Secure IoT Applications Using Scalable Blockchain Models And PQ Primitives

Sichere IoT Anwendungen unter Nutzung skalierbarer Blockchain Modelle und PQ Primitive

Master-Thesis von Muhammad Rameez
Matriculation No.: 2556345
Tag der Einreichung:

1. Gutachten: Gutachter 1
2. Gutachten: Gutachter 2
Betreuer: Rachid El Bansarkhani

TECHNISCHE
UNIVERSITÄT
DARMSTADT

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Secure IoT Applications Using Scalable Blockchain Models And PQ Primitives
Sichere IoT Anwendungen unter Nutzung skalierbarer Blockchain Modelle und PQ Primitive

Vorgelegte Master-Thesis von Muhammad Rameez
Matriculation No.: 2556345

1. Gutachten: Gutachter 1
2. Gutachten: Gutachter 2
Betreuer: Rachid El Bansarkhani

Tag der Einreichung:

Erklärung zur Master-Thesis

Hiermit versichere ich, die vorliegende Master-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den August 28, 2018

(Muhammad Rameez)

Abstract

Distributed Ledger Technologies like blockchain have emerged as a promising area of research in academia and business. Its tamper resistant nature combined with other properties such as immutability, transparency and byzantine fault tolerance make it particularly interesting for applications in Finance, Internet of Things, Supply Chain Management, and Cloud Storage.

In this thesis, I first introduce the basics of blockchain and its related terminologies. Then, I highlight some of challenges faced by this promising new technology along with some potential solutions to those problems. After which, some choice examples of blockchain applications are presented. Next, I focus on the Ethereum blockchain, IPFS and Raiden Network and explore their potential in building powerful new decentralized applications or Dapps.

As part of this thesis, a novel decentralized Supply Chain Management System was designed, implemented and tested. The design of this system was realized using the Ethereum blockchain and was evaluated under various scenarios designed to simulate real world application and usage. Its design has several key advantages over traditional systems. It is secure against distributed denial of service attacks (DDOS) and has additional advantages of being trustless, autonomous, transparent and censorship resistant.

Preface

preface goes here ....

Contents

1 Introduction And Motivation

1.1 Introduction To Blockhain

"Blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block contains typically a hash pointer as a link to a previous block, a timestamp and transaction data" [Wik18b]. It can serve as a distributed ledger that can record transactions without a central server or trusted third party. The transactions are available to all parties and are easily verifiable. It is inherently resistant to data tampering as altering data in any one block breaks the chain and requires that all subsequent blocks be calculated again using the new data. Technical details of blockchains are discussed in chapter [2], however for a high level overview please refer to figure [1]. Notice that each block has a unique signature or hash and is linked to previous blocks through its hash. Blockchain has the power to revolutionize how business is conducted in digital age. Some are calling it the most important innovation since the development of the internet and the world wide web. The proponents of this technology believe that it will fundamentally transform the web itself. Internet of tomorrow will be powered by decentralized applications or Dapps. The first blockchain was invented by a person or group of persons known only by the pseudonym Satoshi Nakamoto. Bitcoin is a form of peer-to-peer electronic cash designed to transfer value between two parties without involving banks or other financial institutions. It was the first to solve the double spend problem in digital currency. Bitcoin paved the way for exponential growth in crypto currency market which together with other Altcoins is worth over 120 billion dollars at the time of writing. The underlying technology which powers Bitcoin, Ethereum and other crypto currencies can be used for much more than just transferring X amount of coins from Person A to Person B. Researchers are employing blockchain technologies to increase efficiency and reduce costs in industries such as Supply Chain Management, Internet of things, Banking and Finance just to name a few.

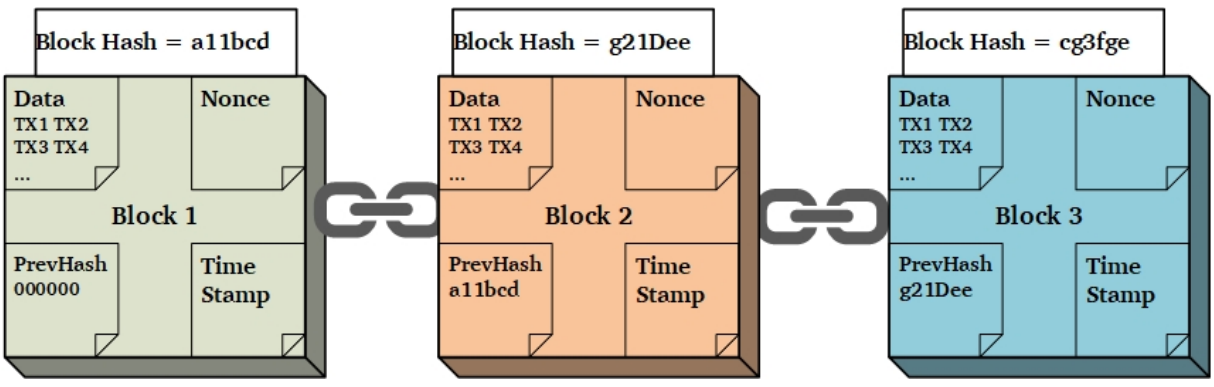

Figure 1: High Level Overview of the Blockchain

1.2 Blockchain Types

Blockchain technologies have experienced rapid growth in the recent years. The rapid pace of innovation has given rise to new models, paradigms and technologies in this sector. We now have multiple competing blockchain networks and solutions jostling for different segments of the market. There is Monero and Zcash focusing on privacy oriented solutions employing technologies like ring signatures [She14] and zk-SNARKS [Chr17]. Others like Ripple and Hyper Ledger are tailoring their solutions for specific segments of the market like banking and enterprise. This accelerate pace of innovation has ignited a fierce debate in the community as to what can and cannot be classified as a blockchain. Although there is no clear agreement on any classification but most publications tend to classify blockchains into two broad categories: Public or Permissionless Blockchain, and Private or Permissioned Blockchain [Blo16].

	Permissionless Blockchains (Public)	**Permissioned Blockchains (Private)**
Network Access	Any one can join the network	Only authorized participants can join
Minning	Any one can produce new blocks	Authorized block producers
Decentralization	Fully decentralized system	Can have limited to no decentralization
Speed	Slower compared to private blockchains	Faster
Transparency	Fully transaparent	Customizable level of transparency

Table 1: Permissioned vs Permissionless Blockchains

1.2.1 Permissionless Blockchains

They are highly decentralized networks that value decentralization, and censorship resistance above everything else. Permissionless systems basically allow any person or entity to interact with the network or run smart contracts [Agi16]. Every participant has equal rights to create, send, and view transactions. They can even choose to become block producers or miners and verify transactions in order to append them to the blockchain. Bitcoin was the first public blockchain and a realization of a vision outlined by Satoshi in his white paper [Nak08]. He identified decentralization, censorship resistance and distributed trust as the most important factors for the success of the peer-to-peer digital cash protocol he was proposing in his paper [Nak08].

Decentralization: Public blockchains are usually highly distributed and decentralized. This makes the network censorship resistant and harder to attack and bring down by any one entity.

Consensus Mechanisms: Decentralization is achieved at the cost of higher complexity hence public blockchains requires sophisticate consensus mechanisms. There are two main types of consensus mechanisms: Proof of Work [2.5.2], and Proof of Stake [2.5.3]. The process of reaching consensus and extending the blockchain is known as mining. Any participating node can run the mining software in order to verify transactions and extend the blockchain [Agi16] [Blo16].

Block Producers: Any node can choose to become a block producer or miner. Public blockchains usually employ a crypto economic model where by miners are rewarded using network assets or tokens.

Privacy: Without a central entity or coordinator transparency becomes an important feature for the participants and miners in order for them to trust the system. This transparency is often achieved by sacrificing some degree of privacy. By default, all transactions and data in a blockchain is public and can be easily accessed with the help of any block explorer.

1.2.2 Permissioned Blockchains

They are sometimes also referred to as private blockchains. It is a closed echo system where participants need permission from an administrator or special node to interact with the ledger. Only preapproved nodes or block producers can verify transactions and run smart contracts [Agi16]. Participants place some level of trust in these block validators or administrators. Permissioned blockchains can be run by members of a consortium in order to increase transparency and efficiency of inter organizational processes. They allow organizations to have better control over proprietary data while facilitating trusted exchange of secure information across organizational hierarchy [Agi16] [Blo16].

Decentralization: Permissioned systems can have varying degrees of decentralization. They can be fully centralized or partially decentralized. Systems like Hyperledger fabric allow fine grained control over governance models and the level of decentralization. In the end the level of decentralization in permissioned systems depends upon many factors including number of participants, their relationship with each other, degree of required fault tolerance, business rules and consensus algorithms participants agree on [Agi16] [Blo16].

Consensus Mechanisms: Permissioned blockchains usually do not need to run complex consensus algorithms. They can run simplified consensus mechanisms. This coupled with the fact that only a limited number of nodes are responsible for producing new blocks helps them become more efficient and scalable [Agi16] [Blo16].

Block Producers: Private blockchains can set out criteria for participants to become block producers. These criteria can be based on certain business rules or participating nodes might be required to meet special conditions in order to become block producers such as demonstrating certain capabilities like minimum hash power, or having possession of certain assets etc. Unlike public blockchains block producers are not rewarded with network assets rather they work together to increase efficiency, reduce business costs and boost productivity [Agi16] [Blo16].

Privacy: They can offer fine grained control over transaction visibility as opposed to public blockchains where basically any one can view any transaction by simply querying the blockchain or using a block explorer. This is a huge incentive for organizations to use permissioned blockchains as they might wish to prevent unauthorized disclosure of sensitive information [Agi16] [Blo16].

1.3 Motivation

Blockchain has exploded as the technology of the future for several industries including cross border payments, peer to peer transactions, regulatory compliance, healthcare and supply chain management. It provides a tamper proof immutable ledger which can be particularly useful in tracking goods and services as they move and change hands across borders in the supply chain. It enables new and innovative means of organizing and tracking data. In the modern era industries are highly interconnected through complex supply chains with their partners and suppliers across the globe. The success of a supply chain depends upon the integration and coordination of all of its participants. Consider the example of an Airbus A380 which is made up of four million individual parts and is built in six different sections in plants around Europe. Its wings are manufactured in Wales, the fuselage comes from Hamburg, Germany and the final assembly takes place in Toulouse figure [2]. This cross border and federated model of manufacturing is possible only through just-in-time manufacturing and supply chains. Airbus and other multinational companies depend on JIT to ensure that their products and services are competitive in the global market. JIT processes depend upon sophisticated supply chain management and Inventory tracking systems to maximize cost-efficiency and minimize delays. Transparency, efficient communication and quick dispute resolution are key to the success of any supply chain. Traditional supply chain management systems are mostly centralized and siloed inside organizational structures. These systems are highly dependent on human actors to update the state of the system. This can lead to side effects such as increased complexity, reduced efficiency, and human errors.

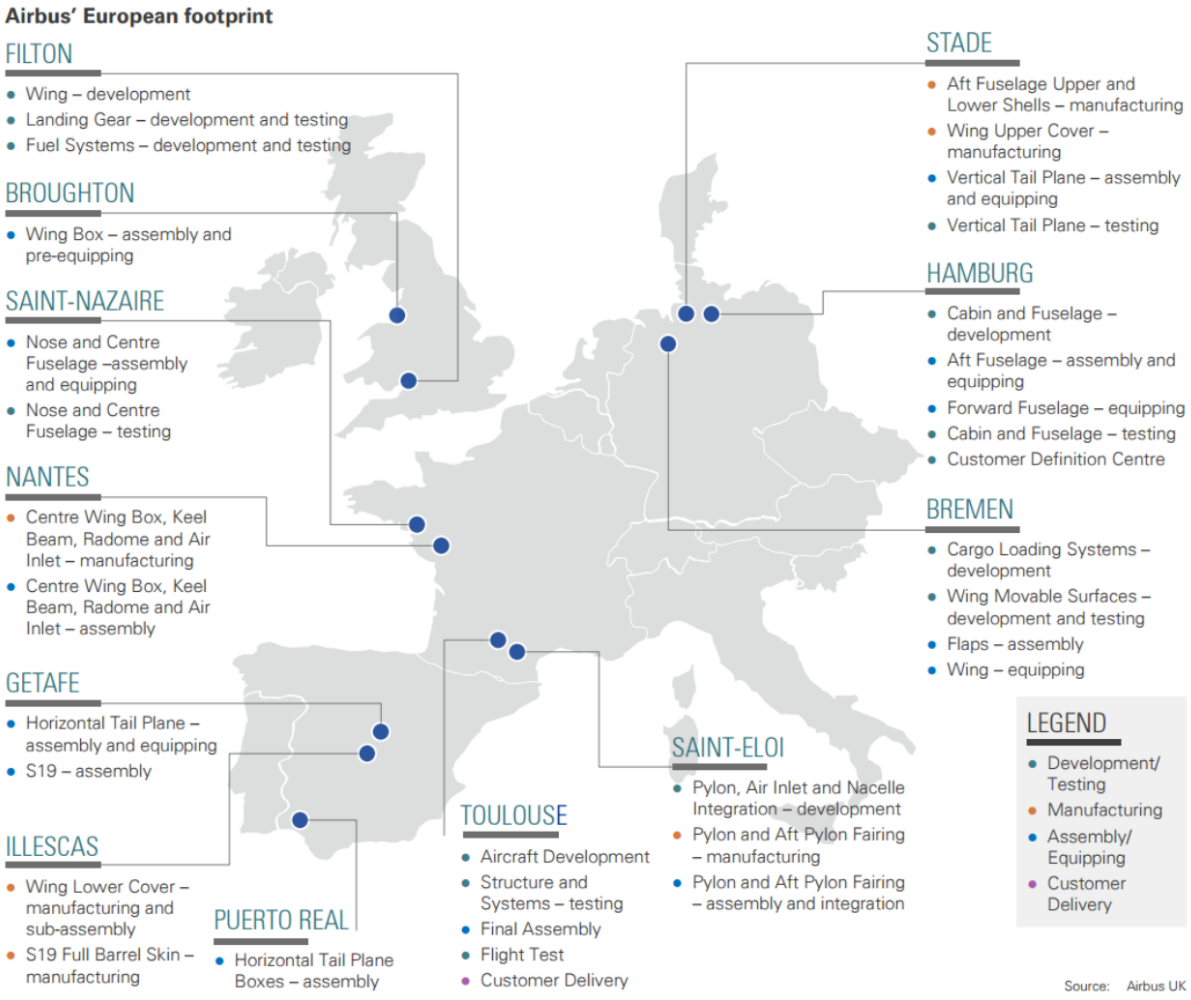

Figure 2: Integrated Supply Chains [Air18]

Blockchains can offer numerous benefits for streamlining processes and increasing transparency across the supply chain. Coupled with Smart Contracts and IoT, supply chain can become one of the killer applications of the blockchain. Smart Contract platforms such as the Ethereum can use tracking data to automate various functions and events in the supply chain life cycle. Ethereum's distributed ledger also provides total transparency to all parties involved. By increasing automation within supply chain processes they can reduce complexity and eliminate errors and delays. Some of the key benefit of blockchains in the context of SCM are follows:

Transparency: Its shared ledger enables all stakeholders to have the same view of the data stored on the blockchain. Transparency is greatly increased due to everyone having real time access to the same data.

Traceability and Compliance: Every transaction recorded on the blockchain is cryptographically verified. This increases traceability, reduces counterfeit and fraud and increases compliance for products.

Security: Any system built on the blockchain is by design highly secure against DDoS and single points of failure. Each transaction on the blockchain is replicated across multiple nodes on a distributed ledger. Each block links to a previous block hence any attacker wanting to modify data in any block will need to modify all subsequent blocks as well.

Trust: Most traditional SCM systems allow participants a very limited view throughout the supply chain life cycle. Usually participants only have access to information necessary to successfully realize the next process of the supply chain. This creates information asymmetry between different stake holders. Decentralized blockchain based SCM systems can allow participants to have same view of the entire system and hence reduce information asymmetry and increase trust.

1.4 Thesis Objective

The primary goal of this thesis is to design and develop a secure and decentralized supply chain management and tracking system. The state of the art for this system will be a smart contract for monitoring supply chain cycle under strict conditions and a decentralized application designed to interact with the smart contract in order to automate supply chain processes. In order to realize this system following questions and issues must be addressed:

(a) Which blockchain platform is best suited for development of this system?

(b) How to reduce complexity and increase automation in supply chain processes?

(c) Can we improve or enhance the blockchain security model by using post quantum signatures?

The exact requirements and design of this system based on a well quantified use case scenario is presented in chapter [5].

2 Blockchain: Technical Primer

This chapter explains some of the technical concepts and terminologies related to blockchain. This technology allows participants to transact with each other using a peer-to-peer network that guarantees censorship resistance, immutability, transaction finality, and protection against double spend attacks. In order to better explain how it works consider figure [3]. Alice wants to transfer two bitcoins to Bob. She uses her private key to creates a signed transaction for transferring these coins to Bob. Every user in the network has pair of keys; a public key that serves as their unique identifier or address and a private key for signing transactions see section [2.2]. The signed transaction is broadcast to the bitcoin network where it waits until it is picked up by a special node called a miner. The miner verifies transaction signatures and batches pending transactions into blocks. Each block carries the hash of the one that came immediately before it. Next step is to calculate the hash of the entire block and append it at the end of the blockchain see figure [3]. Blockchain protocols have built in consensus mechanism to ensure that peers always agree on only one longest chain see section [2.5]. Blockchain is not just a technology it is actually a systems and like most systems it is composed of individual components which come together to make the whole. The next few sections explain the important building blocks or sub components of the blockchain system.

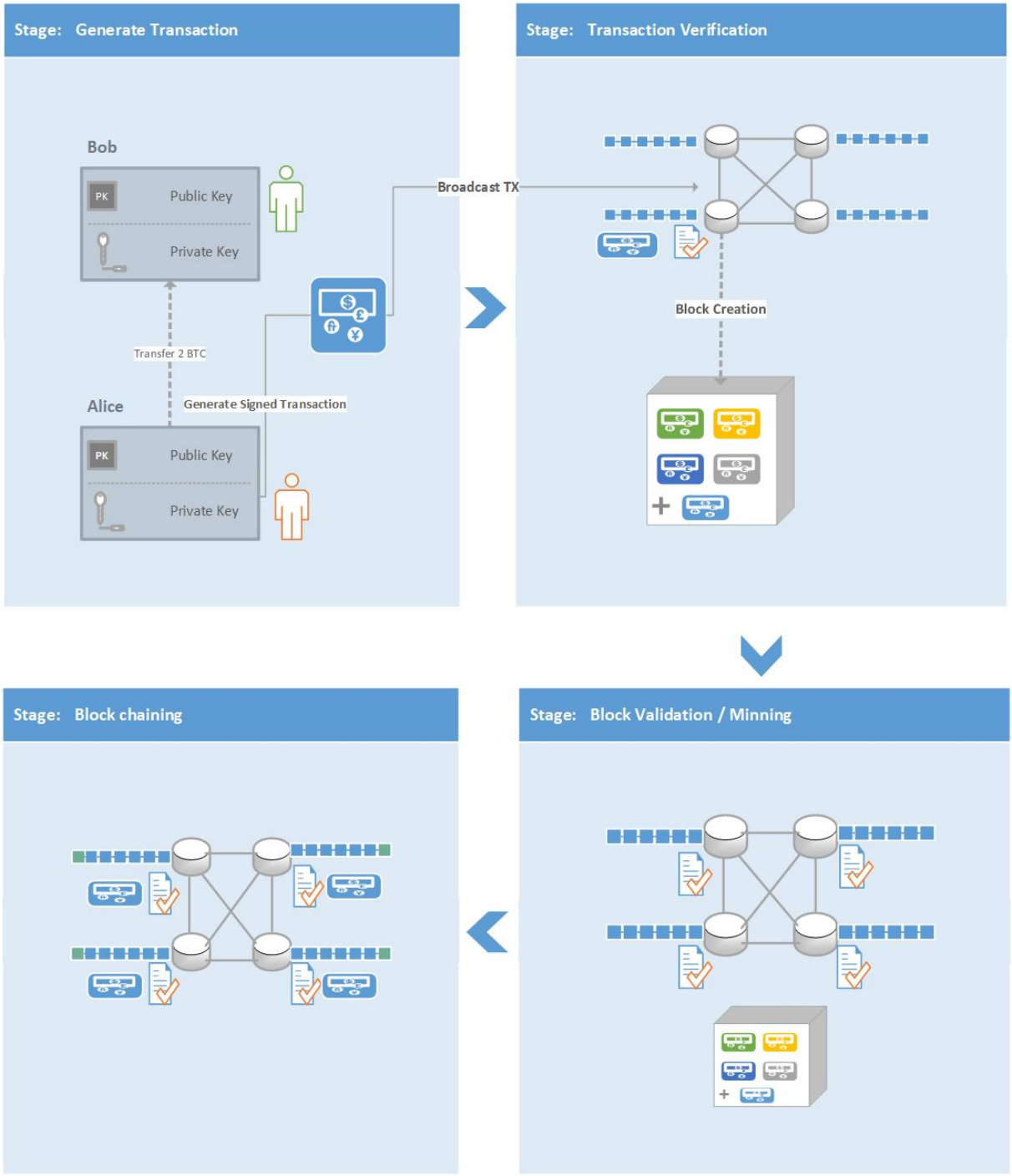

Figure 3: How does blockchain work?

2.1 Distributed Ledger Technology

Distributed ledger Technology refers to a shared and distributed database replicated across members of a peer-to-peer network. Each member of the network receives the same copy of the data. New data can only be added to the ledger when consensus is achieved among the members. Consensus rules and mechanisms [2.5] may vary from network to network. These rules are designed to ensure that data on the ledger remains synchronized across network participants. Blockchain is a special type of distributed ledger where cryptography is used to achieve consensus and ensure transaction authenticity. Information stored on the blockchain is immutable i.e. once recorded it cannot be altered. Blockchain is not the only structure used for DLT. IOTA [Wik18a] and Hashgraph have successfully employed Directed Acyclic Graphs (DAG) [Wik18c] for creating their DLT.

2.2 Asymmetric Cryptography

Asymmetric or public key cryptography is an important building block of any blockchain network. This cryptography technique relies on a pair of keys: A public key which is widely available or shared with everyone, and a private key which is only known to the owner. These two keys are mathetimatically related to each other in that one key usually encrypts and the other key is used for decryption. If the private key encrypts only the corresponding public key can decrypt and vice versa [Wik18e]. Public key cryptography is widely employed for:

Public key Encryption: is an encryption technique where data is encrypted using senders public key. The recipient can only decrypt the data and read the message if he is in possession of the corresponding private key.

Digital Signatures: based on public key cryptography are used in a number of applications including blockchain. Data or message is signed with sender's private key. Anyone can verify the message signature using the corresponding public key. In Bitcoin, Ethereum and other blockchain networks digital signatures are used to guarantee authenticity, integrity and non-repudiation.

2.2.1 Digital Wallets

In cryptocurrency applications we often hear the term digital wallets. It is a program which shows users account balance and helps them transfer coins to other users. In essence a digital wallet is the private key of that user. It provides additional functionalities like signing transactions for transferring coins, and querying the blockchain to get the cryptocurrency balance associated with their private key. Figure [4] shows how digital signatures are used in the blockchain.

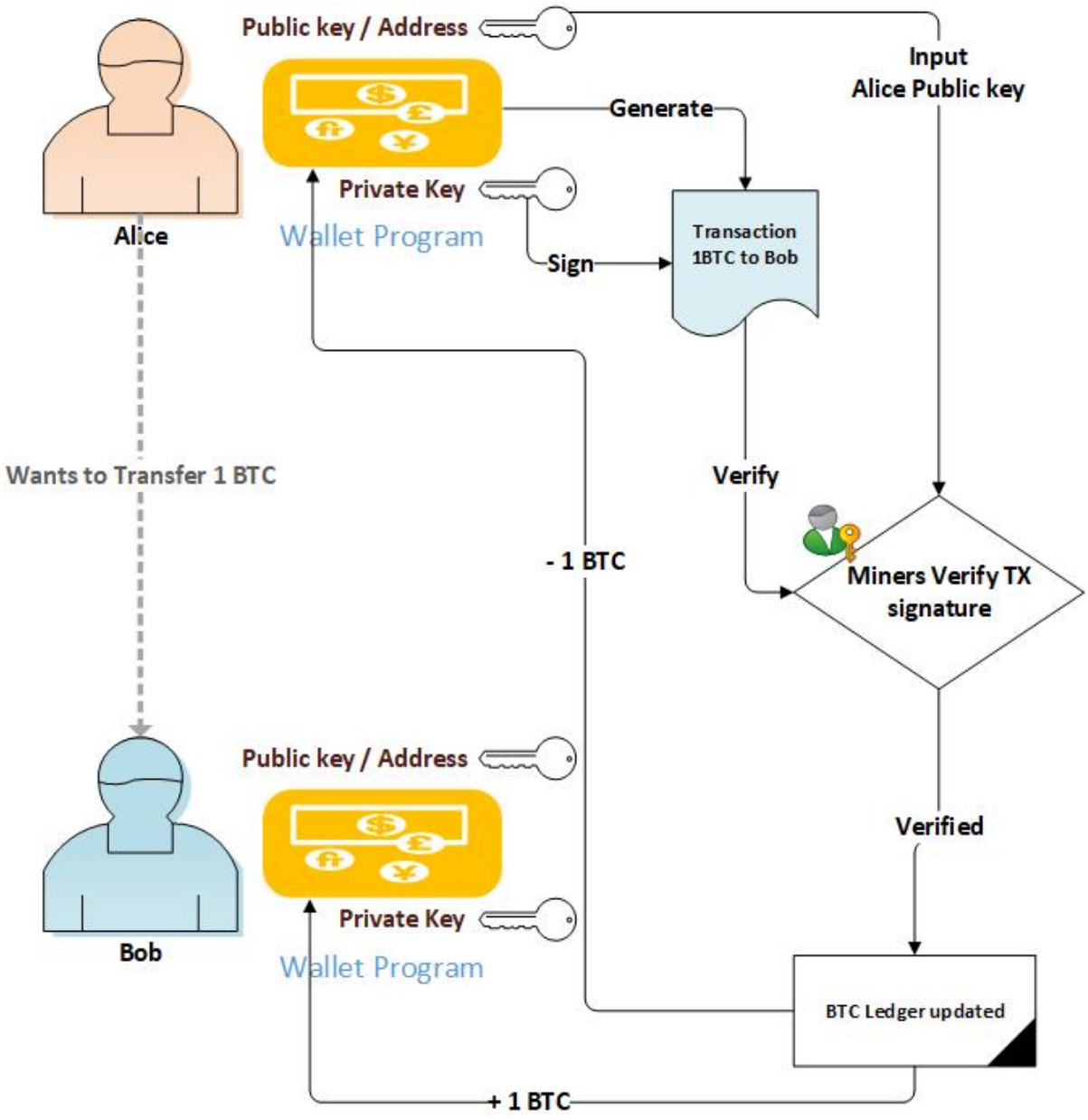

Figure 4: Digital Signatures in Blockchain

2.3 Hashing

Hashing is used to calculate fixed length hashes for variable length data. Hashing algorithms are designed in a way that even a slight change in the input data will result in a vastly different output hash. All cryptocurrency networks use some sort of hashing algorithms in their mining [2.5] process. Ethereum uses an algorithm called Ethash (modfied Dagger Hashimoto) and bitcoin uses SHA-256 [Quy15] hashing algorithm. These algorithms are used as a mechanism to guarantee integrity and to prevent unauthorized tampering and corruption of the distributed ledger. They are used to link blocks with each other in the blockchain. Each new block contains the hash of the blockchain that came before it as shown in figure [1]. Each blocks hash represents the state of the blockchain when it was created. This allows anyone to easily verify the complete state of the entire blockchain. Any attempt to alter data in any block will result in a vastly different hash for that block and will also require that hashes for all subsequent blocks be recalculated.

2.4 Merkle Trees

Blockchain is defined as a continuously growing list of transactions called blocks [Wik18b]. A block contains multiple transactions and a hash as shown in figure [1]. This hash is calculated over the entire block. A block is actually a special data structure which is implemented with the help of a Merkle tree as shown in figure [5]. Andreas Antonopoulos defines merkle trees in his book "Mastering Bitcoin" as *"A merkle tree, also known as a binary hash tree, is a data structure used for efficiently summarizing and verifying the integrity of large sets of data."* [And14] (ch.9). They are used to summarize all transactions in a block using cryptographic hashes. This enables fast and efficient verification of any transaction in a particular block. In a tree comprising of N data elements only $2 * log2(N)$ calculations are required to verify if a particular data element or transaction is included or not. Without Merkle trees it will be prohibitively expensive to run blockchain nodes which would severely impact the decentralization of the system. In bitcoin a Merkle tree is constructed by recursively hashing pair of nodes using SHA256 cryptographic hash function as shown in figure [6] [And14] (ch.9). In the example tree there are four leaf nodes storing hashes of four transactions. The leaf nodes do not store actual transactions rather TX data is hashed and result is stored in the Merkle tree. Each leaf node is designated as H_A, H_B, H_C, H_D and given by the equation:

$$H_A = SHA256(SHA256(Transaction_A))$$

Since Merkle trees are in essence binary trees hence even number of nodes are required to have a balanced tree. Two leaf nodes are hashed together to form a parent node as given by equation (1). In the event of odd number of transactions, the last transaction is duplicated to have an even number of leaf nodes equation (2). The recursive hashing process starts from the bottom and continues until there

is only one node left at the top which is called the Merkle Root. This is the parent hash of all child nodes and summarizes all the data in all transactions. The root hash is placed in the block header.

$$H_{AB} = SHA256(SHA256(H_A + H_B)) \tag{1}$$

$$H_{CC} = SHA256(SHA256(H_C + H_C)) \tag{2}$$

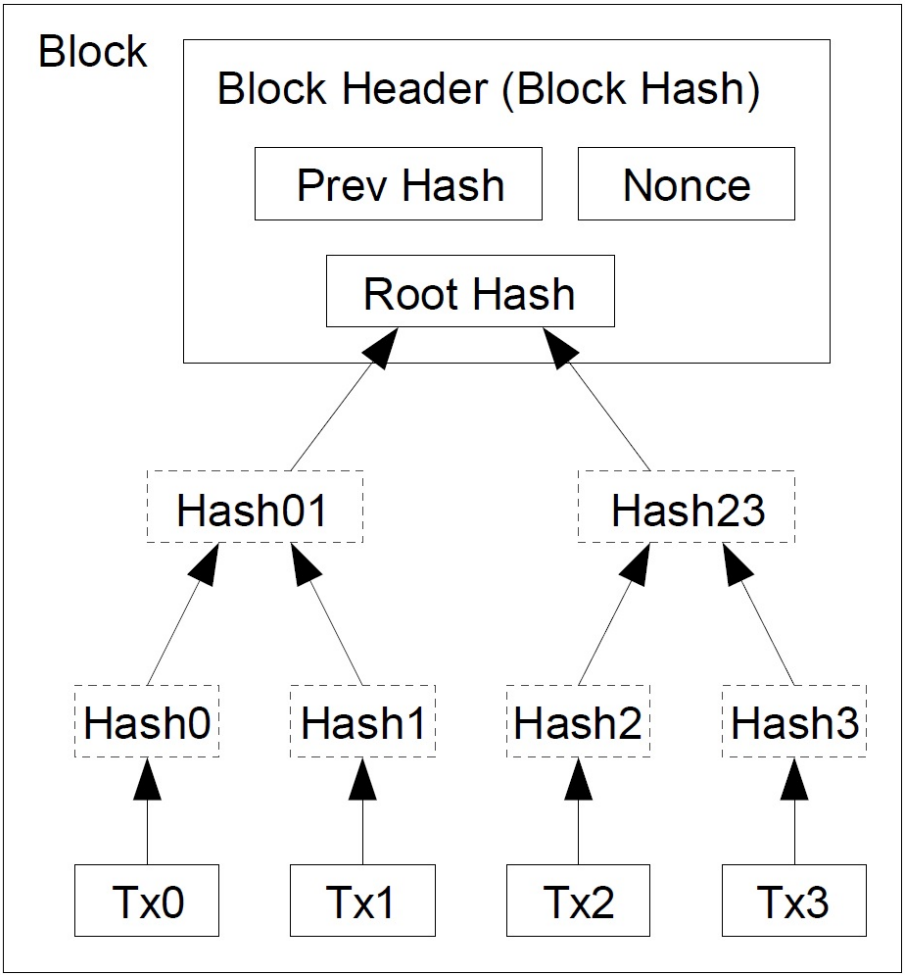

Figure 5: Transactions Hashed in a Merkle Tree [Nak08]

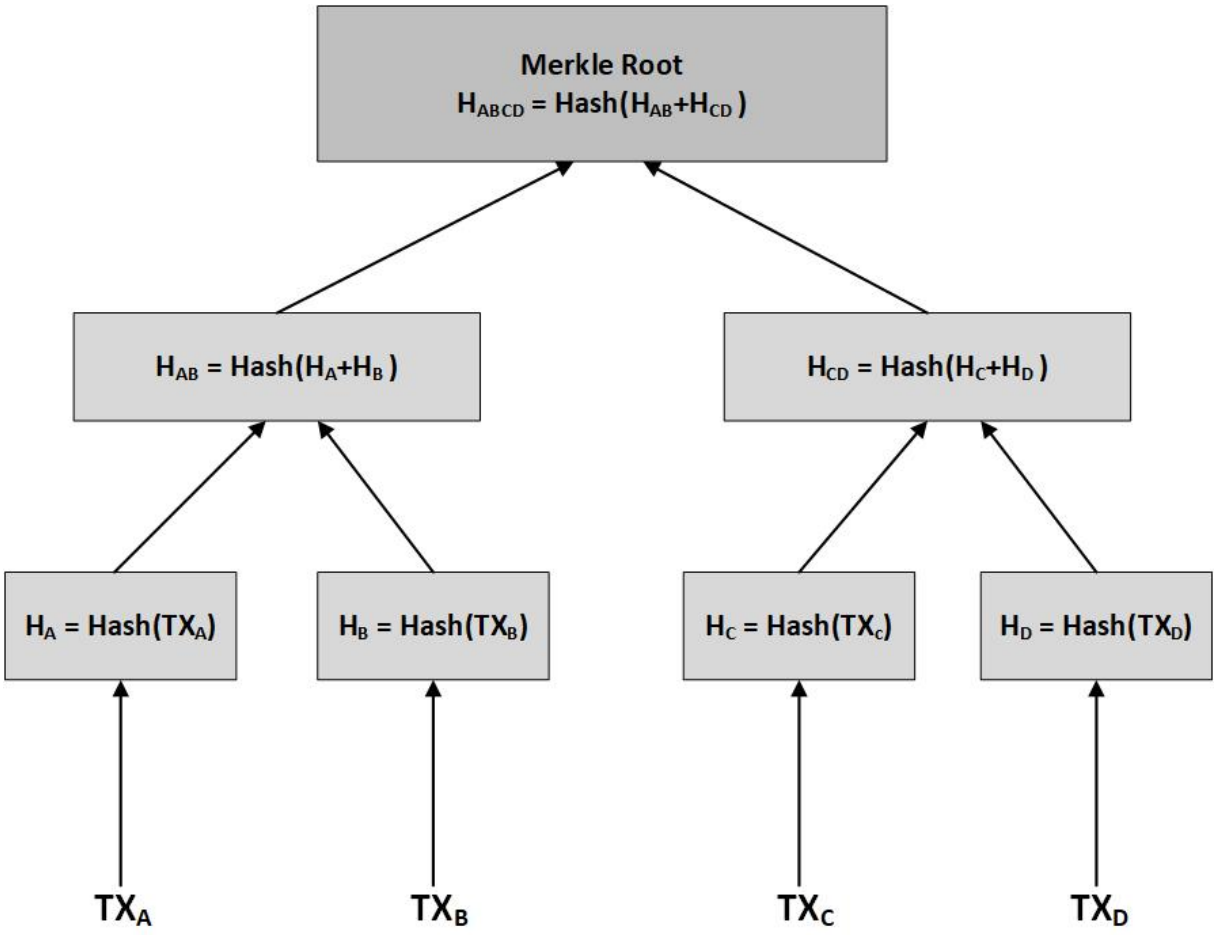

Figure 6: Constructing a Merkle Tree, adapted from [And14]

2.5 Consensus Mechanisms - Mining

Electronic coins are defined as a chain of digital signatures that serves to establish ownership. In order for Alice to transfer one coin to Bob she must sign the hash of a previous transaction and the public key of the next owner i.e. Bob. Anyone can verify the chain of ownership by verifying signatures. This process only verifies that Alice was in possession of the coin at some point in time, it does not guarantee that Alice did not try to spend the same coin more than once. Therefor a mechanism is needed that guarantees that any previous owner (Alice) did not sign any earlier transaction for transferring the same coin. The only way to verify this in a decentralize system is to announce all transactions and to have a mechanism to ensure that all participants agree on a single shared history or order of transactions. Payee (Bob) needs proof that at the time of each transaction, the majority of participants agreed that it was the first one [Nak08]. The process which establishes consensus among all participants is called Mining.

2.5.1 Mining

Mining underpins bitcoin or blockchain's security model. This process is a designed to guarantee security and integrity of the distributed ledger. It serves to protect the network from fraudulent transactions and double spend attacks i.e. spending the same coins twice. It is also the process by which new blocks are generated. Miners spend something of value like electricity in the form of computing power by running complicated algorithms (Proof of Work). They are rewarded by the network with block rewards or newly minted coins. It prevents bad actors or attackers from modifying the state of decentralized ledger against network rules. Attackers will need to control at least fifty-one percent of network hash rate to mount a successful attack. This is virtually impossible in a sufficiently decentralized network like Bitcoin or Ethereum. There are two main type of mining algorithms Proof-of-Work 2.5.2 and Proof-of-Stake 2.5.3.

2.5.2 Proof-of-Work

It was proposed by Satoshi Nakamoto in the bitcoin white paper [Nak08]as means for establishing consensus. Miners solve complicated mathematical problems to validate transactions. Pending transactions are batched into blocks and the miners compete with each other to calculate the hash of the block. The hash output of the block must start with specific number of leading zeroes in order to satisfy protocol rules. The exact number of leading zeroes depend upon the network difficulty and is adjusted automatically every 2016 block. This difficulty determines how easy or hard it is to find the output hash for a block. The function that calculates difficulty is determined by a moving average and targets average number of blocks per hour. If blocks are generated too fast, the difficulty increases and vice versa. This is done in order to compensate for increasing hardware speed and varying interests in running nodes. Proof-of-work protocols can be summarized in the following steps [Jim18].

- Miners try to find the hash output for a block with a fixed number of leading zeroes. They do this by repeatedly changing part of the block called nonce and recalculating the hash output.

- First miner to solve the puzzle and find the hash broadcasts his solution or proof-of-work to the rest of the network.

- Upon receiving the solution other miners verify it to ensure that it is correct. Before they agree to add the it to the blockchain they verify all the transaction in the block to make sure they are valid.

- If majority of miners agree on the solution and agree to add the block to the blockchain than consensus is achieved.

2.5.3 Proof-of-Stake

Proof of Work algorithms require miners to solve complicated math problems to verify transactions and generate new blocks. This approach has some inherent disadvantages. It requires huge amounts of electricity to achieve consensus in large blockchain networks such as Bitcoin and Ethereum. Some estimates have put bitcoins annual energy consumption on the same level as countries likes Austria or Switzerland. POW operates on the basis of one CPU one vote model. This approach can lead to mining centralization by large mining pools and chip manufacturers. Proof of Stake is an alternative approach for reaching consensus and protecting from double spend attacks in a decentralized network. It solves many problems inherent to POW algorithms. It is defined as *"Proof of Stake (PoS) is a category of consensus algorithms for public blockchains that depend on a validator's economic stake in the network"* [Eth18]. POS requires users or forgers as they are called to lock up their digital coins in an escrow to get a chance to validate new blocks. The deposited coins serve as collateral and an incentive for the forgers to behave honestly. If a forger approves fraudulent transaction they will lose the coins they staked and will be banned from participating in the block validation process in the future. The crux of POS systems is the fact that for any attack to be successful the attacker will need to own majority of the coins on the network. Therefore, the attacker will be the one most severely impacted by his own attack [Bit12]. This serves as a huge deterrent against any potential bad actors. Block validators are incentivized with block rewards (combination of Tx fees and coins). They are selected by the network in a pseudo – random selection process based on a combination of factors. Selecting forgers solely on the size of their stake will hugely benefit the rich miners making the rich even more richer. There are several methods to avoid these problems two of which are given below. [Max18][Sha17]

Coin Age based Selection: This method choses validators based on how long their coins have been staked for or the 'coin age' of their stake. The coin age is calculated by multiplying the size of a validators stake with the number of days the coins have been held in escrow. Once a validator generates a block their coin age is reset and they have to wait a fixed amount of time before they can be selected to validate another block [Sha17].

Randomized Block Selection: This method choses validators based on a combination of lowest hash value and the size of their stake [Sha17].

2.6 Challenges:Scaling Debate

Blockchain technology is still in its infancy. It is a novel idea to solve several interesting problems in a trustless and decentralized manner, however in order to compete with existing centralized platforms it needs to be able to scale to handle millions of transactions per second. Let us consider the most common use case where the blockchain is used for making payments or to transfer assets between users. Bitcoin can on average perform 3 to 4 transactions per second while Ethereum can handle up to 20 transactions per second. Compare this to Visa which on average handled over 1100 transactions per second in 2016 and has an estimated capacity to perform up to 100000 transactions in a second [Fre17]. Transaction speed measured in TPS is an important to metric to measure the performance of any financial system. During 2016 and 2017 major blockchain networks saw enormous growth in their user base. This caused exponential increase in transaction volume resulting in congested networks which caused huge delays in transaction confirmations [7]. This had a domino effect on transaction fees as well, causing them to sky rocket as miners are incentivized to pick transactions with higher fees to mine first. The long confirmation delays coupled with high transactions fees caused many organizations and vendors to stop accepting bitcoins. There was an interesting case in 2017 when a conference held to promote the benefits of bitcoin and blockchain stopped accepting bitcoins as a mode of payment due precisely due to reasons outlined earlier. The scaling problem is further amplified in smart contract platforms like Ethereum[4.1] which aim to be a hub for large scale decentralized applications or Dapps. Most existing and proposed Dapps use mircotransaction (MTX) as part of their business model. "Microtransactions are a business model where users can purchase virtual goods via micropayments" [Wik18d]. In order to efficiently run such applications Ethereum needs a way to effectively handle μ-transactions. In most cases these transactions need to be executed immediately and cannot wait for long block confirmation times. According to some estimates using current mechanisms "we're roughly 250x off being able to run a 10m user app and 25,000x off being able to run Facebook on chain" [Fre17]. This requires exponential increase in transactions per second for blockchain to become a viable alternative to centralized solutions.

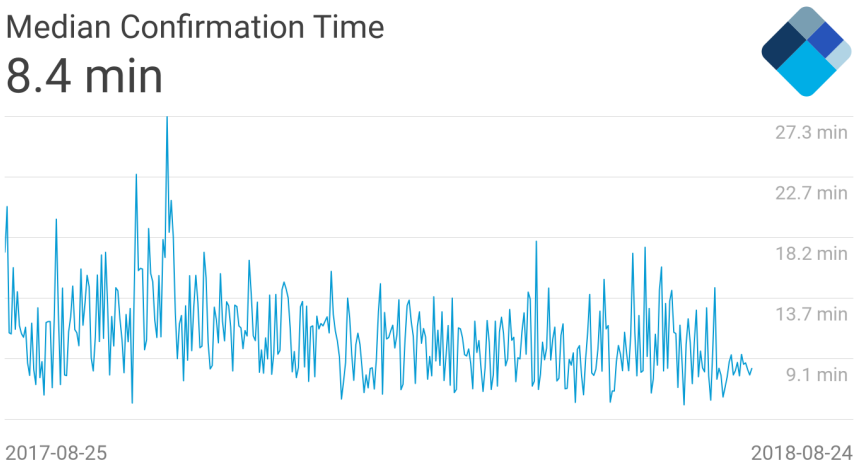

Figure 7: Median confirmation times for BTC transactions [Blo18]

2.6.1 Increasing Blocksize

Transactions are grouped into blocks before they are verified. POW consensus rules require that there is some distance between successive blocks so that each verified block is successively incorporated by a majority of nodes in their copy of the ledger. This means that roughly only one block is generated every ten minutes [Nak08]. In addition, some blockchains like Bitcoin have placed an upper limit on the size of each block. Currently for bitcoin the block size limit is 1 megabyte. One suggestion is to simply increase the block limit to allow more transactions to be verified at any given time. This solution however has many problems first of all increasing block size results in only a linear increase in transactions per second. Secondly, it will adversely impact the decentralization of the network. Larger blocks require higher computational power to process each block and also drastically impact the size of the distributed ledger. This leads to more centralization as not everyone can afford the equipment required to successfully mine new blocks [GoC17].

2.6.2 Payment Channels - Lightning Network

An alternative solution is to use Layer - 2 transaction networks. Lightning network is bitcoins proposed solution for the scaling problem. Lightning network is defined as *"A decentralized system for instant, high-volume micropayments that removes the risk of delegating custody of funds to trusted third parties"* [JP16]. It advocates using payment channels to handle transactions off chain. *"Payment Channel is class of techniques designed to allow users to make multiple Bitcoin transactions without committing all of the transactions to the Bitcoin block chain. In a typical payment channel, only two transactions are added to the block chain but an unlimited or nearly unlimited number of payments can be made between the participants"* [Bit16]. Payment channels are essentially multi-signature bitcoin addresses. In order to spend funds from the channel both parties must sign off on the transaction agreeing to the new balance of the channel. The new balance is stored as the most recent transaction in the channel. Simply put, a payment channel is a smart contract on the bitcoin blockchain which is mostly executed off-chain after creation. In an ideal case, the only two transactions that go on the block chain are the ones for opening and closing a channel [Lig15]. Participants of the channels can make unlimited instant transactions to each other while the channel is open. *"Security is enforced by blockchain smart-contracts without creating an on-blockchain transaction for individual payments. Payment speed is measured in milliseconds to seconds"* [JP16]. This enables users to make off chain payments with confidence. If anything goes wrong blockchain can cryptographically verify the terms of the smart contract and enforce them on-chain [Bit16] [Jef15].

2.6.3 Sidechains

Sidechain is a blockchain that runs parallel to the main blockchain. It extends the functionality of the main chain enabling decentralize transfer of assets and tokens between the two chains. They allow coins to be moved between two separate blockchains. Tokens from the main chain can be securely moved to the sidechain and used in these chains. The token transfer takes places at a fixed predetermined rate [RIC14]. In order to transfer main chain assets to a side chain they are sent to a special address on the main chain. Once this transaction is verified a confirmation is broadcast in the sidechain enabling the network to assign equivalent assets to the users account in the sidechain [Ada14]. They can help with blockchain scaling as they can take some of the pressure of the main chain. Developers can design specialized sidechains to run their Dapps more efficiently while still taking advantage of security and decentralization provided by the mainchain. Sidechains are implemented using a Two – way peg as shown in figure [8].

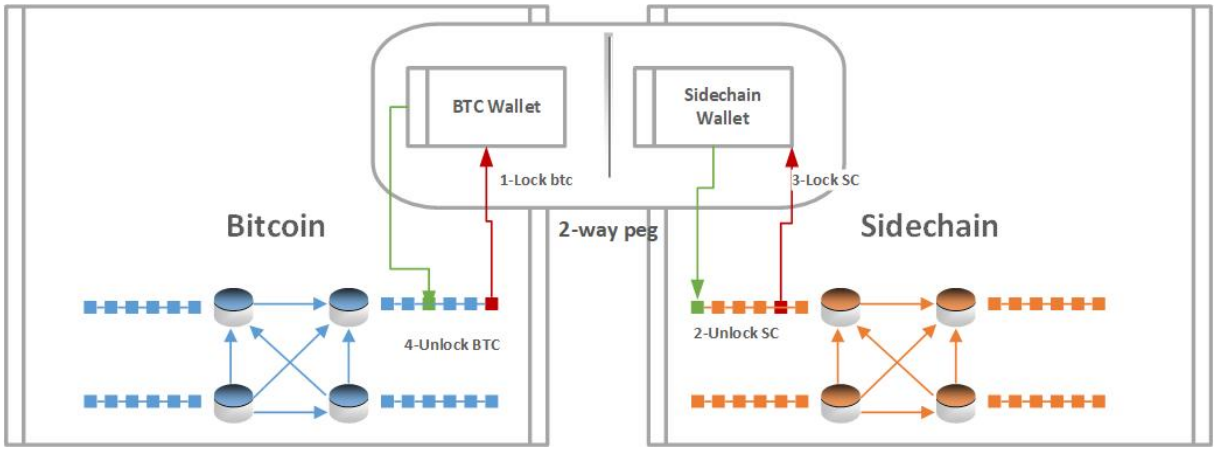

Figure 8: Two way Pegged Sidechain

RootStock RSK SideChain It is a sidechain to bitcoin. It is Two-way pegged to bitcoin. RSK code aims to be backwards compatible to Ethereum i.e. code can be written in solidity or serpent and can be used on Ethereum. RSK aims to be a platform for decentralized applications and smart contracts on bitcoin. Miners are incentivized to mine smart contracts on RSK by rewarding them with bitcoins. Bitcoin miners can simultaneously mine both blockchains and rewarded through a process called “merge-mining”. Rootstock has its own version of Ethereum virtual machine (EVM). Currently the developers are working on what is called a federated peg which is essentially a system of notaries and a Multisignature exit address. The developers aim to go from federated peg to a two-way pegged system based on Simplified Payment Verification (SPV) [And14] [Ser15].

Federated peg: is a system consisting of a set of notaries and a Multisignature exit address. When you send funds to this exit address you can create an SPV proof on RSK sidechain. This SPV proof allows you to convert the locked bitcoins in the federated address into bitcoins on rootstock sidechain. This is done automatically. However, moving funds from RSK back to bitcoin requires collaboration of federators. Basically a smart contract acts as bridge master and controls all unspent transaction outputs. This contract broadcasts a transaction to federators by using a log message. On receiving this message, federators send signatures to bridge master who combines all these signatures in to a fully signed transaction. This signed transaction is broadcast to RSK blockchain where any user can put this transaction onto bitcoin blockchain. This unlocks bitcoins on the bitcoin blockchain [Ser15].

3 Blockchain Applications

Companies and People across the globe are exploring applications of blockchain technology across several industries. This chapter details blockchain applications and projects from various sectors including finance, Internet of Things, Supply chain Management and File hosting and sharing.

3.1 Crypto Currencies

Bitcoin was the first ever application of blockchain technology. It was proposed and developed shortly after the financial crash of 2007. This crash was caused by the irregularities in the existing centralized financial institutions and banks. The biggest problem with traditional banking is that it centralizes trust in a few large financial institutions and banks. This system works only as long as these banks operate reliably and responsibly. The financial crash of 2007 showed that they cannot be always trusted to act responsibly [Pat12]. Bitcoin was developed to address problems prevalent in existing centralized financial system. It solves these problems by developing a system which removes all central entities and trust is established through a system of checks and balances [2]. Cryptocurrency sector experienced huge growth in terms of users and investment during 2016 and 2017 and at one point was worth close to 500 billion dollars [Wil12]. Unfortunately, most of this growth was due to speculative investments and has not yet translated into large scale adoption of Cryptocurrencies in everyday business and finance. Blockchain powered financial systems have huge promise provided they are able to solve some of the challenges outlined in [2.6].

3.2 Internet of Things

IoT is the next wave of automation promising to disrupt industrial and domestic structures and processes. The billions of smart devices coming online could transform homes, cities, offices and factory floors [IBM16]. *"IoT holds the promise to expand business processes and to accelerate growth. However, the rapid evolution of the IoT market has caused an explosion in the number and variety of IoT solutions, which created real challenges as the industry evolves, mainly, the urgent need for a secure IoT model to perform common tasks such as sensing, processing, storage, and communicating"* [Ahm16]. Currently IoT ecosystems are realized using brokered communication models based on client/server paradigm. Devices are connected through cloud servers using the internet even if they are few feet away from each other. Further more centralized models struggle to scale up to meet the demands of billions of users or devices [Ben16]. Blockchains offer an intriguing alternative as a secure and decentralized IoT command, control and communication model. Blockchain and Smart contract based solutions should be more manageable and scalable then traditional ones. Blockchains are inherently tamper resistant hence they will prevent one or more rogue devices from causing a complete system breakdown across a home, factory, or transportation system. Blockchain in IoT sphere has the potential to revolutionize several industries and businesses [IBM16] [Ben16] [Ahm16].

There are several exciting projects working towards this goal. Sections [3.2.1]and [3.2.2] describe two projects at the forefront of blockchain and IoT.

Smart Washing Machine This example is a realization of proof of concept proposal from Samsung. *"Imagine a washer that autonomously contacts suppliers and places orders when it's low on detergent, performs self-service and maintenance, downloads new washing programs from outside sources, schedules its cycles to take advantage of electricity prices and negotiates with peer devices to optimize its environment"* [Ben16]. If the machine is connected to some sort of ledger be it private or public, it can automatically pay the detergent suppliers and repairmen [Ben16] [Pur16].

3.2.1 Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT)

It is a joint venture between IBM and Samsung Electronics. It is developed to serve as a validation platform for projects proposing to connect IoT and Blockchain. It envisions network of devices that are capable of autonomously maintaining themselves. Adept is working towards integrating IBMs Watson IoT platform with blockchain technologies. It is currently still in development stage but proof of concept has already been implemented [Pur16]. It uses blockchains as the backbone of the system using a mix of proof of work and proof stake to secure transactions. The ADEPT architecture supports three foundational functions.

- Peer to Peer encrypted messaging using a secure messaging protocol called TELEHASh [Pur16].
- Decentralized file sharing based on BitTorrent protocol [Pur16].
- Decentralize device coordination and control In the absence of centralize controller, device control and coordination becomes significantly challenging. Adept uses Ethereum or hyper ledger blockchain to implement this in a trustless secure fashion [Pur16].

Ultimately it will enable IoT devices to send data to private blockchain ledgers for inclusion in shared transactions with tamper-resistant records. Devices will be able to communicate with the blockchain in order to update or validate smart contracts. This will improve transparency and reduce conflicts by empowering all stake holders. Each stakeholder will have access to the same data and could easily verify all transactions [Pur16] [Ben16].

3.2.2 Filament

Filament is a technology stack that *"enables devices to discover, communicate, and interact with each other in a fully autonomous and distributed manner"* [Fil16a]. Its main focus is industrial Internet of Things. *"The Filament technology stack is built upon five key principles: Security, Privacy, Autonomy, Decentralization, and Exchange (SPADE)"* [Fil16a]. Filament uses Telehash for secure encrypted device to device communication. Secure Identity is provided by blockchain. Once a secure communication channel has been established between devices, smart contracts are used to interact with them, or to enable them to transact with each other. Smart Contracts in Filament run directly on device and accept or run transactions from other devices based on contractual terms. It uses a protocol suite called "JOSE" (Javascript Object signing and Encryption) to implement smart contracts on the devices [Fil16b]. In order to enable micro transactions on these embedded devices authors of the Filament project propose a solution called Penny Bank. It allows the devices to exchange small amounts of value with each other without involving the blockchain for every single transaction thereby avoiding heavy transaction fees [Fil16a].

3.3 Supply Chain Management

Blockchains allow secure and permanent documentation of transactions in a decentralized ledger. They can be monitored transparently by all parties. This can improve efficiency and reduce human mistakes and time delays. It can also enable users to verify authenticity of products by tracking them from their origin. An example of this is securing supply chains of diamonds from mine to consumers. IBM's Hyperledger Fabric is one of the proposals working in this field. It is permissioned blockchain infrastructure designed specifically for handling supply chain management tasks. Using blockchain technologies customers can verify when and where a diamond was mined, all the places it passed through during its journey to the retailer, and whether or not during any step of the supply chain it crossed any moral or legal grey areas i.e. if it's a blood diamond.

3.3.1 Skuchain

Sku chain is a platform that uses blockchain to provide security, efficiency and transparency to supply chains. Today's supply chain management tools such as ERP systems, Inventory Management systems, Letters of credits, Purchase and Invoicing tools have significant friction and problems interfacing with each other. This results in increased costs and delays in every process of the supply chain. SKuchain proposes tools in order to resolve some of these issues [Sku17].

IMT: *"IMT provides inventory financing that de-risks transactions and unlocks capital opportunities for the entire supply chain. The original contract between the buyer and seller is assigned to IMT in the blockchain. This acts as a Blockchain Based Security Interest that provides the collateral to an investor in the IMT fund. IMT uses its funds to purchase goods from the seller and stores them at a VMI warehouse. Finished goods are*

shipped pursuant to a purchase order from the buyer, a process covered by insurance. The buyer then pays IMT for the goods" [Sku17].

Brackets Smart contracts on the skuchain are called brackets. They are cryptographically secured. They provide some key advantages.

- They are designed to release collateral as a result of being triggered automatically by real world events [Sku17].
- They improve transparency for all participants by providing real time view of transaction state [Sku17].
- *"It enhances liquidity of collateralized assets in a supply chain by improving upon current trade finance instruments such as Factoring, PO Financing and Vendor Managed Inventory Financing. It also creates the opportunity for Deep Tier Financing"* [Sku17].

PopCodes *"Popcodes are Proof of Provenance codes, a crypto-serialization solution to track flow of goods on SKU level. They provide bank-grade traceability to track physical value in the supply chain. Popcodes are sophisticated in their ability to track sub-assemblies, parts and raw materials used to make a finished product. Using Popcodes, an enterprise can gain JIT visibility across the entire supply chain ecosystem, enabling optimal agility and planning. It also provides end-consumer visibility into the entire history of the product"* [Sku17].

3.3.2 Provenance

This project is working on using blockchain technology to enable secure traceability of certifications and other salient information in the supply chain. It aims to become a platform for verifying authenticity of goods. *"Provenance enables every physical product to come with a digital 'passport' that proves authenticity (Is this product what it claims to be?) and origin (Where does this product come from?), creating an auditable record of the journey behind all physical products"* [Ben15]. They are creating a decentralized app for solving certification and chain of custody challenge in sustainable supply chains. It proposes a system to assign and verify certain properties of physical products using the blockchain. There are six different actors involved in the proposed scheme namely.

- Producers
- Manufacturers
- Registrars, they provide unique identity to other actors in the scheme
- Standards organizations, which define the rules of a certain scheme (e.g., Fairtrade)

- Certifiers and auditors
- Customers

The architecture in their white paper [Ben15] consists of number of modular programs. Namely Registration program, Standards programs, Production programs, and Manufacturing programs. Each contract is deployed on the blockchain independently but since all of them work within the same blockchain system they can interact without friction. Technologies such as NFC, RFID, barcodes, and digital tags link physical products to their digital representation on the blockchain. Furthermore, user facing application in the form of smart phone applications will facilitate access to the blockchain. They will aggregate and display information to customers in real time, detailing every step of the supply chain [Ben15].

3.4 Filesharing

Filecoin, SiaCoin and Storj are some of the proposals for creating a decentralized platform for filesharing, storage and cloud computing using the blockchain. The idea is simple users instead of uploading files to a central cloud server hosted at google, Microsoft or Dropbox files are shredded, encrypted and spread across the distributed file storage network based on the blockchain. Only the uploader holds the keys to call smart contracts to decrypt and reassemble the files. People participating as hosts in the network rent out their storage spaces and get paid in return for the services they provide [mis17].

3.4.1 FileCoin

Filecoin *"Filecoin is a decentralized storage network that is auditable and publically verifiable. Clients pay miners for data storage and retrieval. Clients offer data storage and disk space in exchange for payments. The network achieves robustness by replicating and dispersing content while automatically detecting and repairing replica failures"* [Pro17].

Proof of Storage Proof of storage is a class of decentralized challenge response protocols. They allow a storage provider or host to efficiently verify the integrity of the data stored on their device to their users or clients. The client sends encrypted version of its data to the hosting node for storage, while keeping a small portion of that data himself so he can cryptographically verify the integrity of data stored on the hosting node at any time [Pro17].

Proof of Replication Proof of Replication Filecoin introduced a special form of proof of storage protocols called Proof of Replication. It is an extension of Proof of Storage protocol. It enables a miner to convince a user that some data D has been successfully replicated to its own unique physical storage S. It uses challenge/ response protocol to achieve this [Pro17]. Traditional PoS protocols are limited in that they only prove that a miner or host was in possession of data at the time of challenge/response. Filecoin developed PoR protocol in order to provide stronger guarantees against Sybil attacks, Outsourcing attacks and Generation attacks [Pro17]. These attacks are exploited by malicious nodes to gain reward

for storage that they are not actually providing. Such greedy miners reduce the overall capacity and performance of the network. These attacks are discussed below.

Sybil Attacks A malicious attacker may want to claim the reward for storing multiple copies of some data D. They can cheat the system in traditional PoS protocols by claiming to store multiple copies using Sybil identities, while in reality only storing one physical copy of the D [Pro17].

Outsourcing Attacks A malicious miner could exploit the system by quickly fetching the data D he is claiming to store from other nodes at the time of challenge/response [Pro17].

Generation Attacks A malicious miner could rely on small but efficient program to quickly generate the data D when it is requested. This could allow such an attacker to gain reward for storing large amounts of data even when he physically does not have the capacity to do so [Pro17].

Proof of Space Time Proof of Space Time is a novel implementation of PoS. It allows a user to verify that the data was being stored by the miners throughout a period of time. A natural way to verify this would be by repeatedly sending challenges to the miners. This implementation would quickly bottle neck the network by flooding it with larger number of communication requests. Proof of space time instead requires a storage provider to produce a sequential proof of storage for a period of time and then recursively compose them together to generate a complete proof [Pro17].

4 Fundamentals - Technology Stacks

4.1 Ethereum

created by vitalik beutarin, a platform for smart contracts mention different mining algorithm which memory hard and ASIC resistant to prevent mining centralization and monopolies present in bitcoin due to ASICS and large mining pools

4.1.1 Ethereum virtual machine

4.1.2 Merkle Trees in Ethereum

https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/ there is a difference we use three merkle trees instead of 1 to denote state in evm, mention reason for it etc.

4.1.3 Smart Contracts

Use a figure to exaplain how smart contracts are, i.e. draw a figure/ flowchart like showing signed transaction comming in, smart contract executing it, and triggering events or results or altering state of blockchain. etc use the figure of smart contract given on the following papers as starting point https://github.com/ramxis/Thesis/blob/master/Miscellaneous/Recommended/bank-2020—blockchain-powering-the-internet-of-value—whitepaper.pdf

https://blockgeeks.com/guides/different-smart-contract-platforms/

4.1.4 Advantages of smart Contracts

https://medium.com/@ChainTrade/10-advantages-of-using-smart-contracts-bc29c508691a ———————————————————————— describe what smart contracts are and what they can do write about eVM, solidity, and how to communicate with smart contracts from dapps i.e. web3 py3 etc create a graphical figure showing interaction between smart contract and web3 dapp

4.1.5 Block limits and Gas

https://hudsonjameson.com/2017-06-27-accounts-transactions-gas-ethereum/

4.1.6 Future Roadmap

4.1.7 Casper

https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs

4.1.8 Sharding

4.1.9 Plasma

4.1.10 State channels - Raiden Network

4.1.11 Virtual Channels - Perun

text goes here....

4.2 Raiden

4.2.1 Netting Channel Smart contract

4.2.2 Channel Life cycle

4.2.3 Raiden Transfers

4.2.4 Network Protocol

4.2.5 Raiden API

4.3 InterPlanetary File System (IPFS)

4.3.1 Cost of Storage on BlockChain

4.3.2 Curious Case of Crypto Kitties

due to sky rocketting transaction costs largely in part of one dapp called crypto kitties the network became congested https://medium.com/@mycoralhealth/learn-to-securely-share-files-on-the-blockchain-with-ipfs-219ee47df54c https://medium.com/@ConsenSys/an-introduction-to-ipfs-9bba4860abd0

4.4 Quantum Threat to Blockchain

https://medium.com/wolverineblockchain/the-quantum-threat-to-blockchain-2adc429fd88b

5 Decentralized Supply Chain Management System

explaine the use case scenarios from usecase document i.e. section 3 of the document

google visio usecase diagrams w.r.t supplychain and blockchain and take inspiration to design your own usecase diagram

also use the video by IBM to better and more professionally explain the particular use case and its benefits. https://www.youtube.com/watch?v=ZKscEx2lO-4

5.1 Problem Statement

Imagine a company orders a sensitive package for one of their suppliers. The business contract stipulates some guarantees about delivery time, and the conditions under which the package needs to be handled for example at no point should the package be exposed to temperatures above a certain threshold. The package will pass through multiple carriers. The IoT enabled package has embedded sensors to monitor package conditions throughout its journey from supplier to the factory floor. The sensor data is communicated from the package to a blockchain enabled smart contract. All parties have access to the same data. In the event that temperature target is acceded the smart contract will be triggered automatically and the responsible party in the supply chain will be charged with damages stipulated in the contract. rewrite this to fit more closely

5.2 Benefits

I.e allows complete transparency to all participants of the supply chain. Enables / Gives end users or customers to have complete confidence that the product was stored, shipped and handled in accordance to strict safety standards and regulations. The transparency brought by this solution to the supply chain life cycle makes the job of government regulators and safety inspectors much simpler.

5.3 System Architecture

Contract number or reference number is the primary key for the system components to interact with each other

5.3.1 Supply Chain LifeCycle

5.3.2 System Work Flow

Make a diagram

make the work flow diagram like you did for blockchain, use fileserver icon for IPFS one stage shows workflow as relates to packages i.e. registering contract refnumber and defining conditions i.e. registration phase, transfering data, getting keys etc, the second stage shows smart contract / montiroing dapp monitoring data and giving out punishments and rewards etc. Last two stages are raiden and IPFS, IPFS just stores full logs, Raiden interacts with users who manually queries dapp to transfer money to shippers.

5.4 System Components

5.4.1 Decentralized Monitoring Application - Master Node

Include figure of monitoring app

5.4.2 IoT Powered Smart Packages - Sensor Nodes

include figure of pi with sensors

6 Implementation Details

give the algorithm that professor told you

6.1 Hardware Setup

Master Node PI Node

6.2 Software Architecture

6.2.1 Master Node

give class diagrams and some details about monitoring dapp

6.2.2 Sensor Nodes

give class diagrams and some details about sensor nodes

6.2.3 Integrated Payment Solution

6.3 Securing the System Against Post Quantum Adversaries

problems: events didn't work on infura, so had to change architecture from event based system to request resposne system. Going from synchronous system to asynchronous system caused fundamental redesign of the architecture again.

7.1 Testing Environment

ropsten, pi, ganachi,IPFS

7.2 Results

7.2.1 Unit Testing

7.2.2 Scenario - I

7.2.3 Scenario - II

7.2.4 Scenario - III

7.3 Evaluation

7.3.1 Gas Consumption

deployement,each tx cost, word about gas price etc

7.3.2 Transaction Verification Time

dependent on gas price, network congestion etc

8 Conclusion and Future Work

To conclude...

List of Figures

List of Tables

Bibliography

[Ada14] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. Enabling Blockchain Innovations with Pegged Sidechains. https://blockstream.com/sidechains.pdf, 2014. [Online; accessed August 25, 2018].

[Agi16] Agira Tech. 3 Types of Blockchain You Need To Know. http://www.agiratech.com/3-types-of-blockchain-you-need-to-know/, 2016. [Online; accessed August 25, 2018].

[Ahm16] Ahmed Banafa. A Secure Model of IoT with Blockchain. https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain/, 2016. [Online; accessed August 26, 2018].

[Air18] Airbus. Airbus supply chain. https://www.adsgroup.org.uk/wp-content/uploads/sites/21/2016/02/Integrated-Supply-Chains.png, 2018. [Online; accessed August 21, 2018].

[And14] Andreas M. Antonopoulos. Mastering Bitcoin. https://github.com/bitcoinbook/bitcoinbook, 2014. [Online; accessed August 23, 2018].

[Ben15] Benjamin Herzberg. Blockchain: the solution for transparency in product supply chains. https://www.provenance.org/whitepaper, 2015. [Online; accessed August 25, 2018].

[Ben16] Ben Dickson. Decentralizing IoT networks through blockchain. https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/, 2016. [Online; accessed August 26, 2018].

[Bit12] Bitcoin wiki contributors. Proof of stake — Bitcoin wiki. https://en.bitcoin.it/wiki/Proof_of_Stake, 2012. [Online; accessed 25-August-2018].

[Bit16] Bitcoin wiki contributors. Payment channels — Bitcoin wiki. https://en.bitcoin.it/wiki/Payment_channels, 2016. [Online; accessed 25-August-2018].

[Blo16] Blockchain Hub. Blockchains and Distributed Ledger Technologies. https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/, 2016. [Online; accessed August 25, 2018].

[Blo18] Blockchain.info. Median confirmation time. https://www.blockchain.com/charts/median-confirmation-time?timespan=all, 2018.

[Chr17] Christian Lundkvist. Introduction to zk-SNARKs with examples. https://media.consensys.net/introduction-to-zksnarks-with-examples-3283b554fc3b, 2017. [Online; accessed August 25, 2018].

[Eth18] Ethereum wiki Contributors. Proof of stake faqs — Ethereum wiki. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs, 2018. [Online; accessed 25-August-2018].

[Fil16a] Filament Foundation. Distributed Exchange and the Internet of Things. https://filament.com/assets/downloads/Filament%20Foundations.pdf, 2016. [Online; accessed August 26, 2018].

[Fil16b] Filament Foundation. Distributed Exchange and the Internet of Things. https://filament.com/assets/downloads/Filament%20Security.pdf, 2016. [Online; accessed August 26, 2018].

[Fre17] Fred Ehrsam. Scaling Ethereum to Billions of Users. https://medium.com/@FEhrsam/scaling-ethereum-to-billions-of-users-f37d9f487db1, 2017. [Online; accessed August 25, 2018].

[GoC17] GoChainGo. Why Scaling Public Blockchains Is a Lot Harder than just Increasing Block Size. https://medium.com/gochain/why-scaling-public-blockchains-is-a-lot-harder-than-just-increasing-block-size-5c5e7 2017. [Online; accessed August 25, 2018].

[IBM16] IBM IoT blog. Apply IoT and blockchain for accountability and security. https://www.ibm.com/internet-of-things/spotlight/blockchain, 2016. [Online; accessed August 26, 2018].

[Jef15] Jeff Coleman. State Channels. https://www.jeffcoleman.ca/state-channels/, 2015. [Online; accessed August 25, 2018].

[Jim18] Jimi S. Blockchain: how mining works and transactions are processed on the blockchain in seven steps. https://medium.com/coinmonks/how-a-miner-adds-transactions-to-the-blockchain-in-seven-steps-856053271476, 2018. [Online; accessed August 23, 2018].

[JP16] Thaddeus Dryja Joseph Poon. The bitcoin lightning network: Scalable of-chain instant payments. https://lightning.network/lightning-network-paper.pdf, 2016.

[Lig15] Lightning Network. Lightning Network Scalable, Instant Bitcoin/Blockchain Transactions. https://lightning.network/, 2015. [Online; accessed August 25, 2018].

[Max18] Max Thake. What is Proof of Stake? https://medium.com/nakamo-to/what-is-proof-of-stake-pos-479a04581f3a, 2018. [Online; accessed August 25, 2018].

[mis17] How Blockchain Tech Is Changing Cloud Storage. https://www.belugacdn.com/blog/162663814938-how-blockchain-tech-is-changing-cloud-storage, 2017. [Online; accessed August 25, 2018].

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[Pat12] Patrick Kingsley. Financial crisis: timeline. https://www.theguardian.com/business/2012/aug/07/credit-crunch-boom-bust-timeline, 2012. [Online; accessed August 26, 2018].

[Pro17] Protocol Labs. Filecoin: A Decentralized Storage Network. https://filecoin.io/filecoin.pdf, 2017. [Online; accessed August 25, 2018].

[Pur16] Pureswaran, Nair, Brody, IBM. Empowering the edge Practical insights on a decentralized Internet of Things. https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf/, 2016. [Online; accessed August 26, 2018].

[Quy15] Quynh H. Dang. Secure Hash Standard, National Institute of Standards and Technology, (NIST FIPS) - 180-4. https://dx.doi.org/10.6028/NIST.FIPS.180-4, 2015. [Online; accessed August 21, 2018].

[RIC14] RICHARD GENDAL BROWN. A SIMPLE EXPLANATION OF BITCOIN "SIDECHAINS". https://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/, 2014. [Online; accessed August 25, 2018].

[Ser15] Sergio Demian Lerner. RSK White Paper. https://docs.rsk.co/RSK_White_Paper-Overview.pdf, 2015. [Online; accessed August 25, 2018].

[Sha17] Shaan Ray. What is Proof of Stake? https://hackernoon.com/what-is-proof-of-stake-8e0433018256, 2017. [Online; accessed August 25, 2018].

[She14] Shen Noether, Sarang Noether, Monero Research Lab. Monero is Not That Mysterious. https://lab.getmonero.org/pubs/MRL-0003.pdf, 2014. [Online; accessed August 25, 2018].

[Sku17] Skuchain. SkuChain Products. http://www.skuchain.com/#products, 2017. [Online; accessed August 25, 2018].

[Wik18a] Wikipedia. Iota (kryptowährung) — wikipedia, die freie enzyklopädie, 2018. [Online; Stand 22. August 2018].

[Wik18b] Wikipedia contributors. Blockchain — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Blockchain&oldid=855030838, 2018. [Online; accessed 17-August-2018].

[Wik18c] Wikipedia contributors. Directed acyclic graph — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Directed_acyclic_graph&oldid=846566257, 2018. [Online; accessed 22-August-2018].

[Wik18d] Wikipedia contributors. Microtransaction — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Microtransaction&oldid=852232329, 2018. [Online; accessed 25-August-2018].

[Wik18e] Wikipedia contributors. Public-key cryptography — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Public-key_cryptography&oldid=853882522, 2018. [Online; accessed 22-August-2018].

[Wil12] Wilma Woo. CRYPTOCURRENCY IS HALF A TRILLION. https://bitcoinist.com/cryptocurrency-half-trillion-joint-market-cap-hits-500-billion/, 2012. [Online; accessed August 26, 2018].

A Appendix Stuff

the Appendix

B Acronyms

DDOS Distributed Denial of Service

Dapps Decentralized Applications

Altcoins All other coins besides Bitcoin

JIT Just In Time

IoT Internet of Things

SCM Supply Chain Management

DLT Distributed Ledger Technology

TX Transaction

TX Transaction

POW Proof of Work

POS Proof of Stake

TPS Transactions per second

MTX Microtransactions

BTC Bitcoin

PoR Proof of Replication

PoS Proof of Storage