APPLICATION-SPECIFIC BLOCKCHAIN ECOSYSTEM FOR THE INTERNET OF THINGS, USERS, AND ORGANIZATIONS

by

JUAH SONG, B.S.

THESIS
Presented to the Graduate Faculty of
The University of Texas at San Antonio
In Partial Fulfillment
Of the Requirements
For the Degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

COMMITTEE MEMBERS:
John J. Prevost, Ph.D., Chair
Guenevere (Qian) Chen, Ph.D.
Peyman Najafirad, Ph.D.

THE UNIVERSITY OF TEXAS AT SAN ANTONIO
College of Engineering
Department of Electrical and Computer Engineering
August 2018

DEDICATION

Dedicated to Finnegan "Finnie" Pig, the Incredibly Amazing Family American Staffordshire Terrier Therapy Dog: Wielder of the Fearsome Tail-Whip Wiggle-Butt Combo, Bottomless Pit for Food and Things That Are Not Food, Neurotic Hunter of Inadvertently Refracted Light, Extremely Spoiled Canine-Toddler, and Consistent Source of Emotional Support and Conditional Love.

ACKNOWLEDGEMENTS

Abundant thanks to Dr. Prevost, Mevlut Demir, and the rest of CLEAR (Cloud Lab for Engineering Application Research). If not for the guidance and support from the members of CLEAR Lab, I would have been long gone without a single page written in my name.

I must also express my sincere gratitude to Dr. Guenevere (Qian) Chen, Dr. Peyman Najafirad, Elena Carrasco, and Divyaansh Dandona : my discussions with them were crucial in solidifying my understanding of blockchain and IoT. My committee and fellow UTSA students willingly offered their discourse and helpful assessment in spades.

To my family and friends: I have absolutely no question in my mind and my heart that I owe you everything else for pushing me forward when my heels were dug into the ground.

August 2018

APPLICATION-SPECIFIC BLOCKCHAIN ECOSYSTEM FOR THE INTERNET OF THINGS, USERS, AND ORGANIZATIONS

Juah Song, M.S.
The University of Texas at San Antonio, 2018

Supervising Professor: John J. Prevost, Ph.D.

Blockchain technology offers a means to secure data transfer between a network of peers. Current designs of blockchain solutions tend to emphasize specific applications, such as financial transaction or sensor data acquisition. Research in blockchain include focuses in consensus methods, implementation frameworks, as well as proof of concept; the wide variance of these areas indicates the flexibility inherent in blockchain design. The decentralized and/or distributed nature of blockchain makes it an attractive match for managing the Internet of Things (IoT), a catch-all phrase to convey the idea that more and more devices are being built with the capability to communicate autonomously using networks such as the public Internet. Projections for IoT device numbers reach the scale of billions within the next several years. For such an event to be feasible without catastrophic security risk, IoT needs to be made scalable, secure, and have low transaction latency. Blockchain could provide the answer to all three challenges. Furthermore, since data can have different requirements for privacy, latency, or authenticity dependent upon the application, a blockchain could be tailored to reflect the needs of the data transfer. Rather than focus on a large selection of blockchain solutions, a singular solution would improve interoperability between networks. A blockchain solution needs to be flexible in order to cater to the diversity of an IoT ecosystem. This thesis proposes the potential of a secure, global IoT network by means of a self-tailoring blockchain solution and suggests possible first steps toward such a world.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

We live in a world where instantaneity has become less of a luxury and more of an expectation. Messages can be sent almost instantly at the touch of a button. Communication can now be faster, more convenient, and more reliable than the physical letter. This kind of leap in convenience applies to anything that requires information exchange: financial transactions, coordination between entities, persistence and propagation of data. Much of this data transfer is reliant upon the Internet.

A world that enjoys the convenience of near-instant communication knows that *in*convenience stems from a whole slew of factors – many of them nefarious. As with the physical letter, electronically transmitted messages can be altered, forged, intercepted, or read by unauthorized parties. However, threats to integrity, authenticity, availability, and confidentiality are not news. These threats are likely contingencies that require precautions. As with anything of value, these precautions come at a cost: be it time, space, or processing ability. In the jargon of electronic devices and systems, these precautions generally require an increase in latency time, memory space, and computation power.

No aspect of security comes without an input cost. The trade-off between speed of processing and security defines the cost of the message transmission. Different kinds of messages tend to have different requirements. An emergency call, a transmission of bank account information, a weekly status report, or a simple hello to a friend certainly do not share the same urgency. The emergency call needs next to no latency and utmost reliability of transmission; the bank account information needs absolute confidentiality; the weekly status report likely could afford some delay; and the simple hello could be shouted in a crowded room. There's no need to restrict every type of message to the same level of security. Precautionary measures should match the value of the information in order to justify cost effectiveness.

A cost effective system that experiences total failure with extensive down time can lose its cost effectiveness. Messages cannot be transmitted if the transmitter fails, and a secure message that is never delivered is not secure. Technology that cannot afford extended down time likely requires

fault tolerance, typically via distribution of workload and storage.

The broad concepts of message transmission and its reliability – thereby its security – all apply to any modern technology's quest for convenience. The trending topic of the Internet of Things fits well into our society's desire for ease of message delivery. The Internet of Things (IoT) is a term coined to convey that more and more devices are being built with the capability to communicate autonomously through networks such as the public Internet. Additionally, the amount of IoT devices currently in use has already surpassed several billions, and is only increasing [1] [2].

On the other hand, blockchain technology has gained a burst of attention, notably with the release of Bitcoin in 2009 [3]. Bitcoin is a distributed cyber ledger that enables anonymous financial exchange. It is the first widely-known decentralized cryptocurrency and serves as a general starting point for learning about blockchain technology. Notable achievements of blockchain include its use of a decentralized peer network for a trustless system and the immutability of its data once committed to the ledger. However, Bitcoin is known to be resource-intensive, slow to process transactions, and vulnerable to centralization [4] [5].

Despite its limitations, blockchain's offering of immutability, decentralization and fault tolerance mesh incredibly well with the ideals of ubiquitous IoT. If brought together successfully, blockchain-IoT systems can offer a secure environment for a cyber physical world – a world where sensors that acquire data transmit to smart actuators autonomously to affect our living conditions. We cannot reach that state without proper safety nets, protocols, regulations, and security mechanisms.

Given the wide variety of technologies and services in use today, forcing these entities to fit one type of blockchain solution is unrealistic. The future will likely bring about complex interactions between users, devices, and organizations in what can more aptly be described as a virtualized ecosystem.

Both blockchain and IoT are burgeoning topics of research and still have a long way to mature before mainstream adoption. This thesis aims to gather multiple aspects of blockchain and IoT together to form a picture of what the combined technologies could offer when tailored properly

for each application and designed with interoperability as a central goal. Another aim of this work is to explore the implications and needs of such blockchain-IoT ecosystem. Lastly, this work suggests some first steps towards implementing a tailorable solution for a blockchain-IoT system and what metrics must be measured for useful impact.

CHAPTER 2: BLOCKCHAIN IN THE INTERNET OF THINGS

2.1 Blockchain

Emergence in Cryptocurrency

Though cryptocurrency was first mentioned in the 1980s by David Chaum [6], it was unable to gain widespread traction for a number of reasons. Early concepts of cryptocurrency still required the participation of a trusted third party, such as a bank. Any removal of the trusted third party would place payers and payees under the risk of double-spending – the expenditure of an asset more times than it is available for a payer to spend. Expenditures needed to be accountable throughout a network.

Launched in 2009, Bitcoin removed the need for a trusted third party and solved the double-spending problem via blockchain, a cyber ledger distributed among a network of trustless peers. Peers do not have to trust one another, but instead trust in the incentives offered by adhering to the system's set of rules. Parties that want to participate in a transaction announce the event to a number of peers, who each check if the transaction is valid – i.e., the payer owns the assets in question and has not already spent them. Once validated, the transaction data is placed into a block that can be thought of as a larger chunk of data. Participants cannot easily back out of a transaction once it has been verified and appended to a block. That data has been propagated throughout a network of peers. Trying to alter all of those ledgers would be infeasible, largely due to the nature by which the ledgers are created.

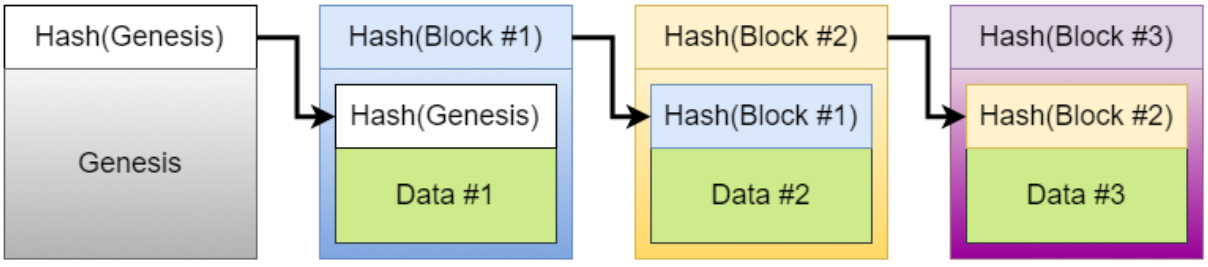
Chained by Cryptography

Blockchain is aptly titled because it is comprised of blocks of data linked via cryptographic hash functions, one-way functions that consistently produce an output with a set length. For example, SHA-256, the hash function used by Bitcoin, takes an input and produces a 256-bit output regardless of the size of the input. Theoretically speaking, a collision – where multiple inputs create

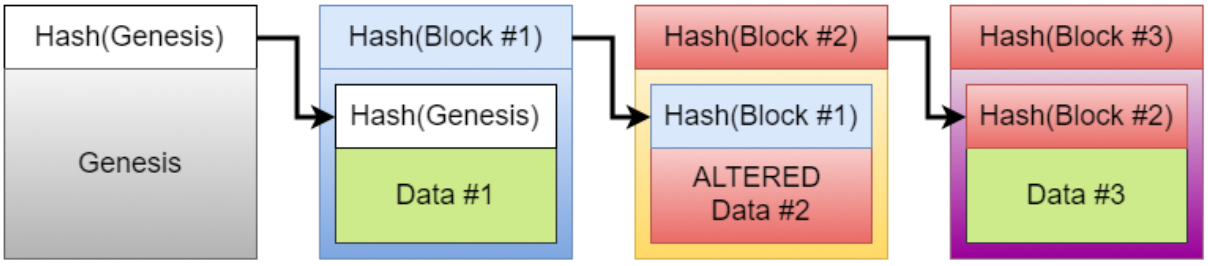
the same output – is possible, but highly improbable. We can reasonably assume that anyone has access to the function, and its cryptographic nature makes creating different inputs with the same output infeasible. For our practical considerations, a hash function offers a method to create a unique fingerprint for any set of differing data.

Figure 2.1a depicts a simplified structure of a blockchain ledger. The genesis block is a special block used to initiate a ledger. The hash of the genesis block is placed into the next block. Transaction data is appended to the most recent block after validation until the block reaches a size limit or a specified amount of time has elapsed (also called epoch time). When the block is "full" (either due to space or time), a node will hash that block and include the newest hash value into the data of the following block. As shown in Figure 2.1b, if any change (indicated in red) is made to the data in an earlier, completed block, the every successive hash value will be altered.

The append-only nature of blockchain signifies that older transactions are more secure from alteration than newer transactions. The more hash values that follow a completed block, the more improbable it becomes to propose alternate inputs. The attempt to alter blockchain ledger data



(a) Original Blockchain



(b) Altered Blockchain

Figure 2.1: Simplified Blockchain Structure

becomes even more staggering when considering that an entire network of peers, ideally, has the same copy of data. However, state replication across a network provides its own massive challenge in consensus.

Consensus

If a network of peer nodes require a copy of the same ledger even as the state of that ledger continually changes, that network needs a robust, deterministic consensus method. For blockchain technology, the most common consensus methods include Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance. This is by no means an exhaustive list, as consensus methods constitute a highly technical research topic. More in-depth overviews of consensus methods can be found in [4] [7].

Proof of Work (PoW)

Proof of Work is the type of consensus method used in Bitcoin. A peer in the network must provide proof that it solved a "difficult to compute, easily verifiable" puzzle [3]. In the case of Bitcoin, by completing PoW before its neighbors, a node announces the solution to the network. The peers of the announcing node can easily verify the solution offered by the first node accept the block created by that node. Bitcoin's hashcash can be thought of as a race to the finish line for the correct answer. Centralization of PoW consensus is limited to the node the finds the answer the fastest. PoW excels in preventing malicious users from flooding a network to influence consensus outcome due to its traditionally computation-heavy nature. The notable drawback of PoW is that same computation-intensive trait. Bitcoin's consensus requires significant consumption of power [8], and much of the in-progress PoW executed by nodes in the network is wasted in the quest for PoW incentives.

Proof of Stake (PoS)

An ongoing challenge for a network of trustless peers is the guarantee of honest participation. Bitcoin incentivizes successful mining with a reward fed from transaction fees and decreasing

reward [9]. Proof of Stake leverages the idea that participants are more likely to be honest if they have stake in the system. By providing "proof of stake," usually through ownership of relevant network currency, participants can mine blocks more easily.

Practical Byzantine Fault Tolerance (PBFT)

PBFT can be thought of as a voting system resilient to a limited number of malicious actors [10]. Classic PBFT tolerance is $3f + 1$ peers with f faulty nodes. Consensus in this manner must take care to manage its upscaling to prevent significant communication overhead. The general trend is to create "round robin" or subgroup voting pools to mitigate scaling issues.

Limitations

Consensus methods like PoW are resource-intensive. An entire network of peers racing to find the answer to a difficult-to-solve puzzle consumes a large amount of computation, and in turn, power consumption [8]. Not only that, but an append-only ledger like that of Bitcoin requires immense memory space. As of July 2018, the Bitcoin ledger surpassed 200 GB in size [11]. Additionally, probabilistic methods like hashcash (Bitcoin) and ethash (Ethereum) have no guarantee of only one correct mining answer. Multiple "correct" blocks can be announced from different areas of the peer network, which causes a fork in the blockchain. Forks can be resolved in a number of ways; the more common method being that the chain that becomes longer is the chain adopted by the whole network. Quantities such as block propagation time affect what fork is favored by which node, which complicates consensus even further [12].

2.2 The Internet of Things (IoT)

IoT future projections vary widely on actual number, but all predictions still place the total number of connected devices in the dozens of billions by 2020 [1] [2]. Despite these numbers, IoT still faces a number of important issues that prevent their complete adoption. In the push to create low-cost devices, IoT leaves much to be desired by means of security due to low compute, memory and

power resource. Additionally, these devices are not uniform – they are heterogeneous, vary widely in application and deployment. Interoperability between IoT devices is ideal, but challenging. Management of these devices must also be rethought – centrally managing a staggering number of IoT devices will and is logistically impractical.

2.3 Merging Blockchain and IoT

If "traditional" blockchain is resource-intensive in memory, computation, and power consumption, merging it with IoT present immediately apparent challenges. Though blockchain sets out to provide decentralized security, a quality that IoT sorely lacks, creating a Blockchain-IoT system requires innovation.

2.4 Approaches in the Literature and in Industry

Pushes in literature and industry tackle Blockchain-IoT systems from several different angles. Consensus methods are either incrementally improved [13] or developed from scratch [14] [15]. Framework systems attempt to leverage cloud, fog, and edge-based resources to reduce latency and scaling issues of current blockchain solutions [16] [17].

More notable is the realization that no one consensus method is suitable for all levels of data transmission [18] [19]. Some suggest a layered blockchain approach, where a different consensus method is used for each stage to account for faster transactions versus more secure transactions [19] [20].

New alternative solutions to merge IoT and Blockchain either suggest to launch off an existing platform like Ethereum [21] or create a new solution entirely. IOTA Tangle is an existing open source solution directed for IoT but does not make use of blockchain; instead making use of directed acyclic graphs as a sort of PoW validation mechanism [22] [23]. IoTeX also deserves a mention as an open source solution that utilizes Delegated Proof of Stake [24].

Altcoins, or "alternative coins," which refers to cryptocurrency alternative to Bitcoin, deserve a mention due to their attempts to improve some aspect of Bitcoin – either through altered con-

sensus, smart contract functionality, or ease of exchange. Stellar [25] and Ripple [26] both offer their own consensus mechanisms, but focus more on financial exchange than IoT application. Ethereum [27] expanded on smart contract functionality for the blockchain, which eases the development of "dapps," or decentralized applications. Smart Contracts are essential to autonomous IoT management at scale. They offer a way to enact actions once certain conditions are met without the need for manual intervention.

Blockchain interaction topologies in literature are covered more thoroughly in Chapter 4.

CHAPTER 3: SECURITY: OLD PROBLEMS, NEW PROBLEMS

Before delving into any description of the security of Blockchain-IoT systems, we need to define the boundaries of the concept relevant to our applications. A system that needs to secure data transmission must consider confidentiality, authenticity, availability, and authority. More simply in respective fashion: Who is able to read the message? Is the message from a reliable source? Is the message accessible? Who controls the message?

Depending on the nature of the data, such as for medical health reports, confidentiality may be required to preserve privacy. Any data sent needs to have guaranteed provenance and integrity. Furthermore, data sent and received should only involved authorized entities.

Another question with data storage is the perceived value as the data ages. How long should institutions retain data before the cost of storage exceeds the value of the data? Alternatively, government regulations could restrict retention windows for this data.

These are old problems, but now framed in the growing world of cyber physical systems enabled by IoT.

3.1 IOT Security

Due to their primarily low-cost nature, IoT devices are not well-equipped to handle all of the cryptographic processing needed for conventional security such as cryptographic key generation, key storage, or complication encryption protocols [28].

Furthermore, the physical security of IoT devices must also be accounted. Tampering or weathering are well within reason to expect for an IoT network. On the cyber side of design, it may be important to ensure some kind of tamper check and autonomous system recovery.

3.2 Blockchain Security

Blockchain systems are not infallible. Common attack vectors on blockchain can include some way to overcome the number of distributed peers (routing attack, 51%attack, or a Sybil attack)

or otherwise create a denial of service. Accessing blockchain resources also introduces potential risk surfaces – user access via password or vulnerable implementation of "wallet" applications. The DAO scandal of 2016 revolved around the malicious exploitation of smart contract code in Ethereum, which caused a loss of over $150 million [29]. Bitcoin assets can be lost if the user loses the private key that links their ownership of bitcoin currency. Such types of pitfalls speaks not to the weakness of blockchain, but to the challenge of properly leveraging cryptographic resource.

A communication-bound technology like blockchain relies extensively on the ability of a peer to receive information from its network. The information does not have to be immediately complete and timely, but ideally the information reaches the peer eventually. If somehow the peer is cut off from its fellow nodes, it suffers from denial of service. Furthermore, if blocks are being rerouted away from an isolated peer to prevent its timely participation in consensus, it is under a routing attack [30].

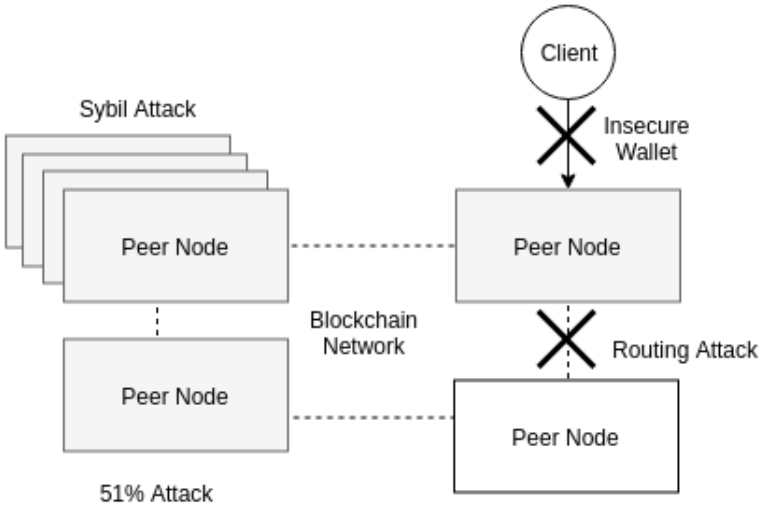


Figure 3.1: Possible attack vectors on a blockchain network. In this case, the peer node outside the inner shaded area is the only non-malicious actor.

Other attack vectors involve influencing the network at large, be it through controlling a majority of the network (51% attack), or pretending to *be* a majority of the network from one source (Sybil Attack). Alternatively, unbidden centralization can also occur in blockchain solutions. Proof of Stake can be skewed by participants with larger stakes. In Bitcoin, centralization has occurred

with the rise of GPU farms and mining pools [5] [31]. The entities reaping most of the rewards for "winning the PoW race" fall to a very short list of mining pool groups.

Other variances of Denial of Service can take advantage of protocols that require a peer to check in every so often. A peer could be cut off from a network just long enough that the rest of the network no longer trusts the victimized peer.

These common attack vectors are important to keep in mind for any development of blockchain-peer based frameworks (Fig. 3.1. Of course, new vulnerabilities could crop up at any time, but keeping afloat of the larger concepts of what makes blockchain fallible is essential for awareness.

CHAPTER 4: THE NEEDS OF A COMPLEX BLOCKCHAIN-IOT ECOSYSTEM

In order for a blockchain-IoT network to flourish, it will need flexibility in several areas so that it can accommodate a potentially diverse set of applications and devices.

4.1 Parameters and Traits of Interest

Latency is a huge factor in any technology that requires data transmission. In an ideal world, latency is always minimal, but such a trait tends to come at a high cost when coupled with stronger security.

With the sheer number of IoT, throughput of data for such things as wireless sensor networks becomes an important consideration. On the other side of the coin is scalability – an IoT system, or a network could have a large number of participants; it could have a wildly fluctuating number of participants. The point is that the system should be able to handle scaling up and scaling down without incurring function-breaking overhead.

Furthermore, the type of data that IoT offers tend to revolve around areas that need confidentiality, such as health status or home security. Access control granularity can be integrated via the public-private key infrastructure already utilized by many blockchain solutions.

Though the triumph of Bitcoin was the removal of trusted third parties and the enabling of a trustless environment, permissioned solutions such as Hyperledger Fabric still make use of certificate authorities. [32]. Blockchain consortia also rely on a somewhat centralized hierarchy for establishment of trust. Stellar Protocol enables users to define their trust circles [25]. The key idea here is that defining a trust network is a capability that cannot be forgotten in future blockchain-IoT networks.

Another trait to consider for a blockchain *ecosystem* would be the topology of interaction between blockchains. Most commonly seen in the literature is a multi-layered approach (Fig. 4.1), suggested in such works as [17] [19] [33]. Each layer tends to represent a different environment.

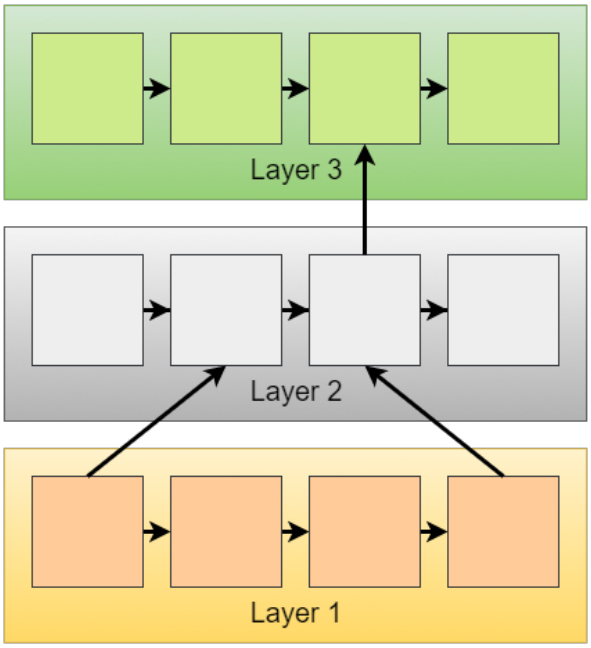


Figure 4.1: Multi-layered Blockchain

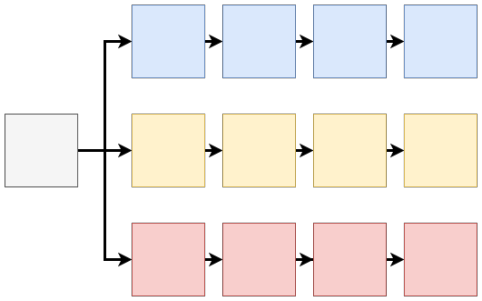
In the case of Figure 4.1, Layer 1 could represent sensor devices, Layer 2 could represent edge devices, while Layer 3 could be hosted on the cloud. For the sake of clarity, only a few arrows are shown linking the layers; however the only restriction would be that communication is limited to adjacent layers only. Directionality of messaging is another important consideration between blockchains. Unidirectional communication from one layer to another could reduce communication overhead, but may limit functionality of the system. Bidirectional communication would be ideal, but increase protocol complexity. Finally, each layer would have their own consensus method for desired latency and throughput.

Alternative to the layered approach, an organization could be in charge of several different services, each hosted on its own blockchain (Fig. 4.2a). To maintain inter-chain coherence, separate blockchains could report to a "status check" (grey) block before continuing its individual block creation. Figure 4.2b illustrates synchronous status reporting between multiple blockchains under one organization. The number of blocks in each service could be dependent on their individual policies for block creation and consensus method, while still be required to check in at regular intervals with each other. This allows for cross-chain immutability, where one chain can provide

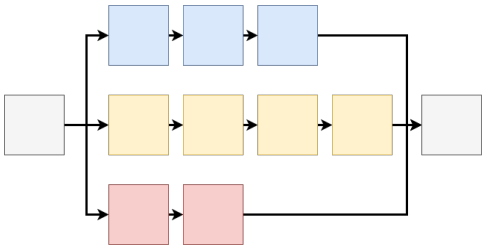
a state check verification for another. On the other hand, asynchronous, on-demand status checks as shown in Fig. 4.2c could be utilized – depending on how often status checks were required, on-demand status checks could reduce overhead for coordinating blockchain services.

The distinction between multi-layered and multi-dimensional is that in multi-dimensional topologies, any blockchain could interact with another, without needing to go through a hierarchy of layers.

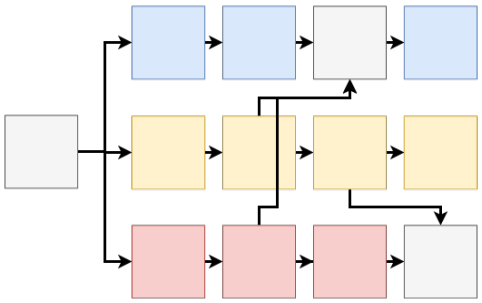
Consider yet another possibility where multiple organizations decide to create a federated system (Fig. 4.3) of services which require cross-checking, either for creation of a trust network or



(a) Multidimensional Organization



(b) Synchronous Status



(c) Asynchronous Status

Figure 4.2: Multidimensional Blockchain Interaction Topologies

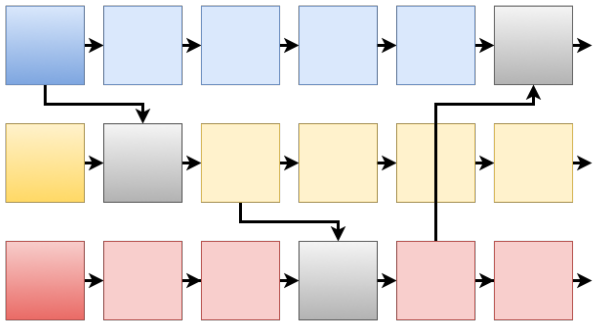


Figure 4.3: Federated Blockchain System

exchange of assets. This setup is less centralized than the multi-dimensional example, but still revolves around a focused set of blockchains which each could be representative of a separate company.

4.2 Target Applications

Target applications for Blockchain-IoT networks largely revolve around financial applications. The inherently transactional nature of blockchain facilitates trade of virtualized assets in an immutable and therefore accountable manner. These virtualized assets do not necessarily have to be directly related to currency, but likely will have value of its own: sensor data, proof of ownership, etc. The exchange of data in such a network boils down to a few broad classifications.

4.2.1 Data Transmission and Persistence

Arguably, data transmission and persistence is the name of the game for all exchanges in blockchain-IoT. The data likely requires high throughput and options for confidentiality.

4.2.2 Device Updates and Upgrades

An important subset to data transmission is the nature of that data. Much of it will need to be devoted to the actual updating and upgrading of software on a device. As with most devices, software and BIOS need constant patching and updating to stay afloat of security risks and interoperable features. Deploying updates could leverage the decentralized and automated nature of smart contract

functionality on a blockchain.

4.2.3 Ownership Transferral

Ownership transferral of assets, such as property deeds, can be virtualized on the blockchain to create a record of accountability that is difficult to alter but easy to access.

4.3 Blockchain Interconnection

The need to connect assets between separate blockchains has been investigated in such works as pegged sidechains [34] and the Interledger Protocol (ILP) [35]. These investigate how exchanges can occur between separate blockchain currencies.

Pegged sidechains are covered more in depth in [34], however, they are briefly overviewed in Figure 4.4. ILP and pegged sidechains share remarkable similarities in their goals to facilitate exchange between blockchains via an intermediary - in Figure 4.4, the intermediary is represented in green. However, both works target financial exchange and are not targeted for IoT applications. Despite one of their goals being a decrease in transaction latency, complications can arise from the individual blockchain operation's specific requirements. These developments indicate a need for some kind of baseline standardization of operation.

4.4 Deployment Options

Deployment in the case of Blockchain-IoT refers to both device and software initiation. The topic of device initialization and Quality of Service (QoS) is beyond the scope of this work, but should be recognized as a key development point for widespread integration of blockchain systems. Without ease of use, laypeople would be hard-pressed to implement such a security mechanism on their devices.

A network in a multi-layered topology as in Figure 4.1 can involve deployment across environments, leveraging edge-, fog-, or cloud-centric blockchains such as in works [36] [37] [38].

We selected Hyperledger Fabric as our blockchain solution to deploy across our network with

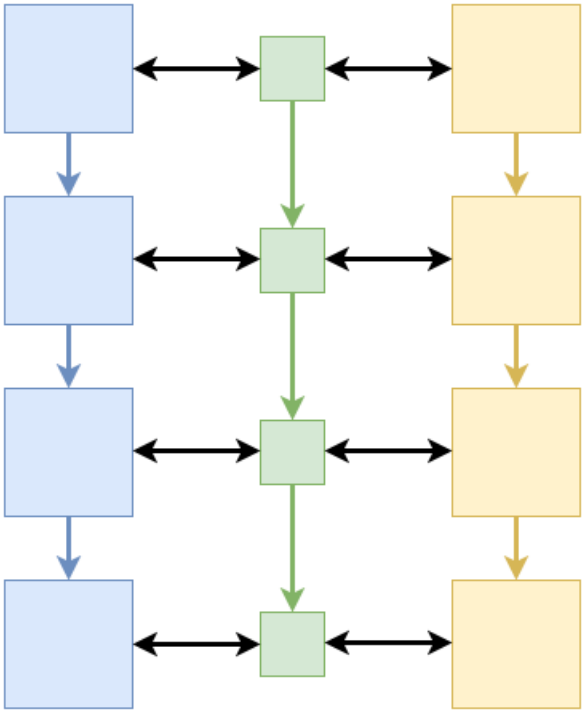


Figure 4.4: Sidechain Topology with Interacting Blockchains

the use of Docker Swarm [39], which is further discussed in Chapter 6. Fabric is a private, permissioned blockchain whose functions are closely coupled with Docker containers [32] [40]. Fabric also decouples transaction validation from ledger block ordering into separate containers. Peer nodes carry out validation and ledger maintenance. Orderer nodes handle consensus and block broadcasting to the peers. The Fabric equivalent to smart contracts is called "chaincode." The usage of Docker containers for blockchain implementation was also investigated in [41].

Containers are lightweight, standalone application packages that consist of code, libraries, other tools needed to run said packages, effectively allowing software to operate independent of the environment in which it is deployed. This is an ideal quality to leverage for heterogeneous systems expected in IoT. Orchestrating containers with Kubernetes or Docker Swarm increases the efficiency with which these applications can be deployed across a large number of end devices.

A vast sensor system collecting data may need to be locally centralized in a permissioned network for purposes of throughput and latency. Such a system may need to tightly manage malfunctioning nodes; rather than attempt to fix that particular node, the system could automatically

opt to kill the application and restart for relatively quick and simplified recovery.

It's possible that the usage of container orchestration with blockchain could introduce redundant overhead with encrypted channels; many blockchain solutions internally utilize encryption for initial communication setup, muuch of what Docker and Kubernetes also set up for their nodes.

Another challenge introduced with container deployment of blockchain nodes would be cryptographic key distribution and management. Spinning up new nodes could still incur a high overhead by virtue of having to generate new cryptographic material and transferring this information securely to its destination.

CHAPTER 5: PROPOSALS FOR AN INTEROPERABLE, APPLICATION-SPECIFIC SOLUTION

5.1 Multidimensional, But Not Always Layered

Layering of blockchain frameworks to account for differing latency requirements is a sensible approach, but the truth of the matter is that in the beginning, entities will not settle on one single blockchain platform. More likely than not, competitors will arise, as they already have, with their own set of rules and their own cryptocurrency exchange. Forward thinking efforts put forth by Interledger Protocol and pegged sidechains attempt to mitigate exchange complexity. Exchanges will not only be needed between financial transactions. Suppose a blockchain account owner in a layered sensor network wants to make a transaction with another independent cloud storage service. Does the account owner have to negotiate up through its own cloud layer to exchange with the independent entity, or do they make a direct exchange? It's possible that a layered system would incur more overhead than necessary, as opposed to allowing for a multi-dimensional topology for that direct access.

Perhaps a sensor acquisition network is entirely owned by one company, never placing its edge-level blockchain on a public network. The sensors remain on a private network, while the data storage on the cloud layer participates in data transactions with other organizations. A multi-layer system, in this case, participates with potentially single blockchains. Entities which track ownership may have no need for any kind of layered system and may not have any desire to form a federation with certain companies.

Even blockchain interaction topologies will necessarily have to vary between different entities that require security for different assets. Again, restricting any system to one type of topology could create more complexity than necessary. "Interblockchain" systems need to allow for flexible exchange.

5.2 Domain Specificity

If a blockchain solution is to tailor itself to an application, there must be some kind of criteria to facilitate an automated decision. The aforementioned paramters of interest should be quantifiable to enable classification, or blockchain settings must be configurable.

The General Sensor Network

Depending on the scale, a sensor network may need to emphasize throughput and low latency over decentralization of consensus. Decentralization tends to come at the cost of latency, so keeping sensor acquisition in a more centralized structure would be ideal for efficiency.

The Smart Homes and Smart Cities

Smart home case studies such as in [37] emphasize the usage of private networks within the home, while a singular hub representing the home owner can connect on a public network. Smart City applications will likely require a vast hybridization of blockchain-IoT systems; emergency broadcasts need to be immutable and immediate. Financial transactions such as on the electric power grid require deterministic output and accountability [42].

5.3 Interconnection

Periodic or on-demand status hashes from a linked blockchain could be all that a multidimensional system needs to remain connected. Interconnection will require device/network discovery, which again returns back to the need for trusted third parties [33] [43] . Though anonymity is an attractive quality for exchange of cryptocurrency, other products often desire the credibility associated with a brand.

5.4 Deployment via Containerization

Interoperability needs to be considered not only between blockchains but also between heterogeneous systems with a wide variety of devices. Orchestrated and containerized deployment of blockchain applications could prove very useful for this very purpose [44] [40].

5.5 Latency and Scalability

Scalability of blockchain systems is largely tied to consensus method and the number of peers expected to participate in consensus. Classic PBFT is known to scale poorly [4] [45].

A prevailing thought on reducing latency is to design "locally centralized, globally decentralized" systems as proposed by [46]. In the realm of blockchain, leave an edge device the locally central permission authority for data handling before pushing up to the cloud layer, where there is the appropriate resource for handling big data from numerous edge hubs. This may also help improve scalability, if the number of participants on local hubs can be limited – introducing more edge hubs to accommodate an increase in scale. Data permanence can be ensured at the cloud level, while potentially private, local networks focus on throughput.

CHAPTER 6: TESTBED EXAMPLE

6.1 Proof of Concept

Proof of concept with Hyperledger Fabric could demonstrate the usage of containers as a means to improve the convenience of software deployment to remote devices via tool such as Kubernetes [44]. Figure 6.1 depicts the data workflow of a Hyperledger Fabric system connected between sensors, edge devices, and the cloud. In this example, there is only one blockchain solution, but the important thing to note is that the consensus process is a decoupled service from the rest of the workflow.

Data acquired by sensors is packaged into a "transaction" by its respective peer. This first peer must then request validation from a configurable number of neighboring peers through a communication-bound gossip protocol. Once enough neighbors respond with an approval, the requesting peer then sends its validated transaction on to the orderer nodes. These orderers are in charge of reaching consensus on the finalized order of all received transaction within a certain amount of time, or block epoch time. After the block is completed, it is broadcast back to the peer nodes, who maintain a copy of the transaction ledger. Hyperledger Fabric can manage an account-based ledger which tracks the states of individual accounts, which makes it ideal for sensor data collection.

Figure 6.2 depicts a physical implementation with Raspberry Pi peers connected to a cloud server. The cloud hosts orderer nodes to handle consensus overhead. This implementation is different than the layered approach presented in Figure 4.1, as this setup runs on a single blockchain solution to first study the viability of container-based blockchain.

Due to the relatively limited space available on a Raspberry Pi, ledgers can be "pruned" to reduce memory consumption, so long as all peers can agree to prune from the same point. This requires careful definition of at what point data can be safely discarded, which can depend on government regulation or company policy.

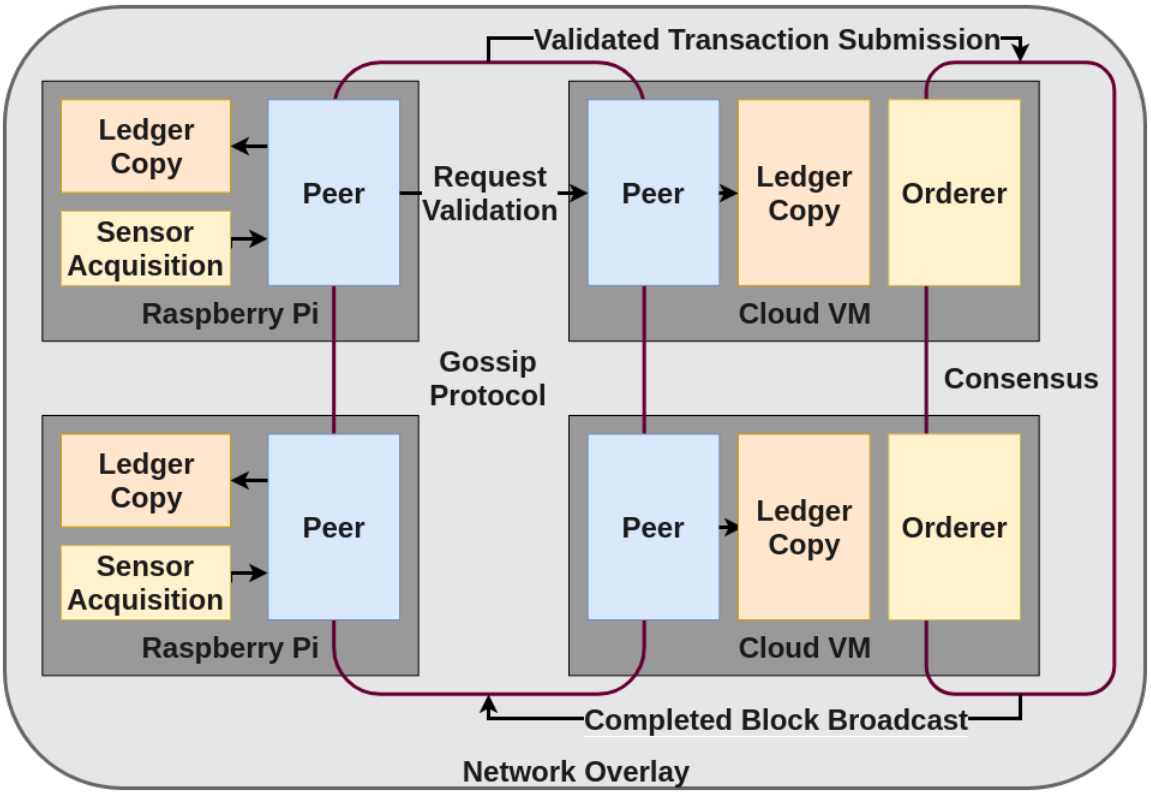


Figure 6.1: Data workflow of an example framework with Hyperledger Fabric.

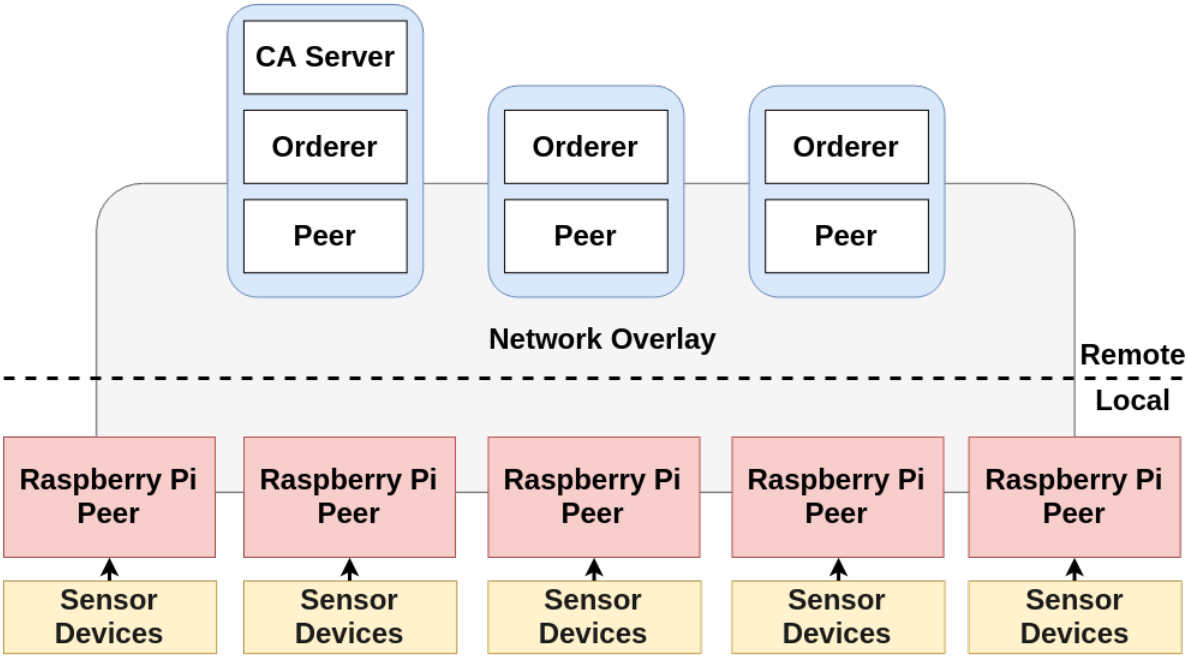


Figure 6.2: Example of a Physical Implementation with Figure 6.1.

6.2 Performance Metrics

Since much of an autonomous solution relies on self-evaluation of particular parameters, any development of such technology needs to meticulously measure these qualities. Performance metrics will have to be made for throughput, latency, scalability, robustness, privacy, and resistance to security risks. Additionally, design details need to be aware of device initiation (QoS), provision of access control, privacy management or guarantee, security of deployment, and usage of key distribution method.

Refining the ability to measure performance in a certain environment can allow for dynamic adjustment, similar to how Bitcoin alters its PoW difficulty to maintain block epoch time to approximately ten minutes. For example, this kind of automated adaptability could be extended to the number of operating orderer nodes to affect block creation times, essentially tailoring latency. The drawback is the affected security of the process, but the possibility of self-tailoring blockchain could also apply to number of active peer nodes, either at the edge or the the cloud based upon conditions stipulated in chaincode.

CHAPTER 7: OTHER CONSIDERATIONS

The Internet of Things provides countless ways for differing entities to interact, be it between users, devices, or organizations. Users can communicate with devices. Organizations can utilize devices to interact with users. More prevalently, devices can connect with other devices. The ability to communicate with devices in a way that can enact a physical response (i.e., remote actuation) brings about the notion that we can virtualize actions, items, places, data, and other countless assets. We are developing into a world that can virtualize almost anything and have interactions with the virtual affect the physical – hence the evolution into a cyber-physical world.

Economic Considerations

As an inherently transaction-based technology, blockchain offers a manner of secure exchange between peers. Combining the transactional nature of blockchain with IoT creates opportunity for the exchange of any and all kinds of virtualized assets. Ownership transfer for goods, property, data, all could be mediated on a blockchain network – made immutable and accountable to all participants.

One of the goals of Bitcoin was the removal of a trusted third party. However, with the complications brought about by the desire for global interoperability, the complete removal of a trusted third party is unrealistic for the near future. Services such as certificate authorities, network discovery, and data warehouses will not be going anywhere any time soon. If blockchain-IoT systems are to become more common, the need for these types of services will only increase, especially due to the need for storage of data ledgers backed up on the accounts of numerous separate peers. Perhaps the traditional trusted third party such as banks or notaries (physical presences) will merely shift to the virtual realm along with our many physical assets.

Political Considerations

Regulations, standards, and protocols – again and again the need for these are mentioned, and dozens of separate organizations are drafting standards to catch up with the rapid development of blockchain technology and what potential it offers to the grand scheme of digital society, as well as what caveats it will carry: threats to privacy, safety, security. Ubiquitous IoT will create data with great volume and velocity as well as exponentially open up attack surface area if not handled carefully. An important consideration frequently discussed with IoT is the matter of privacy [47] [37] [48].

Interacting entities will still need trust. Even in "trustless" systems like Bitcoin, peers could rely on incentivization as the source of trust. With global blockchain-IoT, where will the trust be built? Trust has a cost – do we keep trusted third parties, decentralize with costly Proof of Work, or remain in a centralized system? How realistic is a truly decentralized network when staggering numbers are involved? The questions that plague governmental theory now could be applied to consensus philosophy. The importance of delegation of workload will vary from system to system. There is no singular answer.

Social Considerations

Instant exchange of information, funds, and communication have already drastically changed human interaction. Social media, payment applications, and online shopping already provide instant gratification. Extending our so-called desire for intantaneity to property exchange via secure, accountable platforms such as blockchain will further transform our social dynamic.

CHAPTER 8: CONCLUSION

The natural conclusion that would be remiss if not mentioned: no single solution will fit all, which does create a paradox given the nature of this work. How can a flexible solution be termed non-singular, when that is in fact what has occurred?

Right now, dozens upon dozens of separate blockchain solutions float around clamoring for spotlight [49], likely wanting to become *the* dominant blockchain – the technological "real estate" is ripe for the taking. It would be unrealistic to think that the world will immediately settle for just one. Case in point: once Bitcoin launched, Ethereum followed, as did Ripple, Stellar, and countless other altcoins. Rather than try to suggest the next big blockchain solution, this work offers the perspective of how the interactions between these blockchains should take place, how those interactions can be quantified, and a potential development path. Interoperability was always a challenge with IoT; it makes poetic justice that blockchain experience the same issue.

A huge weakness of blockchain overall is its high dependence on communication. Without block propagation, successful validation requests, the system is defunct. Faulty nodes and down-time can be expected, but in more extreme situations such as environments remote or even hostile, technology running on blockchain becomes crippled without a secure avenue for heavy network communication.

Future work must pick up from where the theorizing leaves off: what is the landscape of consensus methods? What tradeoffs are acceptable for which applications? Settling for pre-established consensus mechanisms is merely a placeholder for something new and improved to come along. As much as decoupling consensus might be deemed an attractive aspect, it cannot be developed in vacuum before integration into a system with pluggable consensus.

BIBLIOGRAPHY

[1] A. Nordrum, "Popular internet of things forecast of 50 billion devices by 2020 is outdated," *IEEE Spectrum*, 2016.

[2] "Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015," November 2015. https://www.gartner.com/newsroom/id/3165317.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," October 2008.

[4] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in *Proceedings of the IFIP WB 11.4 Workshop, iNetSec 2015* (J. Camenisch and D. Kesdogan, eds.), vol. 9591, pp. 112–125, Springer International Publishing, 2015.

[5] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Eighteenth International Conference on Financial Cryptography and Data Security (FC'14)*, November 2013.

[6] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology* (D. Chaum, R. L. Rivest, and A. T. Sherman, eds.), (Boston, MA), pp. 199–203, Springer US, 1983.

[7] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," 2017.

[8] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, pp. 280–285, June 2014.

[9] "Bitcoin developer documentation," 2018.

[10] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, vol. 20, ACM, November 2002.

[11] "Bitcoin (btc) statistics - price, blocks count, difficulty, hashrate, value," 2018. https://bitinfocharts.com/bitcoin/.

[12] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *13th IEEE Conference on Peer-to-Peer Computing*, 2013.

[13] I. Abraham, D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman, "Solidus: An incentive-compatible cryptocurrency based on permissionless byzantine consensus," December 2016.

[14] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," *IACR Cryptology ePrint Archive*, vol. 2017, p. 406, 2017.

[15] A. E. Gencer, R. van Renesse, and E. G. Sirer, "Service-oriented sharding with aspen," 2016.

[16] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in iot using blockchain," in *IEEE MILCOM*, 2017.

[17] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *IEEE Access*, vol. 6, pp. 115–124, September 2017.

[18] M. Vukolić, "Rethinking permissioned blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, 2017.

[19] L. Aniello, R. Baldoni, E. Gaetani, F. Lombardi, A. Margheri, and V. Sassone, "A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database," in *13th European Dependable Computing Conference*, 2017.

[20] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, eds.), (Cham), pp. 297–315, Springer International Publishing, 2017.

[21] M. P. Andersen, J. Kolb, K. Chen, G. Fierro, D. E. Culler, and R. A. Popa, "Wave: A decentralized authorization system for iot via blockchain smart contracts," tech. rep., University of California at Berkeley, December 2017.

[22] S. Popov, "The tangle," tech. rep., IOTA, 2017.

[23] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *Financial Cryptography*, pp. 528–547, 2015.

[24] "Iotex: A decentralized network for internet of things powered by a privacy-centric blockchain," May 2018.

[25] D. Mazières, "The stellar consensus protocol: A federated model for internet-level consensus," tech. rep., Stellar Development Foundation, 2016.

[26] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," tech. rep., Ripple Labs Inc, 2014.

[27] "A next-generation smart contract and decentralized application platform," 2017. https://github.com/ethereum/wiki/wiki/White-Paper.

[28] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010.

[29] "Report of investigation pursuant to section 21(a) of the securities exchange act of 1934: The dao." Securities and Exchange Commission, July 2017.

[30] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *IEEE Symposium on Security and Privacy*, 2017.

[31] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün Sirer, D. Song, and R. Wattenhofer, *On Scaling Decentralized Blockchains*, pp. 106–125. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016.

[32] "Hyperledger fabric," 2015. https://hyperledger.org/projects/fabric.

[33] V. Daza, R. D. Pietro, I. Klimek, and M. Signorini, "Connect: Contextual name discovery for blockchain-based services in the iot," in *IEEE ICC 2017 SAC Symposium Internet of Things Track*, 2017.

[34] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timon, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," October 2014.

[35] S. Thomas and E. Schwartz, "A protocol for interledger payments," tech. rep., Interledger W3C Community Group, 2015.

[36] A. Bahga and V. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 9, pp. 533–546, 2016.

[37] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *Pervasive Computing and Communications Workshops (PerCom Workshops)*, IEEE, March 2017.

[38] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, IoTPTS '16, pp. 29–36, ACM, May 2016.

[39] J. C. Song, M. A. Demir, J. J. Prevost, and P. Rad, "Blockchain design for trusted decentralized iot networks," in *IEEE 13th System of Systems Engineering Conference*, 2018.

[40] "Docker documentation," 2018.

[41] A. Stanciu, "Blockchain based distributed control system for edge computing," in *21st International Conference on Control Systems and Computer Science*, 2017.

[42] T. Lundqvist, A. de Blanche, and H. R. H. Andersson, "Thing-to-thing electricity micro payments using blockchain technology," in *2017 Global Internet of Things Summit (GIoTS)*, pp. 1–6, June 2017.

[43] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, "Autonomic identity framework for the internet of things," in *IEEE International Conference on Cloud and Autonomic Computing*, 2017.

[44] "Kubernetes docs," 2018.

[45] T. T. A. Dinh, R. Liu, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems." eprint, 2017.

[46] H. Kim and E. Lee, "Authentication and authorization for the internet of things," *IT Professional*, vol. 19, no. 5, pp. 27–33, 2017.

[47] N. Fabiano, "The internet of things ecosystem: the blockchain and privacy issues. the challenge for a global privacy standard," in *Internet of Things for the Global Community (IoTGC)*, 2017.

[48] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectivees and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, pp. 104–121, 2015.

[49] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

VITA

Juah Song was born and raised in San Antonio, Texas. She earned her Bachelor of Science in Materials Science and Engineering from the University of North Texas in Denton, Texas. Juah later attended the University of Texas at San Antonio to earn a Master of Science in Electrical Engineering. She has experience ranging from classical music performance and art commissions to database querying and computer programming. Though her hobbies include most arts and crafts, Juah looks forward to careers that will further advance her knowledge in math and science. Upon graduation from UTSA, she plans to work at Oncor Electric Delivery in Fort Worth, Texas.