internet scalable, and structured to handle contention, remaining immutable during its deployment lifecycle. To the authors knowledge, Conte is the first blockchain system to be both permissionless and allow lifecycle control. The simulation results show the system scales in regional deployment with block contributions as frequent as one block per second, while global deployment supports block contribution at 1 per minute. As embedded carrier infrastructure, the Conte design as proposed does not support trustless operation. Further investigation in support of a trustless model has been identified for future research.

Bibliography

- [1] Ajtai, M. Generating hard instances of lattice problems (extended abstract). In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC '96), New York, NY, USA, 22–24 May 1996; pp. 99–108, doi:10.1145/237814.237838.
- [2] Popov, S. The Tangle v1.4.3. 2018. Available online: <https://www.iota.org/research/academic-papers> (accessed on 2 October 2019).
- [3] Chalaemwongwan, N.; Kurutach, W. State of the art and challenges facing consensus protocols on blockchain. In Proceedings of the International Conference on Information Networking, Chiang Mai, Thailand, 10–12 January 2018, 957–962, doi:10.1109/ICOIN.2018.8343266.
- [4] Lin, J.; Shen, Z.; Miao, C.; Liu, S. Using blockchain to build trusted LoRaWAN sharing server. *Int. J. Crowd Sci.* 2017, 1, 270–280, doi:10.1108/ijcs-08-2017-0010
- [5] Ling, X.; Wang, J.; Bouchoucha, T.; Levy, B.C.; Ding, Z. Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm. *IEEE Access* 2019, 7, 9714–9723, doi:10.1109/ACCESS.2018.2890557
- [6] Mafakheri, B.; Subramanya, T.; Goratti, L.; Riggio, R. Blockchain-based Infrastructure Sharing in 5G Small Cell Networks. In Pro-

ceedings of the 14th International Conference on Network and Service Management, 2018; pp. 313–317.

- [7] Weiss, M.B.H.; Werbach, K.; Sicker, D.C.; Bastidas, C.E.C. On the application of blockchains to spectrum management. *IEEE Trans. Cognit. Commun. Netw.* 2019, 5, 193–205, doi:10.1109/TCCN.2019.2914052
- [8] Ernst, J.; Wang, Z.; Abraham, S.; Lyotier, J.; Jensen, C.; Quinn, M.; Harvey, D. A Decentralized Mobile Mesh Networking Platform Powered by Blockchain Technology and Tokenization. 2017. Available online: <https://www.rightmesh.io/whitepaper> (accessed on 10 June 2019).
- [9] Tremback, J.; Kilpatrick, J.; Simpier, D.; Wang, B. Althea Whitepaper. 2020. Available online: <https://althea.net/whitepaper> (accessed on 12 April 2020).
- [10] Yu, G.; Wang, X.; Yu, K.; Ni, W.; Zhang, J.A.; Liu, R.P. Survey: Sharding in Blockchains. *IEEE Access* 2020, 8, 14155–14181, doi: 10.1109/ACCESS.2020.2965147.
- [11] Dziembowski, S.; Faust, S.; Hostakova, K. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Rome, Italy, 5–9 November 2018; pp. 949–966, doi:10.1145/3243734.3243856.
- [12] Buterin, V.; Griffith, V. Casper the Friendly Finality Gadget. *arXiv* 2017, arXiv:1710.09437. Available online: <http://arxiv.org/abs/1710.09437> (accessed on 18 June 2020).
- [13] Buchman, E. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. 2016. Available online: <https://allquantor.at/blockchainbib/pdf/buchman2016tendermint.pdf> (accessed on 14 April 2020).

- [14] Mazieres, D. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Dev. Found.* 2015, 32, 1-45, doi:10.1021/ja982417z.
- [15] The Linux Foundation. Hyperledger Sawtooth. 2020. Available online: <https://www.hyperledger.org/projects/sawtooth> (accessed on 25 August 2019).
- [16] ETSI. 5G System Architecture for the 5G System (3GPP TS 23.501 version 15.3.0 Release 15). 2018. Available online: <https://bit.ly/3vKrrC3> (accessed on 18 April 2020).
- [17] 3GPP. Common API Framework (CAPIF). 2019. Available online: <https://www.3gpp.org/common-api-framework-capif> (accessed on 14 April 2020).
- [18] Stornetta, W.S.; Haber, S. How to Time-Stamp a Digital Document. *J. Cryptol.* 1991, 3, 99–111, doi:10.1002/pssb.201300062.
- [19] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System; 2016, doi:10.1007/s10838-008-9062-0.
- [20] Polyzos, G.C.; Fotiou, N. Blockchain-assisted information distribution for the internet of things. In *Proceedings of the IEEE International Conference on Information Reuse and Integration, San Diego, CA, USA, 4-6 August 2017*; pp. 75-78, doi:10.1109/IRI.2017.83
- [21] Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* 2018, 5, 1184–1195, doi:10.1109/JIOT.2018.2812239.
- [22] Weingärtner, P.T. Tokenization of Physical Assets and the Impact of IoT and AI. Ph.D. Thesis, Lucerne University of Applied Sciences, Luzern, Switzerland, 2019; pp. 1-15.

- [23] Maksymyuk, T.; Gazda, J.; Han, L.; Jo, M. Blockchain-based intelligent network management for 5g and beyond. In Proceedings of the 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT 2019), Lviv, Ukraine, 2-6 July 2019; pp. 36-39, doi:10.1109/AIACT.2019.8847762.
- [24] Buterin, V. Ethereum Whitepaper. 2013. Available online: <https://ethereum.org/whitepaper/> (accessed on 14 April 2019).
- [25] Vukoli, M. Rethinking Permissioned Blockchains [Extended Abstract]. IBM Res. 2017, 3-7, doi:10.1145/3055518.3055526.
- [26] Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Liu, Y. A Survey on the Scalability of Blockchain Systems. IEEE Netw.2019, 33, 166-173, doi:10.1109/MNET.001.1800290.
- [27] Fischer, M.J.; Lynch, N.A.; Paterson, M.S. Impossibility of Distributed Consensus with One Faulty Process. J. Assoc. Comput. Mach.1985, 32, 374–382.
- [28] Yin, M.; Malkhi, D.; Reiter, M.K.; Gueta, G.G.; Abraham, I. HotStuff: BFT Consensus in the Lens of Blockchain. arXiv 2018, arXiv:1803.05069. Available online: <http://arxiv.org/abs/1803.05069> (accessed on 4 April 2020).
- [29] Amsden, Z.; Arora, R.; Bano, S.; Baudet, M.; Blackshear, S.; Bothra, A.; Cabrera, G. The Libra Blockchain. 2019. Available online: <https://developers.libra.org/docs/the-libra-blockchain-paper> (accessed on 4 April 2020).
- [30] Schwartz, D.; Youngs, N.; Britto, A. The Ripple Protocol Consensus Algorithm. 2018. Available online: https://ripple.com/files/ripple_consensus_whitepaper.pdf (accessed on 12 April 2020).
- [31] IEEE 802.11 Working Group. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2012; 2012. Available online:

<https://ci.nii.ac.jp/naid/10011815988/> (accessed on 7 April 2020).

- [32] Mehrnoush, M.; Sathya, V.; Roy, S.; Ghosh, M. Analytical Modeling of Wi-Fi and LTE-LAA Coexistence: Throughput and Impact of Energy Detection Threshold. *IEEE/ACM Trans. Netw.* 2018, 26, 1990–2003, doi:10.1109/TNET.2018.2856901
- [33] Steven, P. Blockchain CSMA/CD Protocol Simulator [Source Code]. 2020. Available online: <https://github.com/stevenplatt/blockchain-CSMA-CD-protocol-simulator> (accessed on 16 August 2020).
- [34] ETSI. 2020. Available online: <https://www.etsi.org/technologies/nfv> (accessed on 14 April 2020).
- [35] 3GPP. Telecommunication Management; Study on Management and Orchestration of Network Slicing for Next Generation Network, Specification #: 28.801. 2017. Available online: <https://bit.ly/3cUFJXZ> (accessed on 14 April 2020).
- [36] ETSI. Network Functions Virtualisation (NFV); Architectural Framework, ETSI GS NFV 002 V1.2.1. 2014. Available online: <https://bit.ly/30YGwSk> (accessed on 2 June 2020).
- [37] Nokia. Cloud Native Core. 2020. Available online: <https://www.nokia.com/networks/portfolio/cloud-native-core/#benefits> (accessed on 22 May 2020).
- [38] ETSI. Network Functions Virtualisation (NFV) Release 3; Architecture; Report on the Enhancements of the NFV Architecture Towards “Cloud-native” and “PaaS”, ETSI GR NFV-IFA 029. 2019. Available online: https://www.etsi.org/deliver/etsi_gr/NFV-IFA/001_099/029/03.03.01_60/gr_NFV-IFA029v030301p.pdf (accessed on 16 August 2020).



Chapter 5

DECENTRALIZING CELLULAR OVERLAYS

Increasing diversity in the blockchain ecosystem has opened up a number of new research paths for its application within wireless networks, including applications related to edge access control and mesh connectivity, as well as spectrum sharing and regulation. However, a byproduct of this diversity is that blockchain, as a technology, now refers to an entire ecosystem of consensus, security, incentive, and deployment models, but there is no framework for how these systems relate to or can be made generally compatible with 5G design. Progress on this lack of native fit and focus has been made with CoNTe, a 5G-specific blockchain designed to pair with and behave as a temporal 5G network function. This work extends the research contributions of the CoNTe 5G blockchain design by providing a generalized deployment model under the ETSI Generic Autonomic Network Architecture (GANA) and allowing the abstraction of core and radio resources for the delivery of decentralized 5G network service overlays.

5.1 Introduction

Blockchain, as a data structure, did not include a currency function at its inception [1]. This functionality arrived later and eventually combined with contract control to create what is most commonly understood as “blockchain” today [2][3]. However, defining more specifically what a blockchain is remains difficult because underneath the high-level concepts of currency, contract, and decentralized ledger are a variety of models for consensus, security, and fault tolerance. At the time of writing, blockchain itself has no standard of deployment, so taking the nonstandard technology and placing it into networks has proven equally difficult. Early interest focused on harnessing the peer-to-peer nature of blockchain for resource sharing; these examples included models of access control [5], network mobility [6], dynamic spectrum access [4]. Other models that place blockchain at the network edge, which is a method that is largely incompatible with a blockchain data structure, whose linear nature does not support ledger updates at millisecond scale [8]. Further research has taken the path of placing blockchain at the network core but still retained implementation-specific contract and payment models, limiting their wider use [8].

To address such unstructured variety and inherited customization, a research project named “CoNTe” returns to the form of blockchain as agnostic storage. CoNTe accomplishes this with a design that is specific to 5G and intended to remain immutable, while also being temporal, so that it can be deployed as the storage of individual network functions to decentralize them. This paper¹ expands on the initial research contributions of the CoNTe blockchain design by providing further details in terms of the consensus algorithm and scaling, in addition to placing it into a standard and generalizable deployment context using the ETSI Generic Autonomic Network Architecture (GANA) model [12]. The remainder of this paper is divided into four parts. Next is a section on background and related

¹Platt, S., Oliver, M. Decentralizing Future Networks: Combining Blockchain and ETSI Generic Autonomic Networking Architecture, IEEE Transactions on Network and Services Management, Submitted - Under Review, June 2021.

work that is provided to elaborate on existing research and present a high-level summary of both ETSI GANA and the CoNTE blockchain, which are the starting point of this research. After this, we show how these two can be combined to create a carrier-agnostic 5G overlay. This section is the main contribution of the paper and details how the CoNTE blockchain is made compatible with any standards development organization (SDO)-compliant 5G network. Section IV covers the evaluation performed to measure the scaling of CoNTE in implementation, and the final section concludes by providing a summary and directions for future research.

5.1.1 Contributions

The paper represents a first step in moving the design of the CoNTE 5G blockchain into production use and provides the following research contributions:

- *Decentralized cellular deployment model*: This paper provides a deployment model for decentralized cellular service in 5G and beyond networks. The model is novel in that it is *generalized* to be both forward and backward compatible with any cellular network utilizing 3GPP-compliant resource slicing and virtual network functions.
- *Expanded CoNTE blockchain simulation*: The deployment model detailed in this research is built upon the CoNTE blockchain design. This research provides further simulation performance results, expanding on those included in the original published CoNTE blockchain design.

5.2 Background and Related Work

With the transition to 5G, network services are intended to become increasingly modular. In release 15, the 3GPP outlines eighteen network

service functions as part of the initial 5G standard. These network services are not strictly required but represent the range of individual activities that can potentially be decentralized using the CoNTe blockchain under the ETSI GANA model. These services are listed below [14]:

- *5G-Equipment Identity Register*
- *Application Function*
- *Access and Mobility Management Function*
- *Authentication Server Function*
- *Data Network*
- *Network Data Analytics Function*
- *Network Exposure Function*
- *Network Repository Function*
- *Network Slice Selection Function*
- *Policy Control Function*
- *Radio Access Network*
- *Security Edge Protection Proxy*
- *Session Management Function*
- *Unified Data Management*
- *Unified Data Repository*
- *Unstructured Data Storage Function*
- *User Equipment*
- *User Plane Function*

Underpinning the ability to isolate individual network functions are SDO architectures such as software defined networks (SDN) and network function virtualization (NFV). These bring with them upstream orchestration capabilities that make it possible to deliver network slicing, infrastructure-as-a-service (IaaS), and cellular network overlays [14][13][19]. With a cellular network overlay, these SDO architectures are used to partition a network virtually to allow dynamic allocation and configuration of network resources. A common use case for this type of network partitioning is the mobile virtual network operator (MVNO) business model. In MVNO deployment, network resources are partitioned and allocated to an extent that an entire cellular carrier can operate under a secondary user access model in which the underlying network infrastructure may be owned by another mobile network operator (MNO) [9]. This research inherits the structures and mechanics that enable cellular overlay networks and extends the current body of work by introducing mechanics of decentralization using blockchain and the ETSI GANA model.

5.2.1 ETSI Autonomic Networking

The ETSI GANA model sits as a layer atop the previously mentioned SDO architectures. With GANA, ETSI did not intend to substitute already existing SDO architectures such as NFV but rather sought to provide a model that could be both agnostic and supplemental to the different SDO architectures that may sit underneath.

At the time of the original ETSI GANA whitepaper, a reference design was given for instantiating the model atop the evolved packet core (EPC) of a 4G design. This design was later updated in subsequent whitepapers to account for 5G NR architecture [30][31][32]. Within the ETSI GANA model are a number of features that are unique to it and may not be accommodated within the base SDO architecture; these features focus largely on its namesake’s autonomicity that is achieved by providing a yet higher higher level of abstraction to allow autonomicity not only within a single managed network, but also potentially with peer networks - making it an especially well-suited model to highlight the implementation of

blockchain decentralization. ETSI GANA delivers its cross-network autonomy in the form of four levels of decision elements (DEs), which are briefly outlined in the sections that follow [30].

Level 1: Protocol Level DEs

Level 1 represents the lowest level of the “control loop” in the ETSI GANA architecture. Within level 1 sits network protocols, such as OSPF, which both make and implement control decisions.

Level 2: Functional Level DEs

At level 2 sit function level decision elements, which perform automation, decision, and control of a bundle of protocols for a unified purpose, such as mobility management or orchestrating data flows to meet a target QoS. Level 2 control loops are often implemented as virtualized or physical network functions and network function chains.

Level 3: Node Level DEs

Automated controls governing operations of a network node as a whole are designated as level 3. These are often controls relating to environment security or disaster recovery and failover between network nodes.

Level 4: Network Level DEs

Level 4 is the highest level of abstraction for operations that are carried out at a network-wide level; it is also referred to by ETSI as the “Knowledge Plane”. By default this level of abstraction is highly centralized and deployed with controllers such as ONIX (Overlay Network for Information eXchange) to deliver MVNO and network overlay services [20]. The ETSI GANA model notes that control at level 4 of abstraction operates at a slower time scale, partly driven by the latency of decision aggregation from the lower levels; however, this also lends compatibility with the

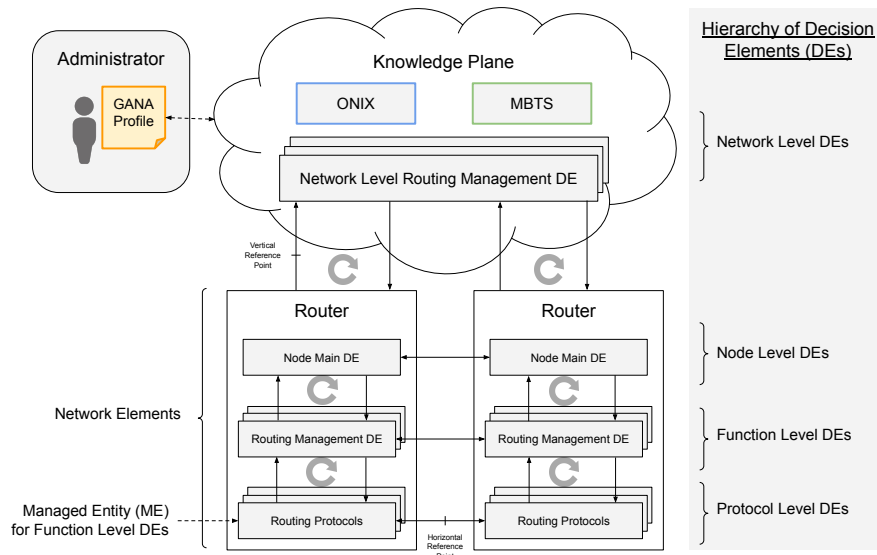


Figure 5.1: Summary representation of the 4 levels of the ETSI GANA model [30]

performance behaviors of the linear record keeping of blockchain. Another important distinction that ETSI makes at level 4 automation is that these control loops may be chained together or otherwise synchronized, allowing coordination of service delivery across multiple providers and heterogeneous SDO architectures. For this reason, the CoNTe blockchain is designated as a level 4 system. Figure 5.1 shows a summary illustration of the 4 levels comprising the ETSI GANA model.

5.2.2 The Decentralized 5G Use Case

As a system that is intended as carrier agnostic, it is important to note why such a service would be used, and who are the operators and consumers of such services. The authors propose that such a model is best suited

for emergency services, disaster recovery, and other wireless services that could otherwise be considered public utility [40][41]. Current precedent exists for such a model with currently deployed emergency calling services. The United States for example, utilizes the model of regulated Wireless Priority Service (WPS)[34], and at the time of writing is actively researching the use of network slicing to move these services away from legacy circuit-switched designs [35].

In this section we cover two potential scenarios for applying a GANA-based decentralized model. This section serves two goals: first, it provides additional detail for scenarios in which a decentralized network could provide utility; and second, it shows specific network configuration examples to clarify the role of the CoNTe blockchain vs. the larger 5G network.

Scenario 1: Disaster Recovery

Decentralizing services is one path of increasing network resiliency. Due to this, scenarios of disaster recovery such as during natural disasters or cyberattacks, are a good fit for a decentralized GANA deployment.

In this scenario, we assume some unknown number of carriers would like to make available a portion of their unused spectrum capacity to other network operators during disaster events. This type of spectrum sharing may be voluntary or mandated by a local regulatory regime. A problem that occurs in this context, however, is that without direct coordination, network operators have no direct awareness of other networks that are experiencing outages and the extent of such outages. Furthermore, it is also assumed that direct coordination is not possible for networks that are offline.

Given a 3GPP-compliant 5G network underneath, this limitation could be resolved through decentralizing an instance of the *unstructured data storage function (UDSF)* by using blockchain as its storage. This network function could then be used to store periodic status updates or keepalive messages from participating operators. If a network operator ceases to send block updates, and has also not sent an update to notify it is retir-

ing its instance of the UDSF, it could then be assumed that the network operator is offline.

Decentralizing an instance of UDSF in this manner raises an additional benefit compared to direct coordination; a network operator is able to proxy these updates and is not required to reveal any data about its internal network, which is not the case using a network ping to an IP address for example. This UDSF could also carry a specific format such that it includes the specific region, city, or tower coordinates where outage has occurred, which again allows a network operator to control which (if any) proprietary network data are exchanged, while also sharing the context needed for other participants to allocate network slice resources in an efficient and targeted manner.

When viewed through the ETSI GANA model, at the highest network level (level 4), network operators now share a *decentralized* knowledge plane consisting of the data stored in an UDSF. Each operator then uses these data from the knowledge plane at level 4, to independently feed decision engines at levels 1-3 that orchestrate resources leading to the radio and device access at the network edge. In this scenario, the resulting access slices and capacity allocated from these shared data themselves become decentralized. At the user equipment side, it is assumed during the outage that these devices scan and submit random access requests to any available and compatible radio towers within range.

Scenario 2: Intelligent Transport Systems

An additional scenario where a decentralized model could provide utility is with intelligent transport systems (ITS). With over a decade of standards and research, ITS provides a useful example case in that it is an existing service that to date, could not be fully serviced by existing architectures. These existing models include ITS standards and guidance published by ETSI in 2009 [18] and the ITU-R in 2011 [17], as well as further protocol definitions including the IEEE DSRC standard [16] and cellular “vehicle-to-everything” or “V2X” provisions that were published as part of 3GPP release 15 [14].

For this example, we assume a scenario where the connectivity powering sensors and vehicles on public road infrastructure is considered a public utility and that a certain capacity of spectrum is allocated at the government level to serve this connectivity. There are a number of ways in which the government can incentivize providers to deliver free service in this spectrum, one of which is to require it as a condition of licensing further spectrum blocks for private commercial use. On the surface, these conditions have the potential to deliver blanket coverage using existing 5G architecture; but a limitation present in this scenario is network compatibility and interworking for the independently managed wireless networks. If the sensors, vehicles, and other connected components of the environment are not managed by a carrier, there is also no authority that exists to validate authorized network access and to implement fairness in load sharing and mobility.

In this environment, deploying a decentralized instance of the *5G-Equipment Identity Register (5G-EIR)* is suggested, as well as the *Access and Mobility Management Function (AMMF)*. Using these two functions, device identity, such as IMEI can be stored and made available without direct ownership, while also allowing carriers to log tower associations in a format that is also universally visible and immutable.

With the above decentralized network functions in place, as long as vehicles, sensors, or other devices support access frequencies and access technologies of the host network, the environment can be considered compatible. However, this still does not address the technical limitation of interworking, specifically IP addresses that are leased and bound to individual networks as devices roam. This specific technical limitation is important because it highlights a scenario where a final working solution requires the combination of blockchain and the ETSI GANA model. Using the ETSI GANA model, as with the prior disaster recovery example, infrastructures at levels 1-3 remain independently managed, with data decentralized for network functions that use blockchain as storage. Even at this point, it is not possible to carry IP addresses to external networks and have routing work properly. Knowing this, we are able to instead operate a form of dynamic DNS at GANA level 4, which sits outside of the

carrier networks, effectively orchestrating routing to enable interworking as devices and networks update tower associations. This dynamic DNS service can be operated wholly by the government as a public utility, by network operators as part of their carrier architecture, or in further formats not mentioned here. The authors acknowledge that in this example, the potential of misuse exists for the mobility data of devices in a network and plan to address this item as an area for further research.

5.2.3 CoNTe: A Blockchain for 5G

Up to this point, we have referenced blockchain in a generic manner. However, there are limitations present in current blockchain technologies that make compatibility limited. CoNTe is a research project started in 2018 with a goal of identifying the general utility and fit of blockchain technologies in wireless networks. This work began with identifying an interworking model [21] and later progressed to specific investigations of decentralized access control [22] and technology maturity [24], eventually focusing on improving compatibility in 5G deployment. The CoNTe blockchain name is a concatenation of the words “Core Network Temporal” [23] representing its goals of being an immutable data store that is also temporal. Starting with a wholly new design meant the protocols powering CoNTe could be chosen with only the consideration of being compatible with existing 5G operations. The following section is an overview of the mechanics of the CoNTe blockchain.

Enabling Permissionless Life Cycle Control

To achieve the benefit of blockchain coordination, while also remaining 3GPP SDO-compliant, a common choke point that was identified was blockchains’ general lack of lifecycle control. The original CoNTe research identifies three limitations that it targets, which together allow a permissionless blockchain that is capable of life cycle control:

Perpetual Growth: The size and resource usage of modern blockchains preclude them from full participation among low-power or resource-constrained

network systems. This is shown in network research such as [28], which require a separation of network operations as a result of using proxy devices able to run intensive proof-of-work calculations. A natural progression in this scenario is to implement an alternative consensus model, or a compression scheme to tune chain operations for the environment rather than modifying the network structure to suit the chain. For example, if a perpetual currency balance is not required, it is further possible to create and decommission chains for single use when data that were stored are no longer of value.

Currency Incentive Model: As a system demonstrated to support contract execution, several experiments have investigated the use of blockchain to incentivize behaviors such as resource sharing in a network environment. In one model from Maksymyuk et al, devices send cryptocurrency payments to base station operators, while base station operators pay for dynamic spectrum access and backhaul connections to carry traffic to the wider internet [10]. The Nash equilibrium model that was used behaves similarly to other existing blockchain models built atop currency incentive. In the network context, however, it assumes a level of parity in the distribution of infrastructure, demand, and incentive that is uncommon in production markets. Current blockchain incentive models could also be viewed as functionally similar to existing research into “neutral carrier” models, which disintermediate carrier and customer and have not gained wide market adoption to date [11].

To address this, the CoNTe research proposes that blockchain can be evolved to be inclusive of operational incentives, such as resource management, network investment levels, and real-time traffic loads, which differ between providers. Early research by Haber and Stornetta offers a possible path forward to highlight blockchain predating digital currency; in this format, the focus is on the latent utility of verifiable shared data instead of currency and contract incentive. As sharing of limited resources such as spectrum increase in the evolution to 6G, it is possible that a higher utility comes from the sharing of data such as spectrum occupancy rather than cryptocurrency payment.

Dependency of Code Execution: Unlike ledger structures, such as the

distributed hash table, blockchain is a strict time-ordered series mandated by its forward hashing. The speed at which code can run is inversely proportional to the volume of new block contribution and dependent new block consensus times [8]. This denotes that a blockchain that sees an increase in block proposal, also sees a decrease in the rate at which these blocks are processed, all else being equal. With Ethereum, because operations are executed within its own Ethereum virtual machine, a slowdown caused by a new block can be partially throttled by increasing the cryptocurrency fee that is charged for new block proposals under its POW consensus. However, this type of control is difficult to replicate in network environments, where creating an API or software representation for the unbounded number of machine operations in heterogeneous networks is impractical. Given two networks of identical generation, it is expected that antenna geometry, sectoring specification, deployment density, backhaul capacity, and service level commitments will differ, conflict, or be changed over time. Unbinding blockchain data storage from code execution such as smart contracts can partially mitigate this risk and related overhead tied to block delay.

The CoNTe Consensus Algorithm

Removing currency, and by extension, transfer contracts, requires deploying a consensus model that does not rely on mining or currency reward to reach finality or ensure security. Departing from conventions used in systems such as Ethereum, CoNTe employs a less common Federated Byzantine Agreement (FBA) model of consensus, first appearing in the Stellar Consensus Protocol [25]. FBA consensus functions in a manner similar to the general internet, where independent networks peer with each other but have no control over who the peers are peered with. This model is what makes the consensus permissionless as network peers and peers of peers relay protocol messaging out to the graph edges. Groups of peers who are all visible to each other are referred to as a quorum slice. Quorum slices that share one (figure 5.2) or more (figure 5.3) overlapping nodes must also agree in order to reach deterministic finality. The consensus reached

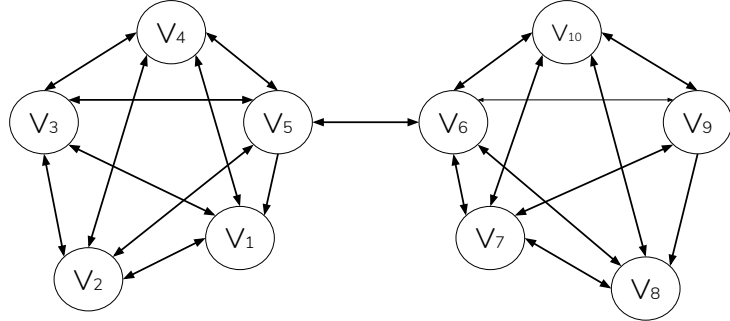


Figure 5.2: Quorum slices that intersect with nodes $\{v_5, v_6\}$.

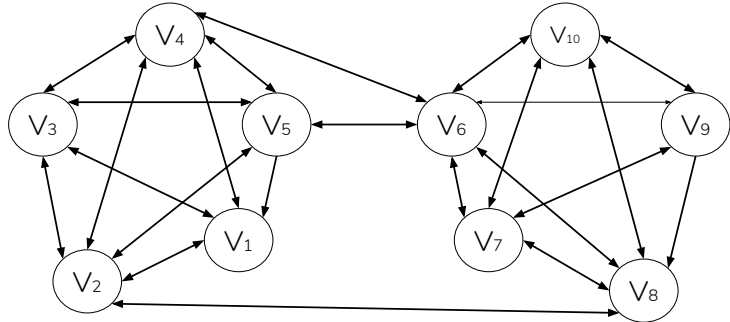


Figure 5.3: Quorum slices that intersect with nodes $\{v_2, v_4, v_5, v_6, v_8\}$.

is referred to as a quorum.

Federated Byzantine Agreement Systems (FBAS) such as CoNTe, deliver safety and liveness of consensus, but make no guarantee of fault tolerance, as defined by the FLP impossibility theorem [26]. The formal definition and relationship of FBAS and quorum are defined below [25][23]:

- Federated Byzantine Agreement System: a pair $\langle V, Q \rangle$ is made up of a node set V and quorum function $Q : V \Rightarrow 2^{2^V} \setminus \{\emptyset\}$ defining one or more quorum slices for a node, where the node is participant to all of its own quorum slices-i.e., $\forall v \in V, \forall q \in Q(v), v \in q$.

- Quorum: a set of nodes $U \subseteq V$ in Federated Byzantine Agreement System $\langle V, Q \rangle$ forms a quorum if $U \neq \emptyset$ and U holds a slice for all members-i.e., $\forall v \in U, \exists q \in Q(v)$, such that $q \subseteq U$.

An important distinction between CoNTe and systems such as Ethereum is that CoNTe is permissionless, but not *trustless*; it is assumed that network peering of carriers is a trusted facility, governed by carrier-partner relationships and network security existing outside of the blockchain itself.

Handling Transmission Contention

The Stellar blockchain was the first to implement the FBA model of consensus and relied on leader election as a means of transmission and congestion control [27]. CoNTe takes an alternate path and does not use leader election or maintain any form of membership list beyond the knowledge of the direct peers. To handle congestion in this context, CoNTe employs a CSMA collision detection model using an exponential back-off timer borrowed from WiFi [28] networks, and defined as $[0, 2^i W_0 - 1]$, where i is the current transmission attempt and W_0 is the minimum sensing period. To the author’s knowledge, CoNTe is the first and only blockchain system to deploy this mechanism for congestion control. Details of the CSMA/CD algorithm are provided in Appendix A.

With this CSMA/CD model, in cases of extreme network delay, it is still possible for two nodes to complete their countdown without receiving a block already initiated by a remote node. This issue in WiFi networks is referred to as the “hidden node problem” [29]. CoNTe employs a secondary algorithm for this exception that allows peers to resequence blocks if they have already received a block with the target index number. This keeps the blockchains’ record consistent, even under extreme delay. A representation of this block renumbering is shown in figure 5.4.

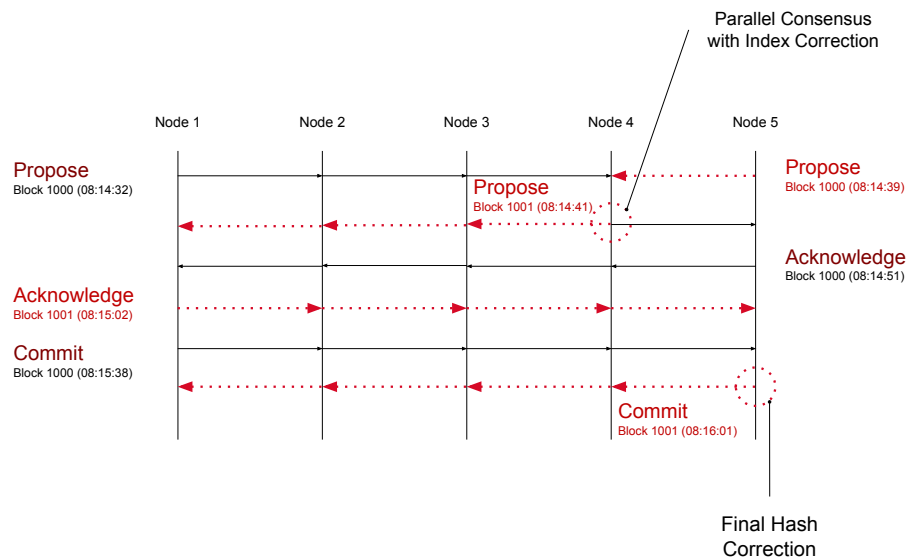


Figure 5.4: Messaging flow during a "hidden node" event; peers operating the CoNTe blockchain will resequence blocks to maintain linear record consistency.

Configuration Comparison

To aid in comparing CoNTe to alternative blockchain platforms, we present a summary of its configuration, using a taxonomy delivered by Nijssse and Litchfield (Table 5.1) [7]. The taxonomy classifies blockchain platforms by fault tolerance, transaction finality, network timing, block proposal, network accessibility, and communication model.

CoNTe diverges most drastically from other blockchains in its configuration with regard to fault tolerance and block proposals. The CoNTe blockchain does not support a native fault tolerance, instead opting for guarantees of safety (that no two nodes will commit conflicting data) and liveness (that all nodes eventually reach consensus). The CoNTe

	Consensus	Fault Tolerance	Transaction Finality	Network Timing	Block Proposal	Accessibility	Communication
Bitcoin \ Ethereum	PoS	50%	probabilistic	synchronous	random	public/private	untrusted
Stellar	FBA	3f+1	deterministic	partial sync	election	consortium	trusted
Hyperledger	PBFT	3f+1	deterministic	partial sync	election	public/private	trusted
IOTA	Hashgraph	3f+1	probabilistic	asynchronous	none	private	untrusted
CoNTe	FBA	none	deterministic	partial sync	none	public	trusted

Table 5.1: Comparison of blockchain configurations [7]

blockchain also does not apply controls over block contributions, such as election mechanisms that would require knowledge of network membership or randomization mechanics such as cryptographic puzzles which could burden resources of systems such as network appliances that are hardware constrained. Individually, each of the components of the taxonomy influences the performance and scalability of a given blockchain system. In the configuration of CoNTe, the components are chosen with initial consideration given to allowing life cycle control, and by extension, general network function compatibility, rather than highest performance.

5.3 Combining Blockchain and ETSI GANA

5.3.1 ETSI MANO Carrier Architecture

Because the ETSI GANA model is an abstract model and does not define the network elements that ultimately sit underneath, our model applies ETSI GANA instantiated atop a network function virtualization management and orchestration (NFV MANO) architecture [33] (figure 5.5).

The CoNTe blockchain is designed to be a standard drop-in component of an ETSI MANO architecture and does not require nonstandard accommodation. It does however, modify the capabilities of certain components, specifically the capability of network functions that become decentralized but still conform to the ETSI GANA model. The following sections detail this implication and its impact on the high-level network architecture.

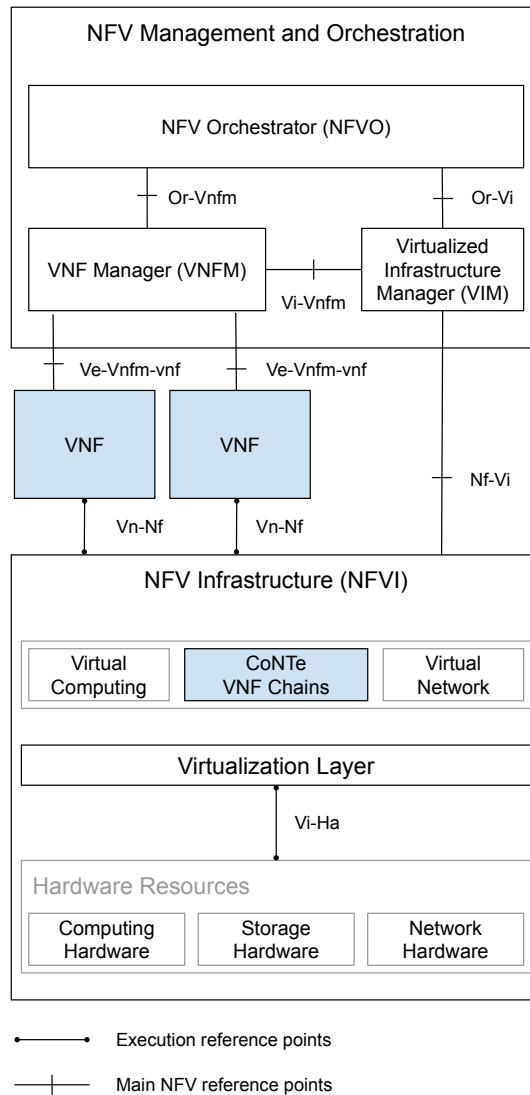


Figure 5.5: Individual CoNTe blockchains (microchains) replace traditional virtual storage for individual network functions within the ETSI MANO architecture [33]

NFV Infrastructure (NFVI)

Unlike monolithic blockchain systems, which store all data in a single instance, the CoNTe blockchain system operates individual chains for each use. These microchains are single use because they are bundled with virtual compute and virtual network resources by network orchestration to deliver individual network functions that run open-ended or with an assigned terminus. Taking a single 5G network function as an example, we look at the authentication server function (AUSF). By using a CoNTe chain as the storage for this function, rather than local virtual storage, a network operator can collaborate with other network peers who each store device identities in the chain. Device identities appearing in this storage receive the benefit of being stored securely in storage that is immutable and by extension, easy to audit. This storage is also decentralized, with no single network owning and controlling the record. Within the physical virtualization infrastructure, the lowest layer of hardware resources is unmodified; this includes storage hardware that may be commodity storage arrays or other existing solutions. Moving a layer higher into the virtualization layer, the CoNTe blockchain is implemented in software as a direct replacement or runs in parallel with traditional virtual storage. In figure 5.5, components impacted by the deployment of CoNTe blockchains are colored in blue.

Because the CoNTe blockchain is agnostic to the network function, using it as virtual storage is theoretically possible with all network functions. Depending on the desired service, network orchestration can bundle CoNTe storage with all functions that serve a network slice or block of users, or it could underpin a smaller subset of network functions used, as illustrated in the AUSF example. This flexibility is important because it gives network operators full control of what information is shared, while retaining full control over the design of services within their own network - the blockchain imposes no design constraint beyond standard virtual storage use. Additionally, exposing and providing targeted access to receive peer block contributions can be done with 5G network exposure functions (NEF), made standard within the 5G release specification by

the 3GPP [14].

NFV Management and Orchestration

Within the management and orchestration layers, the virtualized infrastructure manager (VIM) handles the interaction of hardware storage with VNFs, and by extension is responsible for initializing new CoNTE microchains within physical storage and allocating them to VNFs. The VNF Manager (VNFM) is responsible for managing the life cycle of VNFs, including their initialization and termination. Atop these two, the NFV orchestrator (NFVO) handles the final delivery of network services. With visibility into the operations of the underlying VNFM and VIM, the NFVO creates the virtual connections between VNFs, stitching them together and creating the ability to deliver end-to-end allocation of resource slices to deliver individual network overlays.

5.3.2 ETSI GANA Overlay Design

Again, using our decentralized 5G use cases as a generic starting point, we assume a scenario where an unknown number of mobile network operators agree to provide network access to a set of nonsubscriber devices and public utilities. The following two sections explain how the previously described ETSI MANO architecture is abstracted one level higher using the ETSI GANA model, and decentralized using the CoNTE blockchain, to deliver the final overlay spanning multiple networks.

Levels 1-3: Carrier-Managed MANO

With the ETSI GANA model instantiated atop the NFV architecture, layers 1-3 of the GANA model directly inherit the infrastructure defined by the ETSI MANO architecture explained in the prior section. Figure 5.6 shows a reference of this relationship, with hardware resources, virtual resources, and the resulting virtualized network functions existing under individual mobile network operators. It is important to note that these operators are wholly independent and their infrastructure is not physically

bound or under active coordination in any way. The sole modification at these layers is the inclusion of the new decentralized storage that underpins network functions, which allows decentralization of common data that ultimately allows the operators to deliver network slices in a manner of their choice, accounting for their own resource management, capacity, outage states, and further network context which is not known to outside parties. Extending from this common data stored in CoNTe chains are NEFs exposing external access to the CoNTe microchains for layer 4 of the ETSI GANA model.

Level 4: 5G Overlay Knowledge Plane

The orchestration of services is at layer 4 of the GANA model. The deployment model presented here (figure 5.6) presents an alternate implementation to that outlined in the initial GANA whitepaper. Delivering services to devices that are not under active management by a network provider presents a new context that was not previously accounted for in the GANA model. To handle this class of service, the control mechanisms previously present at layer 4 are disconnected from the network services below and are instead implemented as a passive read-only view into the network resources being made available. This is done using NEFs as mentioned in the previous section. Assuming that device identities are previously registered, exposing resource views in this manner allows an unbounded number of public utility administrators within layer 4 to consume available network slice resources across multiple networks that provide the capacity either on a voluntary basis or under other agreements and regulation.

Decoupling layer 4 in this way without a mechanism of active management to the network below leaves a gap in accounting for how network resources are coordinated between public utilities or how operations such as mobility occur. As shown in figure 5.6, resource management for these transient users happens in parallel, influenced both by individual network operators' resource management and an overlay controller such as ONIX or other UE feedback-driven decision engines managed by the

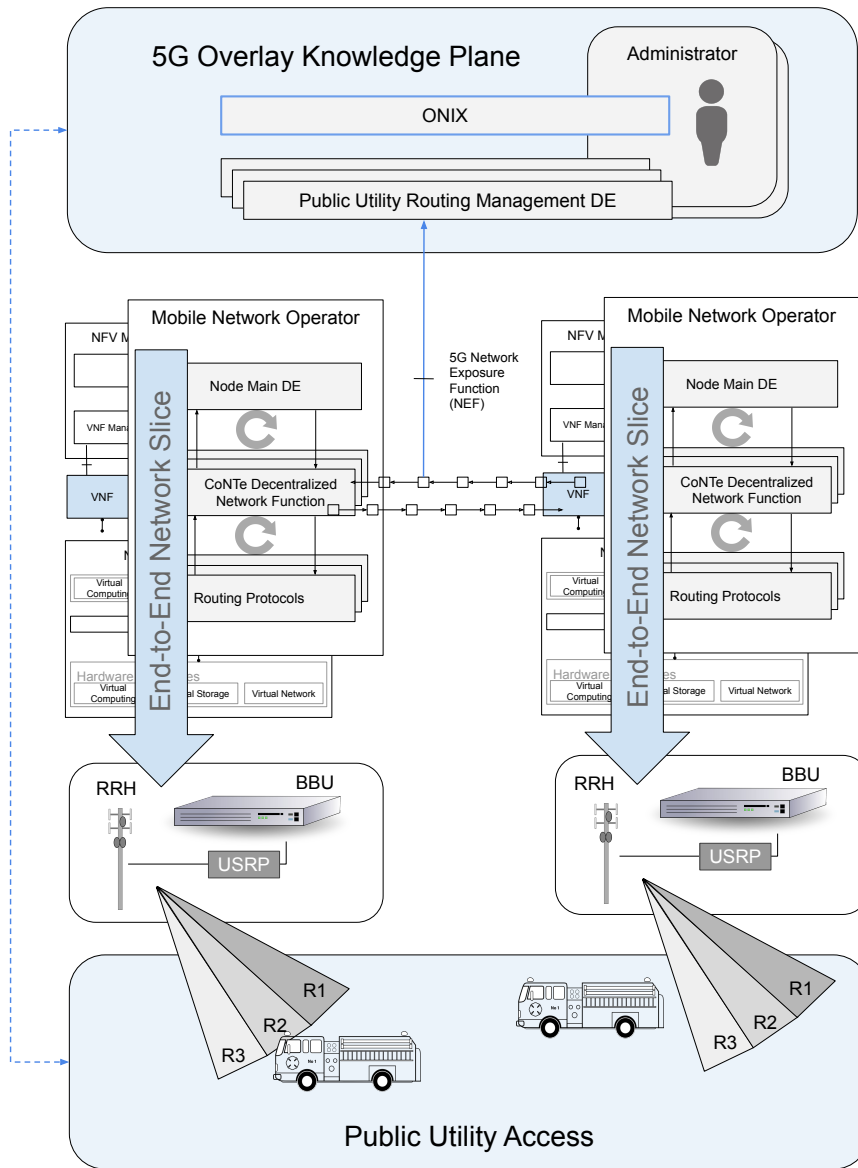


Figure 5.6: Decentralized 5G service overlay, using the ETSI GANA model - instantiated atop a ETSI MANO architecture.

public utility administrator at level 4. For example, a single UE is approved for access to public utility resource slices and would like to access radio slice R1 from network operator 1. Requesting this access is done in a manner identical to traditional 5G subscribers requesting physical channel resources. First, the UE listens for the primary synchronization signal (PSS) and secondary synchronization signal (SSS) on network bands it has compatibility with, identifies a physical serving cell and initiates a random access negotiation with the serving network. Again, assuming the UE identity is known and permitted by the 5G access management function (AMF), the UE is allocated uplink and downlink resource block capacity as determined by the attached mobile network operator. Outside of this operation, the UE is also attached to and reporting its status to the layer 4 knowledge plane and corresponding public utility administrator.

At layer 4, the UE is able to report network context such as location, cell global ID (CGI), received signal strength indication (RSSI), signal-to-interference-plus-noise ratio (SINR), and channel allocation. Receiving this information at layer 4 allows secondary resource management operations to be handled by the public utility administrator without network control. This includes rebalancing UEs based on reported network allocation, quality measures, or network interruption seen or reported to layer 4. This model is also privacy preserving in that only the public utility administrator has visibility of UE activity across networks. Depending on configuration and density of UEs reporting to layer 4, mobility actions could be initiated either by the UE, based on cached information provided by layer 4, or initiated by layer 4 decision engines directly. With this connectivity in place, existing layer 4 overlay controllers, such as ONIX, provide the capability of building forwarding planes for handling IP routing as UEs report cell attachment changes to layer 4; however, the authors acknowledge IP route convergence and maintaining the application state as a potential limiting factor of the model, and have identified it as an area of future research. The IETF’s host identity protocol standard provides a possible solution to routing complications by replacing the IP address with a new host identity tag (HIT) that becomes the addressable destination of application sessions [37]. In such a case, a network controller

such as ONIX serves an additional role of a pseudo-DNS proxy, translating HITs to the known routable IP addresses of UEs as they change underneath.

5.4 Evaluation

By not narrowly defining the application layers and services orchestrated at layer 4, we are able to isolate the sole structural change of such a deployment to the requirement of using the CoNTE blockchain as storage for virtual network functions. This section reviews the initial simulation results of network delay that were published with the initial CoNTE design, and expands them with additional simulations of varying block size, to validate the volume of data that the blockchain can support for storing network functions. Simulations detailed in this section were implemented using the Python programming language and have been open sourced [36].

5.4.1 Performance Under Network Delay

Because the CoNTE blockchain design does not impose membership restriction or other manners of topology constraints, simulations assume a linear bus topology in which all nodes are equidistant and receiving all traffic from all nodes (figure 5.7). This topology provides a simplification in which the network can then be modeled as an implementation of the CSMA/CD method of congestion control. Each node is configured with a 1 Gbps link speed, and in the initial simulation of delay, blocks sent are fixed at 1500 bits in size. Each simulation was run ten times, with the average values being reflected in figure 5.8 and figure 5.9.

Figure 5.8 shows block throughput at 1,500 km, with node counts ranging from 2 to 10 nodes. At the 1,500 km range, which is approximately the distance between Barcelona and Berlin, the CoNTE blockchain design shows scaling that is fairly linear at rates as fast as 1 block per second. Increasing the node distances to 15,000 km shows more clearly

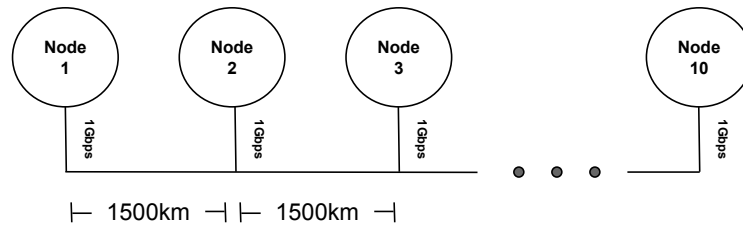


Figure 5.7: CoNTE simulation topology shown at 1,500 km.

the performance limit of the CoNTE blockchain design. At a 15,000 km range, the performance limit of the CoNTE blockchain design is measurable with block throughput at node sizes above 4 experiencing a decline in the total throughput rate. It is important to note that as a system designed for core networks, the CoNTE blockchain is envisioned for deployment at datacenter sites and regional point-of-presence (POP) locations that also often serve as carrier peering locations. In this deployment model, the simulation shows CoNTE is capable of performing at rates of 1 block per minute in a worst case scenario where network cores are all 15,000 km apart.

5.4.2 Performance Under Varying Block Sizes

With the initial simulation of delay completed, we have a baseline reference for the performance of the CoNTE blockchain design. However, this simulation does not investigate scaling under varying block sizes or data volume which is a necessary metric for support of network function data that have varying update sizes. A secondary consideration is that the simple update frequency published with the initial CoNTE design does not provide an easy point of comparison with alternatives such as Ethereum and Bitcoin which are more well-known at the time of writing. Acknowledging that these systems diverge in their respective models

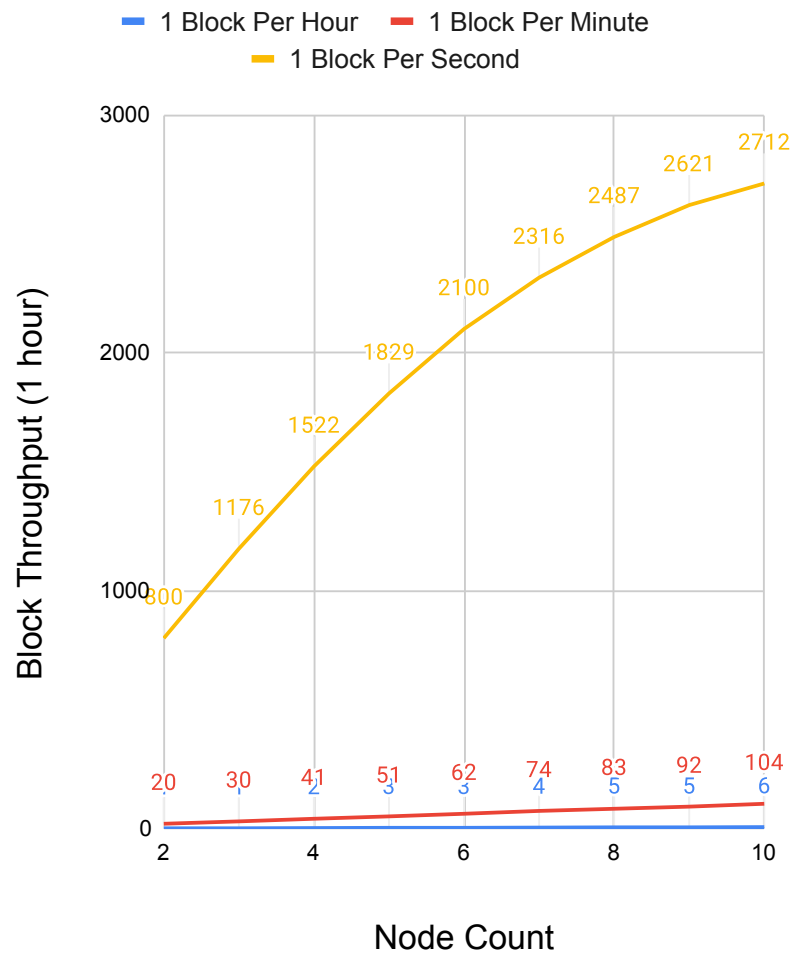


Figure 5.8: CoNTE blockchain throughput scaling at 1,500 km.

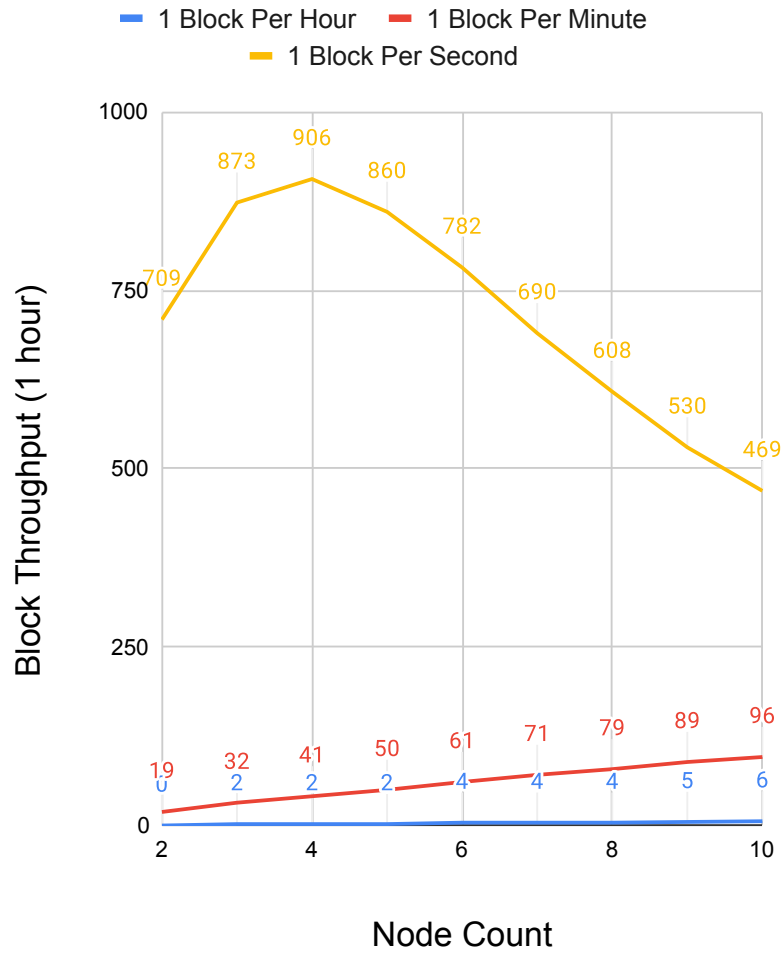


Figure 5.9: CoNTe blockchain throughput scaling at 15,000 km.

	CoNTe Medium Block 1	CoNTe Medium Block 2	Ethereum
Block Throughput	901	907	272
Block Size	30 kbits	1,000 kbits	280 kbits
Total Data (1 Hour)	3.38 Mbyte	113.38 Mbyte	9.52 Mbyte

Table 5.2: Comparison of total data transmission for Ethereum and the CoNTe blockchain with 30 kbit and 1,000 kbit block sizes.

of consensus, block sizing, peer volumes and congestion control, the total data throughput can be considered only as a proxy approximation but was an influence in deciding how to best extend the simulation results. The initial CoNTe design publication contains performance simulations at both 1,500 km and 15,000 km. To extend the analysis, we narrow our focus to the 15,000 km distance results, as the authors feel this best represents a deployment that is global in scale due to it having peers that are continent distances apart. The following section details the simulation results of increasing block sizes. Again, simulations were run ten times, with the average reflected as the final result.

Simulations were run at block sizes of 30 kbits and 1,000 kbits. These sizes were chosen to represent a size range that overlapped the Ethereum block size, which was 280 kbits at the time of writing [38]. The results of these simulations gave interesting results, as the overall block throughput was unchanged even as the CoNTe block size was increased, again having peak block throughput with quorum sizes of 4 nodes at 15,000 km, before gradually degrading. Table 5.2 shows a summary of the total data throughput, where the CoNTe values represent the performance peak, with a node count of 4.

This behavior shows that the total data throughput of the CoNTe chain is linear to the block size, outperforming Ethereum in total data throughput by an order of magnitude at block sizes of 1,000,000 bits. Because this behavior was unexplained by past research, the expected impacts of propagation and transmission delays were implemented in a mathematical model in which the total transmission delay of the standard 1500-bit block was calculated as (4.1), where $dist$ is the distance of nodes, L_{bits} is the

length of bits (block size), V_{prop} is the propagation velocity of the connection medium, D_{prop} is the propagation delay of the connection medium, eff is the connection medium efficiency (fiber), C is connection capacity, and D_{trans} is the transmission delay of sending blocks.

$$D_{prop} = \left(\frac{dist}{V_{prop}}\right)eff = \left(\frac{15,000km}{3 \times 10^8 m/s}\right).69 = 72.46ms$$

$$D_{trans} = \frac{L_{bits}}{C} = \frac{1,500bits}{1 \times 10^9 b/s} = 1.5\mu s$$

$$D_{total} = D_{prop} + D_{trans} \tag{5.1}$$

Calculating the total delay in this manner reveals that delay added by a block of $L_{bits} = 1,500$ is negligible compared to the delay contributed by the node distance itself. This both explains the previous block size behavior and confirms that the initial simulations at 15,000 km indeed represent a worst case scenario or a performance floor for the CoNTe design. Knowing this, we then proceed to confirm at which block size the physical node distance is no longer the largest performance factor by determining the block size at which D_{prop} and D_{trans} become equal (4.2).

$$D_{prop} = D_{trans}$$

$$72.46ms = \frac{L_{bits}}{1 \times 10^9 b/s} \tag{5.2}$$

$$L_{bits} = 72,460kbits$$

With the new crossover value confirmed, simulations of varying block sizes were repeated at 80,000 kbits, 90,000 kbits, 3,000,000 kbits, and finally 7,112,000 kbits; with the later being the equivalent of the Bitcoin block size at the time of writing [39]. Performances at these block sizes did not show performance divergence at 1 block per hour and 1 block per minute rates, but experienced a significant performance increase at the 1 block per second rate which previously degraded at quorum sizes above 4 nodes (figure 5.10).

Having previously calculated the crossover point where block updates become the larger determinant of performance, the results shown in fig-

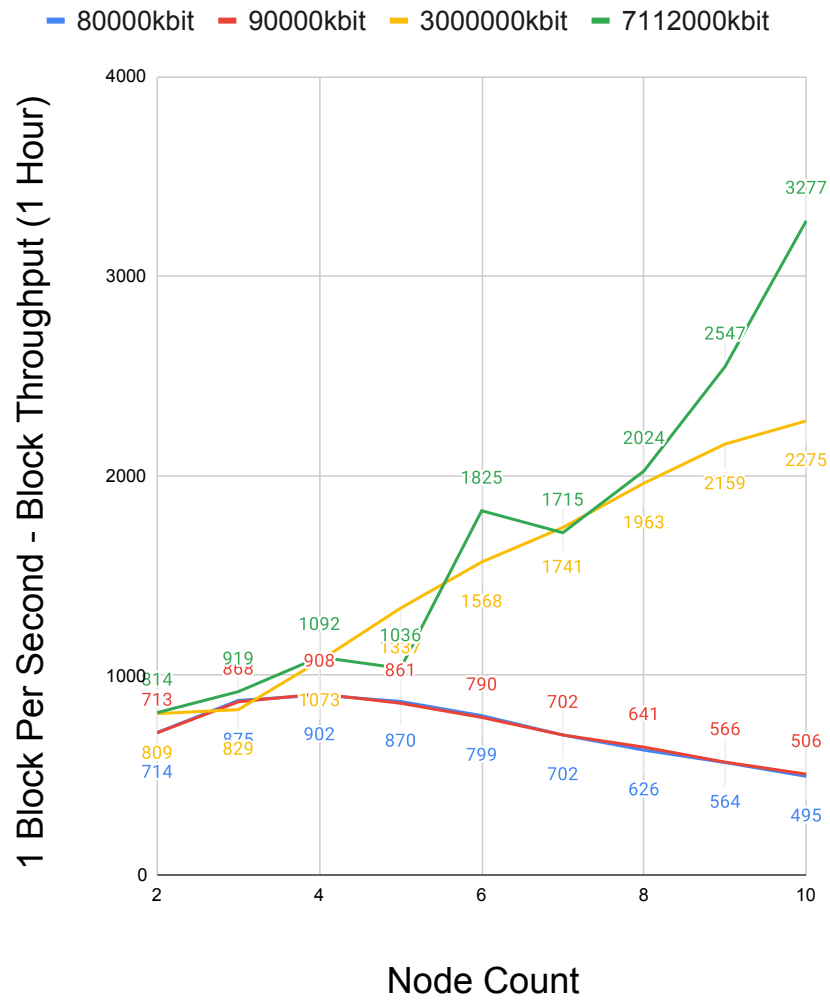


Figure 5.10: CoNTe blockchain throughput scaling at varying block sizes and distance of 15,000 km.

	CoNTe Large Block 1	CoNTe Large Block 2	Bitcoin
Block Throughput	2,275	3,277	6
Block Size	3,000,000 kbits	7,112,000 kbits	7,112,000 kbits
Total Data (1 Hour)	853.13 Gbyte	2,913.25 Gbyte	5.33 Gbyte

Table 5.3: Comparison of total data transmission for Bitcoin and the CoNTe blockchain with 3,000,000 kbit and 7,112,000 kbit block sizes.

ure 5.10 are expected and considered as normal behavior, reflecting a re-balancing of total delay in which transmission delay becomes increasingly large with larger block sizes, compared to delay contributed by propagation. In this view, transmission becomes *more* efficient at the larger block sizes. This is also manifest with larger block sizes triggering fewer back-off timers due to an overall reduction in network idle time during the 1 hour simulation. When combined, these two behaviors create an improvement in block throughput, even though the amount of data being transmitted in the network is increasing. In a manner similar to the comparison of Ethereum, the CoNTe blockchain also outperforms the Bitcoin network, as measured by the total 1 hour data throughput (table 5.3) and confirms that in network function application, the blockchain can support updates exchanged in block sizes up to 7,112,000 kbits (889 Mbytes).

Combining the initial CoNTe performance measures with the behavior and results of simulations added here, it is understood that the CoNTe design has three performance levers: that of node distance (propagation delay), block size (transmission delay), and contention timing. The performance increase experienced at larger block sizes suggests that the frequency of contention may still impose a performance penalty that could be partially offset or tuned by adjusting the contention window minimum back-off timer value under an optimization problem also accounting for block size and node distance. However, this performance tuning of the blockchain itself falls outside the scope of this research.

5.5 Discussion

In this paper, we present a model of deploying decentralized 5G service overlays under the ETSI GANA model. This deployment is achieved by using an ETSI MANO architecture with the CoNTe blockchain functioning as a storage for individual network functions. Under the ETSI GANA model, deploying network functions in this way allows the decentralized sharing of common network data, which in turn enables network providers to voluntarily deliver network resources or entire 5G access slices in a cross-compatible way while independently operating their network underneath. A precedent has been set for coordination of this type in existing emergency calling services and provides a novel path of delivering data connectivity during disasters and for new classes of current and future public utility infrastructures, such as smart road networks. Evaluations undertaken during this research focus on the CoNTe blockchain and its scaling. Simulations added in this paper show the CoNTe design is capable of supporting network function state updates and data exchanges up to 889 Mbyte in size at a 1 block per second contribution rate. Future investigation into the system presented in this research is expected to focus on performance optimization of the core CoNTe blockchain design.

Bibliography

- [1] Stornetta, W. S., & Haber, S. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology*, 3(2), 99-111. <https://doi.org/10.1002/pssb.201300062>
- [2] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, 2016, accessed on 2019-04-14.
- [3] Buterin, V. Ethereum whitepaper, <https://ethereum.org/whitepaper/>. 2019, accessed on 2019-04-14.
- [4] Kotobi, K., & Bilen, S. G. (2018). Secure Blockchains for Dynamic Spectrum Access: A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access. *IEEE Vehicular Technology Magazine*, 13(1), 32-39. <https://doi.org/10.1109/MVT.2017.2740458>.
- [5] Ling, X., Wang, J., Bouchoucha, T., Levy, B. C., & Ding, Z. (2019). Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm. *IEEE Access*, 7, 9714-9723. <https://doi.org/10.1109/ACCESS.2018.2890557>.
- [6] Qiu, J., Grace, D., Ding, G., Yao, J., & Wu, Q. (2019). Blockchain-Based Secure Spectrum Trading for Unmanned Aerial Vehicle Assisted Cellular Networks: An Operator's Perspective. *IEEE Internet of Things Journal*, 1-1. <https://doi.org/10.1109/jiot.2019.2944213>.

- [7] Nijssse, J., & Litchfield, A. (2020). A Taxonomy of Blockchain Consensus Methods. *Cryptography*, 4(32), 1-15. <https://doi.org/10.3390/cryptography4040032>.
- [8] Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2019). ACCEPTED FROM OPEN CALL A Survey on the Scalability of Blockchain Systems, (October), 166-173.
- [9] Mastroeni, L., & Naldi, M. (2010). Spectrum reservation options for Mobile Virtual Network Operators. 6th Euro NF Conference on Next Generation Internet, NGI 2010 - Proceedings, (June). <https://doi.org/10.1109/NGI.2010.5534477>.
- [10] Maksymyuk, T., Gazda, J., Han, L., & Jo, M. (2019). Blockchain-based intelligent network management for 5g and beyond. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings, 36-39. <https://doi.org/10.1109/AIACT.2019.8847762>.
- [11] Infante, J., Oliver, M., & Macián, C. (n.d.). Wi-Fi Neutral Operator: Promoting cooperation for network and service growth. 1, 1-21.
- [12] Ben Meriem, T., et al. (2016). ETSI White Paper No. 16 GANA - Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services. Retrieved from <https://bit.ly/3lZXSru>.
- [13] ITU. ITU towards IMT for 2020 and beyond. <https://bit.ly/2IDOV7G>, July 2020, accessed on 2020-10-14.
- [14] 3GPP. 5g nr (rel-15). <https://www.3gpp.org/lte-2>, April 2019, accessed on 2020-10-14.
- [15] Internet Engineering Task Force (IETF). (2015). Host Identity Protocol Version 2 (HIPv2). Retrieved from <https://tools.ietf.org/html/rfc7401>

- [16] Kenney, J. B. Dedicated short-range communications (dsrc) standards in the united states. Proceedings of the IEEE, vol. 99, no. 7, pp. 1162-1182. 2011.
- [17] ITU-R. IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond. ITU-R M.2083-0, 2015.
- [18] ETSI. ETSI, Sophia Antipolis Cedex, France. ETSI TR 102 638 - Basic Set of Applications (BSA). 2009.
- [19] IEEE. IEEE standards activities in 5g. <https://bit.ly/2IsZLOt>, accessed on 2020-10-14.
- [20] Koponen, T., Casado, M., Gude, N., Stribling, J., Poutievski, L., Zhu, M., Ramanathan, R., Iwata, Y., Inoue, H., Hama, T., & Shenker, S. Onix A Distributed Control Platform for Large.pdf. USENIXConference on Operating Systems Design and Implement, pp. 1-14, 2010.[Online]. Available: <http://dl.acm.org/citation.cfm?id=1924943.1924968>.
- [21] Platt, S., and Oliver, M. A distributed ledger-enabled interworking model for the wireless air interface. Proc. IEEE 5th World Forum on Internet of Things (WF-IoT'19), Limerick, Ireland, April 2019, pp. 402-407.
- [22] Platt, S. & Oliver, M. Towards blockchain for decentralized self-organizing wireless networks. in Proc. IEEE Globecom Workshops ((GC Wkshps)'19), Hawaii, United States, December 2019, pp. 1-5.
- [23] Platt, S., Sanabria-Russo, L., & Oliver, M. (2020). CoNTe: A Core Network Temporal Blockchain Protocol for 5G, 1-13.
- [24] Valle, F. Della, & Oliver, M. (2020). Blockchain's enablers for supply chains : how to boost the implementation in Industry. IEEE Access.

- [25] Mazieres, D. (2015). The stellar consensus protocol: A federated model for internet-level consensus. Stellar Development Foundation, 1-45. <https://doi.org/10.1021/ja982417z>.
- [26] Fischer, M. J., Lynch, N. A., & Paterson, M. S. (1985). Impossibility of Distributed Consensus with One Faulty Process. *Journal of the Association for Computing Machinery*, 32(2), 374-382.
- [27] Stellar Foundation. Intro to stellar. <https://www.stellar.org/learn/intro-to-stellar>, accessed on 2020-01-26.
- [28] IEEE. IEEE 802.11workinggroup.wirelesslanmediumaccess control (mac) and physical layer (PHY) specifications. <https://ci.nii.ac.jp/naid/10011815988/>. 2012. Accessed on 2020-04-07.
- [29] Mehrnoush, M., Sathya, V., Roy, S., & Ghosh, M. (2018). Analytical Modeling of Wi-Fi and LTE-LAA Coexistence: Throughput and Impact of Energy Detection Threshold. *IEEE/ACM Transactions on Networking*, 26(4), 1990-2003. <https://doi.org/10.1109/TNET.2018.2856901>.
- [30] ETSI. (2019). C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA Knowledge Planes (Vol. 1).
- [31] ETSI. (2019). ONAP Mappings to the ETSI GANA Model; Using ONAP Components to Implement GANA Knowledge Planes and Advancing ONAP for Implementing ETSI GANA Standard’s Requirements; and C-SON ONAP Architecture. ETSI TC INT AFI WG 5G POC (Vol. 2).
- [32] ETSI. (2019). Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the

ETSI GANA Knowledge Plane for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV / Clouds Table of Conte (Vol. 3).

- [33] ETSI. (2014). Network Functions Virtualisation (NFV); Management and Orchestration. ETSI. <https://doi.org/10.1109/MCOMSTD.2020.9204597>.
- [34] FCC. Wireless Priority Service (WPS). <https://www.cisa.gov/wireless-priority-service-wps>. January 2020. Accessed on 2020-10-23.
- [35] Carlberg, K., Burger, E. W., & Jover, R. P. (2019). Dynamic 5G Network Slicing for First Responders. In 2019 Principles, Systems and Applications of IP Telecommunications, IPTComm 2019 (pp. 12-15). IEEE. <https://doi.org/10.1109/IPTCOMM.2019.8921240>
- [36] Platt, S. Blockchain CSMA/CD Protocol Simulator [Source Code]. pp. 1-128. Accessed on 16 August 2020. [Online]. Available:<https://github.com/stevenplatt/blockchain-CSMA-CD-protocol-simulator>.
- [37] Internet Engineering Task Force (IETF). (2015). Host Identity Protocol Version 2 (HIPv2). Retrieved from <https://tools.ietf.org/html/rfc7401>.
- [38] Bitinfocharts. Ethereum(eth) price stats and information. <https://bitinfocharts.com/ethereum/>, October 2020, accessed on 2020-10-01.
- [39] Bitinfocharts. Bitcoin(btc) price stats and information. <https://bitinfocharts.com/bitcoin/>, October 2020, accessed on 2020-10-01.
- [40] Sobha, G. V., & Sridevi, P. Usecase of Blockchain in Disaster Management-A Conceptual View. Seventeenth AIMS International Conference on Management, 2019. [Online]. Available:

<http://www.aims-international.org/aims17/17ACD/PDF/A374-Final.pdf>.

- [41] Siemon, C., Rueckel, D., & Krumay, B. Blockchain Technology for Emergency Response. Proceedings of the 53rd Hawaii International Conference on System Sciences, vol. 3, pp. 614-623, 2020.

Chapter 6

ENHANCING MOBILE-CONTROLLED HANDOFF

Traditionally, resource management and capacity allocation has been controlled network-side in cellular deployment. As autonomicity has been added to network design, machine learning technologies have largely followed this paradigm, benefiting from the higher compute capacity and informational context available at the network core. However, when these network services are disaggregated or decentralized, models that rely on assumed levels of network or information availability may no longer function reliably. This paper¹ presents an inverted view of the resource management paradigm; one in which the client device executes a learning algorithm and manages its own mobility under a scenario where the networks and their corresponding data underneath are not being centrally managed.

¹Platt, S., Demirel, B., Oliver, M. Using Transition Learning to Enhance Mobile-Controlled Handoff In Decentralized Future Networks, IEEE Globecom, Submitted - Under Review, June 2021.

6.1 Introduction

Network softwarization in 5G has allowed unprecedented flexibility in how cellular services are configured and delivered. Moving from traditional MVNO agreements and overlay networks existing with 4G, to enabling every function of the network with the ability to be virtualized and made dynamic in 5G and beyond deployment. As previously seen in cloud computing, this rapid advance of software has encouraged a decoupling of hardware from software to the extent that slower moving hardware generations are made general purpose and are able to accommodate increasing heterogeneity of software and services sitting on top [1]. A potential of such decoupling is that in the long term, network infrastructure can be fully disaggregated to the extent that it becomes possible to stitch together wholly new formats of service from multiple Amazon Web Services for *5G ...6G ...and beyond*.

SDN (Software Defined Networking) technologies which previously allowed decoupling of data and control planes for backbone network flows are increasingly being adapted for wireless. These include recent research for adversarial dynamic spectrum access and software radio to enable infrastructure slicing through to the radio access edge [1]. In tandem with these advances, standardization activities including the ETSI GANA (Generic Autonomous Networking Architecture) now provide a reusable model for the separation of higher-level resource orchestration (the cellular control plane) and the dynamic and software driven heterogeneous infrastructures delivering services underneath [2][3]. Extending further from a general separation of data and control planes, recent research and commercial offerings increasingly are pursuing a goal of delivering infrastructures and services piecemeal or decentralizing and abstracting away service providers entirely. These range from a basic expansion of classic MVNO models such as Google Fi [4] and HMD Connect [5]; to dynamic and API consumable wireless services from vendors such as Twilio [6] and Telnyx [7]; and finally a full decentralization of wireless network functions using blockchain technologies [8][9][10].

One difficulty in realizing full decentralization however is classic re-

source management structures which retains global visibility at the base station and cellular core, paired with a subordinate UE (User Equipment) device at the edge. Taking this as a starting point; one question raised is what becomes of the UE device at the network edge and how are network services consumed in the absence of classic network control. With significantly less environmental context available at the UE, addressing device control under this general lack of data requires further research. This paper investigates an enhancement of existing mobile-controlled handoff capabilities by doing all learning *on-device* using the existing mechanic of measuring RSSI (Received Signal Strength Indicator). The remainder of the paper is split into four parts. First we provide a background into the existing mechanics of cellular mobility, recent research into cellular network decentralization, and potential machine learning methods that may be considered as alternatives to the approach detailed in this paper. After this we present our design of a “transition learning” algorithm in section three, followed by our simulation results in section four. The paper concludes with a discussion of results and identification of paths for future research in section five.

6.2 Background and Related Research

The following section provides additional background and related research to highlight the gap and contribution made by the transition learning algorithm being presented in this research. This section covers cellular mobility management, network decentralization, and machine learning applications and limitations.

6.2.1 Cellular Mobility Management

Across network generations and vendor configurations, cellular mobility can inherit a broad range of architectures. At a high level, these can be organized into three categories: network controlled handoff, mobile assisted handoff, and mobile controlled handoff [11].

Network Controlled Handoff

As the most centralized approach, network control handoff places all knowledge and mobility control with network base stations. This approach is largely a carryover of the earliest network design in which UE devices lacked the sensors and compute resources to participate in mobility coordination. In this model, mobility decisions not taken at the network edge can add a non-trivial amount of signaling latency if they include a remote or regional network core.

Mobile Assisted Handoff

UE devices participating in mobile assisted handoff are able to report on-device sensor readings, specifically RSSI which is calculated from the RSRP (received signal received power) and RSRQ (reference signal received quality)[12]. With this data updating periodically, the core network is able to balance the state of the UE device, with its global visibility of the wider capability and status of the network, including total device density, its own backhaul capacity, and the specific commitments and priorities tied to all other services operating from a given base station ahead of making a mobility decision.

Mobile Controlled Handoff

Allowing the UE to handle handoff decisions reduces handoff times compared to the previously mentioned methods [13]. In this model, the UE monitors the measured RSSI values of pilot channels signals received from surrounding base stations and initiates a handoff when certain conditions are met, such as when the RSSI from a connected base station is no longer the highest and drops below a defined threshold with additional padding to limit hysteresis (figure 6.1) [14][15]. The research and transition learning algorithm presented in this paper are targeted at extending the capability of this type of handoff operation.

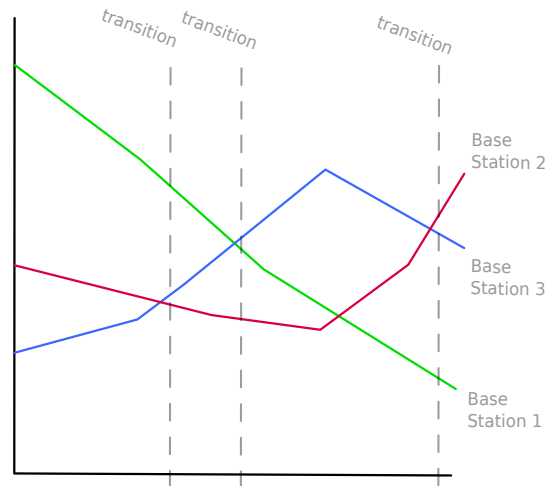


Figure 6.1: Example transitions based on RSSI received at the UE.

6.2.2 Blockchain Network Decentralization

Blockchain at its lowest level is a forward hash-linked data structure. Data stored in "blocks" are hashed and this hash is carried forward and added to new blocks which themselves are then hashed. By including the hash from previous blocks, the data in total becomes cryptographically linked, forming a "chain" [16]. Blockchain technology encompasses an entire category of implementations supporting combinations of cryptocurrency and contracts logic [17] or isolated to be used only as database storage [8].

In network implementation, blockchain has been pursued to allow a broad decentralization of network infrastructures and services. Examples include applications of network access control [9][18], spectrum access auctions [19], and the general use of blockchain technology as an agnostic storage layer used by network functions (figure 6.2) [8]. The latter is significant because it is intended to be generalizable and allow broad decentralization of any network service which is built atop 5G VNF's (Virtual Network Functions).

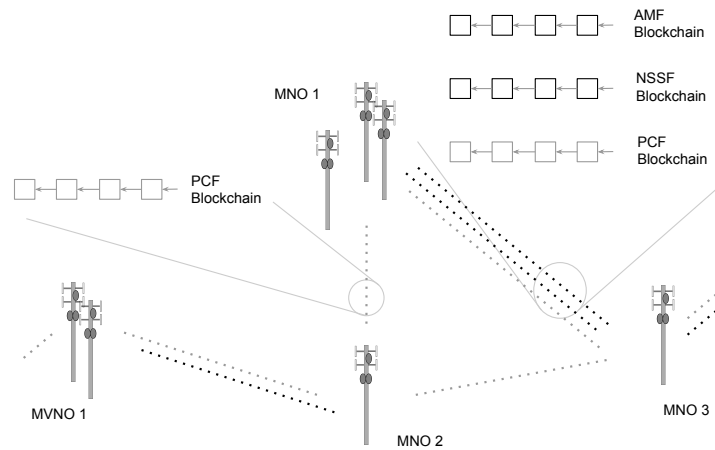


Figure 6.2: Example networks operating individually decentralized network functions [8].

While this paper is not an investigation of blockchain technology itself, it is an important context to highlight as the experiment presented assumes a network environment where the infrastructures are not part of a unitary carrier deployment, but are instead independent with the only commonality being the UE which has access across them. This context is most similar to emergency calling or WPS (Wireless Priority Service) in which a UE, even while not having active carrier subscription, must be permitted access to available networks when placing emergency calls. To the author’s knowledge, there is no deployed available equivalent to WPS for data access [20]. The presented research extends the current body of knowledge in this direction.

6.2.3 Learning Applications and Limitations

Machine learning is a very active path of investigation for enabling autonomy in decision making. Machine learning approaches can be classified into three broad categories depending on the type of feedback signal avail-

able to the learning system: supervised learning, unsupervised learning, and reinforcement learning. This section provides a summary of these three as well as a fourth, more narrow subcategory chosen for the experiment in this paper.

Supervised Learning

Supervised learning models learn to generalize the input-output mappings presented to it by a “supervisor” signal in the form of labeled data. The use of labeled data to train and predict new data points gives precise control of what the model learns through the curation of the labeled dataset. Training supervised learning systems with high quality data that is representative of the ground truth can lead to high levels of accuracy in unseen data points. This level of precise control of what the model learns and dependence on labeled data points is also a drawback of supervised learning systems, as they require both a large and varied amount of representative data to be able to generalize well. Supervised learning methods are less common in cellular deployment, but have been employed for mobile edge computing (MEC) and QoS policy control operations taking place at the less resource-constrained network core [21][22].

Unsupervised Learning

In cases where labeled data is difficult to acquire or outright not available, unsupervised learning approaches can be used to uncover the underlying structures in data. These approaches trade a level of control on what the model learns for the ability to learn underlying structures and make predictions without knowing the ground truth in the form of labeled data. Beyond also requiring a large and varied dataset, a second drawback specific to unsupervised learning is the difficulty in assessing the accuracy of these models derived from unlabeled data without human validation. Human effort is back-loaded with unsupervised learning, compared to supervised learning where most human effort is front-loaded through the labeling of datasets to ensure they represent a ground truth. In 5G and beyond contexts, the unstructured format of unsupervised data learning

has been has often been paired with network stream data and monitoring systems for retroactive self-diagnosis rather than autonomous actuation of cellular resources due to the mentioned lack of control over *what* is learned [23][24].

Reinforcement Learning

Reinforcement learning models learn to map actions to situations in order to maximize a designated reward. A reinforcement learning approach differs from the previous two approaches in multiple ways. First of all, instead of learning from a large dataset, reinforcement learning agents interact with an environment to gather data points and learn how to maximize a reward signal. As the reinforcement learning agent is naive about the environment, it is required to explore the environment as well as exploit any potential source of rewards. This ongoing dilemma between exploration and exploitation means reinforcement learning agents require a high level of interaction. As a result of this ongoing interaction, it is much more adaptable with a minimum need for retraining as it can slowly adapt to changes with each new interaction while expiring old data, allowing it to be relatively storage efficient compared to supervised and unsupervised machine learning models. This structure and behavior make reinforcement learning a better suited candidate for cellular application and operations managed by the UE. Reinforcement learning models are commonly used in wireless for decision making under unknown network conditions and contexts involving resource competition or opportunistic access [25][26][27][28].

Markov Chains and Transition Learning

Markov Chains are a method of representing the probabilities of moving from one state to another. This movement is referred to as a *transition*. By design Markov Chains and Markov processes are intended to model an expected outcome based only on a current state and are considered *memoryless* (6.3). Markov chains are often used to model processes that are stochastic and where past history has decaying or no value over time

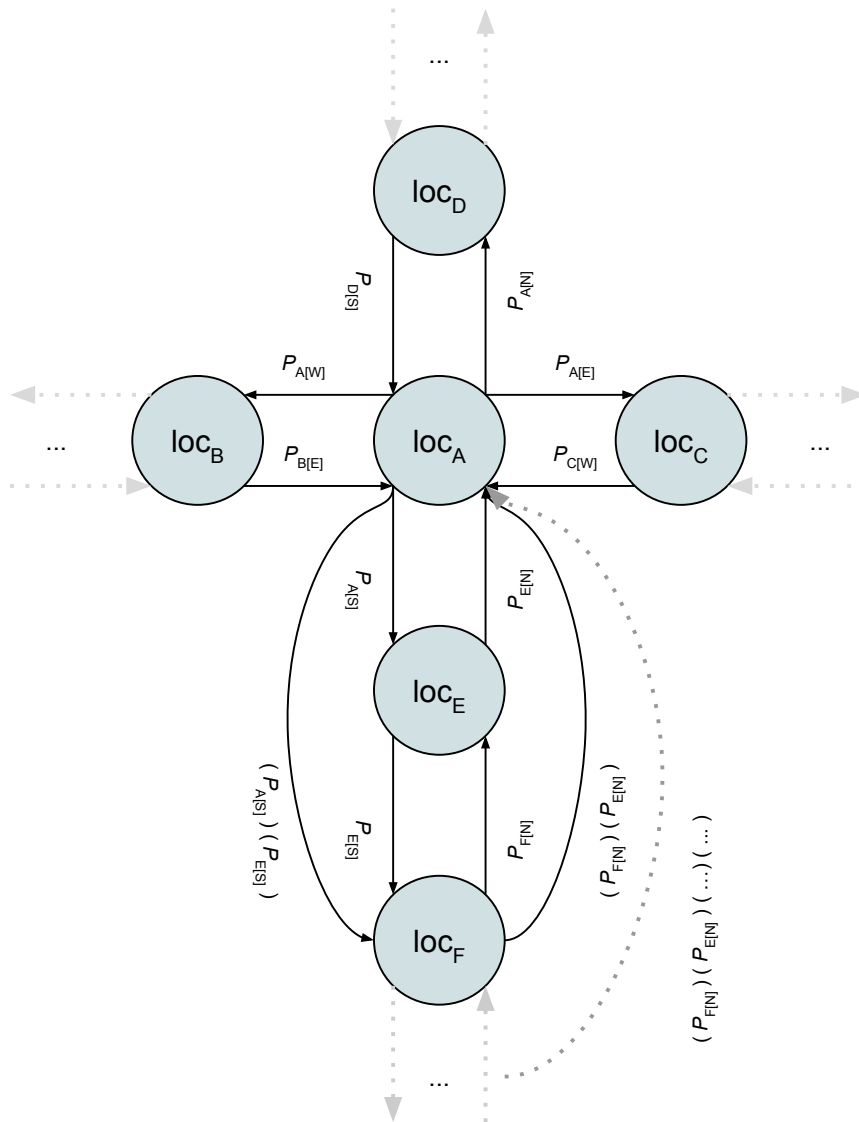


Figure 6.3: 2-D Markov Chain model with North [N], South [S], East [E], and West [W] transitions.

such as in wireless networks [29][30]. In cases where additional context can be gained from previous states, these Markov transitions can be saved for further processing in the form of Transition Learning. Data produced during state transitions in cellular networks has also been used as the training set for the previously mentioned formats of machine learning [31][32]. This paper applies transition learning in isolation, rather than within a large learning algorithm. To the authors knowledge, transition learning has not previously been investigated in isolation as a solution to extend the capabilities of mobile-controlled handoff.

Although a large block of learning algorithms fall into one of these broad categories, they should be understood more as general areas, and less as strict separations as there are exceptions existing which do not map cleanly into a single category as seen with methods such as meta-learning which can provide a cross-category aggregated result [33].

6.3 Transition Learning System Design

In this section we aim to implement an algorithm that extends the capabilities of the RSSI data already existing at the UE to determine if this minimal amount of data can be used to help a given UE take higher performing base station associations under a scenario of mobile-controlled handoff. To do this, we create an algorithm where a UE can store and take decisions informed by a compact history of prior state transitions combined with the performance outcome it received (figure 6.4. The following section details the transition learning algorithm and setup of the simulation environment.

Base Station Association

In the experiment, it is assumed that the UE has access and a policy giving equal preference to all base stations in the environment. In order to represent a traditional preferred roaming list, the UE constantly monitors the 3 closest base stations. The UE is configured to always associate with

the closest base station of the three, mimicking default RSSI association behavior.

Base Station Allocation

Because real world cellular performance is a temporal mix of frequency band, resource block allocation, signal interference, backhaul load and further factors - the experiment abstracts these and defines an “allocation” value to be used as a proxy representing composite performance measured at the UE. Further, the experiment treats the base station allocations as uniform with an isotropic radiation pattern in free space. Allocation values of 5 and 7 were used to present a scenario of significant *allocation* Δ (figure 6.5).

Defining Transitions

To define transitions, the UE begins in some *state* where it checks for the 3 base stations with the highest RSSI defined by their physical proximity (6.1). After completing a random walk, the UE checks whether the rank order of these strongest 3 signals is changed. If it is not changed, the UE does not have a new state and does not evaluate any mobility action. If the UE detects a change in the rank order *and* the strongest signal is also changed (6.2); the UE understands this as a new *state'*. From here the UE takes the default action of connecting to the base station with the strongest signal and calculates the difference in the allocation it received from moving to the new *state'* as an *allocation* Δ . This beginning *state*, final *state'* and *allocation* Δ are stored as *transition_n* (6.3). This *transition_n* is the only value the UE retains in memory.

$$state = \begin{bmatrix} base\ station\ rank_1, \\ base\ station\ rank_2, \\ base\ station\ rank_3 \end{bmatrix} \quad (6.1)$$

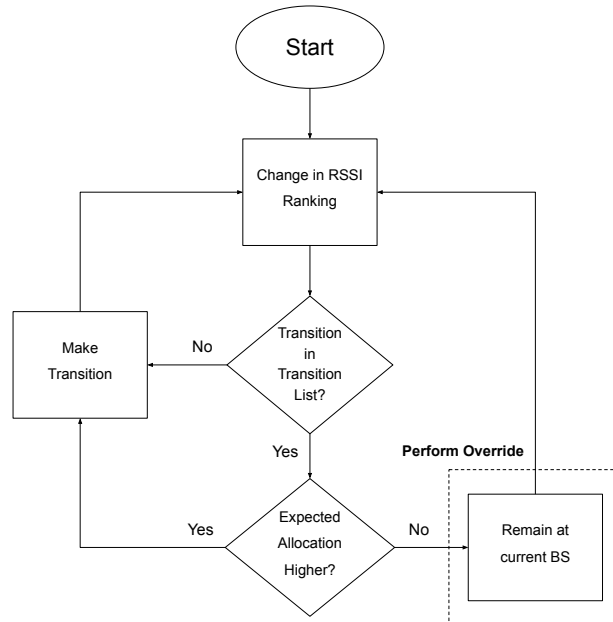


Figure 6.4: Handoff override decision process

$$state(base\ station\ rank_1) \neq state'(base\ station\ rank_1) \quad (6.2)$$

$$transition_n = ("state", "state'", "allocation\ \Delta") \quad (6.3)$$

Transition Learning

Until this point, the UE has been configured with a baseline behavior that mirrors a standard association based on RSSI. To extend this we con-

tribute a new algorithm that learns network allocation outcomes when the rank order of the 3 closest base stations is changed. If the UE has not seen a specific transition before, it continues the default behavior and associates to the base station with the highest RSSI. As the UE performs further handoffs and stores the state transitions, if the UE has seen some $transition_n$ previously, it can choose to perform an “override” and not to perform the handoff if it has learned there is a negative *allocation* Δ expected in that transition. The decision logic of this override process is shown in figure 6.4. The *compute* complexity of the logic is fixed at $O(1)$ due to the logic always using the same two inputs of current allocation and expected allocation to make a decision. The total *algorithmic* complexity of the transition learning process becomes $O(\log n)$ when paired with a binary search algorithm, assuming transitions are stored as a sorted list [34].

Simulation Environment

For the simulation we create an area that is a 23x23 unit grid containing 5 base stations placed at grid positions [0, 0], [22, 0], [22, 22], [22, 0], and [11, 11] (figure 6.5). In this structure the simulation environment presents a 2-D Markov chain with matching state space and cardinality (6.4). Each grid unit of the simulation represents 1 city block.

At the start of the simulation, a UE is placed at position [11, 11] and completes a series of 2,000 continuous random walks of 10 unit steps each throughout the environment. Having all grid positions being equidistant and with an eigenvalue of 1, the sum of probability of the UE transitioning into any given position in the state space converges to 1 after the 2,000 walk trial (6.5) [35]. Additionally, setting a boundary for the simulation environment makes the grid state space irreducible, and combining this with the aperiodicity of the random walk enforces that the probability of the UE arriving to any single space in the environment during a single walk is dependant on the point in which the random walk started (6.6) [35][36]. Transitions and allocations experienced during each 2,000 walk trial are then averaged to provide an average allocation result for

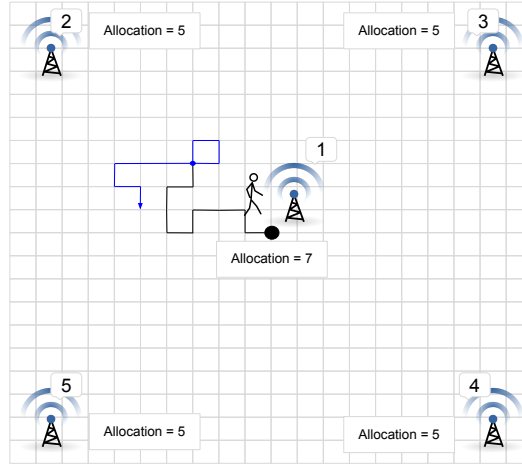


Figure 6.5: The simulation environment using a 10-step random walk and static base station allocations.

the simulation round. A total of 1,000 simulation such rounds were run in order to provide a monte carlo sample of the transition learning algorithm performance. The simulation environment is written in the Python programming language and is available to download from Github [37].

$$P = \begin{bmatrix} P_{0,0} & P_{0,1} & \dots & P_{0,j} & \dots & P_{0,S} \\ P_{1,0} & P_{1,1} & \dots & P_{1,j} & \dots & P_{1,S} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ P_{i,0} & P_{i,1} & \dots & P_{i,j} & \dots & P_{i,S} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ P_{S,0} & P_{S,1} & \dots & P_{S,j} & \dots & P_{S,S} \end{bmatrix} \quad (6.4)$$

$$\sum_{j=1}^S P_{ij} = 1 \quad (6.5)$$

$$\lim_{k \rightarrow \infty} (P^k)_{ij} = \pi_j \tag{6.6}$$

6.4 Evaluation

To characterize the performance of the transition learning algorithm we analyse it under 2 scenarios. The results of the two simulation scenarios are presented in tables 6.1 and 6.2.

	Default Environment		
	<i>% Override</i>	<i>Allocation Average</i>	<i>% Gain</i>
RSSI Default	0	6.01	-
Transition Learning	29.36	6.36	5.5%

Table 6.1: Scenario 1 simulation results

	Sector Load		
	<i>% Override</i>	<i>Allocation Average</i>	<i>% Gain</i>
RSSI Default	0	5.26	-
Transition Learning	30.89	5.65	7.0%

Table 6.2: Scenario 2 simulation results

Scenario 1: Default Environment

The first scenario is the “Default Environment” representing a best case scenario state where the allocations of all base stations is uniform across the entire state space and the final allocation granted is impacted only

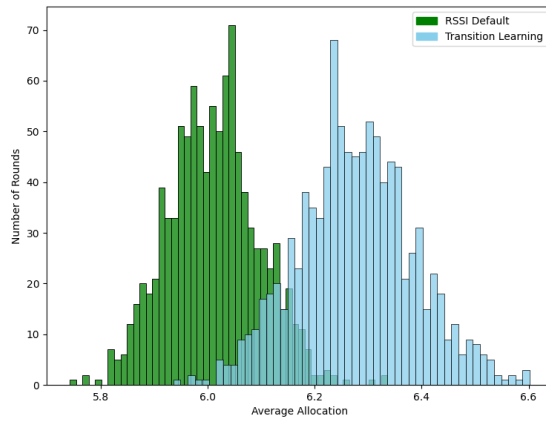


Figure 6.6: Network allocation distribution over 2,000 rounds (Default Environment).

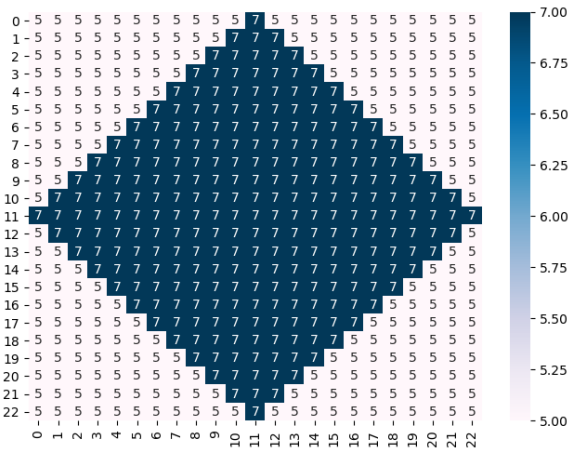


Figure 6.7: Allocation map of Scenario 1 (Default Environment).

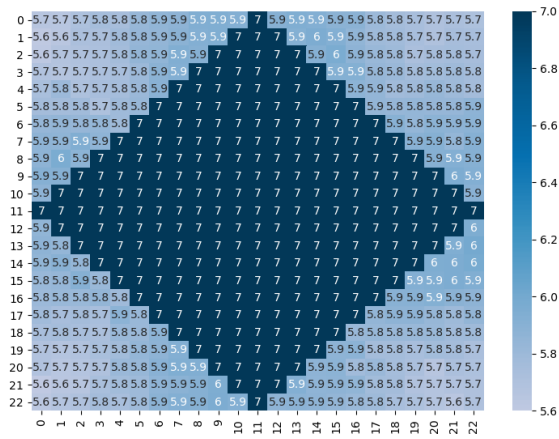


Figure 6.8: Average allocation performance over 2,000 rounds using transition learning (Default Environment).

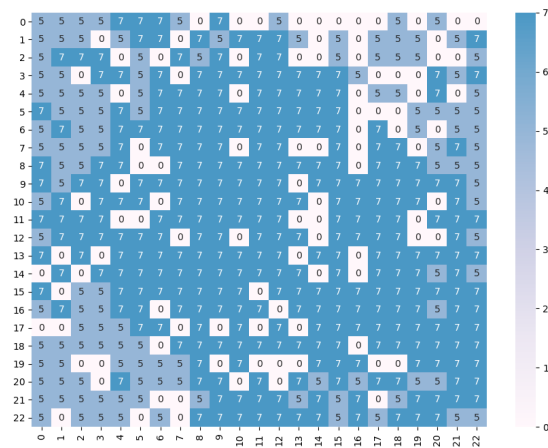


Figure 6.9: Monte Carlo sample of a single random walk round. Allocations marked "0" are unexplored states. (Default Environment).

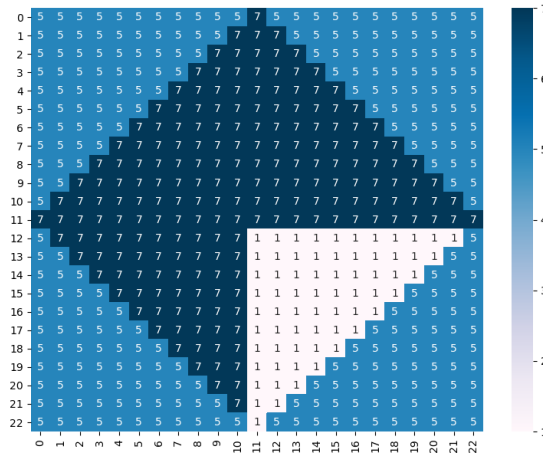


Figure 6.10: Allocation map of Scenario 2 (Sector Load).

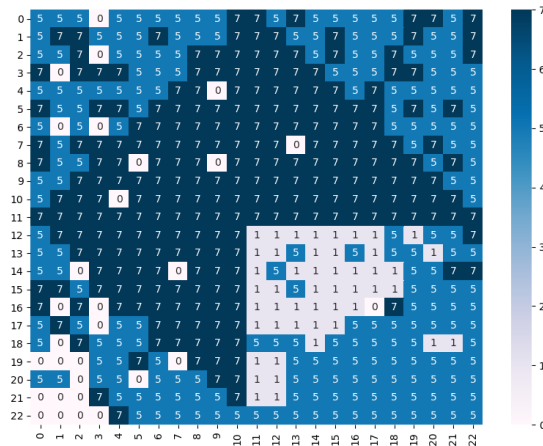


Figure 6.11: Monte Carlo sample of a single random walk round. Allocations marked "0" are unexplored states. (Sector Load).

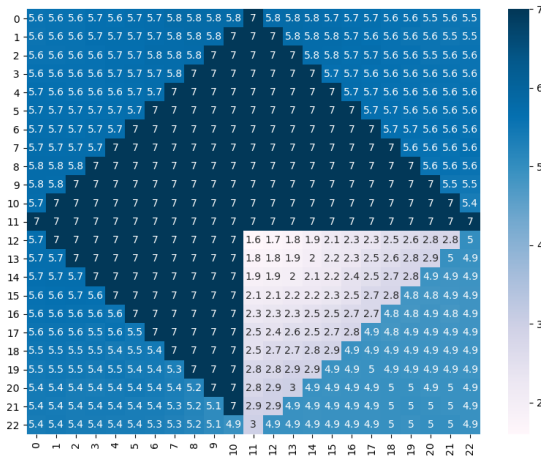


Figure 6.12: Average allocation performance over 2,000 rounds using transition learning (Sector Load).

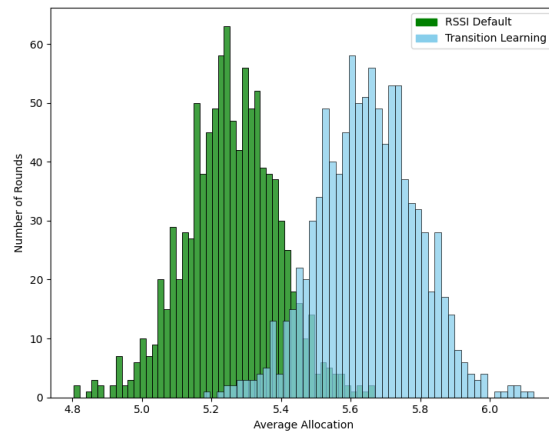


Figure 6.13: Network allocation distribution over 2,000 rounds (Sector Load).

by the choice of base station association. Within the Default Environment, on average the transition learning algorithm performed an override during 29.36% of transitions delivering a net allocation increase of 5.5% compared to base station associations relying only on RSSI (figure 6.6). This scenario provided a predictable result where the amount of overrides performed is roughly correlated to the area of the state space occupied by the base station with higher allocation given the environment geometry (figure 6.7). This result also affirms the original probability relationship that over 2,000 rounds the probability of the UE existing in a given space within the environment becomes 1 (6.5). Figure 6.12 reveals a pattern of higher average allocation in areas bordering the higher allocation zone, corresponding to the increased probability that a random walk from this area has an increased probability of experiencing a transition or transition override resulting from a base station rank change (6.6). Figure 6.9 provides a single round snapshot that gives a higher resolution example of the overrides and resulting allocations that are occurring during individual rounds.

Scenario 2: Sector Load

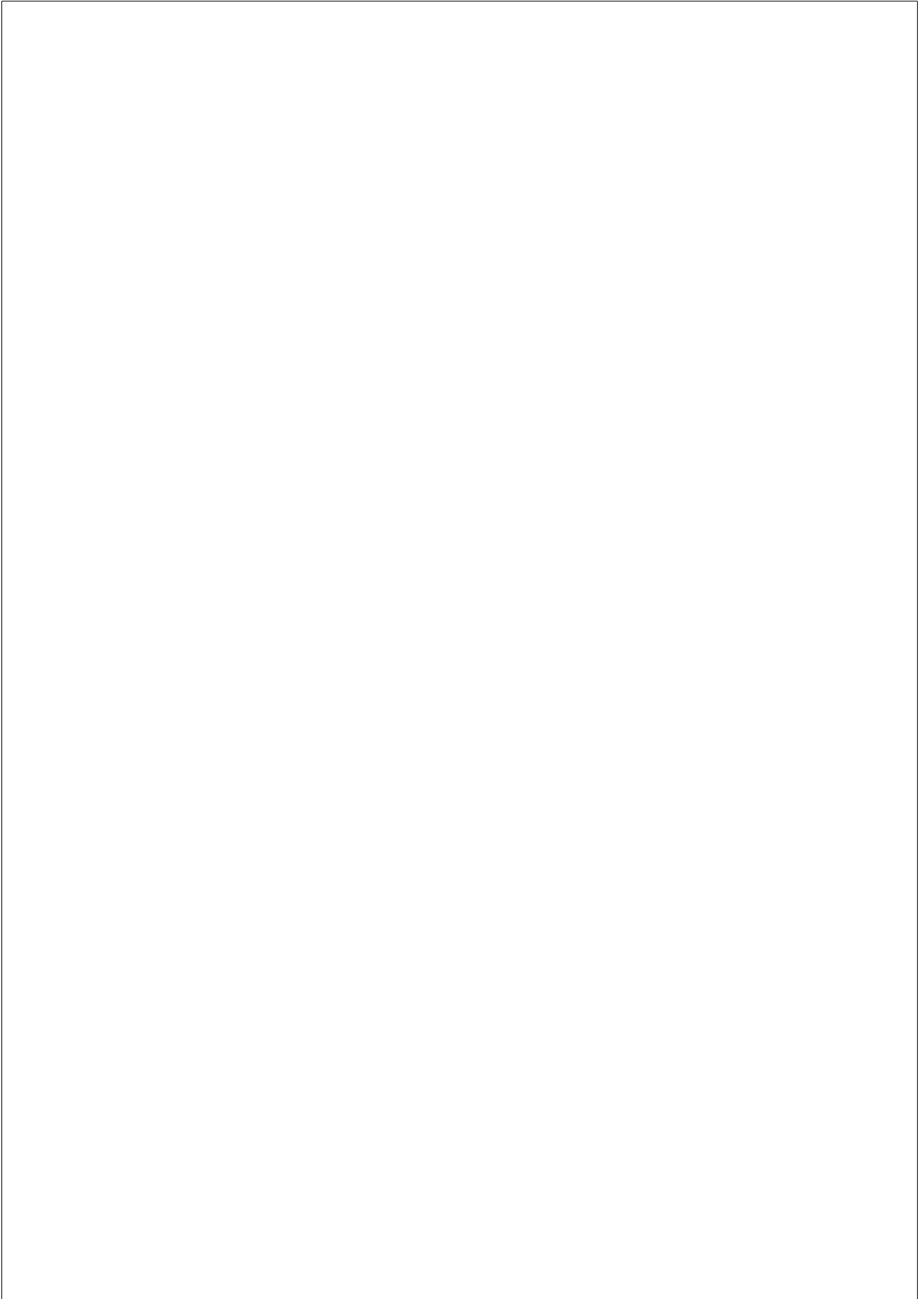
The second scenario evaluated is “Sector Load” and is representative of a scenario where within the coverage of a single base station, there is some subset of coverage (in this case 1 base station sector) that is under significant load, even while RSSI across the state space is unchanged. In this loaded sector, allocation is changed from 7 to 1 (figure 6.10). In this scenario, knowledge of the additional load is not present in the measures available to the UE and is effectively *hidden*. Within the Sector Load scenario, on average the transition learning algorithm performed an override during 30.89% of transitions delivering a net allocation increase of 7.0% compared to base station associations based only on RSSI (6.13). The amount of overrides performed in this scenario is not significantly changed in this scenario, reflecting the proportion of the state space with an allocation other than 5 remains unchanged. The pattern of increased average allocation near edges of higher allocation is repeated here (figure

6.12), but is now shifted towards the base station at position [22,22], reflecting some portion of transitions being learned and then subsequently overridden when involving the base station sector under load. Figure 6.11 again gives a higher resolution example of the overrides and resulting allocations that are occurring during individual rounds of our Scenario 2 with sector load.

6.5 Discussion

Collectively, the authors present this paper as an early result exploring the broader topic of how a network, or more specifically, UE devices can potentially operate after increases in network decentralization. Being able to place additional environment logic at the UE allows the logic the potential to become agnostic and move *with* the UE in a state where network operation occurs peer-to-peer. It is important to note that of the results achieved, raw performance gain values can be considered as secondary, as they are partially a function of the difference between the chosen allocation values during simulation. The primary experiment finding is the underlying behavior relationships and reliability of the transition learning algorithm to attain a better result with $O(\log n)$ complexity - even with hidden environmental contexts such as base station section load.

A potential area of investigation extending from the presented results is the impact and interaction of having multiple UE's within the environment making mobility decisions based on the transition learning algorithm. In this case it can be assumed that all UE's learn similar outcomes from similar transitions and begin to shift network load. In this case such behavior would bring the problem statement closer to existing reinforcement learning experiments in wireless and allow a further comparison of the two.



Bibliography

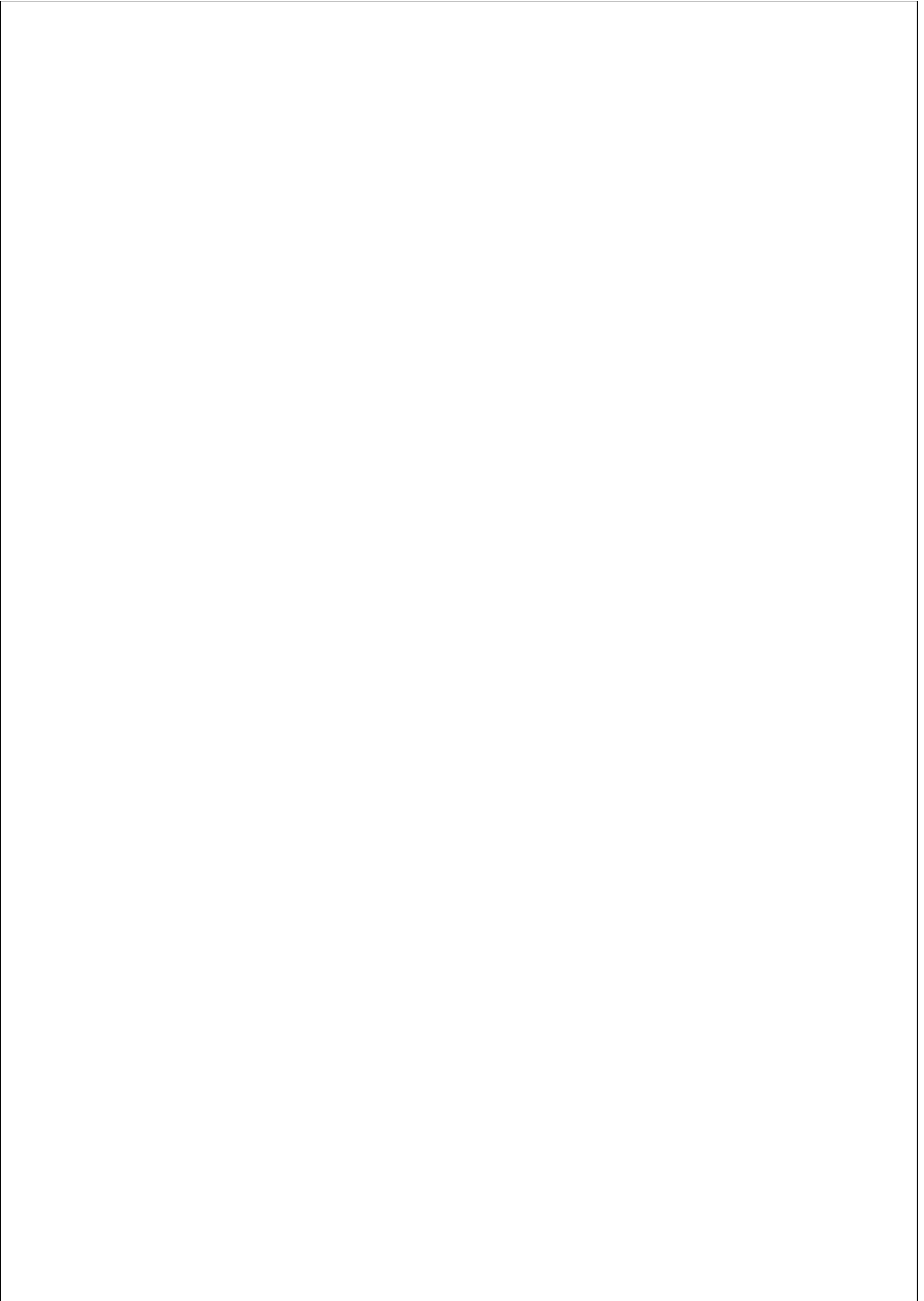
- [1] Barakabitze, A. A., Ahmad, A., Mijumbi, R., & Hines, A. (2020). 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, 167. <https://doi.org/10.1016/j.comnet.2019.106984>.
- [2] Ben Meriem, T., et al. (2016). ETSI White Paper No. 16 GANA - Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services (Issue 16). <https://bit.ly/3u0LN8d>.
- [3] Arzo, S. T., Naiga, C., Granelli, F., Bassoli, R., Devetsikiotis, M., & Fitzek, F. H. (2021). A Theoretical Discussion and Survey of Network Automation for IoT: Challenges and Opportunity. *IEEE Internet of Things Journal*.
- [4] Google. (n.d.). Welcome to Google Fi. Retrieved May 2, 2021, from <https://fi.google.com/about/>.
- [5] HMD Global. (2020). Introducing HMD Connect. The easier way to stay connected. HMD Connect. <https://www.hmdconnect.com/>.
- [6] Twilio Inc. (2021). Programmable Wireless. Twilio. <https://www.twilio.com/wireless>.
- [7] Telnyx LLC. (2021). Easily build and scale cellular IoT products with a single global SIM. Telnyx. <https://telnyx.com/products/wireless>.

- [8] Platt, S., Sanabria-Russo, L., Oliver, M. CoNTE: A Core Network Temporal Blockchain for 5G. *Sensors*. 2020; 20(18):5281. <https://doi.org/10.3390/s20185281>.
- [9] Platt, S., and Oliver, M. Towards Blockchain for Decentralized Self-Organizing Wireless Networks, 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1-5, doi: 10.1109/GCWkshps45667.2019.9024426.
- [10] Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q., & Zhang, Y. (2019). Blockchain and deep reinforcement learning empowered intelligent 5G beyond. *IEEE Network*, 33(3), 10-17.
- [11] Ekiz, N., Salih, T., Kucukoner, S., & Fidanboyly, K. (2015). An overview of handoff techniques in cellular networks. *International Journal of Information Technology*, 2(2), 1-5.
- [12] Cicioglu, M. (2021). Performance analysis of handover management in 5G small cells. *Computer Standards & Interfaces*, 75, 103502. <https://doi.org/https://doi.org/10.1016/j.csi.2020.103502>
- [13] Paul, L. C. (2013). Improvement in Wireless Communication. *Global Journal of Researches in Engineering Electrical and Electronics Engineering*, 13(16).
- [14] Ekiz, N., Salih, T., Kucukoner, S., & Fidanboyly, K. (2015). An overview of handoff techniques in cellular networks. *International Journal of Information Technology*, 2(2), 1-5.
- [15] Chen, Y. J., Hsu, T., & Wang, L. C. (2017, December). Improving handover performance in 5G mm-Wave HetNets. In *GLOBECOM 2017-2017 IEEE Global Communications Conference* (pp. 1-6). IEEE.
- [16] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10), 71.

- [17] Chaer, A., Salah, K., Lima, C., Ray, P. P., & Sheltami, T. (2019, December). Blockchain for 5G: opportunities and challenges. In 2019 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.
- [18] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184-1195.
- [19] Liang, Y. C. (2020). Blockchain for dynamic spectrum management. In *Dynamic Spectrum Management* (pp. 121-146). Springer, Singapore.
- [20] Carlberg, K., Burger, E. W., & Jover, R. P. (2019, October). Dynamic 5G Network Slicing for First Responders. In 2019 Principles, Systems and Applications of IP Telecommunications (IPTComm) (pp. 1-4). IEEE.
- [21] Natarajan, S., & Mohan, S. (2021, January). A Supervised Learning Approach for Reducing Latency during Context Switchover in 5G MEC. In 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-2). IEEE.
- [22] Zhu, G., Zan, J., Yang, Y., & Qi, X. (2019). A supervised learning based QoS assurance architecture for 5G networks. *IEEE Access*, 7, 43598-43606.
- [23] Mismar, F. B., & Hoydis, J. (2021). Unsupervised Learning in Next-Generation Networks: Real-Time Performance Self-Diagnosis. arXiv preprint arXiv:2104.06993.
- [24] Zhu, F., Ba, T., Zhang, Y., Gao, X., & Wang, J. (2020). Terminal location method with NLOS exclusion based on unsupervised learning in 5G-LEO satellite communication systems. *International Journal of Satellite Communications and Networking*, 38(5), 425-436.
- [25] Carrascosa, M., & Bellalta, B. (2019). Decentralized AP selection using Multi-Armed Bandits: Opportunistic Epsilon-Greedy with Stickiness. <http://arxiv.org/abs/1903.00281>

- [26] Shi, Y., Sagduyu, Y. E., & Erpek, T. (2020, September). Reinforcement learning for dynamic resource optimization in 5G radio access network slicing. In 2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.
- [27] Puspita, R. H., Shah, S. D. A., Lee, G. M., Roh, B. H., Oh, J., & Kang, S. (2019, October). Reinforcement learning based 5G enabled cognitive radio networks. In 2019 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 555-558). IEEE.
- [28] Xu, T., Zhou, T., Tian, J., Sang, J., & Hu, H. (2020). Intelligent spectrum sensing: When reinforcement learning meets automatic repeat sensing in 5G communications. *IEEE Wireless Communications*, 27(1), 46-53.
- [29] Khujamatov, K., Ahmad, K., Reypnazarov, E., & Khasanov, D. (2020). Markov Chain Based Modeling Bandwith States of the Wireless Sensor Networks of Monitoring System. *International Journal of Advanced Science and Technology*, 29(4), 4889-4903.
- [30] Yu, K., & Sato, T. (2019). Modeling and analysis of error process in 5G wireless communication using two-state Markov chain. *IEEE Access*, 7, 26391-26401.
- [31] Dutta, H., & Biswas, S. (2021, January). Towards Multi-agent Reinforcement Learning for Wireless Network Protocol Synthesis. In 2021 International Conference on COMMunication Systems & NETWORKS (COMSNETS) (pp. 614-622). IEEE.
- [32] Li, M., & Li, H. (2020). Application of deep neural network and deep reinforcement learning in wireless communication. *Plos one*, 15(7), e0235447.

- [33] He, Q., Moayyedi, A., Dan, G., Koudouridis, G. P., & Tengkvist, P. (2020). A meta-learning scheme for adaptive short-term network traffic prediction. *IEEE Journal on Selected Areas in Communications*, 38(10), 2271-2283.
- [34] Hirschberg, D. S. (1980). On the complexity of searching a set of vectors. *SIAM Journal on Computing*, 9(1), 126-129.
- [35] Gagniuc, P. (2017). *Markov Chains: From Theory to Implementation and Experimentation*. USA, NJ: John Wiley & Sons. pp. 9-11. ISBN 978-1-119-38755-8.
- [36] Oliver, M., and Borrás, J. Performance evaluation of variable reservation policies for hand-off prioritization in mobile networks, *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No.99CH36320)*, 1999, pp. 1187-1194 vol.3, doi: 10.1109/INFOCOM.1999.751675.
- [37] Platt, S. (2021). *5G Mobility Simulator*. Github. <https://github.com/stevenplatt/5G-mobility-simulator>.



Chapter 7

CONCLUSIONS

In this thesis we investigate the general application of blockchain technologies in cellular networks with a goal of finding general patterns of compatibility between the two.

With a base understanding that blockchain technologies can provide a facility for peer-to-peer coordination and decentralization, our early investigation takes a view through the perspective of enhancing existing resource coordination and sharing mechanics, but even this framing leaves the question of finding the best fit, overly broad. Within the large range of operations occurring within a cellular network, the first step on this path was to place blockchain within the context of existing cellular network mechanics. This thesis presents the TCP-Air interworking model for this goal. In this framing, the cellular network is placed as central and the expectation is set that blockchain as a technology in early development was to be viewed as a system which could and should be modified to fit cellular deployment - rather than the inverse of changing the long-standing behaviors of cellular design. The TCP-Air model as presented in this thesis represents a "day 1" understanding of fit between the two systems and much has evolved in the 3 years since that initial writing. While accounting for the rapid blockchain development that occurred during this investigation, the science still holds that blockchain as a data structure continues with certain native traits - including limits on scalability inherited through

linear time-ordered forward hashing. On this basis, the TCP-Air model proves a higher compatibility can be had through deploying blockchain for operations that are less time sensitive and often within the cellular core. Chapter 3 presents early results from this understanding through a decentralized access control deployment running on the OpenWRT WiFi platform.

With a formalized focus presented in chapter 3, the core contribution of this thesis is the CoNTe blockchain protocol presented in chapter 4. Due to the broad and undeveloped nature of the topic, it became the author’s intention to present in the remainder of the thesis, a framing that could show the implication of blockchain deployment on the cellular model holistically. Starting in chapter 4 this begins with the CoNTe blockchain protocol that is custom designed to operate at the network core. The key finding of this design is a proof that blockchain can be made use-case agnostic or general purpose in cellular design; a behavior to the authors knowledge remains unique in the body of research. By proposing a wholly new blockchain design that is tuned to the behavior of cellular networks, this thesis details a system that can be deployed as a virtual network function and by extension be made compatible with global cellular standards such as those from ETSI and the 3GPP. This compatibility is made possible by removing currency and contract mechanics that have become synonymous with blockchain technologies. Doing this removes the necessity of incenting cooperation through direct payments or perpetually increasing the blockchains’ length to guarantee security. It is perhaps easiest to view the consensus model deployed within CoNTe as being functionally similar to how existing route updates work in the global internet. The system in total functions because of the formalized trust of individual network peers with their neighbors; except that CoNTe adds immutable accounting and verifiability of updates within a decentralized blockchain ledger.

Chapter 5 of this thesis moves the contributions of the CoNTe design and presents it in the context of a network deployment which utilizes the targeted cellular standards; in this example the ETSI GANA architecture for autonomic cellular deployment. Using the ETSI GANA model, the

authors show the composition of a 5G network which deploys blockchain as decentralized storage within its network functions. Using this format of deployment we show that it becomes possible to enable sharing of information peer-to-peer to deliver virtualized network functions that are coordinated across independent network providers. The ETSI GANA model as presented in Chapter 5 effectively takes the toy model of distributed access control presented in chapter 3 and expands it to include all network services which are serviced through combinations of 3GPP-compliant network functions. Taken in aggregate, this makes possible the model of decentralized cellular overlays for which the thesis is titled, but it does not yet extend the theory to the user equipment device at the network edge.

The research line of this thesis concludes in chapter 6. Until this point, the research has focused entirely on the cellular network core and services within. The contribution of chapter 6 is to take these contributions and extend them to the network edge to show impacts on individual users and user equipment accessing the cellular resources without a central control. The chapter presents a model of transition learning that proves individual devices as capable of navigating changes in network condition without direct orchestration or augmentation from network base stations. It does this by modifying already existing mechanics of mobile-controlled cellular network hand-off. Earlier portions of this thesis present use cases such as public utilities and emergency response as use cases for decentralized services without direct ownership; chapter 6 is included to provide scientific support to show such use cases are theoretically possible. At the conclusion of research presented in chapter 6, this thesis completes a research line which began with defining a general *fit* of behaviors between blockchain technology and cellular networks, and extends from there to deliver a cellular-native blockchain design, a standards compliant deployment model, and an enhanced model of mobile-controlled hand-off to take advantage of the paradigm from individual devices and user equipment at the furthest points from the network core.

7.1 Future Research

With the completion of this thesis, the reader is encouraged to interpret the findings as early results, and representing only a single format among many for how blockchain and cellular networks can evolve to complement each other. Throughout this document, an intentional focus is placed on the general compatibility of blockchain and its corresponding impact, with limited direct comparison to the performance and mechanics of systems such as Ethereum or the cryptocurrency economy at large. It is the authors opinion that these areas are outside the intended focus of this research, but they do offer a path to carry the presented research line into the future as performance references for security and scalability. An additional area for future research is a deeper investigation of identity within the context of blockchain and network communication. The concept of identity is listed as an early research question at the start of this thesis. In this initial context, the intention was to provide coverage for understanding *device* identity which is requisite for managing machine interaction. As research progressed in this area, it became understood that identity or lack thereof was a much larger investigation than could be covered fully in this work. In current form, the evaluation of both machine and user identity are identified as a gap that can be enhanced with additional research. The authors believe that expanding the current thesis work along these additional paths would contribute greatly to the potential adoption of cellular standards compatible blockchain and blockchain decentralised overlay services.

Appendix A

THE CONTE CSMA/CD ALGORITHM

Algorithm 5: CoNTe CSMA/CD Algorithm

```

1: while True do
1:   min_node = random_node;
1:   min_node.queue = infinity;
   // pick node with shortest back-off;
2:   for node in nodes do
2:     current.back-off = min_node.queue[0];
3:     if len(node.queue)  $\leq$  0 and min_node.queue[0]  $\leq$  node.queue[0] then
3:       min_node = min_node;
4:     else
4:       node;
5:     end if;
6:   end for
   // transmit block;
7:   for node in nodes do
7:     collision_occurred = false;
   // check if collision occurs;
8:     if node.location  $\neq$  min_node.location and len(node.queue)  $\leq$  0 then
8:       delta_location (min_node.location - node.location);
9:       if node.queue[0]  $\geq$  (current.back-off +  $V_{prop}$ (delta_location)) then
9:         will_collide = True;
10:      else
10:        will_collide = False;
11:      end if
12:      if will_collide then
12:        transmitted_packets += 1;
12:        node.collisions += 1;
12:        node.queue[i] = node.exp_back-off_time;
13:      end if
14:      else
14:        successfully_transmitted_packets += 1;
14:        min_node.pop(packet);
15:      end if
16:    end for
17:  end while

```

Appendix B

RETIRED RESEARCH PATHS

During the development of this thesis, a number of research paths were explored and later abandoned. These research paths were terminated for a variety of reasons that are summarized in this appendix.

B.1 BSAFE.Network Consortium

Because UPF is in early stages of blockchain research, an effort was made to engage with the larger research community. Outside of attending meetup groups in Barcelona, this resulted in UPF joining the *BSafe.network* blockchain consortium in 2019 [1].

BSafe.network is a university research network for blockchain technologies, formed in 2017; it is not a formal administrative partnership, rather an informal cooperation among university researchers at participating institutions to jointly research blockchain technologies. At the time of writing, there are 31 institutions participating in the joint effort, including Massachusetts Institute of Technology, University of British Columbia, Telecom SudParis, and now UPF. To join the research consortium, it is required to setup a bitcoin blockchain node within the research network, beyond this, members of the research consortium coordinate and plan with periodic web meetings and a dedicated Slack group chat instance.

The most mature work happening within the network is relating to

’layer 2’ scaling of Bitcoin technology, but a number of participating universities have multiple research efforts existing outside of Bitcoin. After it was decided that Bitcoin was not the desired platform to build the thesis research, participation in the consortium was reduced.

B.2 University of Cape Town Research Stay

The final year of research for this thesis was planned to be a research stay at the University of Cape Town in South Africa. A final research plan and approvals were issued by both Universitat Pompeu Fabra (home university) and the University of Cape Town (visiting university), but were ultimately cancelled due to the SARS-CoV-2 pandemic which was nearing a peak ahead of the planned research stay [2].

B.3 Blockchain For Pandemic Response

As vaccines for the COVID-19 pandemic begin global roll-out, researchers for the first time are able to look retrospectively at the variety of avenues taken to address the rapid pandemic spread and their success in adoption. Among these avenues, Blockchain has seen new research applications in digital contact tracing, vaccine supply chain, and the broader electronic medical record ecosystems reaching broad publication in recent months, among others. As a system without a defined owner, blockchain does not inherit a natural fit in crisis applications where there remains a desire for leadership and central authority. This appendix section holds research that was completed during the primary PhD investigation, but are outside of the core thesis topic. The remainder of this appendix is the full contents of the resulting paper¹, recorded for posterity.

¹Della Valle, F., Platt, S., Oliver, M., ”Review of Blockchain for Pandemic Surveillance and COVID-19 Response”, Electronics, Submitted - Under Review, June 2021.

B.3.1 Introduction

At the time of writing, the novel Coronavirus 2019 or COVID-19 is reported to have infected over 90 million persons while amassing close to 2 million fatalities globally [3]. Traditional paths of addressing the pandemic spread have included social distancing, travel restrictions, administration of antiviral pharmaceuticals, and most recently, delivery of approved vaccines to inoculate the world population. Each of these tasks in isolation has proven to require government scale coordination and increasing cross-border collaboration as the pandemic period has extended, introducing further complication. Viewing COVID-19 in this largest of scales highlights the difficulty of halting a contagion when no single party is in control and no single party has a complete view of the pandemic spread. In this case, the question of who owns, organizes, and is the authority of truth on the shared data is uniquely suitable to the strengths of blockchain database storage. This appeal is further heightened during pandemic events when the variety of organizations reporting data can be quite broad, making data non-uniform as well as in cases when centralized reporting is under-developed or otherwise restricted.

Blockchain as a technology has the unique ability to both decentralize and secure data, while not requiring a direct owner. As a database technology, blockchain in theory, can supplement any application for the purpose of storing data. This data can be internal-use only, decentralized among a consortium, or fully decentralized. Within these data models, varying access models can be applied, such as permissioned or permissionless, and further architecture choices such as how finality and consensus are handled all contribute to its fit for a chosen purpose. Due to the rigid nature of blockchain as an immutable record, care must be given to the initial design and values that are proposed for blockchain storage, with the total deployment deferring to the domain specific context suiting the needs and workflows of the intended end user, whether they be a financial institution, or a medical facility handling records in the COVID-19 related categories previously mentioned.

In developing this paper, the author’s initial intent was to identify po-

tential gaps within the existing body of blockchain research addressable to COVID-19, and propose a technical solution, a new blockchain-based system that fit a previously unidentified demand. It is now understood and proposed by the authors however, that blockchain as a database has achieved a level of maturity as an IT system; such that in most cases, where there is a database, there could also exist blockchain. The authors instead for this paper, intend to deliver a timely review of recent research proposing the use of blockchain to present a holistic view for blockchain applications in pandemic surveillance and COVID-19 response.

The remainder of the paper is organized into five sections. The first details the general medical perspective of pandemic surveillance prior to blockchain and COVID-19. This medical perspective is followed by sections detailing recent blockchain-specific research intended to service IT systems within the ecosystem of pandemic and COVID-19 response. Last, the paper is concluded with a discussion, providing a final summary of the paper and proposing paths for future research.

B.3.2 Pandemic Surveillance Prior to Blockchain

Prior to the 2019 COVID-19 pandemic, over a century of medical experience, dating to before the Spanish Flu pandemic of 1918 up through the SARS coronavirus identified in 2002, medical professionals have established and matured methods of identifying and tracking pandemic spread events [4]. Before highlighting blockchain applications for pandemic surveillance, it is important to raise the medical perspective of such applications. Doing this allows a level of understanding for who are the users of such applications and the corresponding needs. It also gives context to the types of data being stored in such systems and how this data is used. An example of such methods is the SEIR model, an acronym representing Susceptible, Exposed, Infectious, and Recovered [5]. With a limited set of standard data points, such as incidents of infection, researchers are able to probabilistically calculate rates of spread, and the impact of containment measures such as travel bans and quarantine [5]. When combined with health outcomes data, researchers can calculate durations of incubation,

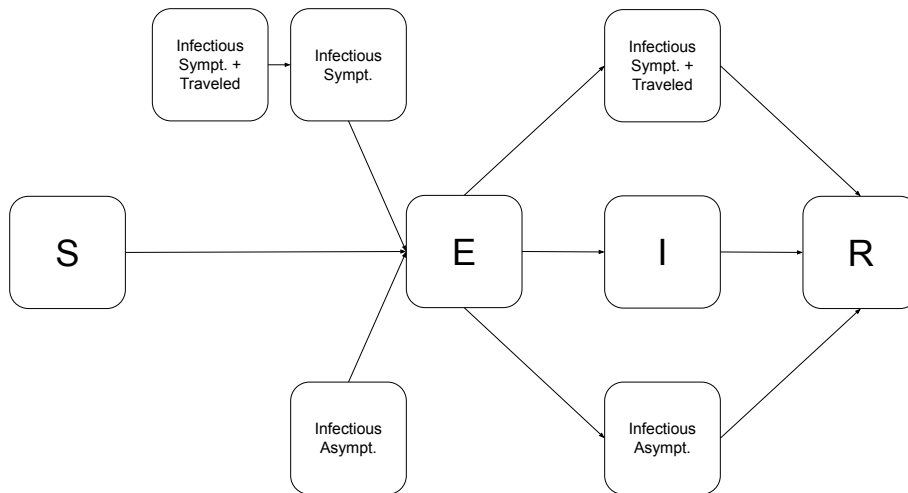


Figure B.1: An example SEIR model, accounting for asymptomatic spread, and spread originating from travel. Adapted with permission from [6].

active infection, and mortality rates. Further combining these with mechanics such as contact tracing can allow the surfacing of nuanced scenarios, where infection occurs and a portion of infected individuals are asymptomatic (Figure B.1.) [6].

Viewing pandemic data at this high level brings into the focus a natural fit for blockchain, where there is an extreme incentive for the sharing of data, but direct coordination may not be possible. Storing this data in a blockchain could also allow more flexibility in who reports data, and the type of data reported. This is significant in scenarios where health systems are not mature, or there are otherwise not sufficient resources to enable strong centralized government reporting.

Making reporting more accessible in this way also has a secondary benefit in making pandemic data more representative. Take for example, the case of imposed travel restrictions during a prolonged pandemic event. In the period between first identification, and the widespread distribution of vaccine resources, a contagious virus can experience seasonality and cross border transmission from regions that are not restricted due to lack of reported data [7]. As a contrast to control on border crossings and domestic mobility, researchers have also investigated and present the global coordination of vaccine and antiviral distribution as a more effective alternative [7]. Such a model is only effective however, to the extent that reported data is representative of actual spread and rates of infection, and a pervasive view of pandemic spread is available.

B.3.3 Blockchain For Digital Contact Tracing

As a system without blockchain technology, the recently released contact tracing system produced by Apple and Google is an oft-cited research reference. The system developed by Apple and Google runs on a user’s smartphone and is designated as opt-in. Once the user opts in, the system relies on bluetooth beacons to listen for other devices which are nearby [8]. By recording these proximity histories, the system can notify users if they have been nearby a person who has tested positive for COVID-19. The system is able to do this because all histories are stored centrally with Apple and Google, who are then able to perform the matching. To provide a level of privacy to these highly central records, the system relies on the identity provided by the bluetooth beacon, which is software generated, rotated on a schedule, and not directly related to the individual person’s identity at a hardware level. Even in this context, the system has been identified as being vulnerable to trajectory mapping, due to the total histories being visible to Apple and Google who are also the only parties who can identify the real world device and user corresponding to temporary bluetooth identities [8].

Organizations who choose to use this format of digital contact tracing make a trade-off between its centralization/privacy and pervasive avail-

ability. Outside of the Apple and Google models, a variety of government developed systems provide additional variety of implementation in digital contact tracing. These include Singapore’s TraceTogether [9], which also runs on user smartphones to collect bluetooth proximity data, but uses real identity stored directly with the central government. There is also China’s Health Code system [10], which requires users to scan barcodes when entering dense areas such as shopping malls, hotels, and restaurants. Data in China’s Health Code system also uses real identity, stored directly with the central government. The system diverges from the Singapore model in that it is less automated and does not rely on bluetooth or other hardware to remain active in user equipment. The Health Code system can be seen as a lighter weight implementation, but is also more enforceable as the QR code scanning is physically enforced in real world locations and cannot be easily bypassed. At a macro level, each of these systems, while appearing general in design, are modeled for a specific audience, each placing differing emphasis on factors such as privacy, enforceability, and technical complexity.

Extending the models previously mentioned, BeepTrace is a recent research proposal that adds blockchain to the contact tracing infrastructure and places its emphasis on user privacy [11]. Similar to the Apple and Google model, BeepTrace relies on voluntary user participation, but differs in most other technical aspects in that it separates all the functions of the system, to have them operated by independent parties. While also running an application on the user phone, BeepTrace does not rely solely on bluetooth beacons for location, it instead proposes tagging location from WiFi, GPS, and cellular towers, in addition to bluetooth beacons. The additional methods of location tagging allows for tracking environment exposure, even under a sparsity of other people; such as a factory location where surfaces, rather than people have been exposed to a person with a positive COVID-19 diagnosis. Figure B.2 shows the full BeepTrace framework and its component parts.

In fact, this tracking for exposure of a location, rather than an individual has been consistently highlighted as a function not easily served by existing digital contact tracing solutions. Location exposure, rather than

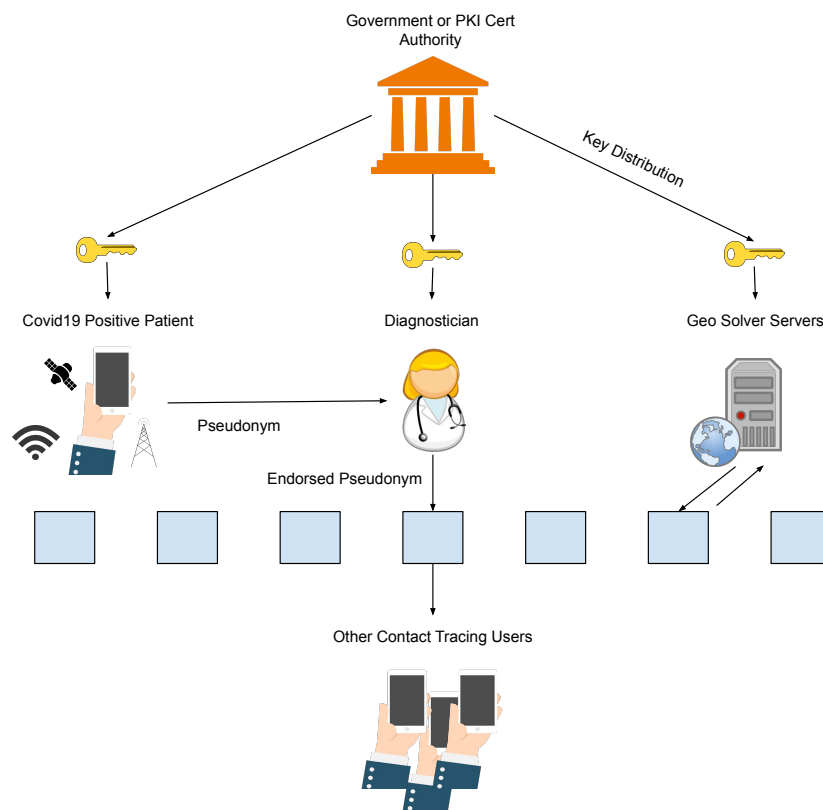


Figure B.2: The BeepTrace COVID-19 tracking framework. Adapted with permission from [11].

people exposure was specifically targeted by Klaine et al, who present a model where WiFi and bluetooth radios are stationary and installed to points of interest to record to a blockchain, occurrences of exposure with persons diagnosed with COVID-19 [12]. In these cases, as well as the Apple and Google case, the identities being matched are anonymized and stored for a trailing period, usually 14 days, to allow matching confirmed cases with instances of exposure retroactively.

B.3.4 Blockchain For Electronic Medical Records

Akin to Industry 4.0, Medical 4.0 has been defined by R. Vaishya et al. as a set of algorithms which help provide real-time information to all the strategic partners in order to bring traceability to the process of disease control through the effective management of the medical supply chain [13]. To deliver this advancement with sensitive medical data, cryptography played a fundamental role guaranteeing the privacy in medical treatments, protecting all sensitive information involved. Given that a blockchain is characterized by robust cryptographic protocols, it might mislead practitioners in deploying blockchain for medical purposes without additional care given to the specifics of the data being stored. In fact, blockchain for Medical 4.0 needs to be carefully designed to assure privacy, and not to publish sensitive information where not allowed. A good balance between data accessibility and data protection is needed [14]. Additionally, practitioners need to take into consideration that the current cryptographic protocols deployed in current blockchains may become obsolete in the next few years, and if sensitive information goes on the blockchain, these data may become public or otherwise become easier to attack in the future, if not deployed in the suitable context.

According to S. Peng et al. a double-level blockchain can be employed to reduce these risks [15]. A double-level means to design a blockchain infrastructure with a higher interoperability, allowing a close interaction between both public (external) and private (internal) blockchains that are maintained separately [15]. This public-private structure allows to mitigate the risks of privacy, keeping sensitive information on the pri-

vate blockchain, whilst in the public one would be permitted to share a larger amount of encrypted data, without fear of privacy leaks [15].

An effective management of the electronic medical records in the medical ecosystem, can foster real time information sharing to all strategic partners, helping the traceability in the process of disease control [13]. In fact, a blockchain-based disease control system can break down data silos, impacting on public and government agencies for local and regional pandemic management. An additional blockchain feature that has been presented as having a specific fit in sharing electronic medical records is the implementation of data oracles which allow integration of external data into blockchain logic or controls. Deploying data oracles in this context allows an alternate method of gating access to sensitive data, while ensuring trust to these data sources by making their public records auditable and immutable [16][17].

B.3.5 Blockchain For Vaccine Supply Chain

Supply chain management (SCM) is an established and essential business process in every organization today. A traditional industrial supply chain is composed of the total of systems required to deliver an end-to-end business process, service, or product. Supply chain management in this classic context the practice of organizing all the data generated by these systems, and is usually aggregated and actioned on, within an Enterprise Resource Planning (ERP) system. As advanced under Industry 4.0, these systems became updated to include higher levels of connectivity, pervasive data, and machine automation. This means that systems producing or consuming resources within a supply chain can self-report, or receive live updates on contingent activities elsewhere in the supply chain. In application, these advances help address information asymmetry which can lead to poor supply chain outcome.

Within the broader context of industrial supply chains, are so-called cold chains which apply supply chain management practices to the production of goods which have the additional constraint of requiring a controlled cold storage environment to prevent damage or expiration. This

body of knowledge focused on cold chain management has served as a starting point of supply chain delivery of temperature-controller COVID-19 vaccines from Moderna Inc, Pfizer Inc and BioNTech SE. This connection can reduce information asymmetry along the cold chain management and reduce management costs, optimizing the long-term freezing conservation. For instance, if the infection ratio is considerably growing in a specific area, a blockchain-based system can promptly provide real-time information for the whole ecosystem and actors involved. This generates faster dynamics for decision making procedures, saving lives.

A blockchain-based medical supply chain can be implemented to supervise the vaccine supply chain and the demand forecasting. B. Yong et al. propose the following specific information be considered in the design phase of a blockchain-based vaccine supply chain are: a) batch packaging record, b) batch production record, c) inspection record, and d) inoculation record of vaccines [19]. In their research, the authors remarked the importance of sending to regulators and institutions entities all the required information in an automatic manner. This can foster the supervising of vaccine chains and it can be achieved by blockchain functionalities to assure control. Also the demand forecasting can be deployed with blockchain stored data, thanks to real-time information, it can reduce costs and improve forecasting within vaccine cold chains by allowing the identification of the need of vaccine per area, enhancing the distribution efficiency of vaccines and reducing the information asymmetry [14]. This can provide a relevant performance improvement of the vaccine storage, given that the current COVID-19 vaccines needs to be kept at temperatures as low as a low minus 70 Celsius for proper conservation [21].

Because blockchain technology is a performance improvement for supply chains [20], efficiency and effective management of medical supply chains can be clearly identified. With a focus on the cold chain management of COVID-19 vaccine, enhancing distribution and logistics aspects, it can directly reduce costs for stakeholders involved [22]. In a global perspective, a proper management of the cold supply chain impacts on the quality and integrity control in the distribution process. According to R.H. Bishara et al. a monitoring program is essential for cold chain

management in pharmaceutical products [22]. For instance, MediLedger pilot project (mediledger.com) achieved some interesting outputs on implementing blockchain technology for the US pharmaceutical industry, increasing trust and safety in the medical supply chains.

B.3.6 Discussion

As blockchain research has matured, there has been an increasingly clear isolation of blockchains’ role as simple storage. To the extent that an application makes use of a database to store information, it can be paired with blockchain storage for its intended effect. After an exploration on commonly used medical procedures for pandemic surveillance, technical blockchain-based solutions (and use cases) have been analysed and discussed, with a sharpening focus on: electronic medical record, digital contact tracing, vaccine supply chain, as they interconnect as part of current COVID-19 pandemic response. Specific care is taken to surface both the benefit and risks of each application.

Taken at a macro level, three trends among the current body of research are notable. The first is a broad risk of overfitting blockchain applications to a narrow and singular use. This most often appears in the form of precise data structures being defined in research experiments. A number of current designs identify a fixed format of block data, a clearly defined user, or a single workflow. Performance measures and comparisons taken against these fixed values make comparison and later reuse more difficult. It applies an amplification of the already rigid structure of blockchain storage in the designs that are being defined. A possible solution for this would be placing an increasing focus on data interoperability as seen in general supply chain and vaccine cold chain applications, where the mix of data, and the users of the data are assumed to be flexible at the start.

A second trend of note is the continued tension between ownership and authority. A large incentive for deploying blockchain technology is the ability to operate and update the blockchain system without a central owner. This however is distinct and separate from not having a central

authority. Taking the provided example of contact tracing applications, the lack of central owner in these systems can also introduce a bias that places the burden of providing data, or of system operation, on individuals. In the specific case of COVID-19 response, this is undesirable in many cases, because the entity requesting the data, or ultimately actions on the data in many cases is a central authority. A blockchain system which does not allow for this flexibility would be precluded from replacing IT systems such as Singapore’s TraceTogether and China’s Health Codes. A recommendation in this scenario is the investigation of more modular blockchain designs, which allow various parts to be enabled, disabled, or replaced; where blockchain does not extend beyond its function as storage, and is not allowed impact on the workflows elsewhere in the system. Returning to the very beginning, the SEIR model of pandemic surveillance provides a good example. When abstracted, scientists adhering to the SEIR model in COVID-19 surveillance may only need a dashboard of the SEIR model counts. Underneath these counts may exist any number of blockchain systems, combining all the systems mentioned in this writing. The system described in effect would serve as a meta pandemic response supply chain. To the author’s knowledge, at the time of writing, such a blockchain system does not exist and is proposed as a possible path of future research.

B.4 Spectrum Protocol

During the first year of investigation, the original title of this thesis was planned to be *“Channel Chain: Blockchain for Automated Channel Selection and Access Control in Shared Spectrum Networks”*. This title reflected the initial intention to choose a single well defined use case with an existing demand for resource sharing, where blockchain could find a complementary fit.

This research line was carried through to include the experimental blockchain that was developed and implemented atop the OpenWRT platform and outlined in chapter 2 of this thesis. After this chapter 2 experi-

ment, development began for a corresponding web platform which at the time was named "*Spectrum Protocol*" and was intended to serve as a dashboard showing the device connection states across a pool of shared bands and various contract permissions. A prototype of the platform was completed, but was eventually abandoned due to software limitations in the OpenAirInterface [23] and Host Identity Protocol [24] applications, which were planned as the platforms for extended the prototype to complete the second half of the thesis. To prove the functionality of the Spectrum Protocol platform, the goal was to deploy a 5G testbed where devices roamed freely across bands, while maintaining persistent sessions with working routing. To achieve this, the earlier designed intended to rely on OpenAirInterface to deliver resource slices from multiple multitenant 5G cores, while Host Identity Protocol running on the device abstracted IP changes by replacing the IP with a Host Identity Tag that could be carried across networks to maintain state. At the time of writing both of these features were still at an experimental stage.

For posterity, the original programming code for the Spectrum Protocol prototype has been open sourced and is available at Github [25]. An image of this early Spectrum Protocol dashboard can be seen in figures B.3, B.4, B.5, B.6, B.7, and B.8.

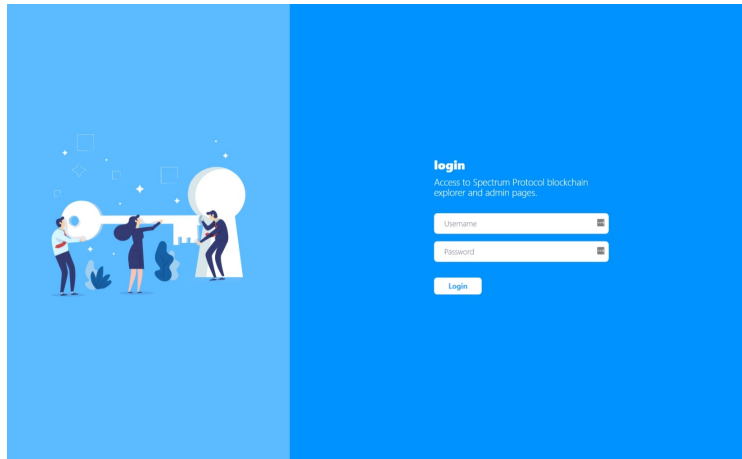


Figure B.3: The Spectrum Protocol login page.

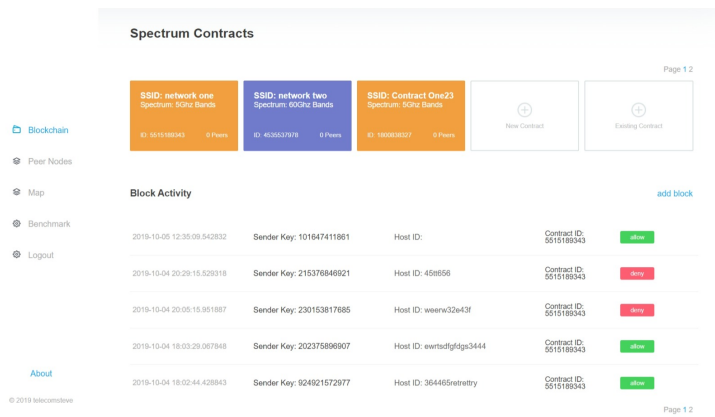
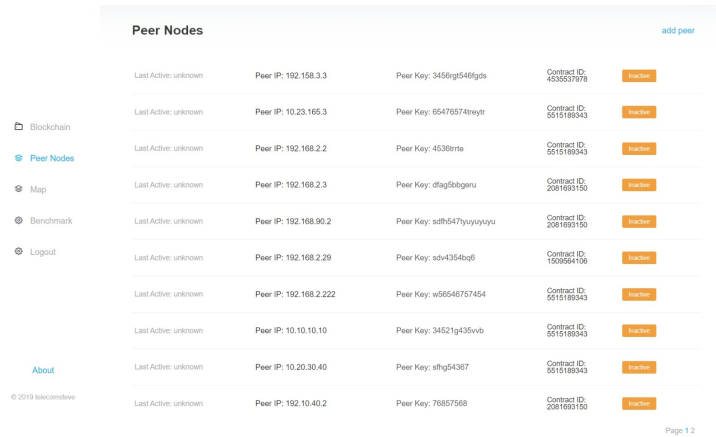


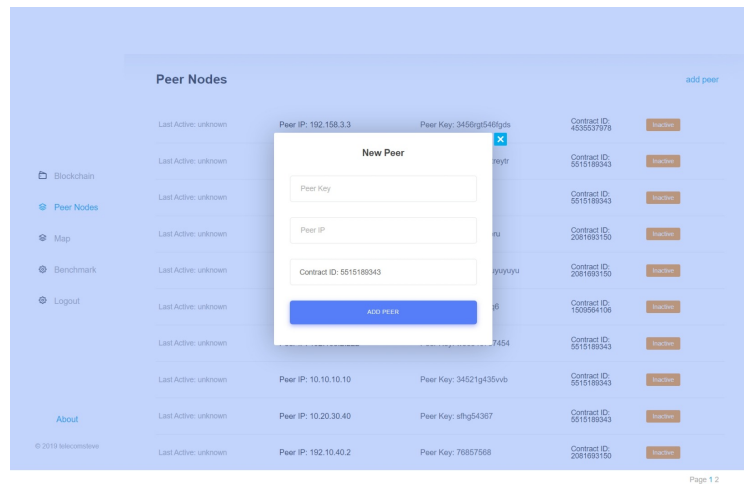
Figure B.4: The Spectrum Protocol main dashboard. On the main dashboard, active contracts with corresponding frequency bands as well as recent activity are displayed.



The screenshot shows a web interface titled "Peer Nodes" with a sidebar on the left containing navigation links: Blockchain, Peer Nodes (selected), Map, Benchmark, Logout, and About. The main content area displays a table of peer nodes. Each row includes a "Last Active" status (all are "unknown"), a "Peer IP", a "Peer Key", a "Contract ID", and an "Inactive" button. The table contains 10 rows of data.

Last Active	Peer IP	Peer Key	Contract ID	Action
unknown	192.158.3.3	3456rg546fgds	453537978	Inactive
unknown	10.23.165.3	65476574weyfr	5515189343	Inactive
unknown	192.168.2.2	4530rte	5515189343	Inactive
unknown	192.168.2.3	dfag5bbgenu	2081693150	Inactive
unknown	192.168.90.2	sdff547yuyuyuy	2081693150	Inactive
unknown	192.168.2.29	sdv4354bqf	1509564106	Inactive
unknown	192.168.2.222	w56546757454	5515189343	Inactive
unknown	10.10.10.10	34521g435vnb	5515189343	Inactive
unknown	10.20.30.40	slfg54367	5515189343	Inactive
unknown	192.10.40.2	78857568	2081693150	Inactive

Figure B.5: The peer nodes page displaying core networks (by IP) and the sharing contracts they are connected to.



The screenshot shows the same "Peer Nodes" page as Figure B.5, but with a "New Peer" modal form open in the center. The form has three input fields: "Peer Key", "Peer IP", and "Contract ID: 5515189343". Below the fields is a blue "ADD PEER" button. The background table is dimmed.

Figure B.6: Adding a new network core into the Spectrum Protocol platform.

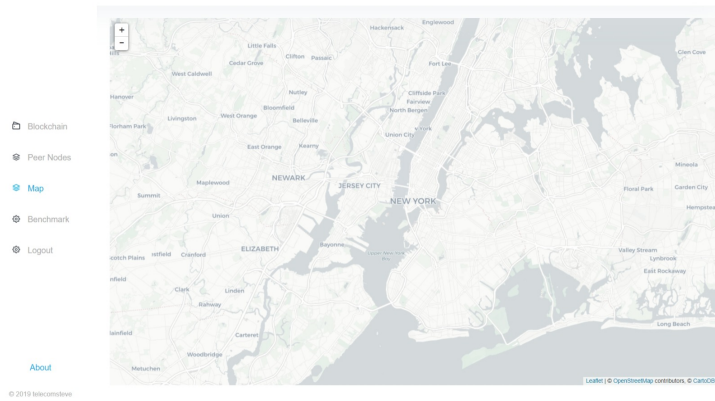


Figure B.7: The map page was intended to show the physical location of base stations and their calculated coverages.

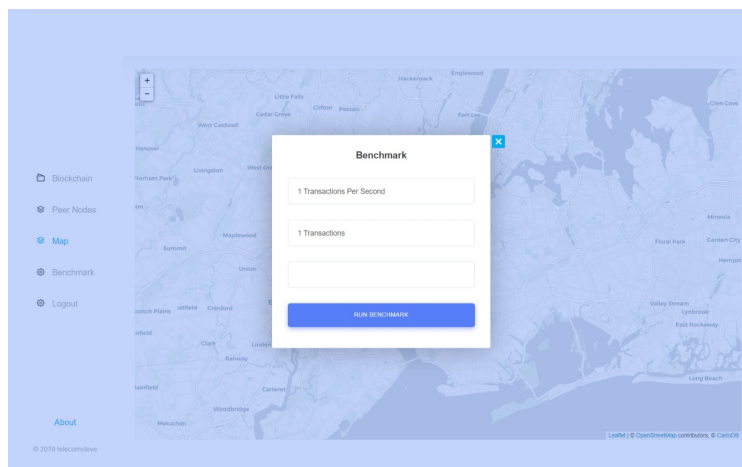
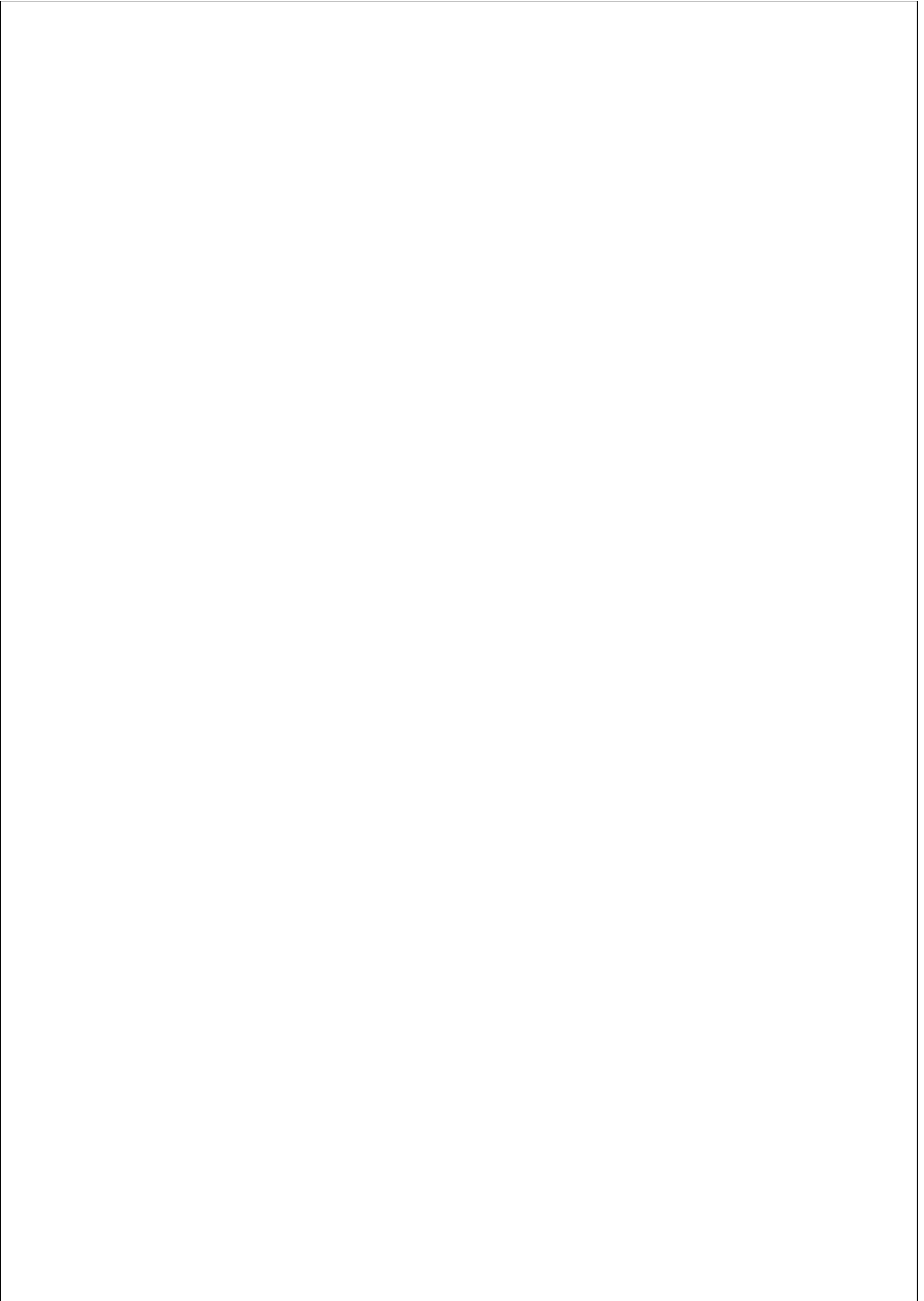


Figure B.8: A benchmark tool was planned for the Spectrum Protocol dashboard as an easy way to run scripted load tests.



Bibliography

- [1] BSafe.network. BSafe.network, The Research Network for Blockchain Technology. 2017. Available online: http://bsafe.network/WhitePaper_BSafe_20170509_v103.pdf (accessed on 16 June 2021).
- [2] Centers for Disease Control and Prevention. (n.d.). Coronavirus Disease 2019 (COVID-19). Centers for Disease Control and Prevention. <https://www.cdc.gov/coronavirus/2019-ncov/index.html>. (accessed on 16 June 2021).
- [3] John Hopkins University. Covid-19 dashboard by the center for systems science and engineering (csse) at John Hopkins university (jhu). [Online]. Available: <https://coronavirus.jhu.edu/map.html>
- [4] Bertozzi, A. L., Franco, E., Mohler, G., Short, M. B., & Sledge, D. (2020). The challenges of modeling and forecasting the spread of COVID-19. *Proceedings of the National Academy of Sciences of the United States of America*. <https://doi.org/10.1073/pnas.2006520117>
- [5] Cooper, B. S., Pitman, R. J., Edmunds, W. J., & Gay, N. J. (2006). Delaying the international spread of pandemic influenza. *PLoS Medicine*. <https://doi.org/10.1371/journal.pmed.0030212>
- [6] Colizza, V., Barrat, A., Barthelemy, M., Valleron, A. J., & Vespignani, A. (2007). Modeling the worldwide spread of pandemic influenza: Baseline case and containment interventions. *PLoS Medicine*. <https://doi.org/10.1371/journal.pmed.0040013>

- [7] Grais, R. F., Ellis, J. H., & Glass, G. E. (2003). Assessing the impact of airline travel on the geographic spread of pandemic influenza. *European Journal of Epidemiology*. <https://doi.org/10.1023/A:1026140019146>
- [8] Google, & Apple. (2020). Privacy-Preserving Contact Tracing - Apple and Google. [Online]. Available: <https://covid19.apple.com/contacttracing>.
- [9] Huang, Z., Guo, H., Lee, Y. M., Ho, E. C., Ang, H., & Chow, A. (2020). Performance of digital contact tracing tools for COVID-19 response in Singapore: Cross-sectional study. *JMIR MHealth and UHealth*. <https://doi.org/10.2196/23148>
- [10] Liang, F. (2020). COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China. *Social Media and Society*. <https://doi.org/10.1177/2056305120947657>
- [11] Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W. B., & Imran, M. A. (2020). BeepTrace: Blockchain-enabled Privacy-preserving Contact Tracing for COVID-19 Pandemic and Beyond. *ArXiv*. <https://doi.org/10.1109/jiot.2020.3025953>
- [12] Klaine, P. V., Zhang, L., Zhou, B., Sun, Y., Xu, H., & Imran, M. (2020). Privacy-Preserving Contact Tracing and Public Risk Assessment Using Blockchain for COVID-19 Pandemic. *IEEE Internet of Things Magazine*. <https://doi.org/10.1109/iotm.0001.2000078>
- [13] Vaishya, R., Haleem, A., Vaish, A., & Javaid, M. (2020). Emerging Technologies to Combat the COVID-19 Pandemic. *Journal of Clinical and Experimental Hepatology*.
- [14] van Engelenburg, S., Janssen, M., & Klievink, B. (2018, July). A blockchain architecture for reducing the bullwhip effect. In *International Symposium on Business Modeling and Software Design* (pp. 69-82). Springer, Cham.

- [15] Peng, S., Hu, X., Zhang, J., Xie, X., Long, C., Tian, Z., & Jiang, H. (2020). An efficient double-layer blockchain method for vaccine production supervision. *IEEE Transactions on NanoBioscience*, 19(3), 579-587.
- [16] Marbough, D., Abbasi, T., Maasmi, F., Omar, I. A., Debe, M. S., Salah, K., ... & Ellahham, S. (2020). Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. *Arabian Journal for Science and Engineering*, 1-17.
- [17] Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2020). Blockchain and COVID-19 Pandemic: Applications and Challenges.
- [18] Banerjee, A. (2018). Blockchain technology: supply chain insights from ERP. In *Advances in computers* (Vol. 111, pp. 69-98). Elsevier.
- [19] Yong, B., Shen, J., Liu, X., Li, F., Chen, H., & Zhou, Q. (2020). An intelligent blockchain-based system for safe vaccine supply and supervision. *International Journal of Information Management*, 52, 102024.
- [20] Della Valle, F., & Oliver, M. (2020). Blockchain Enablers for Supply Chains: How to Boost Implementation in Industry. *IEEE Access*, 8, 209699-209716.
- [21] Korin, N. (2020, November). Using blockchain to monitor the COVID-19 vaccine supply chain. *Pioneers of Change Summit 2020 - World Economic Forum*.
- [22] Bishara, R. H. (2006). Cold chain management-an essential component of the global pharmaceutical supply chain. *American Pharmaceutical Review*, 9(1), 105-109.
- [23] OpenAirInterface Software Alliance. 5G CORE NETWORK. Available online: <https://openairinterface.org/oai-5g-core-network-project/> (accessed on 16 June 2021).

- [24] Internet Engineering Task Force (IETF). (2015). Host Identity Protocol Version 2 (HIPv2). Retrieved from <https://tools.ietf.org/html/rfc7401>.
- [25] Steven, P. Spectrum Protocol [Source Code]. 2020. Available online: <https://github.com/stevenplatt/spectrum-protocol> (accessed on 16 June 2021).