

BAŞKENT UNIVERSITY
INSTITUTE OF SCIENCE AND ENGINEERING

ANALYSIS OF CRYPTOCURRENCIES

GÖRKEM ULUSOY

MASTER OF SCIENCE THESIS

2018

ANALYSIS OF CRYPTOCURRENCIES

KRİPTO PARALARIN ANALİZİ

GÖRKEM ULUSOY

**Thesis Submitted
in Partial Fulfillment of the Requirements
for the Degree of Master of Science
in Department of Computer Engineering
at Başkent University**

2018

This thesis, titled: “**Analysis of Cryptocurrencies**” has been approved in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE IN COMPUTER ENGINEERING, by our jury, on 13 /12 /2018

Chairman (Supervisor) : Prof. Dr. A. Ziya AKTAŞ

Member : Prof. Dr. Mehmet R. TOLUN

Member : Prof. Dr. İbrahim AKMAN

APPROVAL

/ 12 /2018

Prof. Dr. Ö. Faruk ELALDI
Director, Institute of Science and Engineering



BAŞKENT ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORJİNALLİK RAPORU

Tarih: 16 / 12 / 2018

Öğrencinin Adı, Soyadı: Görkem ULUSOY

Öğrencinin Numarası: 21710542

Anabilim Dalı: Bilgisayar Mühendisliği Ana Bilim Dalı

Programı: Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı

Danışmanın Unvanı/Adı, Soyadı: Prof. Dr. A. Ziya AKTAŞ

Tez Başlığı: Analysis of Cryptocurrencies

Yukarıda başlığı belirtilen Yüksek Lisans tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 52 sayfalık kısmına ilişkin, 16 / 12/ 2018 tarihinde şahsım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı %16'dır.

Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç
3. Beş (5) kelimedenden daha az örtüşme içeren metin kısımları hariç

“Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını” inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası:.....

Onay

... / 12 / 2018

Prof. Dr. A. Ziya AKTAŞ

ACKNOWLEDGEMENTS

I would like to thank Prof. Dr. A. Ziya AKTAŞ not just for his critical remarks and valuable guidance during the whole period of my research but also for his moral support, that helped me a lot during my hard times.

Also, I must state my very deep gratitude to my wife for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without her.

Finally, I would like to thank my parents for supporting me spiritually throughout writing this thesis and my life in general.

ABSTRACT

ANALYSIS OF CRYPTOCURRENCIES

Görkem ULUSOY

Başkent University Institute of Science and Engineering

Department of Computer Engineering

During recent years Cryptocurrencies is one of the exciting discussion topics. Unfortunately, there is not yet a reliable reference on this topic.

During this study cryptocurrencies will be investigated including their production techniques and operations. Existing cryptocurrency types will be compared; their strengths and weaknesses will be discussed as well.

Security of cryptocurrencies are analyzed and their possible effects to the daily life and future of humanity will also be debated.

Thus, the major objective of this study is to provide a road map to those who are working and researching in this field.

KEY WORDS: BITCOIN, Cryptocurrency, Cryptocurrency Mining, Cryptography, ETHEREUM, Hacking

Supervisor: Prof. Dr. A. Ziya AKTAŞ Başkent University Department of Computer Engineering

ÖZ

KRİPTO PARALARIN ANALİZİ

Görkem ULUSOY

Başkent Üniversitesi Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Kripto paralar konusu son yıllarda çeşitli çevrelerde tartışma konusu yapılmaktadır. Ancak bu konuda yeterli ve geçerli bir kaynak henüz elimizde yoktur.

Bu çalışma ile kripto paraların ne oldukları, nasıl üretildikleri incelenip, işleyiş yöntemleri karşılaştırılacaktır. Bunu yaparken piyasada mevcut olan kripto para örneklerinin güçlü ve zayıf yönleri tartışılacaktır.

Çalışmada kripto paraların güvenilirlikleri ve güvenlik açıkları konusuna da ayrıca yer verilecek, kripto paraların insanlığı günümüzde ve gelecekte nasıl etkilediği ve etkileyeceği de kısaca irdelenecektir.

Böylece bu konuda çalışma ve uygulama yapacak kişilere bir yol haritası oluşturulması tezin temel amacıdır.

ANAHTAR SÖZCÜKLER: BITCOIN, ETHEREUM, Hack, Kripto Para, Kripto Para Madenciliği, Kriptografi

Danışman: Prof. Dr.A. Ziya AKTAŞ Başkent Üniversitesi, Bilgisayar Mühendisliği Bölümü.

TABLE OF CONTENTS

1	INTRODUCTION.....	1
1.1	Statement of the Problem.....	1
1.2	Literature Survey.....	1
1.3	Organization of the Study.....	5
2	CRYPTOCURRENCIES AND RELEVANT CONCEPTS.....	6
2.1	What is Cryptocurrency (CC)?.....	6
2.2	The Production and the Basic Mechanism of Cryptocurrencies.....	6
2.3	What are Miners Doing?.....	7
2.4	Current Cryptocurrencies (CCs) Examples.....	9
2.5	Properties of Cryptocurrencies.....	10
2.5.1	Revolutionary properties.....	10
2.5.2	Transactional properties.....	10
2.5.3	Monetary properties.....	13
2.6	Cryptocurrencies: Beginning of a New Economy.....	13
3	CRYPTOLOGY AND CRYPTOCURRENCIES.....	15
3.1	Cryptography for Cryptocurrency.....	15
3.2	What is MD5 and why no longer in use?.....	16
3.3	The reason of why Bitcoin uses SHA256.....	16
3.4	Cryptography of Ethereum.....	16
3.5	Role of Merkle Trees in CCs.....	17
3.5.1	Security of SHA256 and Bitcoins.....	18
3.6	Strength of cryptography and brute force.....	19
3.6.1	Brute Force to SHA 256.....	20
4	COMPARISONS FOR CONSENSUS MECHANISMS OF THE AVAILABLE CRYPTOCURRENCIES.....	23
4.1	General.....	23
4.2	What is the Proof of Work (PoW)?.....	23
4.3	What is Trustless and Distributed Consensus?.....	25
4.4	Proof of Work (PoW) and Mining.....	26
4.5	Definition of Proof of Stake (PoS).....	27
4.6	The Reason of Why Ethereum Wants to use PoS.....	28
4.6.1	How are forgers selected?.....	28
4.7	What is Ethereum Casper?.....	29
4.7.1	What can we expect from Casper?.....	34

4.7.2 Is it a safer system than PoW?	34
4.8 Other Consensus Algorithm Types.....	35
4.8.1 Delegated Proof of Stake (DPoS).....	35
4.8.2 Proof of Authority (PoA).....	35
4.8.3 Proof of Weight.....	36
4.8.4 Byzantine Fault Tolerance (BFT).....	36
4.8.5 Directed Acyclic Graphs (DAGs)	37
4.8.6 Proof-of-Importance (PoI).....	38
4.8.7 Proof of Capacity(PoC) or Proof of Space(PoSpace).....	39
5 DISCUSSIONS, SUMMARY AND CONCLUSIONS.....	40
5.1 Discussions	40
5.1.1 Comparison of consensus mechanisms against each other.....	40
5.1.2 CCs in Our Daily Lives	40
5.1.3 The risks of CCs.....	44
5.1.4 Possible weaknesses of CCs	45
5.1.5 Domestic (Turkish) Cryptocurrency attempts	46
5.2 Summary	47
5.3 Conclusions.....	47

LIST OF FIGURES AND TABLES

List of Figures

	<u>Page</u>	
Figure 2.1	Centralized vs decentralized network and nodes	6
Figure 2.2	A summary of Cryptocurrency, Blockchain operation	8
Figure 2.3	Summary of CCs main properties	12
Figure 3.1	Logic of the Markle tree	18
Figure 4.1	PoW vs PoS	24
Figure 4.2	Centralized Network vs Decentralized Network and distributed ledgers	25
Figure 4.3	Payment systems process capacity per second	31
Figure 4.4	Proof of Work(PoW) vs Proof of Stake(PoS) summary	33
Figure 5.1	Visa and CC based payment systems commissions	43

List of Tables

	<u>Page</u>	
Table 2.1	Cryptocurrencies prices and market volumes	11
Table 3.1	The crack time by key length	20
Table 5.1	Comparison of several consensus mechanism.	41

LIST OF ABBREVIATIONS

BFT	Byzantium Fault Tolerance
BTC	Bitcoin
CC	Cryptocurrency
DAG	Directed Acyclic Graph
DAO	Decentralized Autonomous Organization
DPOS	Delegated Proof of Stake
ETH	Ethereum
FBA	Federated Byzantine Agreement
FIPS	U.S. Federal Information Processing Standard
ICO	Initial Coin Distribution
MD5	Message-Digest Algorithm 5
NIST	National Institute of Standards and Technology / USA
NSA	National Security Agency
P2P	Peer to Peer
PBFT	Practical Byzantine Fault Tolerance
PoA	Proof of Authority
PoC	Proof of Capacity
Pol	Proof of Importance
PoS	Proof of Stake
PoSpace	Proof of Space
PoW	Proof of Work
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
XMR	Monero
ZEC	Zcash

1 INTRODUCTION

1.1 Statement of the Problem

Today cryptocurrencies(CCs) forms of money have turned into a global focal point which is being discussed very widely. Yet, banks, governments and various private organizations and individuals know about their value.

In the year 2018, it would be difficult to find any organization on the globe that is not dealing with cryptocurrencies.

However, individuals including investors, advisors, researchers, and developers, are having an extremely limited information and knowledge about cryptocurrencies.

In this study the following questions are tried to be answered:

- What are cryptocurrencies?
- How cryptocurrencies emerged as a side product of digital cash?
- How miners create coins and confirm transactions?
- Security of CCs.
- Mechanism types of blockchain and implementations.
- What will wait CCs and us in today and in the future?

1.2 Literature Survey

Going over the literature on the last two decades, one would summarize the results in this section.

Lamport et al.[1982] discussed a technique that reliable computer systems will handle malfunctioning components that give conflicting output to different parts of the system. A similar technique was implemented by the Byzantine generals against

the vulnerability of the army or traitors many years ago which is now named as Byzantium Fault Tolerance (BFT)¹.

Wang et al.[2004] published a technical paper. This is the first publication about MD5 collision. It meant MD5 was no longer secure algorithm.

Tao et al.[2006] wrote an article about Collision Attack on an earlier algorithm MD5. The authors stated some attacks to MD5 in their research. Their article was not directly related to Cryptocurrencies, but it was directly related to the algorithm which is later replaced by SHA.

Black et al.[2006] had also discussed weakness of MD5 algorithm.

Ciampa[2008] had discussed the cracking methods of some algorithms in his book.

Dougherty[1]^(*) wrote a paper where he discussed weaknesses of MD5 algorithm.

Nakamoto[2] published a white paper in the Bitcoin official web site. Nakamoto is unknown inventor of Bitcoin. This white paper includes some researches about Peer to Peer(P2P) cash system and its mechanisms. This white paper is very important because it was the first research paper before the cryptocurrencies born. It summarized the mechanism of Bitcoin.

Martin and Tokutami[3] studied password cracking. They examined hashed or not hashed, salted or not salted passwords. They discussed some attacking methods such as Brute force, dictionary attack and rainbow tables attack. They discussed how much time it takes to crack a password with these attacks and they explained details of these attacking methods.

Bertoni et al.[2012] called themselves as “Keccak Team” and they are the creator of the Keccak algorithm. In their article they gave technical details about Keccak and SHA. SHA-3 is a subset of the broader cryptographic primitive family Keccak

¹ Byzantium Fault Tolerance (BFT), MD5 Algorithm, Collision Attack etc. are relevant terms and they are presented in detail in the following chapters.

^(*)Web references are given using [] in the text in their order of appearance.

algorithm. Also, it is important because SHA3 is the latest member of the Secure Hash Algorithm (SHA) family of standards, released by NIST on August 5, 2015. Ethereum uses Keccak algorithm to hash.

Garay J. et al. [2014] analyzed the mechanism of the Bitcoin. They proposed another mechanism to Bitcoin which they called Byzantine agreement(BA).

According to Bonneau et al.[2015] Bitcoin is “renaissance of new ideas in designing a practical cryptocurrency”. Also, according to them this innovation touches many areas without Cryptocurrencies.

Evans[2015], describes what Bitcoin and blockchain are. He also mentioned Blockchain Management System(BMS). He mentioned Bitcoin(BTC) with different name which is XBT. Probably the reason of it, commodities' such as Gold, silver, platinum etc have ISO codes and they started with X(example: XAU/Gold, XAG/Silver, XPT/Platinum).

Heilman et al.[2015] presented an eclipse attack to Bitcoin network. They explained details of their attack and at the end they proposed countermeasures for make the eclipse attack harder.

Viglione[2015] discussed the impacts of social technologies identified with administration on cross-country contrasts in Bitcoin costs. Also, he compared approaches of different countries toward Bitcoin with graphics and some statistical methods.

Bitfury Group Ltd.[4] published a whitepaper about Proof of Work and Proof of Stakes. They are the top two mechanisms of mining and transaction confirmation methods of cryptocurrencies. The authors explained these methods one by one and later they compared these methods and gave some CC examples.

Rosic[5] defined a lot of technical terms and explained the mechanism of the blockchain system and how cryptocurrencies emerged. Moreover, he explained a few most popular cryptocurrencies. Also, one can find how crypto currencies effect our daily lives in this article.

Rosic[6] discussed Proof of Work and Proof of Stakes in his web site.

Rosic[7] had an article about benefits of the cryptocurrencies. He claimed that there are some positive aspects of cryptocurrencies.

Baird[2016] in his article mentioned a new system, named “The Swirls hashgraph consensus algorithm”. He suggested it to replicate state machines with guaranteed Byzantine fault tolerance.

Gencer et al.[2016] proposed a new design for Bitcoin that is Byzantium Fault Tolerance (BFT) and they called it Bitcoin-NG(New Generation). At the end of their works they concluded that it is possible to upgrade Bitcoin.

Barski [2017] dealt with hashing, hacking, cracking, security and cryptograph of cryptocurrencies. This presentation was at Chicago Ethereum Meetup in 2017. In his presentation he gave and explained a lot of information about security of CCs.

Sompolinsky et al.[2017] published an article about Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections (SPECTRE) which is another sub branch of DAG like Tangle. They discussed a new framework system which can satisfies general requirements of cryptocurrency.

Gilad et al.[2017] introduced a new Cryptocurrency that is called Algorand in their article. In this article they discussed their technique which is Byzantium Agreements consensus technique. They thought Algorand uses first of its kind of a new technology that fulfills the promise of blockchain.

NEM Foundation[2018] published a technical whitepaper on NEM giving technical details about NEM also they developed Proof of Importance(PoI) method and they implemented it in NEM².

Popov[2018] discussed about the other mechanism of a cryptocurrency named Tangle. Tangle is the sub branch of Directed Acyclic Graphs(DAG) and the most popular implementation is IOTA. According to him the Tangle is next evolutionary step of the blockchain technology. Because usual blockchain which uses the Proof

² NEM (New Economy Movement) is one of the most popular cryptocurrency.

of Work mechanism is getting slower as it grows as well as the transaction fees are increasing. On the other hand, Tangle mechanism is getting faster as it grows.

Larimer[2018] published a white paper on EOS³ giving its technical details. He developed Delegated Proof of Stakes method and he implemented it in EOS.

Magas[8] published an article about Ethereum's new Casper protocol update and what will change in the mining industry with this update.

Magas[9] published another article. In this article she compared traditional payments methods such as Visa, Mastercard with CCs and discussed possibility of traditional payments methods replaceable with CCs.

1.3 Organization of the Study

The thesis starts with a brief introduction and literature reviews. Second chapter defines what Cryptocurrencies and their basic mechanisms are. Also, how they are produced and the logic behind the production process named mining are discussed. Next chapter, namely Chapter 3, gives some information about the strength of Cryptocurrencies and their most common algorithms. Also, theoretically investigate the strength of these algorithms to well-known attacks. Fourth Chapter is about the definition of the different consensus mechanisms of cryptocurrencies. Their advantages and disadvantages are also discussed. In the last Chapter under Discussion part needs and the risks of Cryptocurrencies are discussed. Also, some examples about domestic Cryptocurrency projects are given. Then a brief Summary and Conclusions are given at the end of the chapter.

³ EOS is one of the most popular cryptocurrency.

2 CRYPTOCURRENCIES AND RELEVANT CONCEPTS

2.1 What is Cryptocurrency (CC)?

One may refer Rosic [5] to answer the question of what cryptocurrency is? Take the money in a bank account. It is just a piece of data in a database that can be changed under certain conditions. Thus, money is a verified entry in a database of accounts, balances and transactions. It may be said that cryptocurrency appeared as a side product of trial on Peer to Peer (P2P) money transaction system which is later named as Bitcoin[2]. S. Nakamoto did not intend to invent a currency while working on Bitcoin in late 2008. He was only trying to invent decentralized digital cash system which does not require to build a server room as a centralized entity. It is similar to a Peer-to-Peer (P2P) network for file sharing. Centralized and decentralized network differences are in Figure 2.1[6].



Figure 2.1 Centralized vs decentralized networks and nodes

This idea created cryptocurrency as a digital cash. Nakamoto proved to achieve a consensus without a central authority or central server system. Cryptocurrencies are a part of solution.

2.2 The Production and the Basic Mechanism of Cryptocurrencies

As noted by Rosic[5], cryptocurrencies are produced by miners. But how miners create coins and confirm transactions need to explain. Cryptocurrency such as Bitcoin comprises of a network of associates. Each associate has a record of the entire history all things considered and in this manner the equalization of each record is realized. A transaction is a record that says, “Joe gives some BTC to Jane“ and is signed by Joe’s private key. It is basic public key cryptography, nothing special at all. After signed, transaction is communicated in the network, sent from

one companion to each other associates. Figure 2.2 summarizes the process given by Rosic[5].

The transaction is communicated very quickly by the entire network. Confirmation is a basic idea in cryptocurrencies. For whatever length of time that a transaction is unverified, it is pending and can be manufactured. At the point when a transaction is affirmed, it is an unchangeable reality. It is never again forgeable, it cannot be switched. It is a piece of an unchanging record of chronicled transactions which is called blockchain⁴.

Just miners can affirm transactions. This is miners' role in a cryptocurrency-network also known as blockchain. They take transactions, sign them as substantial and broadcast them in the network. After a transaction is affirmed by a miner, each peer needs to add it to its database. It has progressed toward becoming a piece of the blockchain.

For this activity, the miners get awarded with a token of the cryptocurrency and this is named block rewards. Thus, the miner's action is the absolute most vital piece of cryptocurrency-system.

2.3 What are Miners Doing?

Essentially everybody can be a miner. Suppose somebody creates a lot of peers and produces fake transactions. The system would then fail immediately. Then, Nakamoto decided that the miners need to contribute some work.

One does not have to understand insights about SHA 256 Algorithm. It is just an imperative that one has to understand the premise of a cryptologic riddle the miners contend to explain.

Bitcoins or some of other altcoins must be produced if miners solve a cryptographic riddle. This is part of the consensus no peer in the network can break.

⁴ Blockchain constantly creating summary of records, called blocks, which are associated and tied down using cryptography

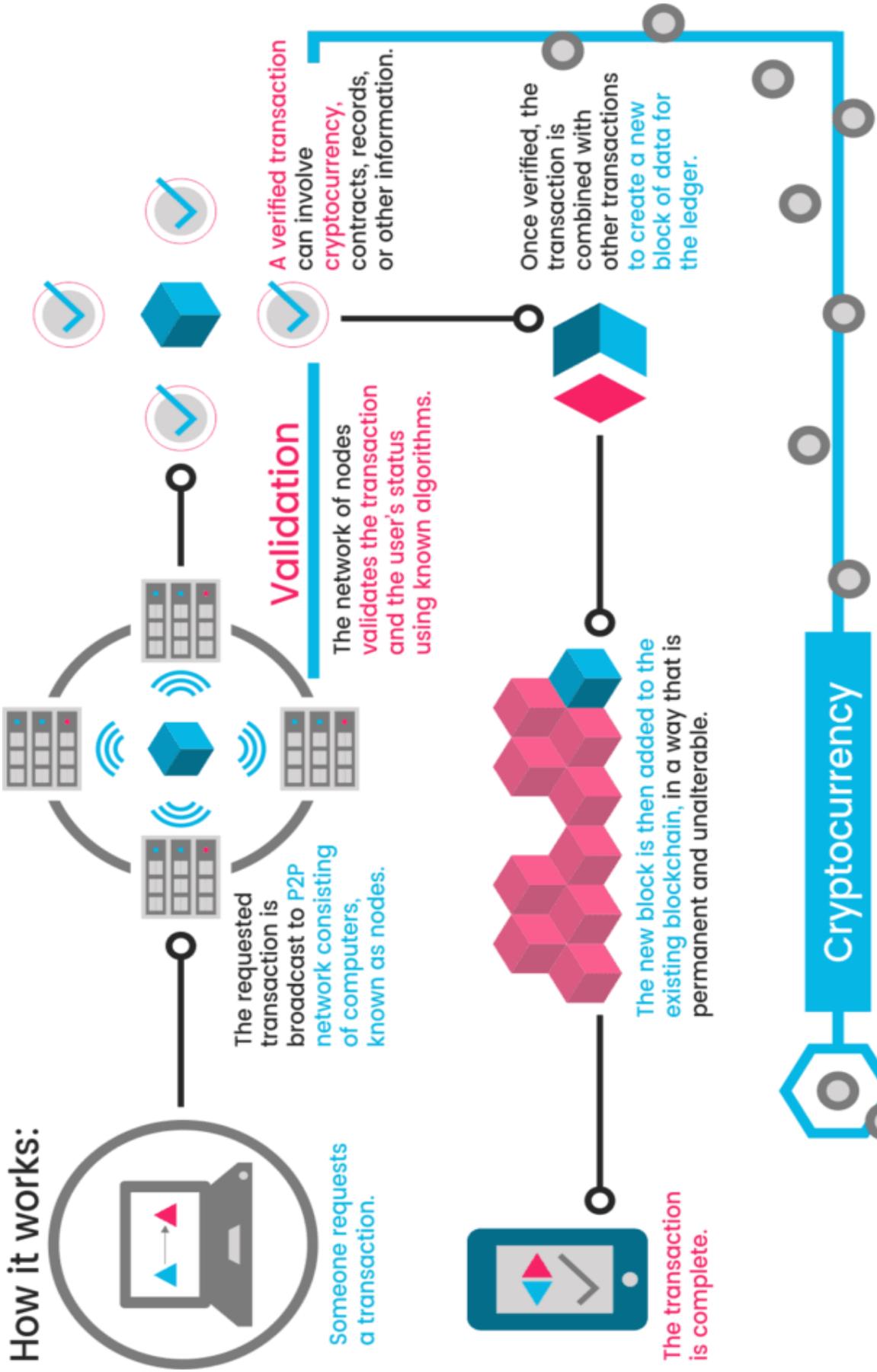


Figure 2.2 A Summary of Cryptocurrency and Blockchain operation

One then needs some hardware to solve these cryptographic puzzles. At the beginning CPUs⁵ could do it. But over time, as the transaction traffic increases CPUs cannot handle all the transactions. Miners discovered GPUs⁶ could do 10-15 times better job than the CPUs. Then, some companies invented ASIC⁷ Machines to solve these puzzles. ASIC is a special CPU, it is invented only to solve a specific algorithm. They cannot do anything without it. But now, some of the cryptocurrency algorithms could solve ASIC and some of them can solve only GPUs and CPUs. One may name Monero (XMR) as an interesting example. One of the largest ASIC company named Bitmain invented an ASIC machine, to mine Monero algorithm named Cryptonight. One should note that ASICs cause a centralized network. Then, some big companies collect most of the ASICs in the world. Centralized network means it could be manipulated: thus, it is not so secure. Then Monero's developer updated their algorithm to CryptonightV7 on 5th April 2018 to resist ASICs. Now ASICs cannot mine Monero. Cryptonight ASICs became totally useless; because the algorithm has changed. Only CPUs and GPUs can solve the algorithm, so it is more secure and more decentralized. Everybody can solve this algorithm even at their home with their own computers.

On 20th October 2018 Monero updated its algorithm again and new algorithm is named CryptonightV8. The Monero's developers promised to update the algorithm every 6 months so ASIC companies can create new ASIC machine but after a few months it becomes useless.

2.4 Current Cryptocurrencies (CCs) Examples

Nowadays there are almost over 2081 cryptocurrency examples circulating in the crypto markets. Probably there are lot more CC's that do not circulate in the markets yet. Table 2.1 lists the most popular 30 CCs in the CC markets with their update (18.11.2018 16:30 (GMT +3) price and volume data [10].

As noted above, there are over 2081 CCs available in the CC markets. Some of their supplies still are produced by miners. Some of them already produced maximum of supply and they are just circulating. Most famous CC example is

⁵ CPU: Central Processing Unit

⁶ GPU: Graphical Processing Unit

⁷ ASIC: Application Specific Integrated Circuit

Bitcoin(BTC). Today (November 2018) there are 17,382,412 BTC supply is circulating in the world. The rest of them are still producing. Maximum 21 Million BTC can be produced. Another most popular CC is Ethereum(ETH). Now there are over 103 million ETH supply that is circulating, and its production is still in progress. From another category IOTA is another most popular CC. IOTA is different from BTC or ETH. Because it is not produced by miners. It's all supply was just created at the beginning by its developer and now it is just circulating and trading. Also, IOTA does not have transaction fee and it has a vision: IOTA wants to become the main currency at the e-commerce.

2.5 Properties of Cryptocurrencies

2.5.1 Revolutionary properties

Bitcoin, as a decentralized network of peers which keep an agreement about records and parities, is more a cash than the numbers one find in his/her financial balance. What are these numbers more than sections in a database which can be changed by individuals nobody sees and by rules nobody knows?

Actually, CCs are sections about token in decentralized consensus databases. They are called cryptocurrencies in light of the fact that the agreement

keeping process is anchored by solid cryptography⁸. Cryptocurrencies are based on cryptography that is, they are not based on any people or simply trust but rather by math.

2.5.2 Transactional properties

Five of transactional properties of CCs are summarized below [5]:

a) **Irreversible:** After affirmation, a transaction cannot be moved back. By no one. Not the sender, not the bank, not Nakamoto, not the miner. No one. If one sends cash, he/she send it. Period. Nobody can help one after his/her transaction. If one sent his/her assets to a fraud or if a programmer stole them from your PC, one cannot move back the procedure. There is not any security measure. .

⁸ Cryptography is the practice and study of method for secure communication in the asset of third parties called hostiles.

Table 2.1 Cryptocurrencies prices and market volumes

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d	
1	 Bitcoin	BTC	\$97.382.937.036	\$5.602,38	17.382.412	\$4.074.529.944	0,05%	1,01%	-12,31%	...
2	 XRP	XRP	\$20.540.673.328	\$0,510052	40.271.748.947 *	\$857.839.999	0,13%	6,49%	1,44%	...
3	 Ethereum	ETH	\$18.177.085.172	\$176,00	103.276.218	\$1.772.678.042	0,13%	1,00%	-16,61%	...
4	 Bitcoin Cash	BCH	\$6.690.397.263	\$383,08	17.464.713	\$280.946.783	0,23%	-1,60%	-28,87%	...
5	 Stellar	XLM	\$4.839.570.542	\$0,251218	19.264.393.065 *	\$100.028.521	-0,07%	3,92%	-6,61%	...
6	 EOS	EOS	\$4.144.915.386	\$4,57	906.245.118 *	\$725.291.759	-0,42%	1,01%	-14,61%	...
7	 Litecoin	LTC	\$2.514.658.713	\$42,47	59.211.413	\$324.087.815	0,44%	1,34%	-17,29%	...
8	 Tether	USDT	\$1.740.070.463	\$0,990691	1.756.421.736 *	\$2.897.907.715	0,07%	0,23%	-0,51%	...
9	 Cardano	ADA	\$1.598.146.652	\$0,061640	25.927.070.538 *	\$15.951.759	-0,21%	1,79%	-18,87%	...
10	 Monero	XMR	\$1.481.234.631	\$89,34	16.579.174	\$26.035.275	0,15%	4,16%	-13,81%	...
11	 TRON	TRX	\$1.236.330.478	\$0,018804	65.748.111.645 *	\$70.562.596	-0,03%	0,53%	-17,70%	...
12	 IOTA	MIOTA	\$1.148.840.823	\$0,413322	2.779.530.283 *	\$5.958.875	0,06%	0,10%	-14,08%	...
13	 Dash	DASH	\$1.137.787.328	\$134,63	8.450.928	\$132.600.829	0,12%	1,47%	-16,05%	...
14	 Binance Coin	BNB	\$1.032.338.688	\$7,89	130.799.315 *	\$13.930.271	-0,14%	3,01%	-16,51%	...
15	 NEM	XEM	\$833.861.649	\$0,092651	8.999.999.999 *	\$7.956.528	-0,19%	-0,21%	-0,45%	...
16	 NEO	NEO	\$809.849.967	\$12,46	65.000.000 *	\$156.636.854	-0,06%	0,02%	-21,30%	...
17	 Ethereum Classic	ETC	\$798.349.419	\$7,52	106.121.991	\$130.208.952	-0,06%	1,26%	-19,29%	...
18	 Tezos	XTZ	\$667.512.932	\$1,10	607.489.041 *	\$1.711.407	-0,06%	0,74%	-16,28%	...
19	 Zcash	ZEC	\$580.936.959	\$110,41	5.261.769	\$182.164.420	0,10%	3,51%	-15,37%	...
20	 Bitcoin Gold	BTG	\$474.695.982	\$27,36	17.349.674	\$5.271.363	0,56%	3,34%	-8,67%	...
21	 VeChain	VET	\$423.173.094	\$0,007631	55.454.734.800 *	\$9.287.155	0,20%	0,56%	-25,12%	...
22	 Maker	MKR	\$419.695.892	\$576,33	728.228 *	\$509.698	0,09%	0,40%	-17,43%	...
23	 Ontology	ONT	\$389.451.294	\$1,34	291.115.881 *	\$17.961.222	0,49%	0,80%	-17,79%	...
24	 OmiseGO	OMG	\$383.870.990	\$2,74	140.245.398 *	\$27.876.217	0,22%	1,30%	-15,95%	...
25	 Dogecoin	DOGE	\$304.280.573	\$0,002600	117.029.266.327	\$13.220.935	0,38%	-0,29%	-18,47%	...
26	 Ox	ZRX	\$296.658.575	\$0,543208	546.123.352 *	\$9.643.280	0,12%	-2,91%	-22,65%	...
27	 Decred	DCR	\$296.137.336	\$33,52	8.835.260	\$1.715.961	0,12%	2,23%	-16,08%	...
28	 Qtum	QTUM	\$274.861.247	\$3,09	89.044.664 *	\$97.385.297	0,02%	1,29%	-19,86%	...
29	 Basic Attenti...	BAT	\$253.203.848	\$0,214433	1.180.808.540 *	\$5.808.978	-0,76%	0,23%	-16,78%	...
30	 Lisk	LSK	\$244.632.731	\$2,18	112.278.435 *	\$4.659.837	0,52%	1,59%	-20,39%	...

b) **Pseudonymous**⁹: Neither transactions nor accounts are related with identities. Everybody just has a Wallet ID.

c) **Quick and global**: Transactions are communicated almost immediately in the network and are affirmed in several minutes perhaps in a moment or two. Since they occur in a worldwide network of PCs, they are totally unconcerned of one's physical area. It doesn't make a difference if you send Bitcoin to anybody in the world.

d) **Secure**: CC balances are secured by an open key cryptography system. Just the owner of the private key can send cryptocurrency. Cryptography and large numbers make it hypothetically impossible to crack this design.

e) **Permissionless**: One does not need to demand that anybody utilize cryptocurrency. It is only a product that everyone can download for free. After one installed it, one can receive and send Bitcoins or any other cryptocurrencies. Nobody can anticipate. There is no guard. These properties are summarized in Figure 2.3 [5].

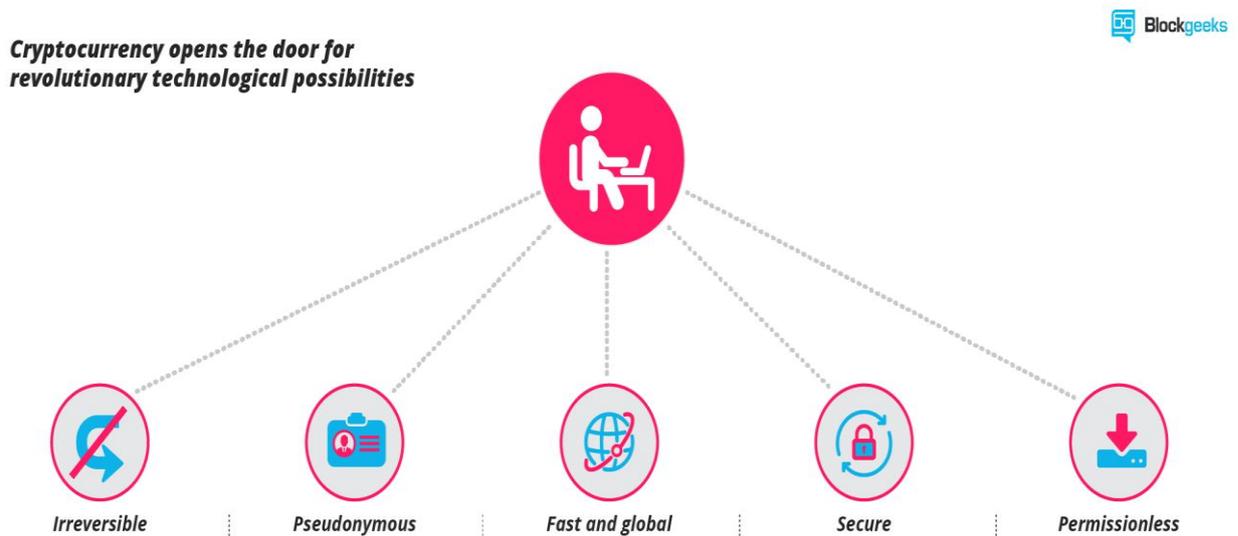


Figure 2.3 Summary of CCs' main properties

⁹ Pseudonymous: is a nickname who don't have to share his/her real identity.

2.5.3 Monetary properties

There are two basic monetary properties [5]:

a) **Limited supply:** Most CCs constrain the supply of the coins. For example in BTC, the supply to this date might change as indicated by number of the miners, transactions and intensity of the new equipment. All CCs control the supply of the coins by a calendar written in their code.

b) **No debt but bearer:** The Fiat-Money¹⁰ on one's financial balance is made by liability, and the numbers, one sees on his/her record speak to only liabilities. It is an arrangement of IOU¹¹. Cryptocurrencies will not speak to obligations. They simply speak to themselves. They are cash as hard as gold coins.

In order to comprehend the revolutionary effect of cryptocurrencies one has to think about both of these properties. Bitcoin as a permissionless, irreversible and pseudonymous methods for installment is an attack on the control of banks and governments over the money related transactions of their natives. One cannot obstruct somebody to use cryptocurrency or one cannot boycott somebody to get a payment, one cannot cancel or roll back a transaction[Viglione, 2015].

As cash with a restricted, controlled supply that is not alterable by an administration, a bank or some other central organization, cryptocurrencies assault the extent of the monetary approach.

2.6 Cryptocurrencies: Beginning of a New Economy

Rosic has noted that [5] for the most part because of its revolutionary properties cryptocurrencies have turned into a win their innovator, S. Nakamoto, did not expect to hope for it. Cryptocurrencies are kind of a digital gold. They are secure from any political intervention[Viglione, 2015].

¹⁰ Fiat money is currency that an administration has pronounced to be legitimate delicate, however it isn't upheld by a physical product. The estimation of fiat cash is gotten from the connection among free market activity as opposed to the estimation of the material that the cash is made of. Verifiably, most monetary forms depended on physical products, for example, gold or silver, yet fiat cash depends entirely on the confidence and credit of the economy.

¹¹ An IOU (abbreviation from the expression "I owe you") is generally a casual report recognizing obligation. An IOU contrasts from a promissory note in that an IOU is certifiably not a debatable instrument and does not determine reimbursement terms, for example, the season of reimbursement.

While cryptocurrencies are more used for payments, they are used as a method for speculation on the markets. CCs brought forth an extraordinarily powerful, quickly developing business sector for financial specialists and investors even speculators. Exchanges such as Bittrex, Binance, Btctürk etc. enable the trade of a lot of CCs.

In the meantime, the praxis of Initial Coin Distribution (ICO¹²), for the most part encouraged by Ethereum's smart contracts to gather a huge number of dollars. The account of "the DAO¹³ " has in excess of 150 million US dollars.

In this rich ecosystem of CCs and tokens, one experiences excessive volatility. It is common that a CC gains 20% a day or sometimes 200%. just to lose the same rate at the following day. If one is lucky, his/her coins can be valued thousands of times in a short time. So, you can be rich in shortcut or poor!

We already presented some of the most popular cryptocurrencies of today as given in Table 2.1[10] but some new born cryptocurrencies may make you rich in a shorter time than the well knowns.

¹²ICO: It can be considered as an alternative mass fund that emerged as a different from the traditional financial system. ICOs are usually an event that lasts a week or more. and people are able to get new coins on the market in exchange for already known crypto coins (Bitcoin, Ethereum etc.).

¹³DAO (Decentralized Autonomous Organization): It is an enterprise managed through rules coded as computer programs called smart conventions. DAO's financial transaction registration and program rules are kept on a block chain. There are several examples of this business model. The precise legal situation of such commercial organizations is unclear.

3 CRYPTOLOGY AND CRYPTOCURRENCIES

3.1 Cryptography for Cryptocurrency

a) Definition of cryptography

Cryptography is a technique for sending mystery messages. One individual encodes a message utilizing a type of key and algorithm and just the other individual at the other end can decode it if he/she knows the encryption key.

b) What in the world does it have to do with cryptocurrency

Most cryptocurrencies do not include the sending of any mystery messages. All their data including transactions in cryptocurrencies like Bitcoin is open and subsequently there is no compelling reason to send "concealed messages" between parties. Nonetheless, some newer CCs like XMR or ZEC actually try to dissemble details of transaction. They use cryptography to hide information.

c) Purpose of cryptography with cryptocurrency

According to Barski[2017], a portion of the devices that were created for customary cryptography end up having other helpful capacities. Two most critical of these are hashing and digital signatures. In this way, despite the fact that neither of these include the sending of covered messages they are as yet thought to be types of cryptography. Hashing is utilized by cryptocurrencies to effectively confirm the uprightness of information. It is a strategy for taking a lot of information and systematically speaking to it as a short number that is hard to recreate. Hashing is utilized intensely to keep up the structure of blockchain information, which holds individuals' record balances. Likewise, it is utilized to encode individuals' record addresses and as a feature of the way toward encoding transactions between records. At long last, hashing is utilized to create math perplexes that make "block mining" conceivable, a key element in numerous cryptocurrencies. Hashing makes substantial utilization of block figures, an innovation that was initially utilized for customary cryptography.

Digital signatures enable a man to take a touch of mystery data they possess and to demonstrate they claim that data, without uncovering it. Cryptocurrencies enable

clients to sign monetary transactions with these digital signatures to demonstrate to the network that the proprietor of a record holding cash consented to a transaction to spend that cash. Digital signatures, as utilized by cryptocurrencies, advanced from "Elliptic Curve Cryptography" which again is an innovation that initially was utilized to make "covered messages" as a major aspect of conventional cryptography.

3.2 What is MD5 and why no longer in use?

MD5 algorithm was designed in 1991 and published in 1992. In 1993, first weaknesses were detected, then greater weaknesses in 1996. It took 8 years for these weaknesses to become into real collisions by Wang[2004]. Seven years later, in 2011, one can create MD5 collisions at will and much more efficiently than with Wang[2004]'s original method, but preimage and second-preimage resistances of MD5 are still as good as ever.

3.3 The reason of why Bitcoin uses SHA256

As noted by Wang[2004], Black[2006], Daugherty[1], Ciampa[2009] and Tao[2013], MD5 is not a secure algorithm since 2000s. So, it replaced by SHA.

Bitcoin utilizes a hashing algorithm named SHA256 (likewise named SHA2– 256) for arranging block information, for the block mining algorithm, and as a feature of the procedure for encoding/decoding transactions and client accounts (client accounts additionally utilize another hashing algorithm called RIPEMD-160). Bitcoin utilizes the ECDSA (elliptic curve algorithm) for digital signatures.

3.4 Cryptography of Ethereum

One may refer Barski et al. [2017] to understand the security of Ethereum. Bertoni[2012] also explained the logic of SHA 3 algorithm.

Ethereum, instead of SHA2, uses another hash algorithm that is SHA3 to arrange block data, as part of the mining algorithm, and for encoding transactions and user accounts, more specifically, a variant of SHA3 called SHA3-Keccak is used. ETH still uses ECDSA for digital signatures, as with Bitcoin.

If one sends cash to an Ethereum address that does not exist, one loses it forever. The reason is briefly explained below [Barski, 2017]:

Cryptocurrencies utilize hashing as a feature of the way toward producing account addresses. On account of ETH, these record addresses are 40 character long, and hypothetically any 40-character string could be a legitimate ETH wallet address, contingent upon the consequence of the hashing step. The Ethereum network has no real method for knowing whether a specific address was mistyped, and consequently it will give you a chance to send cash to a nonsense account address. For example, "0x00" if one asks it to. Theoretically this is a correct Ethereum address format, but it does not mean it belongs to someone. In the event that one does this, his/her cash basically falls into a "black hole" and no one will ever have the be able to rescue it again.

Gratefully, this issue has been lessened to some degree by means of another component named "mixed-case checksum address encoding" that will enable projects to create a mistake for most types of mistyped address.

3.5 Role of Merkle Trees in CCs

One may refer Barski[2017] to see importance of Merkle trees in cryptocurrencies.

Merkle trees are a strategy including hashing that enables one to demonstrate to someone else that a large volume of document contains a little bit of information, without the other individual requiring a full duplicate of this information. Figure 3.1 shows the logic of the Markle tree by leaf to root[19].

One should keep in mind that Merkle trees enable cryptocurrencies to run effectively on obliged equipment gadgets like mobile phones and permit smart contracts (some portion of the Ethereum system) to associate with vast information structures. Since both mobile phones and smart contracts are probably going to assume a major job later on, we will probably hear much more about Merkle trees in the years to come.

The only known way to understand the security of a cryptographic algorithm is to leave it under close examination of hundreds of cryptographers for several years and see what comes out. So, the right perspective here is historical.

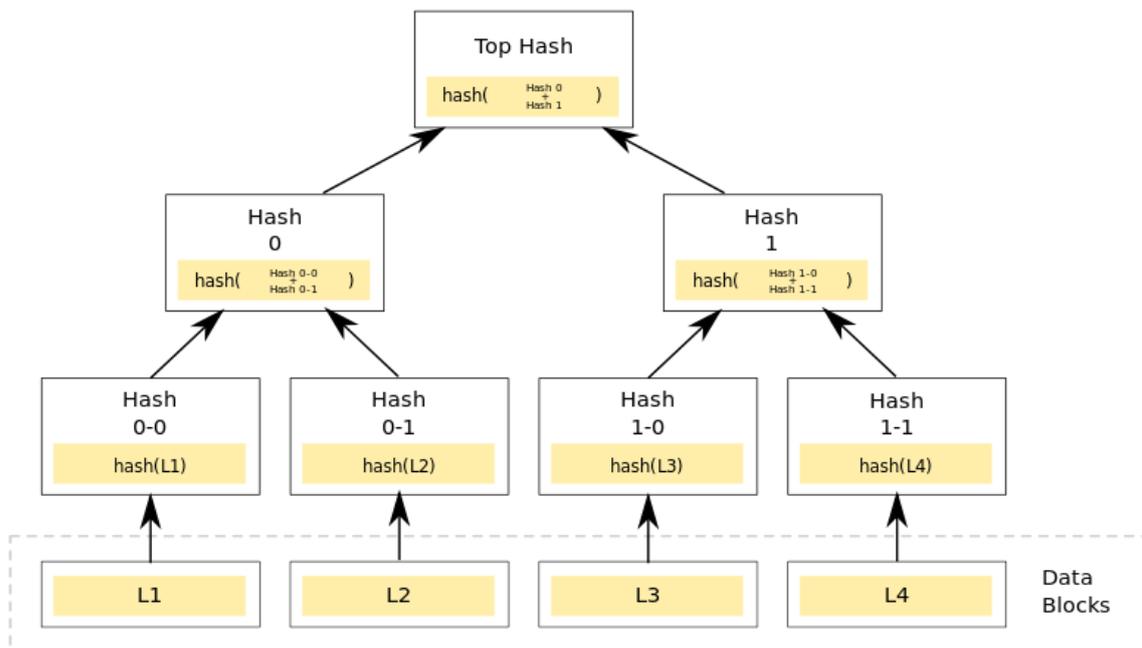


Figure 3.1: Logic of the Markle tree

3.5.1 Security of SHA256 and Bitcoins

SHA-256 was first published in 2001; ten years later in 2011, we still have no clue whatever on the slightest hint of a weakness. This would be suggestive that SHA-256 is indeed robust, and collisions for SHA-256 are not just right around the corner. It seems that collisions are not a real danger for Bitcoin -- it rather relies on preimage resistance, for which not only SHA-256 is rock solid, but even MD5 would still be reliable.

However, it is not so reliable to make statistics on a single measure. In 2007, it was estimated that there was a relatively high risk that the attacks on MD5 could be transported to SHA-1 and then SHA-256/512 -- this prompted NIST(National Institute of Standards and Technology) to organize the SHA-3 competition. It turned out that attacks on SHA-1 have somehow stopped progressing, and there is no attack on SHA-2. Whether this is because SHA-2 is really strong, or because all the cryptographers are busy trying to break the SHA-3 candidates, is not known.

3.6 Strength of cryptography and brute force

“Strong cryptography” or “cryptographically strong” are general terms connected to cryptographic systems or parts that are considered very impervious to cryptanalysis.

The expression "cryptographically strong" is regularly used to depict an encryption algorithm, and suggests, in contrast with some other algorithm, more prominent protection from attacks. In any case, it can likewise be utilized to depict hashing and exceptional identifier and filename creation algorithms.

The Secure Hash Algorithms are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST), as follows:

SHA-0 is a retronym¹⁴ “applied to the original version of the 160-bit hash function published in the year 1993 and named ‘SHA’. It was withdrawn shortly after publication due to a secret "significant flaw" and replaced by the a little revised version SHA-1.” [Tao et al., 2013]

SHA-1 “is a 160-bit hash function which similar the former MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic weaknesses were spotted in SHA-1, and the standard was no longer approved for most cryptographic uses after 2010.”

SHA-2 “is a family of two similar hash functions, with different block sizes are, known as SHA-256 and SHA-512. They differ in the word size: SHA-256 uses 32-bit words and SHA-512 uses 64-bit words. There are also truncated versions of each standard, known as SHA-224, SHA-384, SHA-512/224 and SHA-512/256. These were also designed by the NSA.” [Tao et al., 2013 and Bertoni et al., 2012]

SHA-3[Bertoni et al., 2012] “is a hash function formerly called Keccak, chosen in the year 2012 after a public contest between non-NSA designers. It supports the same hash lengths as SHA-2, and its internal design differs remarkably from the other members of the SHA family.”

¹⁴ **Retronym:** A retronym is a more current name for a current thing that separates the first frame or form from a later one. It is in this manner a word made to separate between two kinds, while already (before there were two composes) no elucidation was required.

The related standards are FIPS PUB 180 (original SHA), FIPS PUB 180-1 (SHA-1), FIPS PUB 180-2 (SHA-1, SHA-256, SHA-384, and SHA-512). NIST has updated Draft FIPS Publication 202, SHA-3 Standard separate from the Secure Hash Standard (SHS).

3.6.1 Brute Force to SHA 256

Referring to Martin and Tokutami[3], it may be stated that breaking the hash algorithm is identical to spotting a collision in the hash algorithm. That implies that one does not have to discover the secret word itself; one simply need to discover a yield of the hash work that is equivalent to the hash of a substantial secret word. Finding an impact utilizing a birthday attack takes $O(2^{n/2})$ time, where n is the yield length of the hash function in bits. Table 3.1 shows the crack time by key length.

“SHA-2 has a yield size of 512 bits, so spotting a collision would take $O(2^{256})$ time. There are no rationale attacks given on the algorithm itself (presently none are known for the SHA-2 hash family).”

Table 3.1 Crack time by key length

Key Size	Time to Crack (theoretically, it depends on the power of the processor)
56-bit	399 Seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

This is the thing that it takes to break the algorithm. In order to understand for what 2^{256} means: Currently it is believed that the number of atoms in the universe is roughly 10^{80} which is more or less equal 2^{266} . Assuming 32-byte input (which is reasonable for this scenario – 20 bytes salt¹⁵ + 12 bytes password = 32byte) Let's

¹⁵**Salts:** In cryptography, a salt is irregular information that is utilized as an extra contribution to a restricted capacity that "hashes" information, a secret phrase or passphrase. Salts are firmly

assume that one computer takes $\sim 0,22s$ ($\sim 2^{-2}s$) for 65536 ($=2^{16}$) computations. So, 2^{256} computations would be done in $2^{240} * 2^{16}$ computations which would theoretically take: $2^{240} * 2^{-2} = 2^{238} \sim 10^{72}$ seconds $\sim 3,17 * 10^{64}$ years

It implies a large number of years. Also, it doesn't improve with the quickest equipment on the planet figuring a large number of hashes in parallel. No humanity innovation even quantum PCs will have the capacity to split this number into something worthy .

So, brute-forcing to SHA-256 is totally useless. The next question is what about dictionary-words attacks. For the purpose of revoke weak passwords, rainbow tables¹⁶ were used usually. A rainbow table is usually just a data table which includes precomputed hash values. The main idea is if one were able to precompute and store every possible hash along with its input, then it would take one $O(1)$ complexity to look up a given hash and revoke a legitimate preimage for it. This is only possible in theory since there is no storage device that could store such enormous amounts of data. "This quandary is known as memory-time tradeoff."

"Salts are a countermeasure to make such rainbow tables possible. In order to discourage attackers from precomputing a table for a specific salt it is recommended to apply per-user salt values. Since users do not use safe or completely random passwords, it is still astonishing how successful one can get if the salt is known and one just iterate over a large dictionary of common passwords in a simple trial and error scheme."

Salts are used to safeguard passwords. Historically a password was stored in plaintext on a system, but over time additional safeguards developed to protect a user's password against being read from the system. A salt is one of those methods.

identified with the idea of nonce. The essential capacity of salts is to protect against word reference assaults or against its hashed comparable, a pre-figured rainbow table attack.

¹⁶**Rainbow Tables:** a string made up of a string and its hash match. To do a mixed-cracking operation, the string to be tested is normally weighed, the hashes are compared, and the experiment can continue with the next test string. This method is inefficient when processing time is required.

Typical password choices are generally of low entropy, whereas completely random values would contain a maximum of entropy.

The low entropy of average passwords makes it conceivable that there is a moderately high possibility of one of one's clients utilizing a secret word from a generally little database of normal passwords. In the event that one google for them, one will wind up discovering downpour joins for such secret phrase databases, frequently in the gigabyte measure classification. Being effective with such an instrument is for the most part in the scope of minutes to days if the assailant is not confined in any capacity. This is the reason by and large simply hashing and salting is not sufficient, you have to set up other well-being systems also. One should utilize a misleadingly backed off entropy-inducing technique, for example, PBKDF2(Password-Based Key Derivation Function 2) depicted in PKCS#5(Public-Key Cryptography Standards 5). One ought to apply a sitting tight period for a given client before they may retry entering their secret word. A decent plan is to begin with 0.5s and after that multiplying that time for each fizzled endeavor. As a rule, clients do not see this and do not flop significantly more regularly than three times by and large. In any case, it will astoundingly back off any vindictive untouchable attempting to attack your application.

4 COMPARISONS FOR CONSENSUS MECHANISMS OF THE AVAILABLE CRYPTOCURRENCIES

4.1 General

In this chapter the main differences between Proof of Work(PoW), Proof of Stake(PoS) and the other methods such as Proof of Capacity, Proof of Authority and some others are explained.

Meaning of mining, or the process of producing new CCs that are released through the network. Moreover, what will change concerning mining methods if the Ethereum community chooses to pass from “work(PoW)” to “stake(PoS)”? Figure 4.1[6] explains the main differences of the PoW and PoS.

4.2 What is the Proof of Work (PoW)?

One may refer Nakamoto [2], Bitfury Group Limited [4] and Rosic [6] for defining Proof of Work. PoW is the most common blockchain consensus algorithm. Confirmation of work is a convention that has the fundamental objective of preventing digital assaults, for example, a distributed denial-of-service(DDoS) attack which has the reason for debilitating the assets of a PC system by sending various phony solicitations.

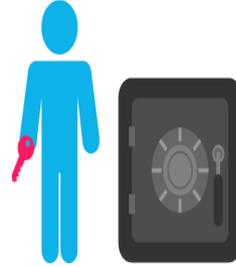
The Proof of work(PoW) idea existed even before Bitcoin; however, Nakamoto connected this method to his computerized currency upsetting the manner in which customary transactions are set.

Today, Proof of Work may be the greatest idea behind the Nakamoto’s Bitcoin white paper[2] – published back in 2008 because it allows trustless and distributed consensus. The most popular PoW implementations are Bitcoin, Ethereum, Litecoin, Dogecoin, and many others. The advantage of PoW is it is working perfectly; but disadvantages are it is working slow and killing the planet because it uses too much electricity!!

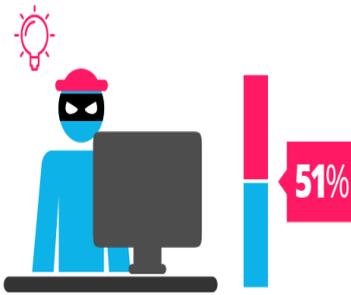
Proof of Work vs Proof of Stake



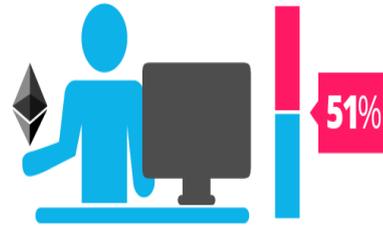
proof of work is a requirement to define an expensive computer calculation, also called mining



Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.



The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem



Proof of Stake currencies can be several thousand times more cost effective.

Figure 4.1 PoW vs PoS

4.3 What is Trustless and Distributed Consensus?

A trustless and distributed consensus system implies that if one need to send as well as get cash from somebody one does not have to trust in outsider administrations. Figure 4.2 explains the distributed ledgers[6].

When one utilizes conventional techniques for installment, one has to trust in an outsider to set his/her transaction (e.g. Visa, Mastercard).

The basic model to clarify this conduct more readily is the following: if Jane sent Morgan \$500, the trusted third-party service would debit Jane’s account and credit Morgan’s one, so unfortunately, they both have to trust this third-party that it is to going do the right thing[6].

“With BTC and a couple of other cryptocurrencies, everybody has a duplicate of the ledger (blockchain), so nobody hosts to trust in third gatherings, since anybody can specifically confirm the data composed.”[6]

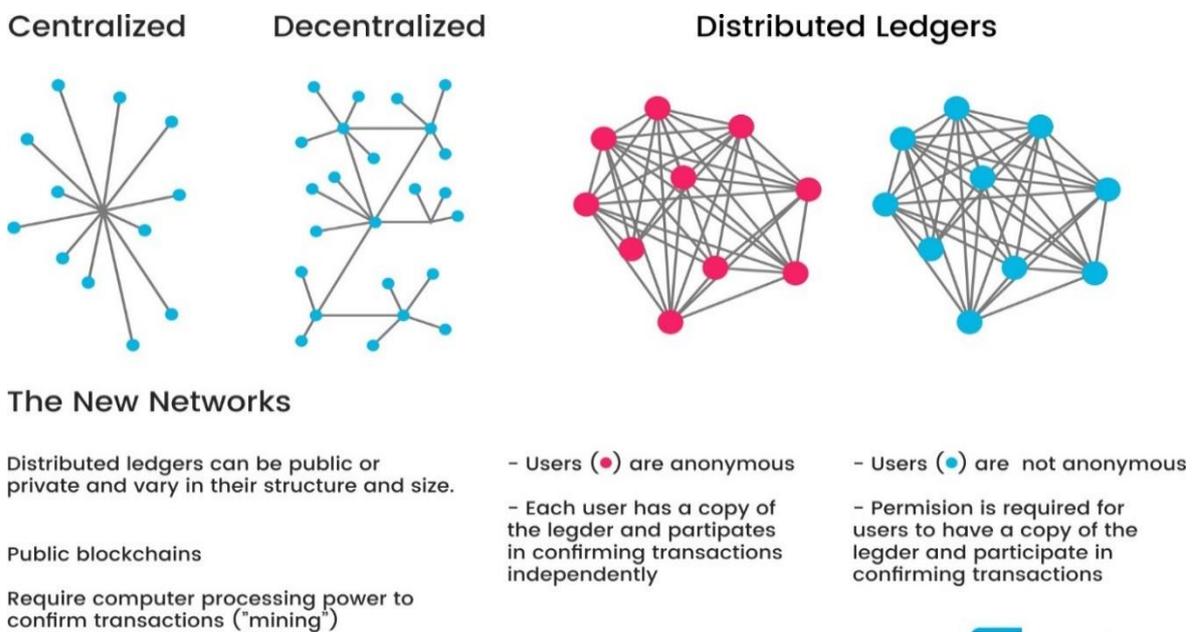


Figure 4.2 Centralized Network vs Decentralized Network and distributed ledgers

4.4 Proof of Work (PoW) and Mining

Going further, proof of work is a prerequisite to characterize a costly PC estimation, additionally called mining, that should be performed keeping in mind the end goal to make another gathering of trustless transactions (the alleged block) on a distributed ledger named blockchain (Nakamoto[2], Bitfury Group Limited[4] and Rosic[6]).

Mining operates with two purposes:

- a) To check the authenticity of a transaction, or prevent double spending;
- b) To produce new coins/tokens by rewarding miners named block reward for executing the task a.

When one wants to make a transaction, this is what happens behind the stage:

- Transactions are packaged together into a block; Miners confirm that transactions inside each block are legitimate;
- Miners confirm that transactions for every legitimate blocks;
- A reward is given to the main digger who takes care of every block issue;
- Confirmed transactions are kept in the public blockchain.

“This ‘mathematical puzzle’ has a key element: asymmetry. The work must be decently hard on the requester side yet simple to check for the network. This thought is otherwise called a CPU cost work, client puzzle, computational puzzle or CPU estimating capacity.”[6]

“All the network miners contend to be the first to discover an answer for the mathematical puzzle that worries the applicant block, an issue that cannot be settled in different routes than through savage power so that basically requires an enormous number of attempts.”[6]

At the point when a miner at last finds the correct solution, one reports it to the entire network in the meantime, getting a cryptocurrency prize (the reward).

From a specialized perspective, mining process is an activity of converse hashing: it decides a number, so the cryptographic hash calculation of block information results in under a given limit.

“This limit, called difficulty of mining, is the thing that decides the aggressive idea of mining: all the more processing force is added to the network. The higher this parameter increments, expanding likewise the normal number of computations expected to make another block. This technique likewise expands the expense of the block creation, forces miners to enhance the productivity of their mining systems to keep up a positive monetary equalization. This parameter refresh ought to happen around each 14 days, and another block is created every 10 minutes.”[6]

The critical thing one has to comprehend is that now Ethereum developers wants to utilize another consensus system called Proof of Stake (PoS).

4.5 Definition of Proof of Stake (PoS)

Proof of stake(PoS) is an alternative algorithm to approve transactions based and accomplish the distributed consensus. (Bitfury Group Limited[4] and Rosic[6])

It is still an algorithm, and the objective is the to create an equivalent algorithm of the proof of work. Yet the procedure to achieve the objective is completely different.

Proof of Stake(PoS) opinion was first appeared on the Bitcointalk forum in the year 2011. But the first cryptocurrency to use this method was Peercoin inf2012, together with Nxt, Qora, Nubits, ShadowCash, Black Coin and Nav Coin.

“Not at all like the Proof-of-Work, where the calculation rewards miners who take care of mathematical puzzles with the objective of approving transactions and making new blocks, with the proof of stake, the maker of another block is picked deterministically, contingent upon its riches, likewise named as stake.”[6]

No block rewards, likewise, all the cryptocurrencies are already made first and foremost, and their number never shows signs of change. This implies in the PoS mechanism there is no block reward, along these lines, the miners get the transaction fees. Along these lines PoS system miners are called forgers.

The most popular PoS implementations are Decred, Ethereum(soon), Peercoin and many others. The main advantages of PoS; attacks are more expensive, more decentralized and more energy efficient[21] but disadvantage is Nothing at Stake but what does it mean? The normal contention against proof of-stake is the Nothing

at Stake issue. The worry is that since it costs validators no computational capacity to help a fork not at all like PoW, validators could vote in favor of the two sides of each fork that occurs. Forks in PoS could then be significantly more typical than in PoW, which a few people stress could hurt the validity of the currency.

4.6 The Reason of Why Ethereum Wants to use PoS

As noted by Rosic[6], “the Ethereum community and its creator, Vitalik Buterin, are planning to do a hard fork¹⁷ passing from proof of work to proof of stake. In any case, why they would like to change from one to the other? In a distributed consensus-based on the proof of Work, miners need high volume of electricity energy[21]. One Bitcoin transaction need the same amount of electricity as powering 1.57 American households for one day (data from 2015). Also, these electricity costs are paid with Fiat currency, prompting a steady descending weight on the advanced currency esteem. In a recent research, experts argued that Bitcoin transactions may consume as much electricity as Denmark by 2020.”

Developers are entirely stressed over this issue, and the Ethereum community needs to misuse the proof of stake(PoS) strategy for a more greener and less expensive distributed type of consensus.

4.6.1 How are forgers selected?

We again refer to Rosic[6] as follows; “If Casper (the new PoS protocol) will be executed, there will obtain a validator pool. Clients can participate this pool to be chosen as the forger. This procedure will be accessible through a component of calling the Casper contract and sending Ether – or the coin who support the Ethereum network – together with it. ‘You automatically get inducted after some time,’ clarified Buterin himself on a post published on Reddit.com. ‘There is no priority scheme for getting inducted into the validator pool itself; anyone can join in

¹⁷ Hard fork is a term associated with Blockchain technology. It simply means that all nodes or users must switch to the most current version of the protocol software. In other words, hardfork is a permanent separation from the previous version of the block. Hard Fork is often used to fix important vulnerabilities in older versions of the software, to add new functionality, or to reverse operations.

any round they want, irrespective of the number of other joiners,' he added. 'The reward of each validator will be somewhere around 2-15%', but he is not sure yet."

Likewise, Buterin contended that there will be no forced point of confinement on the quantity of active validators (or forgers), however it will be controlled monetarily by cutting the interest rate if there are excesses of validators and expanding the reward if there are excessively few.

4.7 What is Ethereum Casper?

Magas[8] noted that on May 8th, 2018 a new version of Ethereum was released under the name "Casper". The new tool introduced under the name of "Hybrid Casper's Cute Finishing Tool" ends the major mining problems such as high electricity consumption[21], not everyone has equal access to mining equipment, centralization of mineral pools and growing ASIC market. This step taken by the Ethereum developers is, of course, part of the network's transition from PoW algorithm to PoS. Many people think that this change in the Ethereum network will be the biggest change the network has seen so far.

a) Energy consumption and commissions

The year of 2017 was a very important year for crypto money because the crypto money market showed both growth in popularity and value. But 2017 showed us something else: neither Bitcoin nor Ethereum can take action as fast as they can compete with the nominal money. In addition to low processing speeds, the amount of electricity consumed to make mining was a source of concern. Electricity consumed by miners has become quite a controversy especially in recent times, sometimes consuming more electricity than electricity consumed by a country [8]. Today, the developers of the foremost crypto money, unfortunately, have not been able to solve the scaling problem. Especially Ethereum is very weak in scaling despite having a very serious number of miners. In fact, from a theoretical standpoint, the more people mining in a crypto network, the more capacity the network has to have. But when we come to practice, we see that all the miners on the network are trying to pass a single block process at the same time, the production process becomes more complex and the network capacity remains at the same level. This means that even if the number of miners on a network increases

by a thousand times, a block on the network will still be produced in ten seconds and the electricity consumption will increase on top.

Difficulty in scaling means having trouble with the commission. Miners prefer transactions where they can get higher commissions because they get their revenues here. This can cause small-scale transactions that do not promise much on a commission basis, for days, perhaps even forever, to wait.

A new problem emerged. The ASIC model mines, which are quite powerful, are not only threatening the market but also the decentralization of networks. One of the mine pools that use ASICs entirely can create a significant portion of the hash power on the network on its own, which can make the network more centralized.

b) Ethereum Archipelago

Many people in the crypto money sector are aware of the problems I have mentioned above. In the last few months that, a fork outbreak started in Bitcoin and many people started to build a new version of Bitcoin. People create their own versions because they are aware of the reasons mentioned above and want to solve these problems. In this 'fork season' some developers chose ASIC while others opt to stay centerless.

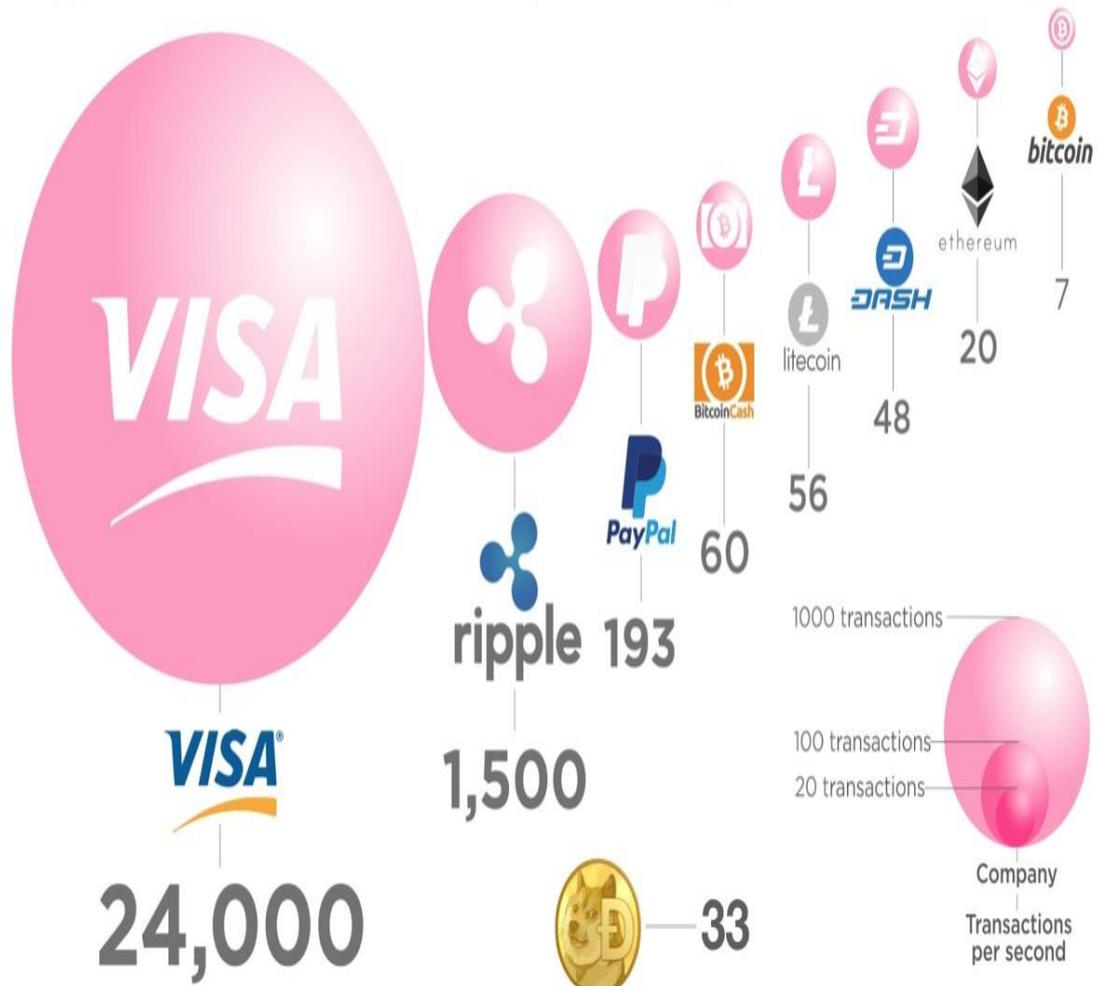
The leading developers in the industry are trying to solve these problems, and the solutions that the Ethereum developers put forward are welcome. The Ethereum team is trying to combine certain scales of both PoS and PoW algorithms.

Casper is the name of the new protocol to be derived from both algorithms. This new protocol makes Blockchain much simpler as it completely changes the policies followed to create blocks on the Ethereum network.

Ethereum developers are now very confident that the PoW system lies at the root of all the problems that crypto money in the market is experiencing. Also, in a network using PoW algorithm, Blockchain can provide limited performance, and the processing capacity of a Blockchain running on this system is not very impressive either. Figure 4.3 shows the process speeds of some of the cryptocurrencies and the well-known payment systems which are Paypal and Visa[15]. For this reason, the Ethereum team wants to leave the PoW algorithm and switch to PoS. The difference between these two algorithms is that the users receive physical computers that consume electricity in the PoW system and process the blocks in a way that is proportional to the cost they make. In the PoS system, the digital coins in the system become a kind of digital computers and process the blocks. In the PoS

system, the income to be received from a block is determined by the amount of coins the block verifiers have, not by the processing power.

Cryptocurrencies Transaction Speeds Compared to Visa & Paypal



. Figure 4.3 Payment systems process capacity per second

c) Sharding

In addition to the PoS algorithm presented in the Casper protocol, there is a new technological development: the crushing process named sharding. In the break sense, the nodes on the network contain only part of the distributed records, and the mathematical codes underlying the nodes ensure that the system is transparent and clear. The founder of the Ethereum network, Vitalik BUTERIN, likened this fracture process to a different island belonging to a single group, namely the archipelago: “Imagine that Ethereum has been split into thousands of islands. Each island can do its own thing. Each of the islands has its own unique features and

everyone belonging on that island, i.e. the accounts, can interact with each other and they can freely indulge in all its features. If they want to contact with other islands, they will have to use some sort of protocol.”

In other words, we can say that the main Blockchain of Ethereum will be broken into various 'parts', that is, it will be broken. All of the parts that will be separated will be connected to the main Blockchain as well as being connected. The purpose of the fracture process is to ensure that operations can be carried out in parallel. Because of this system, each node can pass its own part, while other nodes can continue to work in parallel. We have mentioned above that there is no increase in network capacity no matter how many miners on the network, and that this is a problem. This is exactly the problem that this break-up event solves. Thanks to this system, the network capacity and the processing speed can increase very seriously. At the same time, the problem of scalability is solved.

d) Miners and Validators: Rescue Rangers

The transactions in the 'parts' mentioned above will be implemented by the verifiers in the Casper system as well as the miners. The authenticators will ensure the legitimacy of the operations in the Casper system with the coins they have. If a verifier finds a block that he thinks it should be added to the Blockchain, he will approve the block by depositing a certain amount of the block into the block. If this block is added to Blockchain, the verifier will also receive a prize, which will be awarded at the initial deposit. If a block they add to the block cannot be added to the Blockchain, they will have wasted their coin.

Another task of the verifiers is to create a checkpoint every fifty blocks. These points will ensure that Blockchain is on the right track and will increase the security of the network. According to Vlad Zarhfir, one of the Ethereum developers, there is no reason to attempt any attack on the network's authenticators. He said that ““It's as though your ASIC farm burned down if you participated in a 51 percent attack.

The properties summarized above are depicted in Figure 4.4 [8].

PROOF OF WORK



PROOF OF STAKE



Figure 4.4 Proof of Work(PoW) vs Proof of Stake(PoS) summary

4.7.1 What can we expect from Casper?

Casper is expected to appear in the end of the 2018. Updating will be done via hard fork so that the system will not be compatible with previous versions of the Ethereum software. Casper, which emerged as a scalability solution, offers several solutions to both developers and casual users, as well as being a really important update for Blockchain. Ethereum developers have been working the network for three years to make the network much more decentralized, efficient and competitive, and these efforts are beginning to yield fruit slowly.

In the case of increased network capacity, more processing can be swapped out faster, which allows large companies to build complex structures on the network and to develop ecosystems.

There are still many questions to be asked about exactly how such a new reward system will be implemented, but most of these questions will only be answered in the coming months.

4.7.2 Is it a safer system than PoW?

Referring to Rosic[6]“Any PC system needs to be free from the likelihood of hacker attacks, particularly if the system is identified with cash. Anyway, the fundamental issue is: proof of stake is more secure than proof of work? Specialists are stressed over it, and there are a few cynics in the community. Utilizing a Proof-of-Work system, bad actors are removed on account thanks to technological and economic disincentives. Actually, programming an attack to a PoW network is extremely costly, and you would require more cash than you can have the capacity to steal.

Rather, the basic PoS algorithm must be as hack proof as conceivable on the grounds that, without particularly punishments, a proof of stake-based network could be less expensive to attack. To get over this issue, Buterin created the Casper protocol, designing an algorithm that can use the set some circumstances under which a bad validator might lose their whole deposit.”

4.8 Other Consensus Algorithm Types

In the following some other consensus algorithms which are not popular as PoW and PoS, are summarized.

4.8.1 Delegated Proof of Stake (DPoS)

DPoS is the idea of D. Larimer[2018] who is the creator of EOS which is one of the top 5 popular CCs. In DPoS, CC holders do not vote on the legitimacy of the blocks themselves. However, they vote to choose agents to do the approval for their benefit. There are for the most part between 21– 100 chosen elected delegates in a DPoS system. The representatives are rearranged intermittently and given a request to convey their blocks in. Having few representatives enables them to arrange themselves effectively and make assigned schedule vacancies for each agent to distribute their block. If delegates constantly miss their blocks or distribute invalid transactions, the stakers vote them out and supplant them with a superior representative. In DPoS, miners can work together to make blocks as opposed to contending like in PoW and PoS. By halfway bringing together the production of blocks, DPoS can run requests of size quicker than most different consensus algorithms. EOS is set to be the main blockchain with block times < 1 second! It is obviously faster than Bitcoin's 10-minute block times.

The most popular DPoS implementations are EOS, Steemit, BitShares. The main advantages of DPoS; cheap and fast transactions, scalable and energy efficient but disadvantage is partially centralized.

4.8.2 Proof of Authority (PoA)

Proof of Authority[12] is a consensus algorithm where transactions are approved by confirmed accounts, sort of like the "admins" or "administrators" of the system. These records are the expert that different hubs get their fact from. PoA has high throughput and is upgraded for private networks.

The most popular PoA implementations are POA.Network, Ethereum Kovan testnet. The main advantages of PoA; scalable and high throughput but disadvantage is it is a centralized system.

4.8.3 Proof of Weight

Proof of Weight[13] is an expansive arrangement of consensus algorithms based around the Algorand consensus show. The general thought is that where in PoS, your level of tokens claimed in the network speaks to your likelihood of "discovering" the following block, in a PoWeight system, some other moderately weighted esteem is utilized. Solid instance: Filecoin's Proof of Spacetime is weighted on the amount IPFS (InterPlanetary File System) information you are storing. Different systems could incorporate weights for things like Proof-of-Reputation.

The most popular PoWeight implementations are Algorand, Filecoin and Chia. The main advantages of PoWeight; scalable and high throughput but disadvantage is centralized system. [Gilad et al, 2017]

4.8.4 Byzantine Fault Tolerance (BFT)

One may refer [Lamport et al, 1982], [Baird 2016], [Gilad et al., 2007] and [Gencer, 2016] for this algorithm. There's this exemplary issue is circulated registering that is normally clarified with Byzantine commanders. The issue is that few Byzantine commanders and their individual segments of the Byzantine armed force and have conquered a city. They should choose as one regardless of whether to assault. If a few officers attack without the others, their attack will end in disaster. The commanders are generally isolated by separation and need to pass messages to impart. The most popular BFT implementations are Hyperledger, Stellar, Dispatch, and Ripple. The main advantages of BFT are; scalable, very high throughput and low cost. Its disadvantage is it is a semi trusted system.

A few cryptocurrency conventions utilize some form of BFT to come to consensus, each with their own advantages and disadvantages:

- a) **Practical Byzantine Fault Tolerance (PBFT):** One of the main answers for this issue was coined Practical Byzantine Fault Tolerance. Right now, being used by Hyperledger Fabric, with few (< 20, after that things get a little) pre-chosen commanders PBFT runs unbelievably productively. Advantages are High transaction throughput and disadvantages are Centralized and permissioned.

b) **Federated Byzantine Agreement (FBA):** FBA is another class of answers for the Byzantine commanders' issue utilized by currencies standards like Stellar(XLM) and Ripple(XRP). The general thought is that each Byzantine general, in charge of their own chain, sorts out of this world in to build up truth. In Ripple the commanders (validators) are pre-chosen by the Ripple establishment. In Stellar, anybody can be a validator, so you pick which validators to trust.

In order to sum up for its unbelievable throughput, low transaction cost, and network versatility, this consensus algorithm maybe claimed as the best in practice.

4.8.5 Directed Acyclic Graphs (DAGs)

DAGs are also known as Blockchain killers. DAGs are a type of consensus that does not utilize the blockchain information structure and handles transactions mostly asynchronously. The enormous ace is hypothetically endless transactions every second, except DAGs have also strengths and weaknesses like any other consensus. In the following four of such algorithms are summarized.

a) **Tangle:** Tangle is one of the DAG consensus algorithms utilized by IOTA. With the end goal to send an IOTA transaction, you have to approve two past transactions one received. The two-for-one show preemptive kindness consensus reinforces the legitimacy of transactions the more transactions are added to the Tangle. Since the consensus is set up by the transactions, hypothetically, in the event that somebody can produce 1/3 of the transactions they could persuade whatever is left of the network their invalid transactions are substantial. Until there is sufficient transaction volume that making 1/3 of the volume ends up unfeasible, IOTA is kind of "double checking" the majority of the network's transactions on a brought together hub called "The Coordinator". The Coordinator works like preparing wheels for the system and will be evacuated once the Tangle is sufficiently enormous. [Popov, 2018]

b) **Hashgraph:** Hashgraph is a gossip protocol consensus created by L. Baird[2016]. Nods share their known transactions with different nodes indiscriminately so in the long run every one of the transactions are slandered around to the majority of the nodes. Hashgraph is extremely quick (250,000+

transactions for each second) yet is not impervious to Sybil attacks. So Hashgraph is an extraordinary alternative for private networks, however we are not going to see it actualized in an open network like Ethereum or Dispatch at any point in the near future. [Baird, 2016]

- c) **Block-lattice**[14]: NANO¹⁸ (formerly called Raiblocks) keeps running with a turn on the blockchain called a Block-lattice section. The Block-lattice section is where each client (address) gets their own chain that no one but they can write to, and everybody holds a duplicate of the majority of the chains. Each transaction is separated into both a send block on the sender's chain and a get block on the getting party's chain. The Block-lattice section appears to be excessively straightforward, making it impossible to work, however it's as of now out there running in nature. The exceptional structure leaves the Block-lattice open to some one of a kind assault vectors like the Penny-spend attack, where assailants blow up the quantity of chains hub must monitor by sending unimportant adds up to a wide cluster of void wallets.
- d) **SPECTRE (Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections)**: One may refer [Sompolinsky et al.,2017]; SPECTRE is a proposed Bitcoin scaling arrangement that uses a blend of PoW and DAGs to achieve adaptable consensus. In SPECTRE, the blocks are mined indicating different parents, not only one, so the network could possibly deal with multiple blocks every second. Mining a block indicating some parent blocks underpins those blocks legitimacy. Contrasted with PoW's "longest chain wins", SPECTRE utilizes something like "blocks which have the most children win." SPECTRE has not been attack tested in the real world, and new attack vectors are probably going to develop, yet it feels like an exceptionally sharp potential approach to settle Bitcoin.

4.8.6 Proof-of-Importance (PoI)

One may refer NEM Foundation[2018] for this algorithm. Proof of importance(PoI) is another Blockchain consensus algorithm that thinks about the general efficiency of clients in the network. It was first implemented to NEM (New Economy Movement) that is a blockchain innovation company and targeting to process transactions all

¹⁸ NANO: One of the CCs.

the more proficiently and acquaints notoriety with the cryptosystem. But how does it work? PoI relies upon how much one is active on the network. The more active you are as a user, the more rewards you get. Every user is scored and the higher your score, the more the prizes. This algorithm is intended to compensate the extremely faithful users of the Blockchain. Thus, it encourages more user use the platform. The quantity of coins may swing the votes normally given that transactions of the large amount may define for more transactions. In any case, the algorithm principally relies upon the activities observed by every user and not really the amount they transact.

The most popular PoI implementation is NEM. The main advantage is a wealthy person cannot continue to be richer on the platform because the amount of cash a person owns is not the only factor to consider when measuring an account's reputation but there is a big disadvantage. One main problem with this method is the use of dummy operations that people will reward to send back and forth to deceive the algorithm. The use of dummy operations is an issue that NEM and other major players have not yet consumed.

4.8.7 Proof of Capacity(PoC) or Proof of Space(PoSpace)

Referring to Dziembowski et al.[2013], "Proof-of-space (PoSpace), also known as Proof-of-Capacity (PoC), is a method for demonstrating that one has a legitimate interest in a service (for example sending an email) by allocating a significant amount of memory or disk space to solve a challenge presented by the service provider. PoSpace are fundamentally the same as PoW, except that instead of computation, storage is used. PoSpace is related to, but also significantly different from, memory-hard functions and proofs of retrievability. After the arrival of Bitcoin, options in contrast to its PoW mining system were looked into and PoSpace was considered with regards to digital forms of money. PoSpace are viewed as a more pleasant and greener option because of the universally useful nature of capacity and the lower vitality cost required by capacity. The most popular PoSpace implementation is BurstCoin. The main advantage is not consuming too much energy, so it is nature friendly method. But disadvantage is it will need a lot of hard-drive. One is not calculating with his/her equipment, one just stores the data for anyone else."

5 DISCUSSIONS, SUMMARY AND CONCLUSIONS

5.1 Discussions

5.1.1 Comparison of consensus mechanisms against each other

As noted in Chapter 4, there are a few different consensus mechanism types. Some of them are blockchain and some of them are alternative of blockchain. All of them have advantages and disadvantages. These mechanisms are summarized on Table 5.1. There are a few more mechanisms which are not mentioned in this thesis. They are not popular or just for private use. Firstly, we need to understand these mechanisms not just for cryptocurrencies. One can utilize them for another area as an alternative to the centralized server[Bonneau et al., 2015]. Some mechanisms are not good for public use, so one need to decide the application area first. Proof of Work is the most popular consensus mechanism of the CCs but as noted before miners consume more electricity than a small country. In my opinion it will cause serious damage in a long period. Furthermore, nowadays most of the CCs lost their values, so mining is not so profitable as before. Sometimes PoW hardware spends more than earnings. It is not profitable for majority who lives where electricity is not so cheap. PoS is good alternative and there is also no hardware required. The author's favorite algorithms are FBA and Tangle. Tangle can be very fast and reliable; however, it needs a big network. If it meets the conditions, it can be the new king instead of PoW. Also, it is alternative for the blockchain. It works asynchronous. It means it is fast. FBA is also recommended. In fact Akbank of Turkey started GBP(Great Britain Pound) transfer to Santander Bank UK on Ripple with FBA infrastructure[20]. As it is seen, day by day CCs are becoming a part of our lives.

5.1.2 CCs in Our Daily Lives

During the recent years, the term cryptocurrency has been quickly appearing in the spotlight. At first it appeared to be unusual and to some degree frightening like the credit cards in early days.

Table 5.1 Comparison of several consensus mechanisms.

Mechanism Name	Basic Principle	Speed	Cost	Application Area	Popular Coins
Proof of Work (PoW)	Works on the hard way, but it works perfectly. It is only breakable if someone owe 51% of the whole network. Unfortunately, there are a few examples for this situation.	Slow	Need expensive hardware and consume a lot of electricity.	Public or Private	Bitcoin, Ethereum, Litecoin
Proof of Stake (PoS)	The network trusts the validator (forger) who stakes their own coins; more stake means the higher the chances of validating transactions. Rich get richer.	Fast	No need special equipment. Nature friendly.	Public or Private	STRAT, Qtum ETH(soon)
Delegated Proof-of-Stake (DPoS)	The shareholders delegate production of new blocks to a little and constant number of elected shareholders. Highly competitive but highly profitable.	Fast	No need special equipment. Nature friendly.	Public or Private	EOS, BitShares
Practical Byzantine Fault Tolerance (PBFT)	Preselected nodes maintain consensus even if some of them malicious or are fail.	Fast	No need special equipment. Nature friendly.	Private permissioned blockchain	TON, NEO
Federated Byzantine Agreement (FBA)	Blocks are verified after if signed by a specified majority of signers.	Fast	No need special equipment. Nature friendly.	Public or private permissionless blockchain	Ripple, Stellar
Directed Acyclic Graph (DAG) / Tangle	Working asynchronous. No fixed blocks that are confirmed in a random order on a linear scale. More transaction means faster and more reliable system.	Ultra-Fast on big network. Slow on small network	No need special equipment. Nature friendly.	Public permissioned non-blockchain	IOTA
Directed Acyclic Graph (DAG) / Hashgraph	Nodes communicate randomly using the 'gossip about gossip' protocol and agree on consensus after a certain communication round.	Ultra-Fast	Technology is patented so need to pay a license cost.	Private permissioned non-blockchain	HashGraph
Proof-of-Importance (PoI)	It is similar to PoS but a few additional properties. Every member scored. Higher scored means higher prizes. Wealth is not the only determining factor.	Fast	No need special equipment. Nature friendly.	Public permissionless blockchain	NEM
Proof of Capacity	Storage space is provided to someone else.	Slow	Need lots of HDD or SSD. Not power hungry like PoW.	Public or Private	Burstcoin

One may be more comfortable now with terms such as Bitcoin, and Ether. These are all cryptocurrencies utilizing the Blockchain Technology to protect these coins and innovation as well as users' wallets.

Referring to Rosic[7], there are seven major properties of cryptocurrencies:

a) Fraud: Cryptocurrencies are digital and cannot be mimic or turned around discretionarily by the sender, likewise with Mastercard charge-backs. Thus, people ought to be more cautious.

b) Immediate Settlement: Purchasing real property usually involves some third parties, delays, and payment of fees. BitPay¹⁹ founder T. Gallippi refers to the blockchain as a type of "large property rights database," [11]. Bitcoin contracts can be designed and enforced to bypass or add third party confirmations, consult external facts, or be finished at a future date or time for a small amount of the cost and time required to finish usual resource exchanges.

c) Lower Fees: There are not more often than not transaction expenses for cryptocurrency trades in light of the fact that the miners are repaid by the network. This circumstance can change later. Even though there is no bitcoin/cryptocurrency transaction charge, many hopes that most clients will associate an outsider administration, for example, Poloniex, Binance, Bittrex making and keeping up their bitcoin wallets. These CC markets demonstration like Paypal improves the situation money or Mastercard clients, giving the online trade system to bitcoin, and in that capacity, they're probably going to charge expenses. Figure 5.1 shows the commission of some well-known payment system Visa and other CC based payment systems [9].

d) Identity Theft: When one gives his/her Mastercard to a store, actually one gives him or her entrance to one's full credit line, regardless of whether the transaction is for a little sum. Visas work on a "pull" mechanism, where the store starts the installment and pulls the assigned sum from one's record. CCs utilizes a "push"

¹⁹BitPay is a worldwide bitcoin payment organization headed in Atlanta, Georgia, United States. It was established in May 2011 by Tony Gallippi and Stephen Pair. BitPay provides Bitcoin and Bitcoin Cash payment processing services for traders.

system that enables the CC holder to send precisely what he or she needs to the store or beneficiary with no any longer data.

PROCESSING SYSTEMS COMPARISON

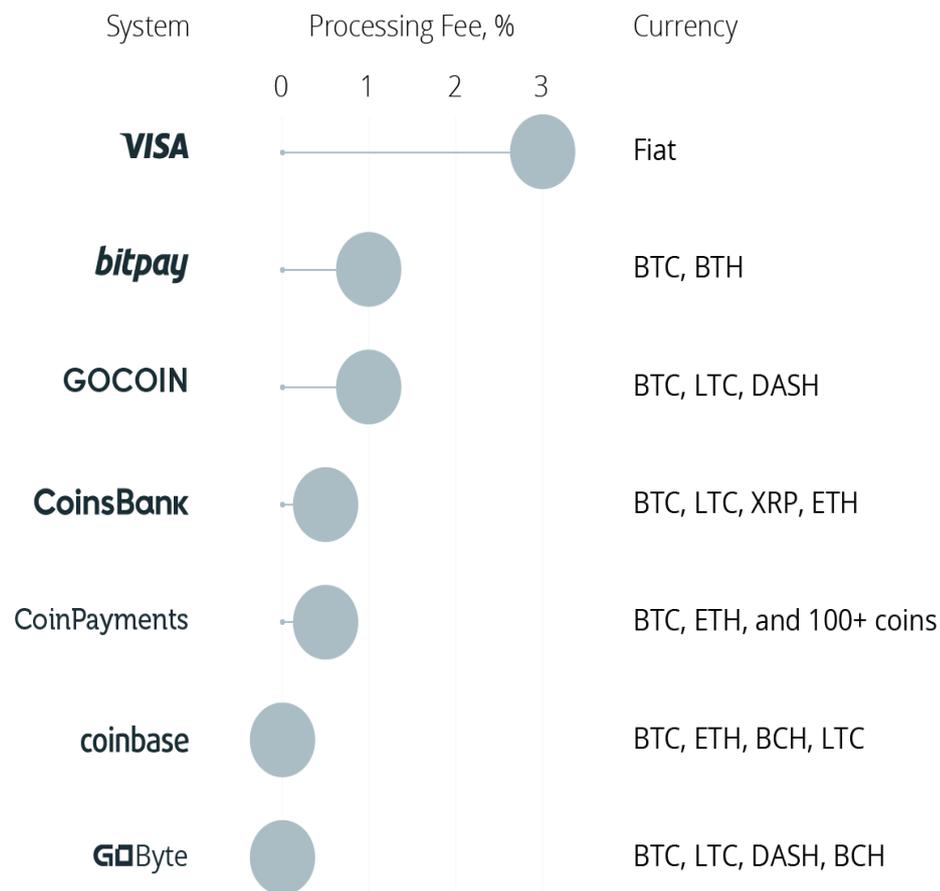


Figure 5.1 Visa and CC based payment systems commissions

e) Access to Everyone: There are around 2.2 billion individuals with access to the Internet or mobile phones who don't at present methodology standard exchange, these people are set up for the Cryptocurrency promote. Kenya's M-PESA system, a cell phone-based cash exchange, and microfinancing administration as of late reported a bitcoin gadget, with one of every three Kenyans presently owning a CC wallet.

f) Decentralization: A global network of computers utilize blockchain innovation to mutually deal with the database that records CC transactions. That is, Bitcoin is

overseen by its network, and nobody central authority. Decentralization means the network works on a peer-to-peer premise. The types of mass joint effort this makes conceivable are simply starting to be researched.

g) Recognition at universal level: Since cryptocurrency is not bound by the trade rates, loan fees, transactions charges or different charges of any nation; along these lines, it tends to be utilized at a global level without encountering any issues. This, actually, saves lots of time and also cash with respect to any business which is generally spent in exchanging cash from one nation to the next. Cryptocurrency works at the general level and subsequently makes transactions very simple.

Generally speaking, cryptocurrencies have far to go before they can replace credit cards and conventional currencies as an instrument for worldwide business.

Reality is, numerous individuals are as yet unconscious of cryptocurrency. People ought to be told about it to have the ability to apply it to their lives. Organizations need to begin tolerating it. They have to make it simpler to join and begin.

The future interest of cryptocurrencies lies in permitting you extreme power over your cash, with quick secure worldwide transactions, and lower transaction charges when contrasted with every current currency.

At the point when utilized legitimately and completely comprehended it would be the initiator of many rising systems that will in a general sense change our worldwide financial system.

5.1.3 The risks of CCs

The risk is that you could lose all of your investment. There are several things that could go wrong. Below they are listed in order of probability from most likely to least likely:

- a) Poor investment decisions cause to a loss of coins;
- b) Coins can be stolen, either from the CC Markets or by a compromised wallet (virus, hackers, etc);

- c) Forgotten or lost passwords leading to an inability to access the funds. (There are no password resets for wallets. One is in complete control of one's funds and completely responsible for securing them);
- d) The coin could be superseded by another technology that is perceived to be superior;
- e) A malicious attack or fundamental programming mistake that breaks public confidence in the block-chain (this is the global distributed ledger on which all accounts, balances and transactions are maintained). (highly unlikely);
- f) Governments attempting to regulate cryptocurrency out of existence (has somewhat been tried already and relatively unsuccessful to date);
- g) Quantum computing could break the encryption that support the security of the network. (this would also break all currently known internet security for every other computerized financial system as well);

Crypto currency is a more secure investment than fiat currency because the security is ensured by mathematics and cryptography rather than the desires of very powerful centralized authorities like the reserve bank. However due to its extremely high level of security and inability for transactions to be reversed it can also be quite financially dangerous if not properly understood so the biggest threat to one's coin investment is oneself.

5.1.4 Possible weaknesses of CCs

So, what are the current weaknesses of Bitcoin and some other altcoins, which could impact investors today or in the future? There are several issues with cryptocurrency technology that should be considered:

- a) First, as I mentioned before there is no central authority. Although no central authority is a positive also sometimes it could become a negative thing. If one loses one CCs for any reason, you have no application to get your bitcoin back.

b) Everyone responsible for keeping safe their Private Keys and Passwords that protect their CC Wallet. If they forgot or lose them, they cannot reach their wallet permanently.

c) All computers and smartphones can be infected with Malware. Some CC Wallet and Mining applications have been hacked, stealing CC that was presumed secure. A good antivirus software, on a virus-free device, recommended for all CC users.

d) In some countries CC exchanges may failed for some reasons including hacking, fraud, or even government intervention.

e) Recently, as Bitcoin became more popular, transaction fees and transaction times have become an issue. This can leave your Bitcoin stuck in the system, unavailable to either the sender or receiver until the transaction is confirmed. Instances of transactions being held up for several days have been experienced by some. There are methods to un-stick these transactions, but this is not for the beginner, as Bitcoins could be lost. You can guarantee your Bitcoin transaction is processed faster by including a larger transaction fee, but this goes against the principle of permanently low transaction fees that Bitcoin originally promised.

f) On the plus side for CC, the online adoption network is the largest there is. One can buy real physical goods using CC, and more online shops for CC appear day by day.

5.1.5 Domestic (Turkish) Cryptocurrency attempts

As in other countries there are also several initiatives in Turkey. There are four known cryptocurrencies that were developed by Turkish developers. These are SikkeCoin, AkcheCoin, Nexpara and Turcoin. As noted before most of the coins have a vision, target and usage area. If a coin does not have a purpose like as our domestic coins, it is very likely that it is a scam. Unfortunately, none of the Turkish cryptocurrencies have been implemented. Nexpara's team announce that "Nexpara stopped the ICO because it could not make the road map according to the legislation. All funds deposited are returned." on their twitter account[16]. Unfortunately, Turcoin investors are not that lucky. Because latest news headlines about Turcoin is "New details on Turcoin's 1 billion lira fraud"[17]. As seen Turcoin

looks like totally fraud. There is no update for Sikkecoin. Their last announce which is on 31 March 2018 is, they are updating Sikke but no new news since then. Also, SPK (Sermaye Piyasası Kurulu) ignore the Sikke has SPK license so they warn investors about do not trust them[18]. When we examine Akchecoin, it looks more professional than the others because they prepared a white paper. They created an e-commerce site that one can shop with Akchecoin. But when we examine in detail, they did not code this coin. They just copy and paste the Waves token infrastructure. Unfortunately, according to their web site they have no update since second quarter of 2018. Probably it is scam too. Also, there is no legal basis for the crypto-currency, as seen in Turkey.

5.2 Summary

In this study, Cryptocurrencies are analyzed. Cryptocurrencies have been theoretically investigated for security and their security vulnerabilities and various hacking methods are briefly discussed. The differences in how Cryptocurrencies are produced, and the methods of production and consensus mechanisms are examined, and the advantages and disadvantages of these methods are discussed and presented in Chapter 4 and 5.1.1.

How these methods affect the future of Cryptocurrency miners and Cryptocurrency investors have been examined. Also, can Cryptocurrencies replace present payment systems in the future discussed.

5.3 Conclusions

As a conclusion that we may note that, blockchain is a revolutionary technology for many usage areas especially in economy. It is more reliable and secure than central servers as well as anonymity is a big advantage. Popular CCs' algorithms are theoretically unbreakable. There are a lot of Initial Coin Offering(ICO) day by day. Unfortunately, most of them are scam or fraud and there is no safety net for investors. Nowadays, most of the coins lost their value on the markets like a punctured balloon. Lots of investors lost their savings. Some countries regulated cryptocurrencies, some did not. But some futurists thought blockchain technology will be use in a lot of area in the future. Consensus mechanisms and their differences are examined and presented in Chapter 4 and 5.1.1. Proof of Work is the most

common mechanism and it is working fine but it is not fast enough to replace Visa or any other payment methods. Also, it is using too much electricity[21]. Proof of Stake is the second most common mechanism and more nature friendly but also it has some weaknesses. Briefly, mechanisms have advantages and disadvantages but still none of them is perfect for every way. Ethereum developers began to change their mechanism. From PoW to PoS. It is a big step to becoming a real-world money. But still cryptocurrencies are too vulnerable for speculations. Their values are so unstable, and it is the biggest obstacle to becoming real world money[10]. Yet, probably cryptocurrencies get over these problems in coming years. Cryptocurrencies are still needed to develop but, in the future, they will definitely be a part of life human life.

List of References

Baird, L. The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance, Swirlds Tech Report, Swirlds-Tr-2016-01, 2016.

Barski, C., Cryptograph for Cryptocurrency, Chicago Ethereum Meetup Presentation, Chicago on 7 September 2017.

Bertoni, G. et al., Keccak Implementation Overview, SHA-3 competition (round 3), 29 May 2012.

Black, J. et al., A Study of the MD5 Attacks: Insights and Improvements, Fse'06 Proceedings of the 13th International Conference on Fast Software Encryption pp. 262-277, 2006.

Bonneau, J. et al., SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, 2015 IEEE Symposium on Security and Privacy, San Jose, California at The Fairmont, May 17-21, 2015.

Ciampa, M., Comptia Security+ 2008 In Depth, pp. 281-297, 2008.

Dziembowski, S. et al., Proofs of Space, published in the proceedings of International Conference Association for Cryptologic Research, 2013.

Evans, C.W., Bitcoin in Islamic Banking and Finance, Journal of Islamic Banking and Finance, Vol. 3, No. 1, pp. 1-11, June 2015.

Garay, J. et al., The Bitcoin Backbone Protocol: Analysis and Applications, published in the proceedings of International Conference Association for Cryptologic Research, 2014.

Gencer, A.E., et al., Bitcoin-NG: A Scalable Blockchain Protocol, Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16), Santa Clara, CA, USA, March 16–18, 2016.

Gilad, Y. et al., Algorand: Scaling Byzantine Agreements for Cryptocurrencies, SOSP '17 Proceedings of the 26th Symposium on Operating Systems Principles, pp. 51-68, 2017.

Heilman, E., Eclipse Attacks on Bitcoin's Peer-to-Peer Network, Proceedings of the 24th USENIX Security Symposium, Washington, D.C., August 12–14, 2015.

Lamport, L. et al., The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems (TOPLAS) Volume 4 Issue 3 pp. 382-401, 1982.

Larimer, D., Consensus Algorithm (BFT-DPOS), EOS.IO Technical White Paper V2, 2018.

NEM Foundation, NEM Technical Reference Version 1.2.1, 2018.

Popov, S., The Tangle, Iota Whitepaper Version 1.4.3, 2018.

Sompolinsky, Y. et al., Spectre: Serialization of Proof-Of-Work Events: Confirming Transactions Via Recursive Elections, published in the proceedings of International Conference Association for Cryptologic Research, 2017.

Tao, X. et Al., Fast Collision Attack on MD5, published in the proceedings of International Conference Association for Cryptologic Research, 2013.

Viglione, R., Does Governance Have a Role in Pricing? Cross-Country Evidence from Bitcoin Markets, Social Science Research Network (SSRN), September 25, 2015

Wang, X. et al., Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, published in the proceedings of International Conference Association for Cryptologic Research, 2004.

Web References

[1] Dougherty, C., MD5 Vulnerable to Collision Attacks, Carnegie Mellon University CERT Vulnerability Notes Database, Vu#836068 , 2008.

[2] Nakamoto, S., Bitcoin: A Peer-To-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf>, 2008.

- [3] Martin, S. and Tokutami, M., Password Cracking, <https://pdfs.semanticscholar.org/488d/15182bda2da72e900fcb531c7224d9f141cc.pdf> , 2012.
- [4] Bitfury Group Limited, Proof of Stake Versus Proof of Work, <https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf>, 2015.
- [5] Rosic, A., What Is Cryptocurrency: Everything You Need to Know [Ultimate Guide], <https://blockgeeks.com/guides/what-is-cryptocurrency/> , 2016, Last Accessed 15 October 2018.
- [6] Rosic, A., Proof of Work vs Proof of Stake: Basic Mining Guide, <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/> , 2016, Last Accessed 18 October 2018.
- [7] Rosic, A., 7 Incredible Benefits of Cryptocurrency, The Huffington Post, https://www.huffingtonpost.com/ameer-rosic-/7-incredible-benefits-of-_1_b_13160110.html, 23 November 2016.
- [8] Magas, J., Casper: What Will the Upgrade Bring to the Ethereum's Network?, Cointelegraph, <https://cointelegraph.com/news/casper-what-is-known-about-the-new-ethereums-network-upgrade>, 16 May 2018.
- [9] Magas, J., Bitpay, Coinbase Or Others: Can Anybody Replace Visa?, Cointelegraph, <https://cointelegraph.com/news/bitpay-coinbase-or-others-can-anybody-replace-visa>, 06 June 2018.
- [10] www.coinmarketcap.com
- [11] Gallippi T., Interview Podcast, Founder of Bitpay, <https://www.bitcoin.kn/2015/01/btck-128-2015-01-24/> , 24 January 2015.
- [12] www.poa.network.
- [13] <https://nulltx.com/what-is-proof-of-weight/>
- [14] <https://www.mycryptopedia.com/nano-block-lattice-explained/>
- [15] <https://howmuch.net/articles/crypto-transaction-speeds-compared>.

- [16] Habertürk.com, NexPara piyasadan çekildi!, Habertürk, <https://www.haberturk.com/nexpara-piyasadan-cekildigini-duyurdu-1875978-ekonomi>, 14 March 2018.
- [17] Sputnik, Turcoin'in 1 milyar liralık vurgununda yeni detaylar, Sputnik News, <https://tr.sputniknews.com/turkiye/201806211033950795-turkiye-dijital-para-vurgun-kocaeli-merkez/> , 21 June 2018.
- [18] <https://tr.investing.com/news/economy-news/spk-usulsuz-kripto-para-faaliyetini-yakalad-535423>
- [19] https://en.wikipedia.org/wiki/Merkle_tree
- [20] <https://www.haberturk.com/akbankta-ripple-uzerinden-sterlin-para-transferleri-basladi--2258911-ekonomi>
- [21] Hern, .A, Bitcoin's energy usage is huge – we can't afford to ignore it, The Guardian, <https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency>, 17 Jan 2018.