CSE 543 Group 7

Security Concerns in Cryptocurrencies and Their Countermeasures

Organization: Arizona State University

Group Members

Matthew Jibben **L**	- 1217425781
Venkata B. Siddhartha K. **DL**	- 1217370037
Saloni Desai	- 1217285030
Rounak Sengupta	- 1215043206
Aditya V. Sharma	- 1215126588
Nida Z. N. Rahman	- 1215143787
Pranay Jagtap	- 1215139991
Meghana Mathew	- 1217212204
Helisha Sangani	- 1217105058

Summary

Under applications of blockchain, we discuss the variety of areas in which blockchain has been applied in the past and in current research. Areas such as finance, ownership, etc. are discussed in detail. It is also noted that certain common issues in terms of security, privacy, ease of use, etc. that were prevalent in these fields has been solved to an extent by incorporating the concept of blockchain, thus improving these domains in terms of productivity and adding value to the industry.

Later, we discuss the methods of mining that are used by different cryptocurrencies. In general, a mining method must be difficult to perform, yet easy to verify. Proof of work methods use a mining function—often a hash function—to get an output that must fit certain requirements. Proof of stake methods attempt to resolve issues with proof of work methods by limiting miners based on how much stake they have in the system. Finally, proof of retrievability methods require users to store data and periodically prove that it is retrievable.

We then discuss different well-known cryptocurrencies including their implementation, security risks, and our insights. We discuss Bitcoin, Ethereum, Namecoin, Blackcoin, Ripple, Litecoin, Peercoin, Decred, and Dash.

Finally, we discuss and evaluate attacks on cryptocurrencies and their defences. The analyzed attacks include the 51% attack, selfish mining, and cryptojacking.

Index

0 Introduction

Objective

Our objective is to provide a comprehensive study around various security concerns associated with Cryptocurrency and their respective defense mechanisms.

Motivation

Since its launch, various cryptocurrency economies have grown at an enormous rate, and are now worth billions of dollars. This exponential growth in the market value of cryptocurrencies motivates adversaries to exploit weaknesses for profit, and researchers to discover new vulnerabilities in the system, propose countermeasures, and predict upcoming trends.

Scope of study

- The major components of cryptocurrencies, its basic characteristics and related concepts.
- The security and privacy aspects that can be found at various stages in the cryptocurrency system, starting from transaction creation to its successful addition in the blockchain.

Members' Responsibilities

Matthew Jibben	- 2.1, 4.1, 5.7
Venkata B. Siddhartha K.	- 4.6, 5.1 - 5.4
Saloni Desai	- 1.3, 4.7
Rounak Sengupta	- 4.2, 5.5, 5.6
Aditya V. Sharma	- 4.5, 6
Nida Z. N. Rahman	- 3, 4.3
Pranay Jagtap	- 2.3, 4.4
Meghana Mathew	- 2.2, 4.8
Helisha Sangani	- 1.1, 1.2, 4.9

1 Cryptocurrency Basics

1.1 Blockchain

A blockchain is a distributed and decentralized database of records or public ledger of all transactions or digital events that have been executed and shared among participating Nodes/users. It keeps details across a peer to peer network of the assets and its movements/transactions. Verification of each transaction in the public ledger is carried out by consensus(agreement) of a majority of the participants in the network. Information added to the public ledger is permanent in practice, as it quickly becomes too computationally expensive to edit past records.

The record of every transaction ever made can be obtained and verified from the blockchain network. Verified transactions are accumulated in blocks, each including the transactions that took place while the block was active. An upper limit is provided in the cryptocurrency system to limit the number of transactions in a single block. Each transaction will be secured through cryptography. Further, all transaction history will later be grouped and stored as blocks of data. Then the blocks together are linked with cryptography and secured from further modification. All the transactions that have happened across the network in this whole process will be stored in an unforgeable, and immutable record. Additionally, these blocks of records are copied to every participating computer in the network to provide access to everyone and the blockchain remains resistant to modification. The greatest advantage offered by blockchain is to store any kind of asset, its ownership details, history of the ownership and location of assets in the network. This also holds true whether it is the digital currency bitcoin, or any other digital assets like a certificate, personal information, a contract, title of ownership of IP, or real-world objects. In general, the core characteristics of blockchain technology are decentralization, accountability, and security. This technique can improve operational efficiency and results in significant cost savings.

Autonomous management of such a blockchain database is carried out using a peer-to-peer network and a distributed timestamping server. Following are the core blockchain architecture components:

- **Node** - A participant user or computer within the blockchain network. Each of the users is considered as a node and every node has their copy of public ledger.
- **Transaction** - Transactions can be any type of record or event or information which is stored in a block of the blockchain network.
- **Block** - A block is used to store a set of transactions. Block is a simple data structure which is a part of a chain in blockchain.
- **Chain** - Blocks are chained through cryptography or put in a sequence in a specific order.
- **Miners** - Some nodes in the network perform verification of blocks before adding it to the blockchain. The process of validating the block and adding it to the chain is called mining. Miners are usually given a reward as incentive to perform work on the blockchain.
- **Consensus** - A set of rules and arrangements for blockchain operations.

A block is a set of transactions that have been added to the blockchain. A block can be thought of like a link in a chain. It possesses parts or all of the records of the transactions that preceded it. Instead of immediately adding the transaction to the blockchain, transactions are first added to a transaction pool or memory pool. Miners gather the transactions from the transaction pool, and try to add this block to the blockchain by verifying the transactions and mining. Each block in the blockchain has a block header which contains the following metadata about the block:

- **Version :** Version is added to the block header to help the computers to read the content of the block properly. Mainly, the version describes the structure of the data in a block.
- **Last Block :** A hash value of the previous block.
- **Merkle Root :** Markel root is generated by repeatedly hashing pairs of nodes until there is only one hash left. This one hash is called a markel root.

- **Time :** Current timestamp.

Each block of the blockchain will have the following data:

- **Data**: data includes transactions and records.
- **Previous hash**: hash value of the previous block

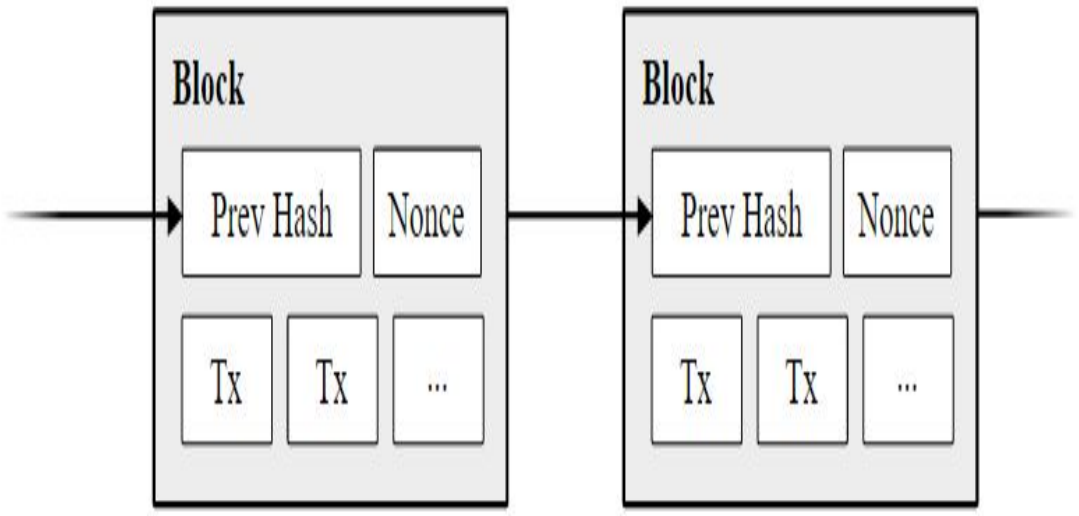

Fig. 1 - Blockchain network [1]

Mining is the process of adding new blocks containing new transactions to the blockchain network. Nodes in the network broadcast information about new transactions when they occur, which are then added to a memory pool. Nodes who have done the transactions will add this transaction in their memory pool. Each node of the network also has an option to mine a new block using the transactions in their memory pool and add it into a blockchain. In order to feasibly mine new blocks, a node needs to have sufficient memory and a lot of processing power. In order to add a block to the blockchain, miners need to solve a cryptographic problem

which uses a lot of computational power. Different cryptocurrencies use different mining functions—some are CPU intensive while others are memory intensive. Mining is important because it ensures that it is extremely difficult to edit previous transactions, preventing fraud.

1.2 Cryptocurrency

A cryptocurrency is designed to work as a medium of exchange which uses cryptography (the science of hiding information) to secure transactions, control the addition of new units, and verify the transfer of valuable assets. The idea of cryptocurrencies was introduced first in 1998, and B-money and Bit Gold were the first known attempts of cryptocurrencies. However, they never came into the real market. Cryptocurrencies are the digital or virtual currencies working on the cryptographic principles. Cryptocurrencies don't have any physical existence and are not tangible—they exist as data and code. Cryptocurrencies provide higher security and usability than many existing currencies.

Cryptocurrencies work using blockchain technology. A public ledger is maintained to keep track of transactions that are generated and transferred across the network. Every individual in a network will have a unique account ID/address. Cryptocurrencies are associated with these accounts, which can be accessed through various applications. Users can use these applications to send and receive money. Transactions are verified by nodes and added to the blockchain ledger.

Cryptocurrencies use many cryptographic protocols to secure the blockchain network. Cryptographic methods that are used in cryptocurrencies include elliptic-curve cryptography, public-private key pairs, and hashing functions like SHA256, SHA512, and MD5. Cryptocurrencies enable the direct transaction between two anonymous users without any third party control like banks or government.

There are many cryptocurrencies available in the market nowadays. The most famous and used cryptocurrency is Bitcoin. Another fast-growing cryptocurrency is Etherem. As compared to other traditional currencies, the anonymous nature of cryptocurrency gives it hype in the market. Users who are participating in the network have an account id which is the only thing visible to others, while other details are private. Through this, users can be kept anonymous.

A core cryptographic primitive for authorizing transactions is the inclusion of digital signatures. Cryptocurrency uses digital signatures in order to achieve three security properties: data integrity, authentication, and non-repudiation that are crucial for digital currency. By using digital signatures, cryptocurrencies archive important security properties. Digital signatures consists of following three steps:

- **Hashing the data** : The first step is to hash the digital data. Hash functions are mathematical functions involving transforming data of any size into a fixed-size output. Hash functions are known to be collision-resistant, so it is infeasible to find multiple inputs with the same output.
- **Signing** : To verify the authenticity and uphold the integrity of digital data, digital signatures, a cryptographic mechanism, are used. After the information is hashed, the sender of the message needs to sign it. At this point public-key cryptography comes into play. The hashed message will be signed with a private key, and the receiver of the message can then check its validity by using the corresponding public key (provided by the signer). The sender of the message generates both public and private keys, but only the public key is shared with the receiver.
- **Verifying :** In this step the receiver checks the validity of the message using the public key of the sender.

1.2.1 Centralized and Decentralized cryptocurrency:

The concept of decentralization is crucial in the development of the blockchain and cryptocurrencies that run on it. A centralized control is not necessary for operation of a decentralized system. To help conduct transactions, centralized cryptocurrency makes use of a middle man or third party. This middle man is trusted to handle their assets by both buyers and sellers. This is also commonly observed in a bank setup, where the bank is trusted by the customer to hold his or her money. The rights of participants on the ledger refers whether a blockchain is centralized or decentralized.

In a decentralized network, anyone can participate and transact on the ledger. To combat the vulnerabilities that arise from this design and to ensure that transactions are correctly maintained, there must exist an alternative mechanism. Bitcoin, for example, is a decentralized blockchain which maintains the integrity of the ledger and prevents people from corrupting the system by using mining and proof-of-work.

On the other hand, a centralized network is made up of parties whose identities are known. Thus, only credible and reputable participants can post to the ledger and ensure the validity of the system. As identities of participants' are known, their transactions can therefore be audited. Ultimately, in any highly regulated industry a centralized distributed ledger must be used - such as in financial services - to minimize vulnerability.

Decentralized and centralized blockchains have their own risks and security concerns. A centralized network has known participants so if any kind of corruption happens in the system it can be resolved by the audit trail. But in a decentralized network we need to track every possible manipulation which is done by an anonymous entity.

1.3 Transactions

A blockchain uses transactions that provide huge speed and transfer cost advantages. In normal transactions, there are a lot of additional costs. When traditional ways of conducting transactions are considered - a lot of middle men are involved. These middle men could be anyone including agents, brokers or lawyers. This adds to the cost of performing transactions. In addition to that, there's paperwork involved. On the other hand, transactions involving cryptocurrencies are simpler and cheaper. They do not require any paperwork either. This increases accountability. It also makes the process more robust and secure.

Digital Signatures:

An electronic coin is used to conduct transactions in bitcoin. An electronic coin is nothing but a chain of digital signatures. A digital signature is a method used to ensure that messages received and sent can be authenticated. Digital signatures can be used in the place of actual signatures in electronic transactions. They help us achieve:

1) **Non-Repudiation**:
   Non- repudiation means that a sender cannot deny sending a message and a receiver cannot deny that they had received the message. Non-repudiation is an important goal of system security. Digital signatures use asymmetric key cryptography which means there is one key that locks or encrypts the message - this key is the public key, and there is another key that unlocks or decrypts the message - this key is the private key. Once a sender has signed the message, they cannot deny having sent it.

2) **Authentication**
   Authentication is required to prevent forgery. It is important to ensure that the messages received are received from a legitimate sender, and they're in fact the person they claim to be. Digital Signatures are implemented using a Public Key Infrastructure (PKI) and there are authorities that create them and ensure they cannot be duplicated or forged.

3) Integrity

Integrity means that data should not be modified in illegitimate ways. Modifications would mean changing, deleting and creating. Digital Signatures help ensure the integrity of data by allowing only authorized parties access to the data and the permissions to modify data.

Each owner transfers a bitcoin to the next by digitally signing a hash of the previous transaction and the public key of the person they're transferring it to. The buyer can verify the signatures and transfer history by using his private key. [1]

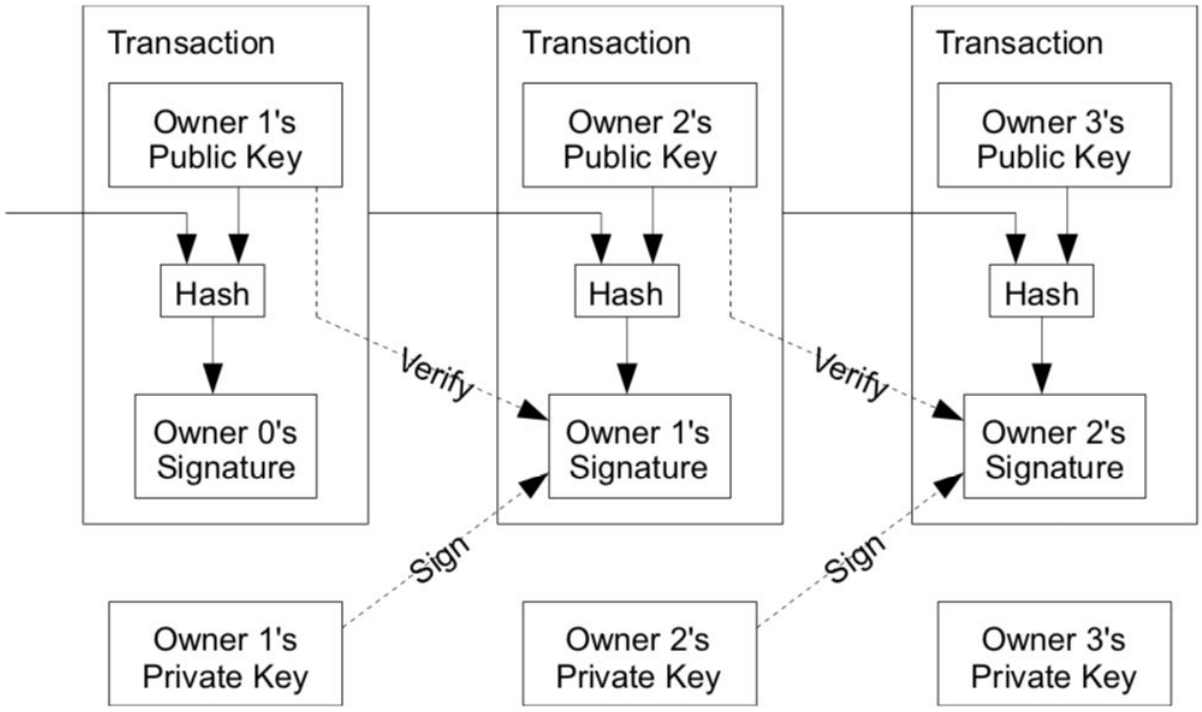

Fig. 2 - Chain of Digital Signatures that form a bitcoin [1]

The buyer cannot verify whether or not the spender has spent the same money more than once, and thus, to solve this problem, we require a central authority that checks each transaction for double spending. This trusted central authority is similar to a web wallet- e.g. 'mint'. When a

transaction is complete, the coin has to be sent to mint, and it issues a new coin - and only new coins issued by mint can be guaranteed to be impervious to double spending.

The issue with the solution mentioned above is that the responsibility to ensure that the entire system works correctly lies on the shoulders of one central authority and every transaction has to go through that authority.

A second solution to this problem can be proposed if a payee or the buyer could themselves verify that there has been no double spending. In order to be aware of the absence of a transaction, the payee needs to be aware of all the transactions. This can be done by publicly announcing all the transactions. All the participants must agree on the order in which they were conducted. The payee requires proof that at the time of each transaction, the majority of nodes agree that it was the first transaction received.[1]

Timestamp Server:

A transaction can be publicly announced with the help of a timestamp server. A timestamp server takes as input a hash block of items, timestamps it, and widely publishes the timestamped hash. The time stamp proves that the transaction existed at the time of hashing. Each timestamp includes the previous timestamp in its hash, thus, forming a chain and reinforcing the timestamps that came before it [1].

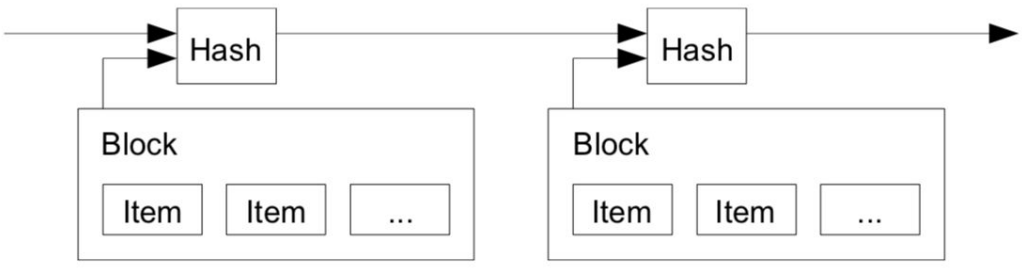

Fig. 3 - Working of Timestamp Server [1]

2 Consensus Protocols

2.1 Proof of Work

Proof of work is a common mining method used by popular cryptocurrencies such as Bitcoin, Litecoin, and Ethereum. Proof of work requires miners to validate transactions and add them to the public ledger by performing some resource-intensive task, usually for some reward. The successful completion of this task should produce an easily verifiable result, such that other miners can test and verify that the task was completed. By using a resource intensive task, it becomes difficult for a single malicious user to have enough power to outnumber everyone else and create their own invalid transactions within a blockchain. [4]

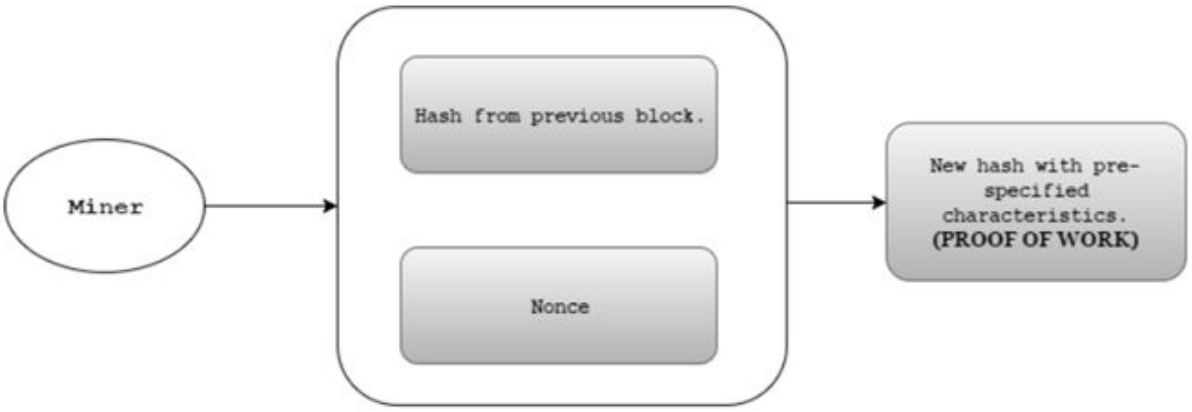

Fig. 4 - A simplified view of Proof of work Mining [4]

Proof of work cryptocurrencies follow similar methods to implement mining. Miners hash the header of the previous block and a nonce and check the hash against certain requirements. Different cryptocurrencies use different mining functions: Bitcoin uses SHA256, Ethereum developers designed a unique hash algorithm called EtHash, and many others use Scrypt, a key-derivation function, for mining. The resulting output is checked against the cryptocurrency's requirements. In the case of bitcoin, the result is required to have a certain number of leading zeros in order to be accepted. The mining algorithm is normally designed so that the number of blocks mined per day is relatively constant, allowing for better control of the currency currently in

circulation. For Bitcoin, this means updating the number of necessary leading zeros based on how many active miners there are. [4]

2.1.1 Security risks

Proof of work basically creates a “voting” system such that a single person has more votes based on their available computational power. Because of this, it is possible for corrupt individuals to take advantage of a small cryptocurrency and create false transactions. With larger cryptocurrencies like Bitcoin and Litecoin, it is extremely unlikely that one person could have more CPU power than the rest of the network. However, less popular cryptocurrencies can become vulnerable to this attack. This is known as the 51% attack. This vulnerability can be addressed using Proof of Stake, which restricts the mining capacity of a user based on their stake.

2.2 Proof of Stake

Proof of stake (PoS) is a type of consensus algorithm that attributes the transaction validating power of a miner on basis of his stake in the system [4]. An entity who owns a higher number of coins will be allowed to mine more transactions than another with lower holdings in the system. This effectively caps the maximum number of coins that can be mined by an individual in proportion of his or her ownership stake. The rationale being people with higher stake in the system are inherently inclined to maintain the security of the system.

2.2.1 Advantages over PoW

Proof of stake attempts to solve some inherent problems with the Proof of Work (PoW) mechanism. Firstly since the PoW strategy determines the mining power of an entity on basis of it’s computational capabilities, there may arise a scenario where the transaction validating power rests with an external entity and not with the stakeholders of the cryptocurrency. This makes the system more vulnerable than PoS strategy where the miners are the stakeholders and thus would lack malicious intent as they would want to protect their earnings. The Proof of Stake is more resistant to 51% attack than Proof of Work since the attacker first needs to gather more than 51% stake in the system. But launching an attack will lead to erosion of system

security and value of the cryptocurrency which would ultimately prove to be disadvantageous for the attacker.

Secondly, Proof of Work requires solving resource intensive puzzles for validation which means that a part of earnings is traded for fiat currency to finance these tasks. It would lower the valuation of cryptocurrency.

Thirdly, since the reward for mining new blocks is halved periodically in cryptocurrencies such as Bitcoin, it is expected that miners would lose interest as the high costs of computations may overtake the compensation offered as rewards.

There are two main hurdles faced by systems implementing pure Proof of Stake strategy [67], one of which is fair initial distribution of the cryptocurrency. As discussed above, the stake of the individual is important to the process transaction validation and thus initial distribution impacts the security of the system. One solution is to use PoW for distributing the initial money only. Another hurdle is due to attacks on network fragility such as bribe attacks. A bribe attack allows the malicious users to double spend, by paying bribes to other shareholders in return for approval of her branch by signing it. These complicit shareholders do not have to worry if the attack fails as they would not lose anything.

Peercoin was the first cryptocurrency to implement a full-scale PoS consensus model.

2.3 Proof of Retrievability

Proof of Retrievability is a unique consensus mechanism which is used by Microsoft and it works on the basis of proof generated by the generating system or the prover to the verifier indicating that the file generated is correct and the client can retrieve the same. This greatly reduces the communication cost as we only transmit the encoded version of the file rather than the actual file while the actual file is archived. Thus, we are able to create a challenge response protocol which is both effective and efficient. Cloud computing has gained momentum and more and more companies have adapted to this emerging trend. Due to features like scalability, a lot of companies rely on cloud service providers for storage purposes. With the growth in storage on cloud, there is an increase in the need for a mechanism that can effectively provide information assurance with regards to the files that clients store on the cloud. Proof of retrievability is a consensus mechanism that allows for a client to produce a challenge for the

prover or archival system which could be the cloud service to check if their file can be retrieved. Another important domain which has been growing is electronic payments and the problem with payments systems was the centralized nature and the issue of trust based model which was overcome by Bitcoin which used a peer-to-peer model and Bitcoin worked with Proof of work mechanism. Permacoin, which is another cryptocurrency was the first to replace Proof of work in Bitcoin by Proof of retrievability. By adding proof of retrievability mechanism in the existing cryptocurrency system, it was able to track how much memory each node is investing in storing a file or part of a file.

In more efficient forms of this protocol, the original file is archived and only a token or a challenge is generated and provided to the client which reduces communication cost dramatically. So, the way this works is, the system will encode the file and pass the file to a storage service where it is archived and this encoded file is used to generate a challenge/key for the client. The client can then use this to check if a file can be retrieved from the storage / prover. This provides information about how much memory or storage is being invested by the node. An important technique used for detecting adversarial activity by most versions of POR is called “spot-checking”. The challenge consists of sampled sub parts of the original file. The client is responsible for performing computation based on this and encoded information.

The important components of the system are as follows:

- File Encoder - Responsible for encoding the file to be archived and the encoded version is pushed forward to the prover/storage server/archive
- Key Generator - Responsible for polling the file encoder and encoded file to generate a key which is then pushed forward to the client/verifier so that they can check with the server if the file is available.
- Verifier/User - This node is responsible for verifying if it is able to retrieve the entire file that it owns and which is stored on archive servers using the key generated by the key generator.
- Prover /Archive - This is the server that stores the encoded file forwarded by the encoder and is responsible to send a response proving that it has the file when challenged by the client/user/verifier.

The object file is passed to the file encoder where the original file is encoded and passed on to the archive to be stored. The key generator polls the file encoder and generates keys for the encoded file which is then forwarded to the client or verifier. This key allows the verifier to challenge, prove or archive and to get access to the file.

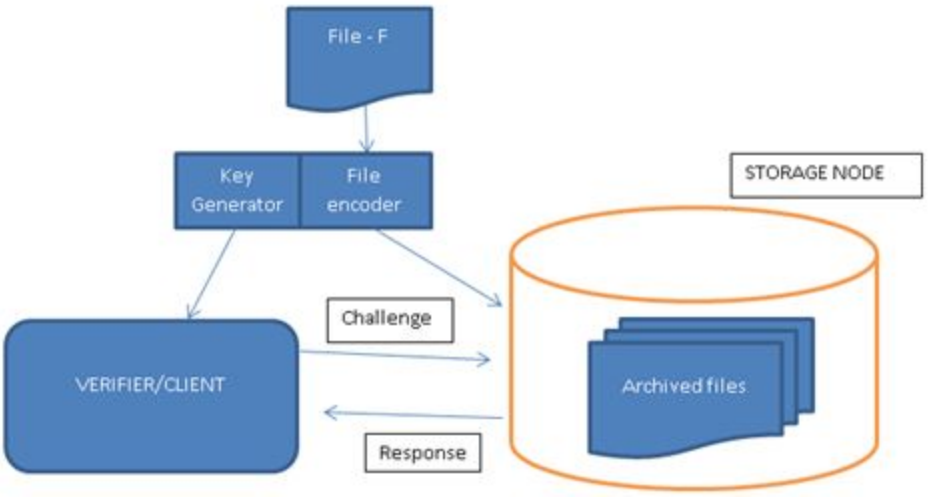

Fig. 5 - Block diagram representing a simple overview of POR mechanism for large files. Source: Based on explanation and representation(fig.1) in [37]

Insights & Summary:

The primary insight that was derived upon initial reading of papers on Proof of retrievability was that the Proof of Retrievability mechanism greatly reduces the computational overhead that occurs in other consensus mechanisms like Proof of Work. This is because Proof of Retrievability requires minor computational overhead and this computation allows to deduce useful information like how much memory/storage was spent by node and if the file can be retrieved completely as opposed to other mechanisms like PoW wherein each node is expected to spend certain computational energy to solve some problem and this is considered as the proof in order for the block to be accepted. It is also important to understand that, since the file to be stored is being encoded by the encoder, the network bandwidth required is lower and it reduces the network overhead as the entire file is not transmitted over the network. Some important crypto currency systems like permacoin are basically modified versions of Bitcoin where Proof of Work is replaced with Proof of Retrievability which results in reduced usage of

resources. This Proof of Retrievability is an important concept for cloud computing where storage services are provided. For example, Amazon Web Service consists of services like S3 in their service stack which is used as a data lake by many companies and has been in great demand recently. S3 is a perfect example of storage service provided by a third party which can be used by clients and it follows a pay as you use model. Proof of Retrievability is an excellent mechanism to test data integrity as it uses a challenge-response method which allows the server/prover to prove to the client/user that they possess the file and it is accessible completely. Proof of Retrievability is a good way for clients to verify that about the integrity of the file that they shared on the storage node. The different types of schemes for Proof of retrievability are static and dynamic as listed below[38].

Static-

- Basic scheme - In this scheme, only a small part of the file and not the entire file is encrypted and this helps in reducing the storage requirement on server and processing on client.
- POR for large files - This is as explained in the fig 4 above wherein a single key is generated based on the encoded file and this is used to create a challenge and get a response.
- Compact POR - This only works for static information and it uses two auditors which use pseudorandom function and digital signature to make the system more secure.
- 2-Phase protocol - This makes use of “spot-checking” discussed earlier wherein a part of file is checked for adversarial activities and client performs a computation for the same based on some additional information in the file.

Dynamic-

- Data correctness - uses some additional metadata added by third party auditors and allows for dynamic updations, insertion and deletion of the data.
- Public Auditability - Consists of a Third party auditor that holds a private key which can be used to check integrity of cloud storage.

Some of the implementations of Proof of retrievability are Storej and Permacoin.

3 Applications Of Blockchain

Blockchain has numerous applications, some obvious and some not so obvious, but before delving deep into the applications of blockchain, it is important to address the idea that has brought meaning to the existence of blockchain – Bitcoin. Blockchain is defined as “a decentralized, distributed public ledger”. In simpler terms, blockchain serves as a “record-keeping technology” for the bitcoin network.

Although blockchain was first discussed in 1991, it took around 20 years for it to be applied in a real-world environment and its very first application was in the Bitcoin technology. Following this breakthrough, researchers have now associated blockchain with various applications beyond cryptocurrency as mentioned in [50] in fields of Finance, Internet of Things (IoT), Healthcare, Government Applications and Identity. These applications are discussed in detail below:

3.1 Blockchain in Finance

As mentioned above, application of blockchain in cryptocurrency was one of the most important discoveries with regard to blockchain technology. Treleaven et al. shed light on how blockchain works in the field of finance in [51]. Each transaction made in the form of Bitcoin, Litecoin, etc. is recorded in the form of a block which holds information such as the legitimacy of the transaction, details about the sender and the receiver, the amount involved in the transaction and other similar data. In this manner, blockchain helps eliminate the presence of a third-party vendor such as a bank, thus making the transaction between the two parties seamless in nature. Transparency and reliability of the peer to peer transfer network is ensured using a computational logic and irreversibility of records to avoid fraud as described in [52].

On a more specific level in the financial domain, blockchain is known to be applied in areas such as asset management, insurance claim processing and cross border payments. Verma et al. propose an architecture of blockchain for asset management in [53] where transaction of intelligence, surveillance, target acquisition, and reconnaissance assets are processed in coalition operations. Blockchain in asset management eliminates inefficiencies caused in

traditional methods where all parties involved such as the sender, receiver, broker, funds manager, etc. maintain their own record of activities that are very much prone to human error.

Insurance policies make up a large portion of the value adding sector of the financial field, and an important concern that accompanies this is insurance fraud. Apart from claiming insurance policies being a cumbersome task for the general public, fraudulent data fragmentation, missing policies, and missing claims kindle a lot of discomfort amongst the policy providers as well as investors. The research of Gatteschi et al. in [54] evaluates the ideas of introducing blockchain technology in the field of insurance to mitigate risks. Their research concludes that although this technology is still in its nascent stages, if implemented with care, can transform the insurance sector and eliminate fraudulent activities. This is accounted to the transparent nature of the blockchain technology where computation and strong encryption properties ensures the identity of the insurers is legitimate and the assets owned by them are secure.

Amongst the many types of money transactions that occur in today's world, cross-border transactions are ones that prove to be most expensive, time consuming and prone to money laundering. By using blockchain, there are many third-party companies that offer a seamless way to achieve such transactions with ease. As mentioned in [55], blockchain eliminates the need for a third-party vendor between the sender and receiver whereas in traditional methods of cross-border transactions, third-party vendors that use SWIFT payments are required for the conversion of currency thus resulting in a long process that are prone to theft and laundering.

3.2 Blockchain in Property Ownership

In [56], the authors suggest a maturity model for blockchain technology, where features such as the architecture, upgradation and integration process, storage, maintenance procedure, and business efficiency allow blockchain technology to be applied to the ownership of "Smart Property". Property, in its tangible form such as real estate, vehicles, etc. or intangible such as the stock market, patents, etc. can be combined with blockchain to make their ownership, transferability and maintenance simple. Property sale and ownership is logged in a digital ledger such as blockchain, and ownership is ensured using a digital "Smart Key" as mentioned in [57].

Digitizing the entire ownership process using blockchain reduces possibilities of fraud, loss of property, theft, and fees incurred by the middleman involved in transactions.

Within Smart Property using blockchain, specific areas where blockchain application is currently predominant are in the domain of money lending and physical hand-held devices incorporated with blockchain (smart devices). Manda et al. propose a method in [58] in which conventional money lending processes are replaced with a peer to peer lending process using blockchain. This can be used instead of allowing borrowers to fall into the hands of unfaithful lenders and lose the funds mortgaged by them as collateral. As a public ledger, blockchain is immune to such frauds and saves borrowers from potential bankruptcy. Furthermore, the digital nature of blockchain saves time and ensures there is no need to file and process a large amount of paperwork that is usually followed in hard money lending. In the case of hand-held devices, our daily use appliances such as mobile phones, laptops, car keys, etc. are all encrypted using passwords in order to prevent unauthorized access. The disadvantage is that all these devices are tangible in nature and can be stolen, lost, or prove to be difficult to transfer or maintain. Incorporation of blockchain that maintains a public ledger of the ownership of these devices helps solve this issue.

3.3 Blockchain in Internet of Things (IoT)

In today's world, as technology advances by the day, IoT is becoming a hot topic of research. When a device such as a car or a temperature control system connects to the internet and uses some programmatic logic or is able to make decisions on its own, it becomes part of the Internet of Things. As of this year, the number of devices that take part in this widespread IoT network is close to 26.66 Billion. The work of Lin-bo et al. discusses the major problems involved in IoT in [59], which include major security and privacy concerns as well as glitches in techniques proposed to handle the extremely large amount of data produced by these devices in an effective and efficient manner. Various issues with IoT include security of private information such as ideas specific to companies, government secret information, etc. Once proper security and privacy mechanisms ensure safety of data, there arises the issue of storing, maintaining, and analyzing large volumes of data and converting it to information to be used in analytics platforms and incorporated in applications.

Most of the above-mentioned issues have been solved using blockchain. Dorri et al. suggest a scalable architecture to incorporate blockchain in IoT in [60] to ensure security and privacy of the devices. The blockchain ledger ensures that details regarding the devices can only be viewed and accessed by authorized personnel. Research performed in [61] proposes a data management platform that enables users to perform analysis on the large amount of data that is collected from IoT devices to extract information without having the issue of being capable of storing a very large volume of data.

Integrating blockchain with IoT has given rise to a large number of smart devices. Smart devices are those which when connected to the internet are capable of performing on their own without human interference. Commonly used smart devices are connected to a certain third party who has access to all the information collected by devices, thus leaving individuals with no choice but to blindly trust this third party. This can be detrimental when the smart device is related to security systems. Blockchain ensures that such appliances remain secure without the need to involve a third-party by using Proof-of-Authority as a consensus mechanism as mentioned in [62].

Another interesting example of how blockchain has improved the field of IoT can be seen in the industrial sector where blockchain mechanism is integrated with supply chain management. Chen et al. shed light on the current issues of supply chain that cause a negative impact in quality management in [63]. These issues include varying interests of employees involved in supply-chain, misinformation with regard to the production process, and limitations in the quality inspection process. The paper also suggests a sensor-based framework to tackle these issues where the sensors incorporated at the production and supplier end gives the industry a complete view of the underlying process with room to correct errors, thus improving the quality of goods. Blockchain helps manage these sensors by storing large volumes of data, ensuring security of this information, encrypting delicate data, and providing a means to transfer the information whenever appropriate. This ensures that the information is only accessible to trusted and authorized employees.

3.4 Blockchain in Smart Contracts

Contracts make up an essential part of all agreements and in most cases require an intermediate third-party to ensure that the two main parties participating in a contract agree on all terms and conditions. Using blockchain technology to make contracts “smart” eliminates the need for this third party. Apart from this, the digitized nature of blockchain also ensures no fraudulent terms or practices once the contract is agreed upon, thus making the process seamless and easy. Alharby et al. discuss a comprehensive study in [64] where blockchain is used to create and enforce a contract between two parties without including an intermediate party. The blockchain mechanism ensures that all consenting parties are well aware of the terms of the contract and all required processes are carried out automatically once both parties have agreed to the terms. The paper also summarizes key issues of blockchain when being used in smart contracts, such as the reliability of the computational algorithm used, security, privacy and performance issues.

One of the greatest applications of blockchain in the form of smart contracts is in the healthcare industry where decentralized applications are designed to bridge the gap between the hospital and essential services such as the pharmacy and insurance company. Health records are transmitted to these services with ease using blockchain technology with proof-of-delivery as mentioned in [65]. Other applications include contracts that deal with ownership such as artist rights in the music and film industry as well as patent rights for inventors and organizations.

4 Cryptocurrencies

4.1 Bitcoin

Bitcoin is the most popular and influential cryptocurrency, and as such it is a large target for hackers and security analysts. Bitcoin uses a peer-to-peer network that uses

Mining

Mining is performed using a Proof of Work method similar to Hashcash. In order to add new blocks to the ongoing ledger, miners must use SHA256 on the previous block's header with an added nonce. By incrementing the nonce, miners can search until they find a hash that matches the necessary requirements, at which point they will broadcast the solution and gain a reward. The hash is required to have a certain number of leading zeros such that the problem becomes more difficult as more miners become active. For Bitcoin, the problem is altered so a new block is found approximately every 10 minutes.

Branches

When a correct nonce is found, the miner can broadcast the nonce for the block they are working on, showing that the hash has the necessary leading zeros and gaining a reward. In doing so, it is very easy for someone else to compute the hash themselves to verify it. When two miners find a solution and broadcast it at the same time, nodes will receive different blocks at different times. In this case, the tie is broken based on which branch becomes longer first, so all nodes work on whichever branch is currently the longest. [1]

Block header :

Each block contains the hash of the previous block, the list of transactions, and a nonce for mining. By including the hash of the previous block, blocks are "chained" together. This makes it extremely difficult to alter transactions on previous blocks, as doing so would cause the hash to change for all of the following blocks and would require a large amount of computation.

In order to save space, transactions are stored in a Merkle tree. [1]. This is accomplished by hashing each of the transactions, then forming a binary tree structure where two bottom nodes are hashed to form a new hash, and so on. Only the root of the Merkle tree must be saved in the block header. This structure is useful because it saves space and can still be easily verified. If any of the transactions have been altered, the root of the Merkle tree would be different as well.

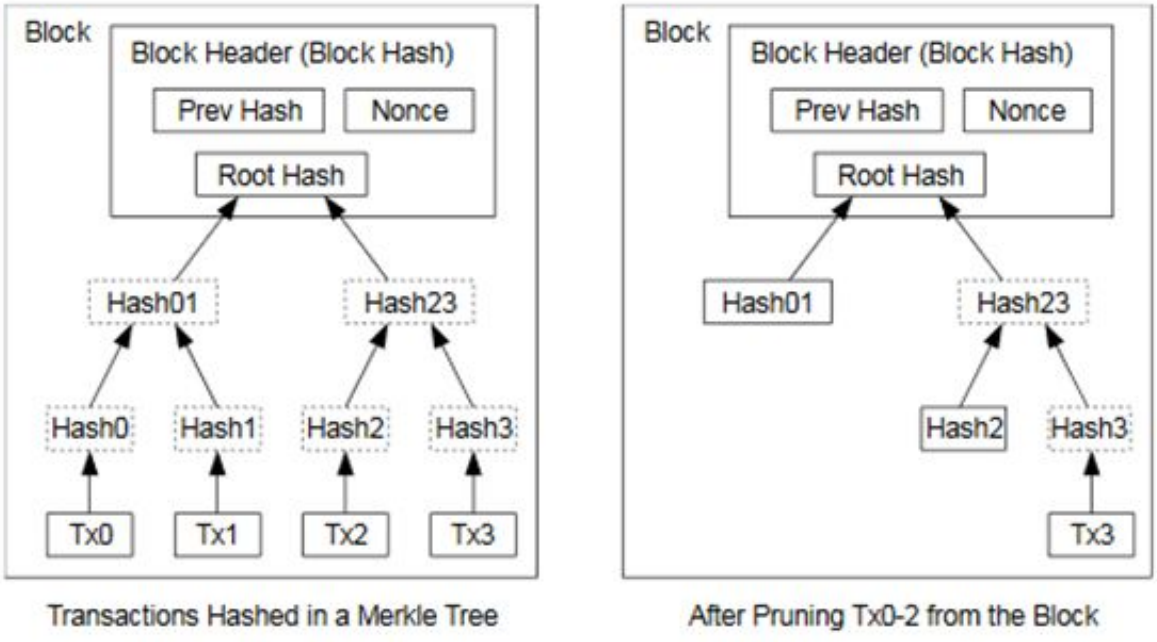

Fig. 6 - Structure of a Merkle Tree [1]

Privacy

Since all transactions are publicly available, anyone can verify that transactions are valid by ensuring that the payer has access to the paid funds. This is a feature of Bitcoin as it gives added security, however at the cost of anonymity. To combat this, privacy can still be maintained by making public keys for transactions anonymous. Further, a new key pair can be generated for each new transaction so that multiple transactions are not linked to the same user [1].

Security risks

Double spending

Double spending is a well-known security risk of Bitcoin. This occurs when a malicious user agrees to pay a vendor for some product and creates two transactions at near the same time, essentially allowing funds to be used twice. However, this can be circumvented by using observers in the network to quickly notify vendors of double spending.

Finney Attack

Another form of double spending is possible through the Finney attack. This attack occurs when a malicious user privately mines a block and adds a transaction of their own funds to themselves. Before releasing the block, they create a public transaction to a vendor. Once this transaction is accepted by the vendor, the user can release their pre-mined block, returning funds to themselves. For this attack to work, however, the malicious miner must have considerable computational power, and the vendor must accept the transaction very quickly. Vendors can avoid this attack by waiting for multiple blocks to be mined before accepting a transaction, since the malicious user is unlikely to have the computational power to out-mine the rest of the community.

Selfish Mining

Certain attacks are possible when using a mining pool. Mining pools use groups of miners to collectively work on finding new blocks while sharing the rewards. Through special strategies, mining pools can perform the block discarding attack or selfish mining by hiding when they successfully mine a new block. The selfish mining pool can continue to mine on top of their private chain until the public miner's chain is near the same length. The selfish mining pool's chain now becomes the main chain because it is the longest fork, resulting in (1) the selfish miners getting a larger reward, and (2) the honest miners lose the rewards they worked on. Due to the possibility of losing rewards, honest miners can easily be convinced to join the selfish mining pools. However, to be truly effective the selfish mining pools will need a very large amount of computational power [2].

Pool Hopping

Pool hopping is an exploit that uses information shared in pools to determine how much they will gain from collaborating. If the other members of the pool have already completed a large amount of mining, a user can conclude that they will not receive a large share from working with the pool and would be better off switching to another pool or working independently [2].

Other risks

Many other risks are possible through Bitcoin based on its specifications. Users can lose their entire Bitcoin wallet if they lose access to their private key. This can easily happen either through losing the data, having a corrupted hard drive, or any other means. When this happens, those Bitcoins are lost and will stay orphaned indefinitely, as there is no way to retrieve them. Additionally, opponents criticize the amount of anonymity that Bitcoin offers, since it allows for criminal activity to go untraced.

4.2 Ethereum

Ethereum is a programmable blockchain. Like any blockchain, Ethereum depends on a distributed system (P2P network protocol) consisting of numerous PCs around the world. Rather than giving clients the capacity to utilize a couple predefined activities (like transactions), Ethereum permits its clients to run practically any code they need. The code is put away on the blockchain for others to communicate with and is frequently alluded to as Smart Contracts.

The PCs (nodes) in Bitcoin's system keep up and update the blockchain. In Ethereum, they additionally run the Ethereum Virtual Machine (EVM). The EVM is a supercomputer that consolidates the entirety of the computing power of the hubs in the network altogether. This computing power is utilized to run the client submitted code (usually, the smart contracts) on the blockchain. To execute these, the EVM charges a little exchange expense (called transaction fee) in return for the computational force utilized by the smart contract. This charge is called

'gas' and it is paid in Ether, which is the reason Ether ought not so much be viewed as a cryptographic currency, but instead, as the oil to run the network as a whole.

Essentially, Ethereum is a supercomputer, which lets clients run any code they want.

Smart Contracts

As referenced earlier, Ethereum permits individuals to deploy smart contracts on the blockchain. What a smart contract is, is a self-executing bit of code, which characterizes and executes agreements between different parties. 'Smart agreements' was first brought about by Nick Szabo in 1994. He contemplated that code is flawlessly ready to characterize a progression of relations, parameters, and actions.

In Ethereum, smart agreements can be written in Solidity, an Ethereum explicit programming language. These smart agreements would then be able to be transferred to the blockchain and will keep existing there. Since the blockchain is secure and unchanging, one can completely believe that a smart contract on Ethereum will execute like proposed. Self-execution essentially results in counterparty risks and moral hazards to be eliminated from the condition, as the contract implements its own arrangements.

Smart agreements can be utilized for a wide range of transactions. They are entirely reasonable for straightforward transactions, in which commitments of the two gatherings can come down to effectively certain arrangements of necessities.

Summary and Insights

What Bitcoin did was permit people to trade money without including any intermediary actors, similar to banks, payment processors or the legislature. For Bitcoin's utilization case, the trust that they give is no longer required.

Ethereum's effect might be increasingly extensive. As nearly anything can be coded and made sure about on its blockchain, other middlemen that give trust might be removed. Contingent upon how much worth you accept these mediators bring beside trust, these actors could incorporate public accountants, financiers, the protection divisions, land offices, online commercial centers for merchandise and ventures like Uber and eBay and so on. The argument goes that nearly anything of significant worth for which go-betweens are important to give trust should be possible all the more productively on the blockchain.

In spite of the fact that this contention is imperfect, unmistakably blockchain advances enable people from around the globe to manage each other by dispensing with counterparty risk from the equation. Unavoidably, this implies, somewhat, believed middlemen lose their significance in our financial framework. We will see a move away from these gatherings towards distributed administrations and the sharing economy. A move away from a brought together economy to a circulated one.

The web appropriated data in a way that was not possible before the ascent of the innovation. The blockchain takes into consideration the trustless trade of significant worth over the web, pushing us to challenge how we have organized society, characterized esteem and compensated investment. This is the reason blockchain innovation is alluded to as the main thrust behind the 'web of significant worth' or the Internet 3.0. Ethereum is now the greatest convention that permits the production of smart contracts, DAO's and DApps, and many trusts it may very well turn into the foundation of this new web.

Blockchains can possibly give proficient, quick, secure, solid and auditable transacting of worth. Like the web before it, the blockchain vows to overturn upcoming challenges and upset enterprises. Blockchain advancements are pushing us to challenge how we have organized society, characterized by worth and remunerated involvement. This is the reason some allude to blockchains as the empowering innovation for the web 3.0, or the internet of value.

As nearly anything can be coded and conveyed on Ethereum's blockchain, Ethereum may very well shape the base of this new web. Be that as it may, high potential comes connected at the hip with publicity, and discussion of the web 3.0 brings issues taking after the ones encompassing the website emergency.

4.3 Namecoin

Namecoin is a cryptocurrency that is still under a lot of research but is architecturally very similar to Bitcoin. The similarities include the fact that Namecoin was developed from the same software as that of Bitcoin and follows the same Proof-of-work algorithm. Namecoin was initially meant to share the same transactional database as that of Bitcoin but anticipating certain computational conflicts, Namecoin now has its own blockchain transactional database.

Due to the above-mentioned similarities, Namecoin and Bitcoin were initially mined simultaneously until 2013, when NameID was launched as mentioned in history of Namecoin in [18]. NameID allowed users to create a user profile on the Namecoin blockchain thus creating namespaces. This was accompanied by an OpenID that let users log into websites using their namecoin identities.

Based on the research of Kalodner et al. in [19], it is found that Namecoin addresses the issue of decentralized namespaces. The issue of decentralized namespaces is one that states that the Domain Name System (DNS) cannot ensure the property of allowing users to choose names, security of the system and decentralized nature of the system at the same time. This is because a secure user chosen name system has to be centralized in nature for effective functionality of the system. Namecoin solves this issue by maintaining a “name/value store” that is capable of holding arbitrary data along with following protocols similar to that of Bitcoin.

This namespace feature is a distinguishing feature as that is what separates Namecoin from Bitcoin. The namespace allows users to establish their identity and thus trade using their own individual information. This is made possible using three operations, namely NAME_NEW, NAME_FIRSTUPDATE and NAME_UPDATE. NAME_NEW is the very first step that allows a user to register and pick a coin. NAME_FIRSTUPDATE associates the chosen name with a value. Finally, the NAME_UPDATE operation updates, renews or trades a name depending on the choice of the user. The namespace registration protocol for Namecoin is figuratively described in [19] and is shown below in Fig 7:

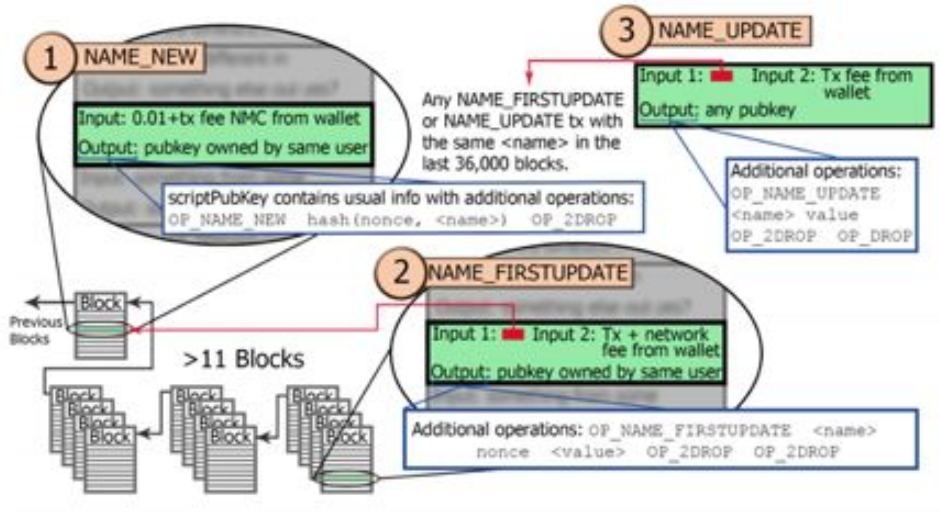

Fig. 7 - Namecoin registration process as described in [67]

Although namespaces may be a great breakthrough in the domain of cryptocurrency, Namecoin does give rise to a far more alarming economic issue. In theory, namespaces are capable of registering an infinite number of names but practically speaking, there are only a finite number of names that can be remembered by humans. Therefore, amongst the many registered names, only a few hold economic values and will be involved in trading.

4.4 BlackCoin

BlackCoin is a cryptocurrency system which was launched in 2014 by Joshua Bouw and is claimed to be the ‘original Proof of stake coin’ in the whitepapers as it is the first cryptocurrency system to use a purely PoS based mechanism since the release of its second version (PoS version 2). Just like any other cryptocurrency system, Blackcoin is a peer-to-peer system which utilizes a decentralized design. The consensus mechanism used in Blackcoin is Proof of stake where in every user generates a token thus generating stake. In its early versions, Blackcoin was meant to be an experiment to test the concept of proof of stake. As the system stabilized and BlackCoin proved itself to be a stable and reliable cryptocurrency system, they introduced PoS protocol v2.0.

Proof of Stake:

In the Proof of Stake consensus mechanism, instead of performing computation like Proof of Work or computing information about memory usage using challenge-response like Proof of Retrievability, the emphasis is on figuring out the block's access to a certain amount of coins before being approved by the network. There are a few problems that exist with the basic Proof of stake protocol. The problem of "greedy honest nodes" is an important issue in the Proof of stake mechanism wherein , the honest nodes which do not exactly have any hidden negative motive save up their coins by keeping their coins off the network and they use these coins once in a while to get higher rewards[21].Another issue is that it is possible for an attacker to become the most powerful node in the network[21]. To overcome these issues, BlackCoin came up with a new version of the Proof of Stake consensus mechanism which has been discussed in details in the BlackCoin whitepaper[21]. As the major issue with PoS lies in the concept of coin age and many nodes were starting to get greedy and trying to farm for more stake, in the newer version of PoS, coin age was removed to avoid this issue and this encouraged all the nodes to be online more often[21]. Other changes to the protocol include changing the hash function to SHA256d from the original hash function which was scrypt and was simply used because it existed with PoW and does not have any recognized benefits, the stake modifiers are changed at every interval in this new version and there is also a change with block timestamp[21]. Thus, after the initial phase of blackcoin when it was a mix of PoW and PSs, today, BlackCoin is a purely PoS coin.

Insights and summary(BlackCoin):

BlackCoin was initially implemented as a proof of concept to figure out how Proof-of-Stake consensus mechanism can work as opposed to the existing Proof of Work and it turned out to have a positive outcome and this led to a genuine usable digital cryptocurrency. In the initial days of BlackCoin, it was operated with a mix of PoW and PoS as it was in an experimental phase with the PoS mechanism but soon after it stabilized it was transformed into a pure PoS. BlackCoin has made a major contribution in the field of Cryptocurrency and Blockchain by showing the world how Proof of Stake should be utilized. They managed to pinpoint the issues PoS held and delivered solutions in the new version. One of the many improved features is that users are responsible for issuance of a token which lets nodes be responsible for the network

integrity making the cryptocurrency system truly peer-to-peer. It is much more efficient that cryptocurrencies that work with Proof of Work because there are no computation required to prove their legitimacy and thus a lot of computational power which is otherwise wasted can be saved.One of the disadvantage that is evident in the PoS framework used by BlackCoin is that it is very easy for the rich to influence the system by buying more coins and gaining more stakes by investing more.

Insights on PoS vs PoW: When we compare and decide between two consensus mechanisms to be used by cryptocurrency systems, there are two factors that impact your decision. These two factors are how feasible the protocol is which implies that the protocol should not create high overhead and the second factor to influence this decision is security. In the case of PoS and PoW, PoS is a clear winner in terms of the computational efficiency as PoW requires for nodes to perform work to prove to the network that its a genuine block which requires a lot of computational power while on the other hand, PoS simply uses the value of stakes to determine how relevant or trustable a block is. In terms of security PoS has more concerns and vulnerabilities which can be exploited. Although the second version released by BlockCoin overcomes many of these issues, it is still not as secure as PoW in terms of immutability. But on the other hand it is very difficult to cause attacks like 51% attack in PoS than PoW.

4.5 Ripple

Ripple is a real-time money exchange Cryptocurrency system released in 2012 by Jed McCaleb and Chris Larsen working on its own blockchain based ledger system. Ripple has seen a significant rise in popularity and net worth growing exponentially, only to be behind Bitcoin. Ripple as a company has a very specific pre-defined goal of improving the current payment methods by using its own blockchain methodology. Ripple's developers have set a bar of 100 billion coins, and do not intend to bring the coins to the market forever. Due to its reliance on the company and its developer's, Ripple does not attract a few of the Cryptocurrency traders who have the mindset that Cryptocurrency should exist and operate without the intervention of the company.

According to Ikuya [31] and Fry et al. [39], the primary purpose for the invention and rise of Ripple Cryptocurrency was not to create an alternate currency system, but to act to serve as a

method of exchange and as a distributed payment system. This brings to light the fact that Ripple was built to scale and therefore accepts other Cryptocurrencies and lets its users trade them. This aid to scale the system and make it flexible for users is deemed as the cause for the sudden surge of Ripple and also giving a tough battle to Bitcoin. Due to its unavailability in the market prior to 2012, Ripple still faces an uphill task in comparison to Bitcoin.

The rise of Ripple can also be attributed to its “small world” philosophy as mentioned by Reiff [40]. Reiff also goes on to say that the openness of Ripple has allowed Vulnerabilities to develop and the structure of Ripple also permits man in the middle attack on certain nodes within the network to disrupt few users' access.

One of the advantages of using Ripple is its speed of transaction. It can complete several transactions within a second and Johan [30] brings this comparison to light when comparing Ripple to Bitcoin. Johan also talks about the rise in Ripple Coin price is directly proportional to the Bitcoin price improvements and that makes it stand out from other coins because they do not move ahead with Bitcoin and stay stagnant mostly. Johan also points out that the biggest con to Ripple coin is the fact that the Ripple network that runs the blockchain for the Ripple coin can exist without using the Ripple coin and that it is highly centralized.

Derousseau [41] discusses the Fork effect on Ripple is his book and goes on to say that the concern of fork is negligible or incoherent because of the closed system run by Ripple in comparison to other blockchain systems. To counter the fork effect, Derousseau presents that Ripple uses an Amendment system to make it run smoothly where developer’s provide amendments to the blockchain to make it pass. In an ideal scenario, the pass mark is attributed to be above 80%. This ensures that no hard fork will typically affect the Ripple system and unlike Bitcoin and Ethereum blockchain systems, Ripple doesn’t use Miners.

A survey by Gunay [42] indicates that positive information on Ripple’s worth in the clearnet has a positive influence on its value. Gunay also goes on to say that Ripple has a statistically significant long-run relationship with a confidence level of 95% even with the consideration of structural breaks. Gunay provides statistical evidence to the claims made by Johan that the value of Ripple increases with the increase of Bitcoin and gives a picture that the correlation coefficient of Ripple is 1.4 times of that of Bitcoin. In simpler words, this means that, with Bitcoin’s value increasing by 1 unit, Ripple’s value would increase by 1.4 units.

In a blog by GetSmarter [43], Ripple is reported to have high processing capacity, less energy consumption in comparison to its competitors such as Bitcoin, Litecoin and other cryptocurrencies. Ripple also does a great job of preventing a distributed denial of service (DDOS) attacks by making each transaction cost exponential.

Ripple cryptocurrency unlike most cryptocurrency works in a very centralized manner where the Ripple coins do not operate independent of the Ripple network. The growth of Ripple Coin is most comparable with that of Bitcoin as it stands second to Bitcoin in the Cryptocurrency market. Due to its reliance on the developer's, not many traders are a fan of the Ripple Coin. One thing to observe and not is the fact that Ripple coin attracts businesses and investment banking firms as opposed to its rival, Bitcoin, which primarily is targeted at Individuals. Another important observation made from the research done on Ripple coin is that it works in a different way compared to other cryptocurrency protocols which primarily use blockchain systems. Ripple, on the other hand, uses its own algorithm called the Ripple Protocol consensus algorithm (RPCA), using its own ledger through the RippleNet.

The growth value of Ripple coin seems to be incredible as it grows 1.4 times the units Bitcoin grows by. The success of the Ripple coin is due to its "small word" philosophy. Ripple is incredibly faster for each of its transactions. It can perform multiple transactions in a second, whereas a Bitcoin transaction nearly takes 10 minutes. Ripple coin is considered as the second best cryptocurrency only behind Bitcoin.

Though Ripple coin can surpass and avoid DDOS attacks and few other security issues due to its own Consensus algorithm, it is still susceptible to attacks on certain nodes which can cause failure of the system and disrupt the access of certain users.

Surveying and evaluating the Ripple coin holistically, it can be concluded that Ripple coin is an important and useful discovery to this generation of Internet and electronic money, because it not only acts as a real-time money exchange Cryptocurrency system, but also acts to serve as a distributed payment system. It has good rapport among Banking firms and it can be extended towards individuals too, if the developer's of the Ripple coin make it more centralized and make the operation independent of the company. Another aspect the Ripple coin developer's should consider is to increase the cap of the coins currently existing and bring in the mining factor.

Considering these changes, if made, Ripple coin can take over Bitcoin as the most used and valued Cryptocurrency system in the future.

4.6 Litecoin

Bitcoin was the first cryptocurrency to come into practical use and since then many alternate cryptocurrencies came into existence with differences ranging from very little to entirely different protocols being followed. One of the cryptocurrencies that varies a little from the Bitcoin protocol is the Litecoin or LTC that was released in October 2011 by Charlie Lee who was working in Google at the time and was the former Engineering director at Coinbase. It was released by him via the open-source client Github on October 7, 2011[13].

It was the first Cryptocurrency to use Scrypt hashing algorithm for mining. This hashing algorithm is advantageous in that it's strength lies in the time-memory trade off; that is, an attacker would need more memory to complete the attack faster and it's memory requirement makes it expensive, hence slowing down any attack.

The primary differences between Litecoin and Bitcoin are :

Bitcoin	Litecoin
Block generation time is 10 mins	Block generation time is 2.5 mins
Transaction confirmation is slower compared to Litecoin	Transactions are confirmed faster than in Bitcoin
Hashing algorithm is SHA 256	Hashing algorithm is Scrypt
Lesser maximum of Bitcoins than Litecoins	More total number of Litecoins than Bitcoins
Mining devices for Bitcoins are cheaper due to use of SHA 256 hashing algorithm	Mining devices are are complicated and expensive to produce as Scrypt algorithm is used

SHA is computationally intensive	Scrypt is memory intensive

4.7 Peercoin

Peercoin was invented to overcome the disadvantages posed by bitcoin's Proof of Work consensus model. Peercoin was introduced in the year 2012 when two researchers Sunny King and Scott Nadal proposed a peer-to-peer cryptocurrency that does not use a Proof-of-Work centralized model. Peercoin is an energy efficient, secure and size effective blockchain.[66]

Peercoin uses Proof-of-Stake type consensus and thus considers time as a scarce resource. Validating new transactions and blocks in peercoin is known as minting and people who do it are called minters. Coin Age is used to determine who gets to mine the next block. Coin age is given by the product of the number of coins owned by a minter and the number of days those coins have spent in the minter's wallet. A minter who has been collecting coins for a long period of time is given preference over a new minter while selecting someone to mint the next block.

A comparison of Peercoin and Bitcoin [66] :

Peercoin	Bitcoin
The consensus algorithm used in peer coin is Proof-of-Stake.	The consensus algorithm used in bitcoin is Proof-of-Work.
Peercoin has been active since 2012.	Bitcoin came before Peercoin and has been active since 2009.
The distribution method used by Peercoin is PoW block reward/ PoS block reward.	The distribution method used by Bitcoin is PoW block reward.
The distribution in peercoin is unlimited.	The distribution in bitcoin is limited.
The transaction fee is static.	The transaction fee in bitcoin is not static.
The estimated transaction bandwidth in	The estimated transaction bandwidth for

peercoin is eight transactions per second.	bitcoin is seven transactions per second.
A block is generated every 8.5 minutes.	A block is generated every 10 minutes.
Peercoin has a block size limit of 1 MB.	Bitcoin has a block size limit of 1 MB.

A comparison of Peercoin and Ethereum [66] :

Peercoin	Ethereum
The consensus algorithm used in peer coin is Proof-of-Stake.	The consensus algorithm used in Ethereum is Proof-of-Work.
Peercoin has been active since 2012.	Ethereum has been active since 2015.
The distribution method used by Peercoin is PoW block reward/ PoS block reward.	The distribution method used by Ethereum is PoW block reward/ initial coin offering.
The distribution in peercoin is unlimited.	The distribution in Ethereum is unlimited.
The estimated transaction bandwidth in peercoin is eight transactions per second.	The estimated transaction bandwidth in Ethereum is eight transactions per second
The transaction fee is static.	The transaction fee is not static.
A block is generated every 8.5 minutes.	A block is generated every 12 seconds.
Peercoin has a block size limit of 1 MB.	There is no fixed block size limit, the block size limit is dynamic.

The biggest difference between Peercoin and other cryptocurrencies like Bitcoin and Ehtereum is the absence of the Fee market. A Fee market is a system designed to order and prioritize transactions and to provide monetary incentives for transaction validators. Peercoins fee is fixed at 0.01 PPC per kb. [66]

4.8 Decred

Decred is a cryptocurrency that utilizes a hybrid Proof-of-Work (PoW) and Proof-of-Stake (PoS) mining system[23]. It ensures a more open form of governance that gives miners and users the same amount of power and influence over the system. A unit of the currency is called a decred (DCR).

Validation of blocks and significant policy decisions are decided on through a voting mechanism. Individuals who wish to participate in governance can take advantage of PoS strategy. They must lock their DCR coins for a specified number of days called the maturity period to purchase tickets. The Ticket price is adjusted dynamically every 144 blocks. Voting is classified on basis of its effect on the chain and they are as follows:-

1. On chain voting
    - It deals with validation of blocks and voting on consensus rule changes. After voting on the ticket is called, the locked DCR is returned to the users wallet. The accrued interest on the locked amount is also paid if the person has successfully voted as an incentive to encourage participation.
    - For Block voting, the majority of the randomly selected tickets called to vote must vote for the block mined by the PoW. If voted against, the block reward of the miner would be forfeited. This protects the system from malicious block miners who may attempt to validate invalid transactions.
    - For Consensus Rule Voting, vote on whether to activate proposed consensus rule changes must be approved by at least 75% of non-abstaining tickets to take effect. This ensures a fair mechanism to ensure the needs of the majority of stakeholders are upholded.
2. Off chain voting

    It deals with more fundamental issues such as amendments to the Decred constitution and are proposed in Politeia. Cryptographic techniques are used to prevent sybil attacks and unfair censorship.

Proof of work mining is used to create blocks which consist of transactions from the pool. Generating proof of work involves processing of network transactions to build new blocks. Unlike in other currencies discussed, this newly created block is verified by ticket holders via proof of stake strategy. For every valid block, the miner receives the fees from all of the transactions included in the block and a block reward. As in bitcoin, the block reward reduces by a factor of 100/101 every 6,144 blocks. The hash function used is BLAKE-256.

Decred is popular for its efficient self governance system of checks that other contemporaries like Bitcoin lacks.

4.9 Dash

Dash is an open source cryptocurrency which stands for digital cash. It was forked from the bitcoin protocol and is a decentralized autonomous organization (DAO) which is governed by masternodes that are users who meet the requirements needed to become masternodes. Masternodes are essentially the same as the other nodes but have some extra powers. They are responsible for making new decisions for this entire system. Some requirements are that the masternode requires to own at least 1000 dash coins, static IP address and they need to have sufficient resources needed for mining like CPU, RAM, disc space and network bandwidth. A proof of service protocol ensures that masternodes have the most current blockchain protocol and are online. Dash coin uses the proof of work algorithm as a mining algorithm and it uses a X11 hashing function which uses 11 rounds of hashing to hash the data and the average time needed to mine a coin is around two and a half minutes. Masternodes mainly have functionalities like hosting a copy of the blockchain, validating the transactions of the other nodes on the network. The system of dashcoin also includes miners and simple nodes along with the masternodes. Compared to other cryptocurrencies, dash coin has two additional types of transactions namely “InstantSend” and “PrivateSend”. InstantSend bypasses the step of mining but requires the consensus of masternodes to validate a transaction. On the other hand, PrivateSend makes transactions untraceable. Dash is a self-funded and self-governed blockchain protocol, with instant payments which run on a network of incentivized Masternodes.

- **Masternodes :** Dash is run by masternodes which are responsible for making new decisions for the entire system. Any node/user can be a masternode by investing 1000 Dashcoins and high computational power. Dash is an incentivized network, so the masternode gets 45% of the reward for every dash block mined by that masternode.

- **InstantSend :** IDash provides an InstantSend feature which allows participants to send and confirm transactions in a very few seconds. InstantSend is approved by masternodes directly without mining.

- **PrivateSend :** Bitcoin transactions are not fully anonymous so one can trace their participants. To address this, dash provides PrivateSend transactions which are fully private transactions. For making transactions fully private, it mixes participating users' unspent dash before executing the transaction.

5 Attacks on Blockchain and Defense

5.1 Selfish mining

As we know by now, a blockchain is a chain of blocks connected to each other such that subsequent blocks that are added to the chain are related by some properties to the previously present blocks in the chain. Each of these blocks contains transactions carried out by the users which are verified by miners who are responsible for this validation and coming up with new blocks to be added to the blockchain.

When a new block is added to the blockchain, the miners get an incentive/reward for the work done by them in validating the transactions of the block and publishing the block. In case of a block race, there are two blocks being published at almost the same time. The blockchain is forked at this point because of two different branches being created at this parent block as the protocol requires the miner to choose the block which he sees first to further work upon. Different miners will see one of the two blocks published and start working on it. Eventually, the longer branch is selected as the branch to which the mining community must add the subsequently mined blocks.

The problem arises when there is a miner or a group of miners, such as a selfish cartel, which finds new blocks but keeps them to themselves and does not publish it. That is, they maintain a private branch local to themselves as opposed to the public branch on which the other party i.e honest miners are working, to take advantage of the incentives they will get in doing this. It is based on the withholding of blocks strategically such that they will be published at a convenient point of time (with respect to the chain of blocks which are public). Here, selfish behavior is being incentivized over honest behavior, eventually causing most participants to adopt the selfish behavior despite this being detrimental to the global interest of the community.

There are two parameters that selfish mining depends on to become successful: the mining power of the selfish cartel defined by α and the mining power of the honest miner γ, that may mine on a block released by the selfish cartel in a block race. The amount of computational power that a miner or a pool of miners control out of the total computational power is called the

mining power. The higher the γ value, the lower the α can be as this means that more of the honest miners are helping build the private block belonging to the selfish cartel.

In “Majority is not Enough: Bitcoin Mining is Vulnerable”, Eyal and Sirer extensively study this concept of selfish mining [48]. Thus, as Eyal and Sirer show, if γ = 0, then selfish mining is profitable at α ≥ 0.33 or 33%, whereas if γ = 0.99 then selfish mining is profitable at α ≥ 0.009.

The following is the strategy of the selfish cartel in case if :

1. The honest miners discover a new block :
    - If the private branch being maintained by the cartel is shorter than the public branch of the blockchain, then set the private branch to be equal to the public branch.
    - If the public branch is shorter than the private branch of the cartel by zero or one block, then the selfish cartel publishes the entire private branch.
    - If the public branch is longer than the private branch of the cartel by more than one block, then the selfish cartel publishes the first unpublished block belonging to the public chain.

2. The selfish group discover a new block :
    - Add this new block to the private chain being maintained by the cartel.
    - If there is a block race between the selfish cartel and rest of the miners, use the private branch being maintained by the cartel i.e. publish it to win the race.

A selfish mining cartel with significant mining resources would cause two problems :

1. The transaction approval time may increase as the transactions approved by the selfish private branch would not be public which would lead to increase in the number of block races. Those blocks that lose in a block race need to have the transactions contained in them re-approved in a later block.
2. The cryptocurrency would be more vulnerable to double-spending as both the cartels and honest miners may add mutually exclusive transactions to the private and public branches.

The harmful effects of selfish mining are that if it becomes more profitable to selfish mine than to mine honestly, more number of miners will resort to the selfish mining strategy which may lead to the fatal case of the selfish cartel holding more than half the mining resources that may lead to the centralization of the cryptocurrency. This is also known as the 51% attack. Mining groups with over a quarter of the power i.e. 25% can earn more than what is legally possible for them to earn, and groups with over 33% can easily selfish mine, and large pools with over 50% is extremely problematic[49].

5.2 51% attack

Once a selfish cartel/group holds more than 50% of the mining power or 51% to be precise, they can control the network's mining hash rate, preventing new transactions from being verified by the miners thereby halting the payments between some or all the users. The cartel will not be able to create new coins or alter older blocks but will be in a position to reverse transactions that were completed while they are in control of the network, i.e double-spending coins.

Delving into the details of the attack, let there be two blockchains of length n and m where n > m. These blockchains have a common ancestor. Let chain n belong to the honest miners and the other belong to the attackers who are holding more than half of the network's capacity. Now both groups can generate a chain of length k where k is greater than n with profitability pK-l where l is the length of chain belonging to the honest group of selfish cartel and p being the fraction of mining capacity held. So if the attacker (selfish cartel) chooses k to be large enough, they will find a longer chain than their honest counterparts.

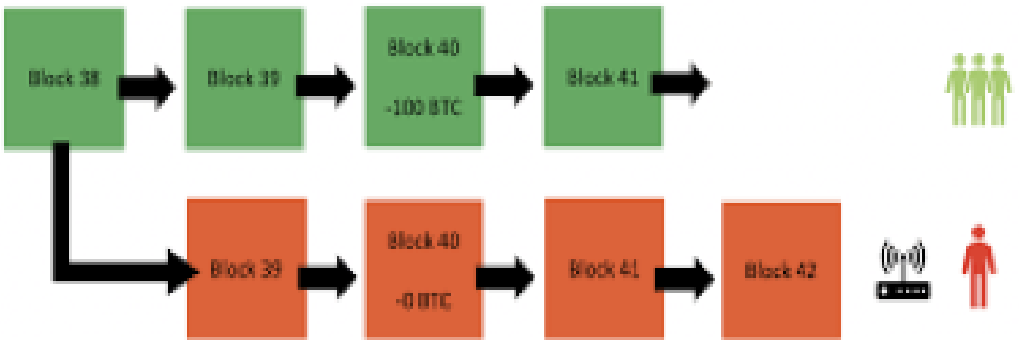

Fig. 8 - Honest vs Selfish Block chains [68]

In the figure shown above, the green blocks are the ones found by the honest miners and the red blocks are the ones found by the selfish cartel (malicious miner). The malicious miner does not broadcast his chain until the right time, and when he does at the opportune time, all balances of the individuals as well as the previous transactions will now be in accordance with this new chain. Because it is the longest longest chain, honest miners join it as protocol demands mining on the longest chain.

5.3 Preventing selfish mining

One of the effective measures to prevent selfish mining or defend against it is by using a new mining strategy which defends against selfish mining called the Freshness Preferred(FP) strategy [32]. In this strategy, it is proposed that timestamps be added to each block and that these timestamps be taken into consideration by the miner during a block race in making the decision of accepting a block. This strategy detters selfish mining by reducing the profitability of selfish mining with the use of unforgeable timestamps to penalize miners that don't publish blocks when found. This strategy increases the threshold of mining power needed to profitably selfish mine from 25% to 32%.

FP strategy works as follows:
In case an FP miner receives two blocks within a very short interval of time:

1. In case the two blocks belong to chains of equal length, the block with the most recent timestamp which is valid is accepted by the miner and the other one is rejected. If both the timestamps are equal, the miner selects the block that was first seen by him.
2. In case the blocks are coming from two branches of differing lengths, the miner accepts the block from the branch of the greater length.

In any other case :

- The miner behaves according to the usual protocol required by the cryptocurrency.

In case of the cryptocurrency being Bitcoin, the block with the most recent timestamp is selected by the FP miner to work upon, over the block which arrives earliest which is usually the norm. This means that block races are won by blocks that have the most recent timestamps as these

are put in when the blocks are created and that withholding blocks reduces the percentage of honest miners that will mine on the withheld block. As stated before, the lower this value of honest miners mining on the selfish block i.e γ, the more the increase in the threshold for mining power i.e. α required by the selfish cartel to be successful.

Another strategy to prevent the formation of large pools of miners that may exceed 50% of the mining power is the Two-Phase PoW proposed by Eyal and Sirer which disincentivizes large pools[49]. This consists of two separate crypto puzzles to be solved as opposed to the current single cryptopuzzle which is very easy to delegate to the members of the pool. The idea is to make delegation of the PoW to the pool members by the pool manager more difficult because as long as this is easy, huge pools can be built.

The two phases of finding solution in a Two-Phase PoW strategy is as follows[49]:

1. The double hash of the header (SHA256(SHA256(header))) is smaller than a difficulty parameter X
2. The header is signed with the coinable transaction's private key, and the hash (SHA256(SIG(header, private key))) of that signature is smaller than a second difficulty parameter Y.

Phase 1 is identical to the current procedure in the Bitcoin protocol. The additional phase 2 is what brings control to the size of the mining pool being created i.e. the number of miners that can be added to the pool by the pool manager.
After phase 1, when the miners are confident about a possible solution, they must pass the second difficulty parameter Y by finding a hash that is below this value. This hash is the hash of the result of signing the block with the private key that controls the payment address. If this second difficulty parameter is small enough, the pool manager cannot discover a solution to the second stage by himself. The second stage requires the same power and is as costly as the first phase to accomplish and therefore needs to be distributed just as widely. The fact that this second phase cannot be outsourced to untrustworthy third parties because it requires the pool manager to give the private key to each pool participant for them to sign means there is a possibility for the miner to take away all the coins for himself. Therefore, the manager must trust

the participants in his respective pool and would not be able to admit untrusted individuals into their pools.

5.4 Insights into selfish mining and the 51% attack

As explained in the previous sections, if a mining group is in the control of more than half of the network's power, the group can perform all sorts of malicious activities like halting the payments between some or all the users or can double-spend coins by reversing transactions that happened when they were controlling the network. Even if the group does not perform any of these malicious activities, the morale or the mining network goes down when a group has that much power with them. To prevent this, we have seen two methods by which selfish mining becomes very difficult to be profitable if not impossible.
The two methods we've seen to prevent selfish mining and 51% attack are:

1. Maintain a timestamp in each block and during a block race, select the block that was created the latest.
2. Two Phase proof of work wherein after miners find a viable solution to the problem there is another problem to be solved which enforces the pool manager to consciously admit miners he trusts into the group as the miner needs to be given the private key of the pool.

In this first solution, selfish mining is prevented in that if the selfish cartel which has been hiding its private blockchain publishes it at once to defeat the honest chain, most miners are not likely to accept it as the timestamp on those blocks will much older than the timestamp on the most recent block in the honest chain.

In the second solution, the pool size is being controlled as there is a disincentive for large pool sizes because the pool manager has to share the private key for the block to be signed by the miners in the pool and therefore, untrusted miners will not be admitted to the group.

5.5 Cryptojacking

Cryptojacking came up in the cybersphere as the valuation of the digital currency area took off in the course of recent months and alludes to where a hacker hijacked the processing power of a PC to mine cryptographic money for the hacker's sake. AdGuard revealed in November 2017 that more than 220 cryptojacking sites were found among the best 100,000 sites as indicated by Alexa. What's more, this pattern isn't probably going to subside at any point in the near future.

The expression "cryptojacking" burst onto the scene when it was discovered that The Pirate Bay was trying different things with Coinhive in September 2017 to check whether the non-profit could create more income through its site. Coinhive permits you to add content to a website page and mine the digital money Monero (XMR) by using a guest's processing power.

Cryptojacking, a kind of cyber attack where an attacker hijacks an objective's processing capacity to mine cryptographic currency for the attacker's benefit. Analysts from Fudan University, Tsinghua University and the University of California Riverside have distributed the primary precise investigation about cryptojacking in reality called "How You Get Shot in the Back". [25]

Right now, have contemplated different attributes of cryptojacking contents. They assembled CMTracker, a conduct-based indicator with two runtime profilers for naturally following Cryptocurrency Mining contents and their equal areas.

They discovered 2,770 exceptional cryptojacking tests from 853,936 well known website pages, including 868 among the top 100K in Alexa list. By utilizing these examples they increased all the more away from the assaults, including their effect, appropriation systems, jumbling, and endeavors to evade detection. They further found that an alternate arrangement of organizations profits by this movement due to the unique wallet ids. Not just this, to remain under the radar, they likewise update their attack domains.

Cryptojacking and CMTracker Design

Researchers planned and actualized an indicator called CMTracker to distinguish this attack. From that point forward, they crept Alexa's top 100K sites and discovered 2,770 cryptojacking pages. They determined the harm of cryptojacking, showing that it costs more than 278K kWh additional force day by day, and hackers are winning in any event 59K US dollars day by day. They dissected various parts of the attack areas and the practices of contents.

Be that as it may, how does CMTracker work and how could it figure out how to discover almost three-fold the number of cryptojacking areas as the latest reports? Two conduct based profilers are utilized, one to recognize mechanized mining contents, known as the hash-based profiler, and one to screen the calling heap of a site, known as the stack-structure based profiler. For the hash-based profiler, if a site utilizes in excess of 10 percent of its execution time on hashing, it is accounted for as a cryptographic money excavator. [26]

The thought for the stack-structure profiler goes something like this: Mining assignments won't occur as the client is loading the page; rather, at least one dedicated thread is made since mining cryptocurrency accompanies an overwhelming outstanding task at hand. On the off chance that hackers use code obscurity procedures to avoid hash-based profiling, at that point the rehashed standards of conduct of the miner's execution stack can be utilized to recognize cryptocurrency miners.

The stack depth and call chain of mining contents are rehashed and regular. By seeing whether a dedicated thread rehashes its call chain occasionally and whether the call chain possesses in excess of 30 percent of the entire execution time right now, a cryptocurrency miner is accounted for to be present. Alongside the condition for a hash-based profiler, these two limits are the lower limits from cryptojacking in reality.

The last check is made manually, taking a gander at the terms of service of every site to check whether there is any client understanding that makes it understood to the client or verifiable in their understanding that their handling power is being utilized for cryptographic money mining while at the same time visiting the site. The investigation found that solitary 35 sites were "friendly”.

As announced by CryptoTicker, in the long stretch of June 2018, the cybersecurity organization McAfee had uncovered that a large number of sites worldwide have fallen prey to a

cryptojacking malware that powers their guests' PCs to mine digital money without them realizing when perusing the site. Programmers have broadened their action into the territory of cryptojacking, the disease of client frameworks to seize and utilizing them to dig for digital forms of money. The coin excavator malware developed by 629% to more than 2.9 million known examples in Q1 2018 from just about 400,000 examples in Q4 2017.

The Main Players in the Cryptojacking Game

Who is answerable for cryptojacking? The examination likewise explores the players, and the figure underneath shows a certifiable case of the collaboration between every one of these players. By utilizing the appropriation of various mining members from an irregular subsection of their example, a few answers are given.

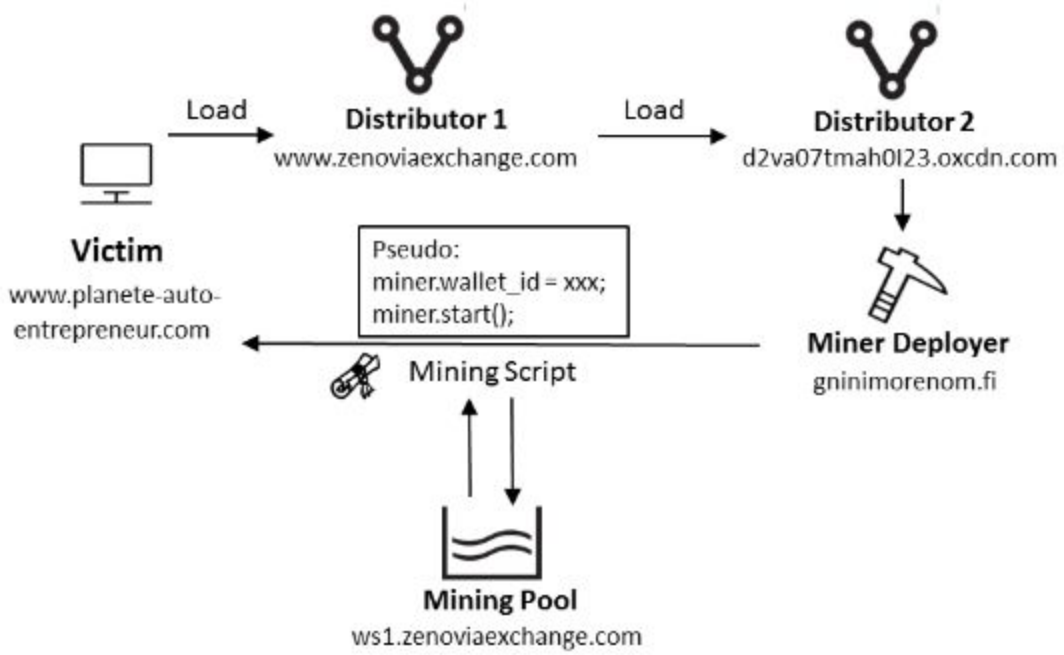

Fig 9. The cryptojacking procedure imagined and the players included [26]

Most member spaces happen in close to three vindictive examples, and just a little level of mining pools, mining distributors or miner deployers are found in excess of 10 site pages. The outcomes propose that blacklists might be inadequate as malicious miners are not centrally controlled.

Another key outcome is that advertisers and mining administrations are for the most part connected to cryptojacking sites. For example, it noticed a pattern of promoters going to malicious mining, referring to zenoviaexchange.com, a website like Coinhive, for instance of a previous advertising service provider that is presently a miner.

Likewise, by contemplating the dissemination of wallet IDs related to mining contents and finding that a given wallet ID is generally connected with under three malicious site pages, the information prompts the end that a wide range of actors profits by abusing cryptographic money mining services.

To more readily comprehend the elements of cryptojacking, the examination likewise reveals some insight into the existing pattern of malicious miners. Around 20 percent of the miner deployer's areas that are cryptojacking pages in the example vanish in less than nine days, yet distributors move to more new places at a lower rate.

5.6 Insights into Cryptojacking

Given that cryptojacking members can utilize progressively complex measures to sidestep identification, it makes one wonder whether browser extensions or antivirus programs can shield clients from this kind of digital robbery. The specialists propose that most defensive measures depend on blacklists and afterward proceed to assess the viability of two of the most broadly utilized blacklists in a 15-day analysis: NoCoin and MinerBlock.

The outcomes show that under 51 percent of malicious assaults are recognized, and - because of the way that blacklists are refreshed each 10 to 20 days when contrasted with nine or less for mining deployers - this difference implies that the malevolent actors are constantly one stride ahead, as cryptojacking domains relocate or vanish at a higher rate. Thus, the identification rate doesn't increment, despite the fact that inclusion does.

To viably battle cryptojacking, scientists propose a conduct-based way to deal with location, which would then be able to be actualized by browser extensions and antivirus programs. As demonstrated by the examinations, it takes three seconds for the CMTracker to dissect a site page for cryptojacking and, when joined with a whitelist for those sites having unequivocal reference to the gift of preparing power in the client terms of service, could adequately diminish malicious mining. [25]

These specialists likewise point to digital money mining services as having given lacking consideration to the maltreatment of their services; mining scripts are run without client warning and clients can't kill these scripts. Subsequently, they recommend that the mining services like Coinhive, which controls half of all cryptojacking domains, should bear a portion of the responsibility. Mining services could do this by actualizing a pop-up window or something like advising the client, permit them to deny the ask for and disable the mining procedure.

5.7 Evaluation of Countermeasures

The Freshness Preferred strategy is a countermeasure for selfish mining which increases the necessary mining power needed to profitably selfishly mine. Where possible, this method should be used. Cryptojacking is a method of cryptocurrency mining that allows a malicious miner to use other user’s computing power for themselves. This is possible through malware as well as malicious websites. Completely ending this method of mining is difficult due to users not always updating antivirus protection or their browsers. Blockchains are flawed in the sense that they are always vulnerable. If a single member of the network holds enough mining power, they can take control of transactions in the blockchain via the 51% attack. While this vulnerability exists, blockchain cryptocurrencies are known to “work in practice, not in theory” [5]. Because it would be extremely difficult for any one entity to hold that much mining power, cryptocurrencies can run without issue.

6 Security around Blockchain Systems

Recent research on having a secure decentralized system has led to the development of blockchain systems. Blockchain systems have proven to reshape the economy of the world by not having centralization and removing the dependency on a single entity or organization. However, having everything decentralized makes one question the security and integrity of the platform. The possibility to exploit the system and, in turn, cause thefts has brought concerns to users regarding the security of blockchain.

There can be many attacks that can exploit blockchain systems, and can be categorized in many ways. Bach et al. [29] and Saad et al. [44] discusses potential attacks possible on blockchain categorized by the blockchain applications. Saad et al. [44] go on to explain the different attacks such as Selfish Mining Attack - where certain user's keep their operating blocks private to increase their value, Majority Attack - which is also known as the 51% attack - can be used by a single user or multiple users which occupy or own a majority of the blockchain network to cause an attack, and network attacks - such as the DNS attack, BGP hijacks, spatial partitioning, eclipse attacks, and DDOS attacks which can cause the failure of the entire blockchain network. Other classified attacks include block withholding attacks, Consensus Delay, time jacking attacks, Cryptojacking, wallet thefts, balance attacks and many more. Given the numerous attacks possible, the security of the blockchain is under question.

Research has been focused to find a solution to the vulnerabilities in blockchain and make it a more secure system. Li et al. [7] have done an extensive survey on the security and privacy of the blockchain systems and have reported the possible attacks and the security measures to tackle them which have been proposed in the past by other researchers.

In 2012 Luu et al. [45] proposed a security measure for the Blockchain system called SmartPool that gets the transaction information from the nodes and stores it. The miner associated with the blockchain then conducts a computation using hashing and returns the results to the node. This novel methodology allows to secure the blockchain system from any Mining attack. SmartPool maintains the decentralized nature of the blockchain, and also brings in efficiency and security to the blockchain in terms of mining attacks. Li et. al [7] have given a design for the proposed SmartPool system as shown in figure 10.

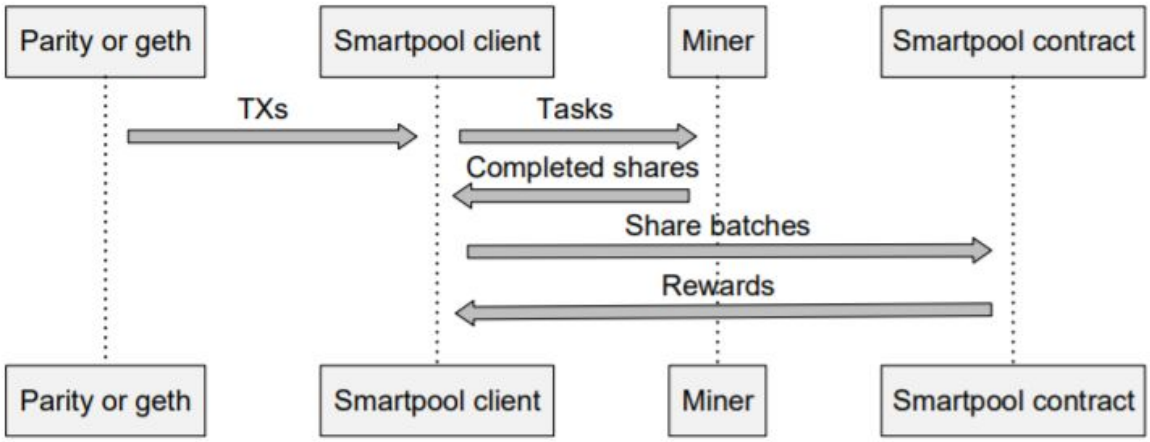

Fig. 10 - Block diagram for SmartPool [7]

Other findings include Arthur et al. [11] proposing a quantitative framework to handle the execution performance and security provisions for the blockchain. Additionally, Kosba et al. [46] proposed a novel framework for preserving the privacy of blockchain systems. The framework known as Hawk is used for users to have privacy around their blockchain without writing any code or using any encryption techniques.

Zhang et al. [47] also discuss potential security measures required to be taken to make blockchain more secure. The authors introduce a novel methodology called Mixing where multiple cryptocurrencies can be used to create a Mixcoin which makes it difficult for hackers and attackers to track the user performing the transactions, thus preventing specific attacks. Anonymous signatures including group signatures and ring signatures were proposed by the author to hide out the identity of the user performing the transaction. Another measure pointed out by the authors, was the use of Homomorphic Encryption which ensures that the decryption done on encrypted data would yield the same results as decryption done on plain data, and hence preventing any cipher attacks. Attribute based encryption, Multi-party Computation and Game based Smart Contracts were among other novel solutions proposed by Zhang et al. [47] to maintain the privacy and security of the blockchain system.

7 Final Conclusions and Recommendations

The majority of cryptocurrencies available today run using blockchain, a decentralized ledger of transactions that is built upon by miners. Miners perform difficult computations to add new blocks to the blockchain, usually by finding a hash value that has certain characteristics. Miners are given incentive to add to the blockchain through rewarding currency.

Blockchain was invented and has existed for a considerably long amount of time before gaining the popularity that it has today. This is accounted for by the wide number of applications that blockchain is readily being deployed in in today's world. Apart from transforming the entire finance sector in the form of cryptocurrencies and trading, blockchain is also widely used in multiple other sectors. It is largely applied in fields of ownership, Internet of Things, Contracts, etc. Each of these fields use blockchain in numerous sub-applications. Finance includes not only cryptocurrency but also loans, money lending contracts, trading and so on. Ownership is further categorised into ownership of property, goods, patents, etc. Smart contracts include important deeds between two non trusting parties, government records, identity information, and much more. It is noted that each of these applications demand a certain high level of security and privacy which is readily provided by the blockchain technology. Blockchain ensures mitigation of fraud, loss of money or data, and ensures that the data is only accessible by parties that have authorization to view or use it.

Because the discussed cryptocurrencies rely on a decentralized peer-to-peer network of miners rather than a centralized authority, certain advantages and disadvantages arise. This system does not rely on trusting a centralized authority, which means it is resistant to corruption within an organization. However, many security risks become possible, albeit difficult, with this system. Powerful individuals can take control of a blockchain if they control greater than 51% of the total mining power in the network. A powerful individual or organization can also work against the rest of the network to undermine their work and gain more rewards with an exploit known as selfish mining. However, this requires enough mining power to mine faster than the rest of the network. While many exploits are theoretically possible, they require an insurmountably large amount of mining power in order to be viable.

Blockchain as a decentralized network works in a very different way compared to most frameworks and networks. Here, there is no single authority and single owner. Each user is responsible for his/her own block of network in the blockchain. This non-reliance on a single

entity has a lot of advantages, but also comes at the cost of questioning the security and integrity of the platform. Analyzing the research done on the security of blockchain, it can be observed that there are multiple attacks possible on blockchain which have been discussed previously. Each of the attacks has its own consequence on the blockchain network and since it is a decentralized network it is impossible to stop the entirety of the attacks. Only the amount of damage done can be controlled by adapting several preventive measures for the blockchain.

There are pros and cons for each security measure discussed above, such as Mixcoin which can hide the authentication of the user performing the transaction. However, there is a heavy time and energy consumption in processing the transaction. Again, for anonymous signatures, the time involved in performing the digital signatures is exponentially high and is not seen as a good metric while performing blockchain transactions. While using a single security measure, there may be other vulnerabilities that may arise and handling that would cause a lot of time and effort.

Every security concern needs to be addressed individually, and hence all the security measures mentioned above must be carefully weighed against their pros and cons and a trade-off must be made while applying one. Security measures for blockchain systems should not be generalized and should be adapted and implemented according to the needs and requirements of the application.

References

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[2] Conti, Mauro, et al. "A survey on security and privacy issues of bitcoin." IEEE Communications Surveys & Tutorials 20.4 (2018): 3416-3452.

[3] Yuan, Yong, and Fei-Yue Wang. "Blockchain and cryptocurrencies: Model, techniques, and applications." IEEE Transactions on Systems, Man, and Cybernetic Systems, 48.9 (2018): 1421-1428.

[4] Mukhopadhyay, Ujan, et al. "A brief survey of cryptocurrency systems," 2016 14th annual conference on privacy, security and trust (PST). IEEE, 2016.

[5] Bonneau, Joseph, et al. "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," 2015 IEEE Symposium on Security and Privacy. IEEE, 2015.

[6] Bucko, J. O. Z. E. F., D. Pal'ová, and M. Vejacka. "Security and trust in cryptocurrencies." Central European Conference in Finance and Economics. 2015.

[7] Li, Xiaoqi, et al. "A survey on the security of blockchain systems." Future Generation Computer Systems (2017).

[8] Vyas, Chinmay A., and Munindra Lunagaria. "Security concerns and issues for bitcoin." the proceedings of National Conference cum Workshop on Bioinformatics and Computational Biology, NCWBCB. 2014.

[9] Back, Adam. “Hashcash - A Denial of Service Counter-Measure.” http://www.hashcash.org/hashcash.pdf, 2002.

[10] Nicolas T Courtois, Marek Grajek, and Rahul Naik. “Optimizing sha256 in bitcoin mining”. In *Cryptography and Security Systems*, pages 131–144. Springer, 2014.

[11] Gervais, Arthur, et al. "On the security and performance of proof of work blockchains." *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016.

[12] M. Bastiaan, “Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin,” Jan 2015

[13] C Lee. Litecoin, 2011

[14] Casino, Fran & Dasaklis, Thomas & Patsakis, Constantinos. (2018). A systematic literature review of blockchain-based applications: Current status, classification and open issues, 2018.

[15] Evan Duffiel, Daniel Dia, Dash: A PrivacyCentric CryptoCurrency

[16] Halpin, Harry, and Marta Piekarska. "Introduction to Security and Privacy on the Blockchain." 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2017.

[17] Puthal, Deepak, et al. "The blockchain as a decentralized security framework [future directions]." IEEE Consumer Electronics Magazine 7.2 (2018): 18-21.

[18] Kirillova, Elena Anatolyevna, Albert Valentinovich Pavlyuk, Irina Aleksandrovna Mikhaylova, Teymur E. Zulfugarzade, and Sergey Sergeevich Zenin. "Bitcoin, lifecoin, namecoin: The legal nature of virtual currency." Journal of Advanced Research in Law and Economics 9, no. 1 (31) (2018): 119-126.

[19] Kalodner, Harry A., Miles Carlsten, Paul Ellenbogen, Joseph Bonneau, and Arvind Narayanan. "An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design." In WEIS. 2015.

[20] Bowers, Kevin & Juels, Ari & Oprea, Alina. (2008). Proofs of Retrievability: Theory and Implementation. IACR Cryptology ePrint Archive. 2008. 175.

[21] Pavel Vasin “Blackcoin’s proof-of-stake protocol v2” URL: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf 71, 2014

[22] Peters, R. (2017, December 28). What is BlackCoin Coin. Retrieved from https://captainaltcoin.com/blackcoin-cryptocurrency/

[23] Jepson, Christina. “DTB001: Decred Technical Brief.” 2015, https://cryptorating.eu/whitepapers/Decred/decred.pdf.

[24] Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]. SIGMETRICS Performance Evaluation Review, 42, 34-37.

[25] Hong, G., Yang, Z., Yang, S., Zhang, L., Nan, Y., Zhang, Z., ... & Duan, H. (2018, January). How you get shot in the back: A systematical study about cryptojacking in the real world. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1701-1713).

[26] Eskandari, S., Leoutsarakos, A., Mursch, T., & Clark, J. (2018, April). A first look at browser-based cryptojacking. In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 58-66). IEEE.

[27] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32.

[28] Gervais, Arthur, et al. "On the security and performance of proof of work blockchains." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.

[29] Bach, L. M., Branko Mihaljevic, and Mario Zagar. "Comparative analysis of blockchain consensus algorithms." 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2018.

[30] von Amsterdam, Johan. "Ripple versus Bitcoin: The battle of the cryptocurrencies (Volume 5)." (2018).

[31] Takashima, Ikuya. "Ripple: The Ultimate Guide to the World of Ripple XRP, Ripple Investing, Ripple Coin, Ripple Cryptocurrency, Cryptocurrency." (2018).

[32] E. Heilman. One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. IACR Cryptology ePrint Archive, 2014:7, 2014.

[33] G. Andresen, Neutralizing a 51% attack, Galvin-Tech 2012

[34] Jiawei Yuan and Shucheng Yu. 2013. Proofs of retrievability with public verifiability and constant communication cost in cloud. Cloud Computing ’13. Association for Computing Machinery, New York, NY, USA, 19–26.

[35] Tariq, Noshina, Muhammad Asim, Feras Al-Obeidat, Muhammad Zubair Farooqi, Thar Baker, Mohammad Hammoudeh, and Ibrahim Ghafir. "The security of big data in fog-enabled IoT applications including blockchain: a survey." Sensors 19, no. 8 (2019): 1788.

[36] Lewis, Rebecca, John McPartland, and Rajeev Ranjan. "Blockchain and financial market innovation." Economic Perspectives 41, no. 7 (2017): 1-17.

[37] Ari Juels and Burton S. Kaliski. 2007. Pors: proofs of retrievability for large files. In Proceedings of the 14th ACM conference on Computer and communications security (CCS ’07). Association for Computing Machinery, New York, NY, USA, 584–597.

[38] HegdeRA & PrakashM, “A Survey on Proof of Retrievability and its Techniques”, International Journal of Engineering and Techniques, Vol.2, No.2, (2016)

[39] Fry, John, and Eng-Tuck Cheah. "Negative bubbles and shocks in cryptocurrency markets." International Review of Financial Analysis 47 (2016): 343-352.

[40] https://www.investopedia.com/news/what-biggest-security-threat-ripple-cryptocurrency/

[41] Derousseau, Ryan. The Everything Guide to Investing in Cryptocurrency: From Bitcoin to Ripple, the Safe and Secure Way to Buy, Trade, and Mine Digital Currencies. Simon and Schuster, 2019.

[42] Gunay, Samet. "Impact of Public Information Arrivals on Cryptocurrency Market: A Case of Twitter Posts on Ripple." East Asian Economic Review 23.2 (2019): 149-168.

[43] https://www.getsmarter.com/blog/market-trends/eight-types-of-cryptocurrencies-compared/

[44] Saad, Muhammad, et al. "Exploring the attack surface of blockchain: A systematic overview." arXiv preprint arXiv:1904.03487 (2019).

[45] L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smart pool: Practical decentralized pooled mining, in: 23 USENIX Security Symposium, 2017.

[46] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: IEEE Symposium on Security and Privacy, 2016, pp. 839-858.

[47] Zhang, Rui, Rui Xue, and Ling Liu. "Security and privacy on blockchain." ACM Computing Surveys (CSUR) 52.3 (2019): 1-34.

[48] I. Eyal, E. G. Sirer., Majority is not Enough: Bitcoin Mining is Vulnerable, arXiv:1311.0243, 2013, http://arxiv.org/abs/1311.0243

[49] I. Eyal and E. G. Sirer. How to disincentivize large bitcoin mining pools, 2014.

[50] Miraz, Mahdi H., and Maaruf Ali. "Applications of blockchain technology beyond cryptocurrency." *arXiv preprint arXiv:1801.03528* (2018).

[51] Treleaven, Philip, Richard Gendal Brown, and Danny Yang. "Blockchain technology in finance." Computer 50, no. 9 (2017): 14-17.

[52] Tapscott, Alex, and Don Tapscott. "How blockchain is changing finance." Harvard Business Review 1, no. 9 (2017): 2-5.

[53] Verma, Dinesh, Nirmit Desai, Alun Preece, and Ian Taylor. "A block chain based architecture for asset management in coalition operations." In Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII, vol. 10190, p. 101900Y. International Society for Optics and Photonics, 2017.

[54] Gatteschi, Valentina, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, and Víctor Santamaría. "Blockchain and smart contracts for insurance: Is the technology mature enough?." Future Internet 10, no. 2 (2018): 20.

[55] Achanta, Ravishankar. "Cross-Border Money Transfer Using Blockchain-Enabled by Big Data." White Paper, External Document (2018).

[56] Wang, Huaiqing, Kun Chen, and Dongming Xu. "A maturity model for blockchain adoption." Financial Innovation 2, no. 1 (2016): 12.

[57] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper 3, no. 37 (2014).

[58] Manda, Vijaya Kittu, and Satya Prakash Yamijala. "PEER-TO-PEER LENDING USING BLOCKCHAIN." Advance and Innovative Research (2019): 61.

[59] Lin-bo, DU Tian-xu XIE, and X. U. Ying-qin. "The key technologies and primary urgent problems of IOT [J]." Microcomputer Information 5 (2011).

[60] Dorri, Ali, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. "Lsb: A lightweight scalable blockchain for iot security and privacy." arXiv preprint arXiv:1712.02969 (2017).

[61] Ayoade, Gbadebo, Vishal Karande, Latifur Khan, and Kevin Hamlen. "Decentralized IoT data management using blockchain and trusted execution environment." In 2018 IEEE International Conference on Information Reuse and Integration (IRI), pp. 15-22. IEEE, 2018.

[62] Singh, Pranav Kumar, Roshan Singh, Sunit Kumar Nandi, and Sukumar Nandi. "Managing smart home appliances with proof of authority and blockchain." In International Conference on Innovations for Community Services, pp. 221-232. Springer, Cham, 2019.

[63] Chen, Si, Rui Shi, Zhuangyu Ren, Jiaqi Yan, Yani Shi, and Jinyu Zhang. "A blockchain-based supply chain quality management framework." In 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), pp. 172-176. IEEE, 2017.

[64] Alharby, Maher, and Aad Van Moorsel. "Blockchain-based smart contracts: A systematic mapping study." arXiv preprint arXiv:1710.06372 (2017).

[65] Zhang, Peng, Michael A. Walker, Jules White, Douglas C. Schmidt, and Gunther Lenz. "Metrics for assessing blockchain-based healthcare decentralized apps." In 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-4. IEEE, 2017.

[66]Peercoin documentation, accessed on March 23, 2020 at 10:33 am. Available [online]: https://docs.peercoin.net/#/comparison-with-other-blockchain-networks

[67]Bentov, Iddo, Ariel Gabizon and Alex Mizrahi. “Cryptocurrencies Without Proof of Work.” Financial Cryptography Workshops 2014.

[68] Jimi S. “Explanation of the 51% attack and the double spend attack” 2018 https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474