Seminar Report

on

“Cryptocurrency”

Submitted to the

Savitribai Phule Pune University

In partial fulfillment for the award of the Degree of

Bachelor of Engineering

in

Information Technology

by

Akanksha Patil

(Exam Seat No.72164357E)

Under the guidance of

Mrs. S. A. Hadke

Department of Information Technology

Bharati Vidyapeeth's College of Engineering for Women

Katraj-Dhankawdi,

Pune - 411 043.

2021-22

CERTIFICATE

This is to certify that the seminar report entitled **"CryptoCurrency"** being submitted by **Akanksha Patil (72164357E)** is a record of bonafide work carried out by her under the supervision and guidance of **Mrs. S. A. Hadke** in partial fulfillment of the requirement for **TE (Information Technology Engineering) – 2019 course** of Savitribai Phule Pune University, Pune in the academic year 2021-22.

Date:

Place: Pune

Mrs. S. A. Hadke
Guide

Prof. Dr. D. A. Godse
Head of the Department

Prof. Dr. S. R. Patil
I/C Principal

This Seminar report has been examined by us as per the Savitribai Phule Pune University, Pune requirements at Bharati Vidyapeeth's College of Engineering for Women, Pune - 43 on _____

Internal Examiner

External Examiner

ACKNOWLEDGEMENT

It is indeed a matter of great pleasure and privilege to present the Seminar on "Cryptocurrency". This is to acknowledge and thank all the individuals who played important role in shaping this seminar report. Without their constant guidance and assistance this project report would not have been completed.

We wish to express true sense of gratitude towards our respected guide, Mrs. S. A. Hadke ma'am who at very discrete step in study of this report, contributed her valuable guidance and help to solve every problem that raised.

We wish to thank our H.O.D. Prof. Dr. D. A. Godse for opening the doors of the department towards the realization of the seminar report and for his boundless co-operation.

We would also like to thank our honorable principle Prof. Dr. S. R. Patil sir who created a healthy environment for all of us to learn in best possible way.

We also express our gratitude to all the Staff Members of Information Technology Department for providing the necessary facilities for the completion of this seminar work in our college. And last, but not the least we also express our thanks to all our friends for their undying support shown during the preparation of this report. We owe all our success to them.

THANKS…!!!

Akanksha Patil

Signature

ABSTRACT

CryptoCurrency had made a revolution in the field of online payment systems because of their Security and high-speed transaction. As see the growth of Blockchain Cryptocurrency many of the researchers, developers, investment agents, traders are moving towards this cryptocurrency ecosystem. Many of the cryptocurrencies exist like ether, Litcoin bitcoin, Tether, ripple but the most popular cryptocurrency is bitcoin cryptocurrency.

In this paper, we broadly Focus on a detailed analysis of Cryptocurrencies, Issues facing current currency and how cryptocurrency overcomes those issues, Type of Cryptocurrencies, how blockchain plays an important role in creating currency. Also present detailed of widely used Cryptocurrency Bitcoin, online exchanges, Bitcoin Miners, Wallets, Proof of Work. I present how cryptography plays an important role to secure transactions. Finally, we discuss the Benefits, Trust issues of cryptocurrency.

The result can help users to determine a trade-off between the risk of double-spending attempts and the transaction time delay or confidence before accepting transactions. These results can also assist blockchain aspirants in how blockchain is used for transactions and how they use their skills of blockchain for cryptocurrency mining and develop suitable strategies to get involved in the mining process and maximize their profits.

Keywords: Blockchain, Cryptocurrency, Bitcoin, Miners, Trust

CONTENTS

ABBREVIATIONS

1. BTC - Bitcoin
2. ETH - Ethereum
3. LTC – Litecoin
4. XTC – Monero
5. ZEC – Zcash
6. POW – Proof-of-work
7. DOS – Denial of Service

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION TO CRYPTOCURRENCY

A cryptocurrency is a virtual currency which is used to by services or anything for that we don't need to spend physical currency like Indian rupees, Doller all the transaction takes place online. It is virtual or online ledger with cryptography to secure and ensure transactions.

Cryptocurrency is a digital currency or virtual currency and it is secured by Cryptography. Many of the cryptocurrency are decentralize and it is based on blockchain technology. Blockchain is distributed ledger of decentralize data that is securely shared. Cryptocurrencies are like Bitcoin, Ether, Litecoin, Tether, Ripple etc. are types of cryptocurrencies. There are more than 2100 cryptocurrencies exists right now but most popular cryptocurrency is Bitcoin which is developed in 2008 by Santoshi Nakamoto. From that time this virtual currency comes into picture.

MOTIVATION BEHIND CRYPTO CURRENCY

The Motivation behind this topic is as we can see in our daily life, we done transaction but sometimes what happen our transaction interrupt because of some issues like technical issues, Account Hacked, Transfer limit, High transfer changes to overcome on such issues Crypto Currency digital currency we can use because it does not require central authority for transaction and it is distributed across network everyone has copy of transaction because of that no one can alter the transaction. Because of that it is highly secure.

ORGANIZATION OF THE CRYPTO CURRENCY

- Chapter 1 covers an introduction of the Crypto currency and motivation for choosing this topic and organization of report in which session what explained.
- Chapter 2 covers Literature Survey In which basically three technical papers are covers. Base technical paper for seminar is Trust in Blockchain cryptocurrency in which it covers key elements of cryptocurrency, Trust issues. Reference Paper 1 is A peer-to-peer electronic cash system which is base of cryptocurrency transaction system. Reference Paper 2 is Blockchain security and Privacy.
- Chapter 3 covers System architecture of cryptocurrency and Algorithm proof-of-work (POW) which is used to validate transactions.

- Chapter 4 covers Applications of Cryptocurrencies which tells where cryptocurrency is used.
- Chapter 5 It include comparison chart of traditional currency i.e. Fiat currency and cryptocurrency.

Chapter 2
LITRETURE SURVEY

[1] Muhammad Habib ur Rehman , Khaled Salah , Ernesto Damiani and Davor Svetinovic "Trust in Blockchain Cryptocurrency System" vol. 67 Page numbers-17 Month year -Nov. 2019.

INTRODUCTION

Blockchain Crypto Currency has been involved new form of money during the last many years. Bitcoin is a First and very popular Crypto Currency and gained more popularity. The first Cryptocurrency which is bitcoin which is created on January 03, 2009 and which is totally based on Blockchain Technology. The first Transaction was made through it on May 10, 2010 which is done by Laszlo Hanyecz purchased two pizzas for 10 000 Bitcoins. From that time Bitcoin is a leading Crypto Currency having 52.5% total market among more than 2100 alternate Cryptocurrencies.

Blockchain is an immutable distributed ledger, is an underlying technology behind Cryptocurrency.

The elements of blockchain include

- Complex Cryptography function for security and immutability.
- Linear and nonlinear data structure for storing and manage Crypto Currency transaction.
- Peer-to-Peer Network for multiparty transaction verification.
- Distributed consensus protocol for handling centralization and double-spending.

Cryptocurrencies and other blockchain based technologies are more attraction for industry and investigating sectors. Considering massive growth of blockchain based Cryptocurrency market with total value market being $294+ billions USD, as on June 30 of 2019. Many big corporations are investing in Crypto Currency and accept it as major trade. Crypto Currency are holding total 85% of total market capital.

The word Crypto Currency is derived from encryption technique which is meant by secure the network. Crypto Currency do not have any central authority it is maintained through distributed consequences. Blockchain method which is used to insuring integrity of transactional data, and it is most essential part of Cryptocurrencies.

Apart from that Crypto Currency face criticism for many number of reasons like

- Illegal activities (Money laundering, tax evasion)

- Exchange rate volatility
- Vulnerabilities of the infrastructure underlying them

But Some of the Cryptocurrencies are more private than others. Bitcoin Cryptocurrency is one of Private Currency. Bitcoin is poor choice for illegal business online. However analysis report helped to authorities to arrest and prosecute criminals. More privacy oriented crypto currencies such as Dash, Monero or ZCash which are very difficult to trace.

The main Contribution of this Reference paper is basically divided into the following sections:

I. Key Elements of Cryptocurrency Ecosystem and different roles of different stakeholders in it.

II. Detailed Risk analysis of different factors and how they affected the overall ecosystem.

III. Key Trust Issues of directly and indirectly impact on Crypto Currency trustworthiness.

IV. Compare different Crypto Currencies and their underlying technologies infrastructures to investigate trustworthiness.

V. Analysis of gap between state-of-art in academic research and industry research to find challenges towards more trustworthy cryptocurrencies.

VI. Short–term and long–term research strategy to identify key research directions for future researchers to build more trustworthy cryptocurrencies

DESCRIPTION

Key Elements of Crypto Currency:

A. Crypto Currency :

On the top of the security features of cryptocurrencies, Cryptocurrency has to ensure the basic three features of money that is it should be measurable, exchangeable, valuable. In

addition that Cryptocurrency has a feature called pseudonymization means hiding the original identity of transacting stakeholders. It is decentralized to enable the multiparty transaction. It is fewer transaction fees than traditional money transfer fees as well as fast money transfer. Other feature like convertibility means we can convert cryptocurrency to money and vice versa. It is irreversibility i.e. once a transaction is done it cannot be rolled back. A lot of effort needs to ensure secure transactions between two stakeholders. There are more than 2100 active Cryptocurrencies exists today. Cryptocurrency almost covers more than 81% of the total market capitalization.

Cryptocurrency	Year of Launch	Maximun Supply	New Coin Creation Frequency	Tnx / Sec.	Network	Block Time	Consensu Mech-anism	Hashing Algo-rithm	Difficulty Ad-just-ment	Unit of Mea-sure-ment
Bitcoin [2]	2009	21 mn.	12.5 per block	7	NA	8 mins 40s	PoW	SHA256	2016 blocks	Satoshi
Ethereum [36]	2015	unlimited	3 per block	20	Ethereum	15 sec.	PoW	Sthash	1 block	Wei
Ripple [37]	2012	100 bn.	1 bn. per month	1500	RippleNet	near instant	NA	NA	1 blok	Drop
Bitcoin Cash [38]	2017	21 mn.	12.5 per block	60	NA	10 mins	PoW	SHA256	6 blocks	Satoshi
EOS [39]	2018	unlimited	upto 5%	2800	EOS.IO	0.5 sec.	DPOS	DPOS	NA	NA
Stellar [40]	2014	unlimited	upto 1%	1000	Stellar	5 sec.	NA	NA	1 block	Lumen
Litecoin [41]	2011	84 mn.	25 per block	56	NA	2.5 mins	PoW	Scrypt	2016 blocks	Photon
Tether [42]	2014	NA	NA	NA	NA	NA	NA	NA	NA	Tether
Bitcoin SV [43]	2018	21 mn.	12.5 per block	7	NA	10 mins 22s	PoW	SHA256	2016 blocks	Satoshi
Tron [44]	2017	100 bn.	NA	NA	NA	NA	DPOS	NA	NA	NA

Fig 2.1 Top ten Cryptocurrencies

B. Wallets:

Cryptocurrencies manage the user identities for his security purpose using long random sequences of character is called public key and private key. Public key is nothing but public username and private key is secret password. Cryptocurrency wallets are software which is used to store, create, manage the keys, for performing the transaction. Some of open-source and community and commercial entities are release variety of wallets have high security and feature like rich user interface. Example like hierarchical deterministic (HD) wallets which is privacy preserving wallet also it provide extra layer of protection for allowing user. It has some other notable feature like currency exchange, debit cards, zero-fee off-chain and on-chain, linked credit, key recovery services, insurance coverage.

Wallets are two types cold storage wallets and hot storage wallets. Cold storage wallets are offline and it actually connect with online when user perform

transaction. This type of wallets are basically hardware wallets. The challenge of this wallet it is not safe to carry physically. Apart from that hot wallets are connected to store online information. Hot wallets are in the form of mobile or desktop applications. And these wallets are sometimes insecure due to accessibility through internet.

Some other types of wallets are simplified payment verification (SPV) wallet, Multisignature wallets, brain wallets. Multisignature wallets are like joint account in traditional bank system. It has multiple private keys to tranfer currency. SPV wallets are ligh-weight, fast and storage-sufficient.

Wallet	Type	No. of cur-rencies	Easy of use	Security level	Anonymity	Cold Stor-age	Fees/ Cost	User Con-trol	Hosted	Decen.	Validation	HD	MFA	Open Sourc	Integrated Ex-change
Ledger Nano S [46]	hardware	1000+	average	high	high	yes	70 USD	yes	no	yes	SPV	yes	2FA	yes	no
Ledger Blue [54]	hardware	1000+	easy	high	high	yes	270 USD	yes	no	yes	SPV	yes	2FA	yes	no
KeepKey [55]	hardware	50+	difficult	high	medium	yes	129 USD	yes	no	yes	SPV	yes	no	no	no
Jaxx [56]	mobile, desktop	80+	average	medium	high	yes	free	yes	no	no	centralized	yes	no	no	yes
Trezor [57]	hardware	9	average	medium	medium	yes	EUR 149	yes	no	yes	full node	yes	2FA	yes	no
Guarda [58]	mobile, desktop, web	38	easy	medium	high	no	free	yes	yes	no	SPV	yes	no	yes	yes
Exodus [59]	desktop	100+	easy	medium	high	no	free	yes	yes	no	full node	yes	no	yes	yes
Ethos [60]	mobile	150+	easy	high	medium	no	free	yes	yes	yes	SPV	yes	3FA	no	no
Paytomat [61]	mobile	18+	easy	high	high	no	various	yes	no	no	centralized	yes	no	no	yes
Coinomi [62]	mobile, desktop	500+	easy	high	medium	yes	free	yes	yes	no	spv	yes	no	no	yes

Fig 2.2 Top Ten Cryptocurrency wallets

C. Online Exchanges

Online Exchanges are enable interplatform and cross platform. Exchanges are basically divided into category such as brokerage services, trading platforms and order booking exchanges. Brokerage services popular for buy and sell cryptocurrency. Order Booking exchanges include cryptocurrency trading engine. Trading includes digital product and services, national flat currencies. Exchange provides us services in two different modes 22% exchanges are large exchanges and 4% exchanges are small exchanges. By the risk of theft from internal security services exchanges enables Two factor authentication that is verify identity using password and passcode. To make exchanges highly secured the exchanges use three-factor authentications by add of hardware based digital identity verification mechanism.

D. Blockchain Technologies

Blockchain is distributed, decentralized ledger technology. It has complex mathematics and cryptographic function. Blockchain ensures creation of new currency. It operates as permissionless or permissioned. Permissionless means open and public blockchains and permissioned means private, cloud based blockchains.

Features of Blockchain are:

- Trustless = prevent currency control from central authority
- Decentralization = Reduce chance of hacking by adding complex mathematical functions to ensure scams and frauds.
- Distributed ledger Technology = to avoid unauthenticated / malicious record changes.
- Security and Privacy = Use of complex cryptography algorithm.
- Faster transaction

Blockchain technology has benefit to reduce exchange cost compared with centralized transaction such as payment networks, banks.

E. Stakeholders

Cryptocurrency stakeholders are:

1. Persons, Applications, Users who send and receive Cryptocurrency.

2. Service enablers, developers, companies all this provide development and trading platform for currencies.

3. Executives, Regulators companies and representatives design policies and design rules for legal and ethical use of cryptocurrency.

4. Validators the person who mine and validate transaction. It is also called Cryptocurrency miners.

Trust issues of cryptocurrency (disadvantages)

A. Price Manipulation and volatility:

As we know Cryptocurrency trade of online, open, and unregulated environments so equilibrium supply and demand keep changing continuously. The volatility of prices as we see it remains high because a lot of traders lose their money.

B. Insider Trading

In a traditional ecosystem, the government protects consumer rights and ensures compliance with conflicts. Cryptocurrencies are traded in open, unregulated environments and it is an open opportunity for developers, public and private cryptocurrency development companies. In insiders trading suddenly hikes and downfall in cryptocurrency because of regular customer lose their amount. To stop this insider trading needs to form self-regulation of cryptocurrencies with traders and technical teams.

C. Parallel and Shadow Economy

Parallel and shadow economics are opening up in cryptocurrencies. In a Parallel economy, people use cryptocurrency over fiat currency to perform transactions. But in Shadow Economy, the shadow economy is totally hidden and all the transactions of cryptocurrency are run over the dark web. Controlling cryptocurrency over the dark web is impossible to control. This shadow economy is a relative challenge to control.

D. Lack of transparency

A decentralized cryptocurrency system is open and has transparency which leads towards a more trustworthy system. To ability to understand the technical and non-technical results of cryptocurrency is a major bottleneck. Users must know the technical and non-technical details behind cryptocurrency, exchanges, wallets. To understand transaction prioritization mechanisms, trading cost, volatility rate, the momentum of currencies, transaction patterns, and awareness about trading rules and regulations on trading platforms to ensure the cryptocurrency ecosystem. The transparency in that system can be achieved by providing information on wallets and exchanges.

Wallet companies need to ensure educate users or traders about the storage of public and private keys in the wallet, security behind the wallet, key backup plans, support of currencies, and other features. And exchanges company should provide information to traders listed flat currencies and cryptocurrency, conversion rate and mechanism rate, the conversion process of cryptocurrency to fiat currency and fiat currency to cryptocurrency, transaction patterns. Apart from wallets and exchanges, users should be aware of technical infrastructure, fees calculation formulas. The lack of transparency leads to mistrust between cryptocurrency traders and the development community.

E. Governance and Regulations

Most of the cryptocurrencies are open trustworthy platforms for users, and because of this openness, it is a big attraction for malicious attackers and nonethical users. Because of this issue governments and developers trying to create a legally compliant cryptocurrency system. Cryptocurrency has various types of exchanges, payment networks without territorial considerations. Each territorial has different regulations. Therefore complexity in governing is a very big challenge.

F. Privacy and Security

The openness of the Cryptocurrencies ecosystem on decentralized networks raises privacy concerns. Because participants and privacy history are not fully exposed. Current currency ecosystem networks users are easily tracked because of their transaction patterns, public keys, and IP addresses. In privacy-preserving cryptocurrency, this is the main trust issue. Cryptocurrencies are decentralized in order to track attackers and fraudulent transactions are hard to find out.

ADVANTAGES AND DISADVANTAGES

Advantages :

a. It is in detail description of Trust issues of cryptocurrency.
b. It discuss key elements of Crypto Currency in very easy language.

Disadvantages :

a. It did not explain how blockchain plays important role for creation of cryptocurrency.
b. It did not discuss about mining.

[2] , "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf, Accessed: May 21, 2019.

INTRODUCTION

This is a base technical paper on Bitcoin Cryptocurrency which is written and published by anonymous developer Santoshi Nakamoto. In 2008 Santoshi Nakamoto publish that technical paper and from that Cryptocurrency comes into the picture. The identity of that developer has not been revealed yet no one knows about S. Nakamoto whether it is a group of people or a company or an individual developer.

The technical purely discussed peer-to-peer version of electronic cash that allows electronic payments to be sent directly from one person to another person online without using any central financial authority. To achieve this Digital Signature provides a solution for that main benefit is still lost trusted third party still required to prevent double-spending amount. The solution of the double-spending amount problem solves using a peer-to-peer network. The cost of transactions in fiat currency is more, limiting the minimum transaction size. And there is cutting of probability of small amount of transaction. In some cases, a certain percentage of fraud cannot be acceptable. Sometimes there is some issues like transfer limit, account hacked, transfer limit, High transfer charges.

So, to overcome such a problem electronic based payment system is based on cryptographic proof instead of trust. It allows transactions between two parties directly to each other without the need of a third party. It can be achieved through a proof-of-work algorithm to secure transactions and build trust. The message is broadcasted in-network and that message comes on each node of the network and is stored as a form of a digital notebook. So, no one can alter the transaction record.

The Paper Covers Following important points as follows:

- Transaction
- Timestamp Server
- Proof-of-work
- Network
- Simplified Payment Verification

- Privacy

DESCRIPTION

A. Transactions

It is defined as a transaction of electronic coin is a chain of digital signatures. Each user transfer coin to the next user with digital signing with hash of previous transactions. And the public key of owner added to the end of coin. It can be verify the signatures to verify the chain of ownership.

The problem in transaction user should not be spend double to verify that there are miners who verify transaction and check transaction double-spending. After every transaction the new coin issue to the miners. The problem with this entire money depends on company of miners so as we see every transaction just like a bank.

But In bank during transaction, they now the identity of user but here in this case miners don't know the identity of user all the information is encrypted form. All this accomplish without need of third party transaction is publicly announced and all the participants must be agree on that transaction. And then transaction proceed.

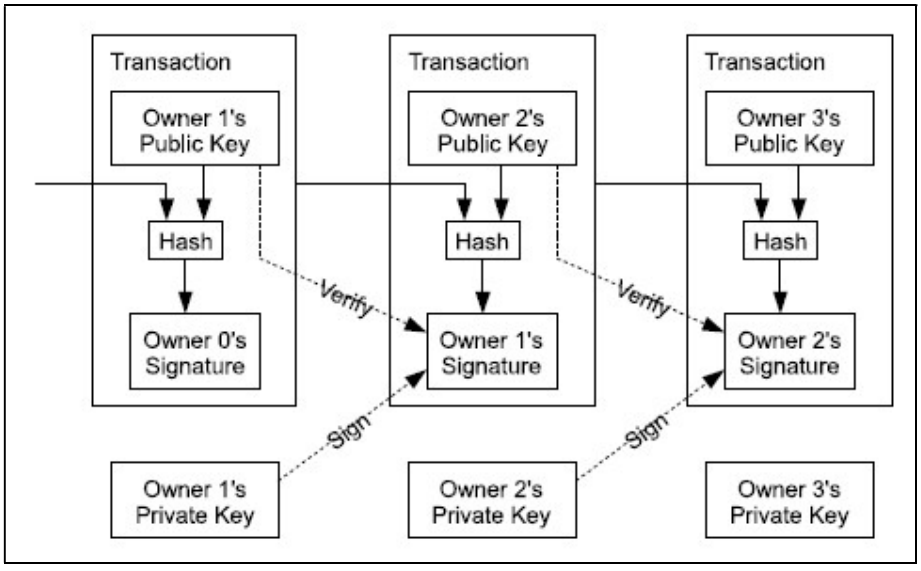


Fig 2.3 Transaction System

B. Timestamp Server

Timestamp proves that how much time need to data to get in hash. Each timestamp include previous hash and it forms a chain of that. With additional timestamp reinforcing the ones before it.

C. Proof of Work

To implement distributed timestamp on peer-to-peer basis we need proof of work. The proof of work scan hash value such as SHA-256 and that hash begin with 0 (zero) bits. The average work required in the number of zero bits required and that can be verified while execute hash.

For timestamp implement proof-of-work by increment nonce in the block value found and gives block hash value and proof-of-work satisfied and block can be chained.

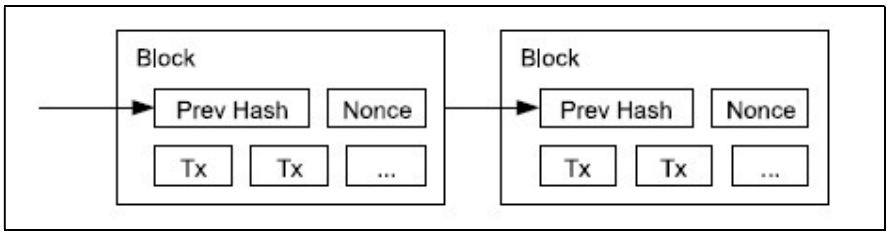


Fig 2.4 Proof of Work

D. Network

Following steps to require run network:

1) Firstly broadcast new transaction all over the network.
2) Then Each node should be collect new transaction into a block.
3) Each node finds proof-of-work and then it broadcast the block all over the network.
4) Node accepts the transaction if it is valid and not already spend.
5) At the end node express their acceptance and working on creating another block in the chain by accepting hash value of previous block

E. Simplified Payment Verification

To verify the payments without running full network node. The user only need a copy of header and long chain of proof oof work in which we are querying until the network gets convinced and Merkle branch linking that transaction block it's timestamped in. It doesn't check transaction and link them in chain.

As such verification depends on as long as honest control nodes in network. While network nodes verify transaction themselves. One security strategy to protects against

attackers it accept alert message when attacker tries to modify the transaction block and try to confirm.

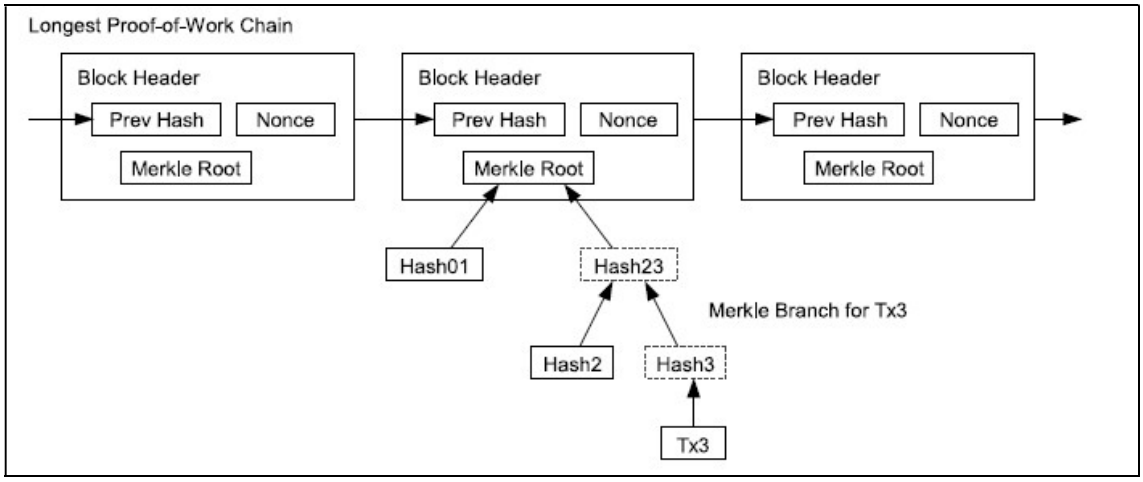


Fig 2.5 Payment Verification

F. Privacy

In traditional banking system privacy is maintained by restricting limited access of information and it has involved third parties. But in cryptocurrency announce transaction publicly, but privacy can be still maintained by breaking flow of information in another place. The public can able to see someone is sending amount to someone else without linking the transaction to anyone.

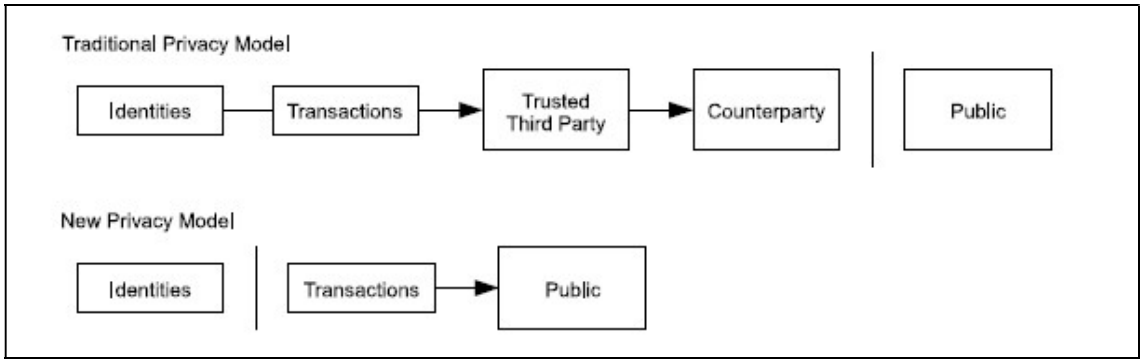


Fig 2.6 Privacy Model

ADVANTAGES AND DISADVANTAGES

Advantages :

a. This research paper tells about bitcoin cryptocurrency.
b. It tells how bitcoin transaction done.
c. It tells proof-of-work algorithm in easy manner.
d. It tells how bitcoin miners work.

Disadvantages :

a. It did not tell about price manipulation of bitcoin.
b. It did not tell about key trust issues of cryptocurrency.

[3] - Ehab Zaghloul, Tongtong Li, Matt W. Mutka, Jian Ren "Bitcoin and Blockchain: Security and Privacy" Page numbers-25 Date of Publication: 22 June 2020

INTRODUCTION

Blockchain technology is proposed to enable decentralized digital/online currency. Bitcoin cryptocurrency is widely used. Blockchain has widely been used in healthcare, e-voting, tracing sensor data, etc. In this, we can see a comprehensive review and analysis of major security and privacy issue of Bitcoin and blockchain. Then we will see types of attacks on cryptocurrency, three different types of wallets in terms of security, types of service, and their trade-offs.

To validate nodes referred to miners. And compute to mine group of transactions into a block and earn BTC. Mining is the process of solving hard crypt puzzles which are also called Proof-of-work (POW). It requires extensive computational power. The first software of Bitcoin which is implemented by Santoshi Nakamoto this is known as Bitcoin Core. It is an open-source project with a large number of developer communities contributing to it.

Bitcoin and many cryptocurrencies are appeared today and still continue to do today. The blockchain technology characteristic is shared by mainly emerging technology. The majority of this system clone with Bitcoin currency. The cryptocurrency is similar to other trading markets like the stock market with various trading platforms. This trading occurs continuously across the world virtually 24/7. Coin prices in cryptocurrency are continuously rising and dropping.

DESCRIPTION

Bitcoin Security and Network attacks

A. Denial of service Attack

DOS arracks floods the network with huge traffic to interrupt the legitimate services and also participating component connected to Bitcoin network. For example It DOS attack in mining pool it eliminates miners from mining pool and giving advantages to other miners. To avoid such attacks bitcoin developers continuously updating implementation. The newer version analyze network connection which is more closely try to eliminate suspicious nodes from connecting. Developer strives limit of transaction from being flooded through network.

B. Sybil Attack

Peer-to-peer attacks are vulnerable to cyber-attack. In this attacker send multiple pseudonymous identities from single network node. In that way attacker generate unfair number of shares on network IP addresses. The attacker can monopolize other connection of node and control the data propagating on them. The solution of that attack is is more convenient to have one-to-one relationship between computing nodes and vote instead of having one between an IP address and vote. An attacker reproducing multiple IP address but every node is busy in proof of work.

C. Eclipse Attack

Eclipse attack originally in to monopolize all outbound and inbound connection of node within peer-to-peer network. By monopolizing connection of node the attacker control and view blockchain node. The solution of attack populate the tried and new tables of nodes with bogus IP addresses by frequently sending the victim nodes unsolicited address messages. When the tables of nodes are full, they begin evicting random IP addresses to replace them with the newer ones.

D. Routing Attack

The purpose of routing attack intercept the transmitting message and make changes in them. The work present proposed a routing attack on Bitcoin via the Internet infrastructure. Border Gateway Protocol (BGP) is used for transmitting data between systems.

Bitcoin Network Privacy

All Bitcoin transaction are traceable, public, and permanently stored in Bitcoin network. Bitcoin address are only information used to define where bitcoins are allocated and where they are send. The addresses are created privately by each user's wallet. block chain is permanent, it's important to note that something not traceable currently may become trivial to

trace in the future. For these reasons, Bitcoin addresses should only be used once and users must be careful not to disclose their addresses.

Following Points to preserve privacy of Bitcoin Network:

1. Everytime use new address to receive payments.

   To protect privacy we should use new Bitcoin address at every time to receive new payments. Additionally we can use multiple different wallets to store our Bitcoins.

2. Be careful with public spaces

   Be careful not to publish information about transaction and purchase that allow someone identify Bitcoin address

3. Your IP address can be logged

   Hide your computers IP address with tool called Tor so it cannot be logged

4. Limitations of mixing services

   Some online services offers mix traceability between user by receiving and sending back the same amount using independent Bitcoin address.

ADVANTAGES AND DISADVANTAES

Advantages

a. It tells about bitcoin privacy.
b. This research paper discuss in detail about types of attacks on bitcoin.

Disadvantages

a. This paper only discuss about Bitcoin not all currencies.

Chapter 3

SYSTEM ARCHITECTURE OF BLOCKCHAIN CRYPTOCURRENCY

Cryptocurrency is digital currency transaction built on blockchain technology. The cryptocurrency transaction is decentralized.

The following diagram shows architecture of cryptocurrency:

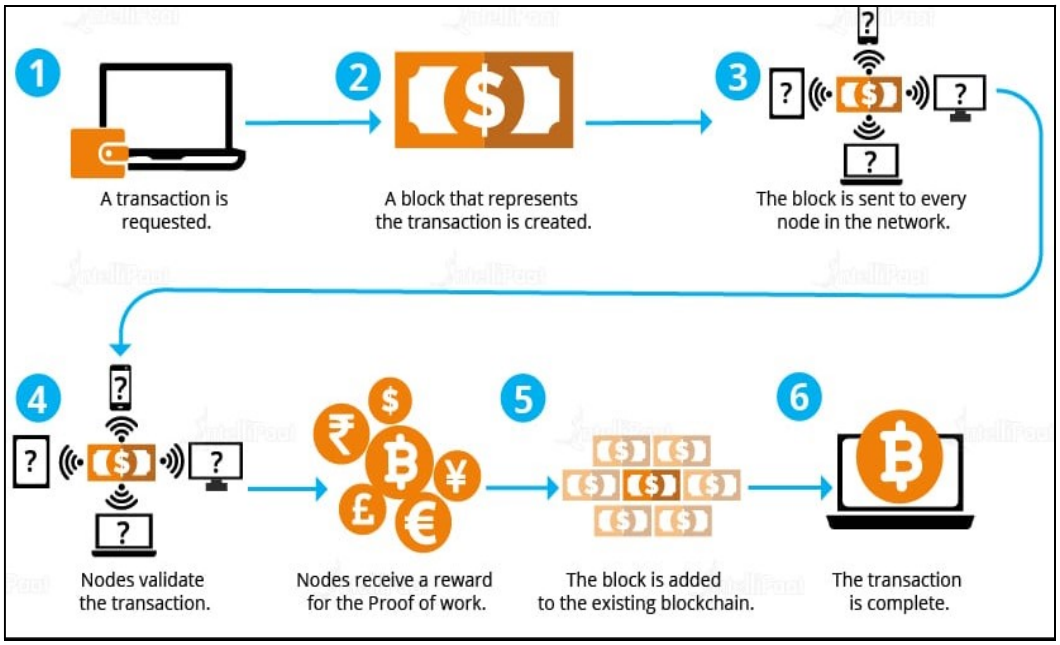


Fig 3.1 Crypto Currency Architecture

1) Transaction Requested :

   Firstly transaction is first initiated by the user. User can initiate transaction using cryptocurrencies online platform, Like eToro, Coinbase, Kraken, Bitfinex, Bittrex, Poloniex, CEX.IO etc.

2) Transaction Block created :

   The transaction block create which contains transaction information, hash whatever transaction we store according to that hash value create and hash of previous block. The block of transaction is called as geneces block. In this way chain of block is created.

3) Send the block :

Created block send in all over the network to proceed further process. To validate the transaction the block is send across the network.

4) Validate the Block :

   To check weather the block is valid the cryptocurrency miners are play important role miners solve difficult mathematical puzzles to validate the transaction block and this is called proof of work algorithm. And the miner who solve complex mathematical problem gets rewards. For solving this puzzles miners require very high CPU computational power. The miners who solve puzzles gets a rewards 6.5 Bitcoin when he/she doing bitcoin mining.

5) Block is added :

   Once block is validated by miners it is ready to added in public ledger. Ledger is nothing but digital notebook which has entry of all transaction records. And this block some time to add in blockchain based on currency for example Bitcoin need 10 Minute, Litecoin need 2.5 Minute to add block in Blockchain.

6) End the transaction :

   Once block of transaction added to the blockchain the transaction done successfully, cryptocurrency reach to destination user successfully. And here the initiated transaction ends. This transaction done without need of third party and within low cost.

ALGORITHMS (PROOF-OF-WORK)

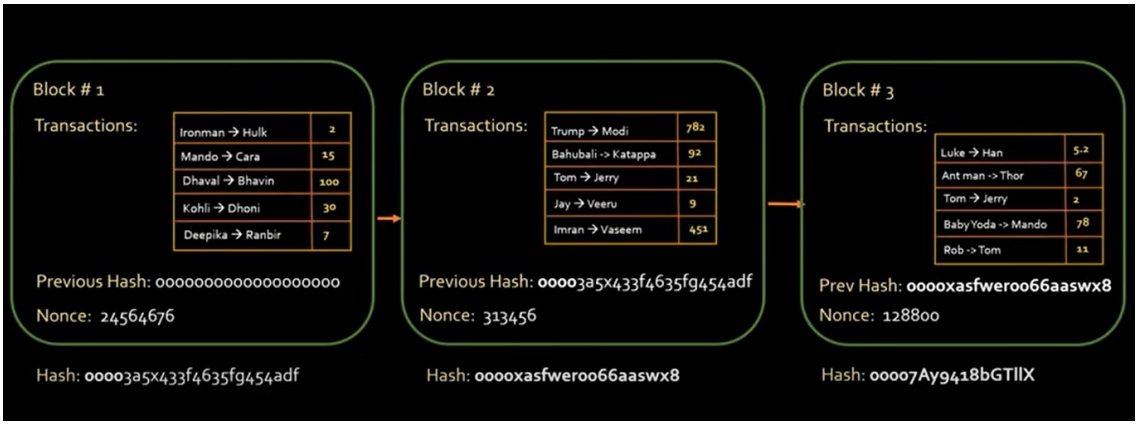
Cryptocurrency is nothing but a ledger. It has set of transaction. It is more like a bank account and at end it has balance. Let's us take example of Bitcoin to understand proof-of-work step by step.

Bitcoin ledger stores millions of transactions. It has millions of transactions since bitcoin was invented. It needs to store them in blocks storing them continuously is not possible so the blocks are stored in the form of liked list. First node which has address of next

node similar to those blocks are stored. Block size of Bitcoin is 1 MB. So, in 1 MB we store transactions and them move to next block for further transaction and all these blocks are linked together. Bitcoin has some security mechanism to avoid frauds for that it uses cryptography. It uses SHA256 cryptographic hash function to secure transactions.

In bitcoin or in a blockchain the actual block it has transaction, block number, previous hash and bitcoin protocol is such we need to convert whole block into string and we need to supply this function to SHA256 function and it produce a hash and the protocol of bitcoin require that first few digits are zero and how many digits it's changes time to time. Right now, it's 20 digits. So first few digits should be zero that is difficulty level.

So now it has only hash value we need to check first digits zero so new variable introduce i.e. nonce it is like number ones and add this number to the string and check weather number produce valid hash with first digits zero. We need to increment Nonce until we get valid hash. It is like a guess work. When we get correct nonce number then the block is valid and this process is called Bitcoin mining or proof-of-work algorithm. And the Bitcoin miners get reward and every four year reward gets half.



Difficulty level is 4

Fig 3.2 Bitcoin Mining Example

Python Code of Proof-of-work (Bitcoin Mining)

```
from hashlib import sha256
MAX_NONCE = 100000000000

def SHA256(text):
    return sha256(text.encode("ascii")).hexdigest()
```

```
def mine(block_number, transactions, previous_hash, prefix_zeros):
    prefix_str = '0'*prefix_zeros
    for nonce in range(MAX_NONCE):
        text = str(block_number) + transactions + previous_hash + str(nonce)
        new_hash = SHA256(text)
        if new_hash.startswith(prefix_str):
            print(f"Yay! Successfully mined bitcoins with nonce value:{nonce}")
            return new_hash

    raise BaseException(f"Couldn't find correct has after trying {MAX_NONCE} times")


if __name__=='__main__':
    transactions='''
    Apurva->Riya->20,
    Kajal->Priya->45
    '''
    difficulty=4
    import time
    start = time.time()
    print("start mining")
    new_hash =
mine(5,transactions,'0000000xa036944e29568d0cff17edbe038f81208fecf9a66be9a2b8321c6
ec7', difficulty)
    total_time = str((time.time() - start))
    print(f"end mining. Mining took: {total_time} seconds")
    print(new_hash)
```

Result

Fig 3.3 Bitcoin Mining Result

Chapter 4

APPLICATIONS OF CRYPTOCURRENCY

1) **Low Cost Transfer of Money**

   Well known use of cryptocurrency is sending and receiving money at low cost and high speed. For example sending of Litecoin (LTC) transaction need only two and half minute and cost of sending coin is just $0.40 transaction fees.

2) **Earn Interest on Bitcoin and other Cryptocurrencies**

   We can earn interest on crypto through popular examples includes DeFi lending and crypto staking. The interest offers on traditional bank is low all the time as compare to cryptocurrencies.

3) **Make private transaction**

   Privacy of digital currencies such as Monero (XMR), Zcash (ZEC) enables user to make anonymous financial transactions. Means any person can transfer without explain to the bank.

4) **Send non-cash transaction**

   Powerful use of cryptocurrency is non-cash transaction. Enables user to send non-cash transaction anywhere from the world, with low lost So this is very big of the cryptocurrency.

5) **Get paid for post contents**

   Worlds first blogging and social media platform for example Steemit, it enable publishers to receive the rewards in the form of digital currency i.e. cryptocurrency who provides high quality of content to network. Steemit boosts high number of customers.

6) **To Rent out your extra hard drive space to the cloud**

   Decentralized blockchain based cloud storage for example Storj allows user to earn cryptocurrency by exchanging their hard drives storage space to those need it on peer-to-peer basis.Storj is faster secured and cheaper cloud storage platform. Other than

Strorj decentralized cloud solutions are siacoin, Filecoin it not only provides cheaper and provide security.

7) **Travel the World**

Due to the growth of cryptocurrency past some years now it is possible to travel across world by spending cryptocurrency. Travel agents such as CheapAir and Destinia it accepts bitcoin as a payment method for book flights, hotels, car rentals. And those who wants to stay in apartments while travelling they can book using bitcoin (BTC) and ether (ETH).

8) **Buy a Lamborghini**

We can use Cryptocurrency to buy a Lamborghini. Bitcoins luxury marketplace DeLouvois enables the crypto rich to purchase sports cars. The marketplace also offers to buy luxury goods such as art, real estate, wines using digital pockets.

Chapter 5

COMPARISON OF Fiat CURRENCY AND CRYPTOCURRENCY

Basis	Fiat Currency	Crypto Currency
Definition	Fiat currency is controlled by Government and it is in physical form or maybe represent electronically.	Crypto Currency is decentralized digitally encrypted currency which is not linked to any Government. .
Issued By	Central authority	Operate independently
Intermediaries	Require for transaction	Not require
Unit	Dollar, Rupee, Pond, Euro	Bitcoin, Ether, Litecoin
Legal	Legal in all the countries	Not Legal in some countries
Exchanges	Exchanges can be in physical and online form	Exchange can be done only in online form
Tangibility	Fiat currency have tangible appearance in the form of coin and notes.	Crypto Currency cannot be touched or sensed in any way.
Storage	Fiat currency stored in bank	Crypto Currency stored in digital wallets

Table 1 Comparison Between Crypto Currency and Fiat Currency

CONCLUSION

I have studied Crypto Currency which is an interesting and exciting concept and which has the power to alter the global finance market better. Cryptocurrency is an impressive technical achievement, but it remains a monetary experiment. Even if cryptocurrencies survive, they may not fully displace fiat currencies. The technologies used in Crypto Currency are very interesting which provide security to the transaction. The interest of People in investing in cryptocurrency is increasing day by day because of less transaction cost, cost One day because of the power of cryptocurrency whole market will work on cryptocurrency.

REFERENCES

[1] Journal article- Muhammad Habib ur Rehman , Khaled Salah , Ernesto Damiani and Davor Svetinovic "Trust in Blockchain Cryptocurrency System" vol. 67 Page numbers-17 Month year -Nov. 2019

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf, Accessed: May 21, 2019.

[3] Journal article- Ehab Zaghloul, Tongtong Li, Matt W. Mutka, Jian Ren "Bitcoin and Blockchain: Security and Privacy" Page numbers-25 Date of Publication: 22 June 2020

Trust in Blockchain Cryptocurrency Ecosystem

Muhammad Habib ur Rehman, Khaled Salah, Ernesto Damiani, and Davor Svetinovic

***Abstract*—The recent growth in blockchain-based cryptocurrency ecosystem has been attracting researchers, developers, investors, regulators, and speculators to develop new economic and business models for trade, investment, and taxation. Currently, the cryptocurrency ecosystem is immature with multifaceted trust issues at all levels from technology providers to users and governments. In this article, we present a detailed analysis of trust issues in the cryptocurrency ecosystem, including a detailed taxonomic discussion of the key trust aspects including price manipulation, price volatility, insider trading, parallel economy, shadow economy, reputation systems, transparency, centrality, token economy, governance, regulations, design, usability, privacy, and security. We also present a comparative analysis of the top 10 cryptocurrencies that are holding about 85% of the total market capital. Finally, we present a detailed summary of the key trust issues and their potential immediate, short-term, and long-term solutions. This article reveals that significant effort is required to develop a fully trustworthy cryptocurrency ecosystem.**

***Index Terms*—Blockchain, cryptocurrency, privacy, security, trust.**

I. Introduction

BLOCKCHAIN-BASED cryptocurrencies have been continuously evolving as a new form of money during the last decade. Bitcoin, as the first cryptocurrency, has gained popularity because of its ability to address the centralization and double-spending issues [1]. Cryptocurrencies empower us to publicly transact over the Internet without approval of a centralized authority. Although the ideas behind cryptocurrencies are relatively old, Bitcoin has effectively integrated these ideas and it has gained the cryptocurrency market dominance [2]–[4]. The first Bitcoin was created on January 03, 2009, and the first notable transaction was made on May 22, 2010 when Laszlo Hanyecz purchased two pizzas for 10 000 Bitcoins. A decade since its inception, Bitcoin is still a leading cryptocurrency having 52.5% of the total market share among more than 2100 alternate cryptocurrencies.

Manuscript received May 8, 2019; revised July 30, 2019 and October 10, 2019; accepted October 18, 2019. This work was supported by Center for Cyber-Physical Systems, Khalifa University, UAE. Review of this manuscript was arranged by Department Editor K.-K. R. Choo. *(Corresponding author: Davor Svetinovic.)*

The authors are with the Center for Cyber-Physical Systems, Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi, United Arab Emirates (e-mail: muhammad.rehman@ku.ac.ae; khaled.salah@ku.ac.ae; ernesto.damiani@ku.ac.ae; davor.svetinovic@ku.ac.ae).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEM.2019.2948861

Blockchain, as an immutable distributed ledger, is the underlying technology behind cryptocurrencies. The core elements of blockchain include complex cryptographic functions for security and immutability, linear and nonlinear data structures to store, manage, and process cryptocurrency transactions, peer-to-peer (P2P) networks for multiparty transaction verification, and distributed consensus protocols to handle centralization and double-spending issues [5]. Considering the massive growth of the cryptocurrency market, with its total market value being $294+ billions USD, as on June 30 of 2019 [6], many big corporations are investing in cryptocurrencies to accept them as major trade instruments [7], [8]. However, the cryptocurrencies and their underlying technologies are still in their infancy and creating mistrust among many stakeholders. In this article, we present a detailed analysis of the cryptocurrency-related trust issues. As many of the presented issues will be related to the other blockchain-based systems, this work falls in the more general *blockchain trust* research area. In addition, we present a detailed review of previous work to outline the research gaps in this important area.

Since their inception, cryptocurrencies and the other blockchain technologies have attracted more attention from industry and investment sector than academia. As such, blockchain technology is probably one of the few research areas that is led by the industry practitioners instead of academic researchers. Therefore, to the best of our knowledge, the existing literature still lacks a comprehensive analysis of the issues and the open challenges that directly or indirectly affect the stakeholders' trust in the cryptocurrencies and blockchain technology in general. A few survey studies in cryptocurrency and blockchain domains are available but they are discussing these domains from different perspectives, e.g., Romano and Schmid [9] surveyed the literature for applications of blockchain technologies beyond cryptocurrencies, Berentsen and Schar [10] presented a short overview of cryptocurrencies from the perspective of Bitcoin, Bonneau [11] presented a detailed review of research challenges and issues related to Bitcoin and its blockchain system. Similarly, Zheng and Xie [12] presented an initial review of blockchain technologies and applications. Several other review papers were published by researchers to discuss specific research issues related to privacy of data in blockchain [13], [14], security challenges in blockchain [15]–[18], trust-free shared economy [19], generic strategies of software ecosystem in the context of cryptocurrencies [20], [21], blockchain architecture [22], scalability [23], and IoT–blockchain integration [24]. A few more initial studies were done by various authors [25]–[31]. However, none of the

studies focused on interweaved technical and nontechnical trust issues that are present in the cryptocurrency ecosystem.

The main contributions of this article are as follows:

1) We present the key elements of the cryptocurrency ecosystem and the role of different stakeholders in it.
2) We present a detailed risk analysis of different factors affecting the overall ecosystem.
3) We analyze key trust issues that directly or indirectly impact the adoption and trustworthiness of cryptocurrencies.
4) We compare the top ten cryptocurrencies and their underlying technology infrastructures to investigate the relative trustworthiness of each.
5) We present the gap analysis between state-of-the-art in academic research and industry research to find the major research challenges toward more trustworthy cryptocurrencies.
6) We outline a comprehensive short- and long-term research strategy to identify key research directions for future researchers to build more trustworthy cryptocurrencies.

The rest of this article is organized as follows. Section II presents the research method. Section III presents the preliminary discussion of the cryptocurrency ecosystem. Section IV outlines the taxonomy of trust issues in the cryptocurrency ecosystem. Section V presents the gap analysis between state-of-the-art and state-of-the-practice and the comparison of top 10 cryptocurrencies. This section also outlines the short- and long-term research agenda in order to develop trust among cryptocurrencies and key stakeholders. Finally, Section VI concludes this article.

II. Research Methodology

This article is a general domain system review study that combines a standard literature review with domain requirements elicitation in order to identify the domain trust requirements. As such, it suffers from general repeatability and completeness issues common to the review and survey studies. To deal with this problem, we have tried to complement requirements elicitation with systematic taxonomy development method and systematic literature review in order to minimize repeatability and completeness issues. In particular, in order to identify the key requirements, systems, and stakeholders and develop a coherent taxonomic discussion, we followed the taxonomy design method presented in [32]. The method consists of the following steps as depicted in Fig. 1:

1) Metacharacteristics: we determined the metacharacteristics of the objects of interest with the focus on the identification of the key elements of the cryptocurrency ecosystem. We collected and classified the data and literature considering relevant characteristics of all of the key elements. Based upon the inter-relatedness of the selected characteristics, we searched scholarly databases by executing different queries using the key search terms based on metacharacteristics: cryptocurrency, blockchain, trust, stakeholders, wallets, exchanges, payment networks, miners, mining systems, regulators, governance, users, blockchain operators, service enablers, developers, and validators. We ensured the coverage of the different combinations of key terms by following the systematic review research methodology presented in [33]. Fig. 2 presents the details of this process, while criteria for the inclusion, exclusion, and quality assessment are presented in Tables I and II, respectively. We used 14 main scholarly databases (Web of Science, IEEE Xplore, ACM digital library, ScienceDirect, SpringerLink, Wiley's Online Library, IET, Semantic Scholar, Microsoft Academic, CiteULike, CiteSeerX, DBLP, Google Scholar, and arXiv). In addition,

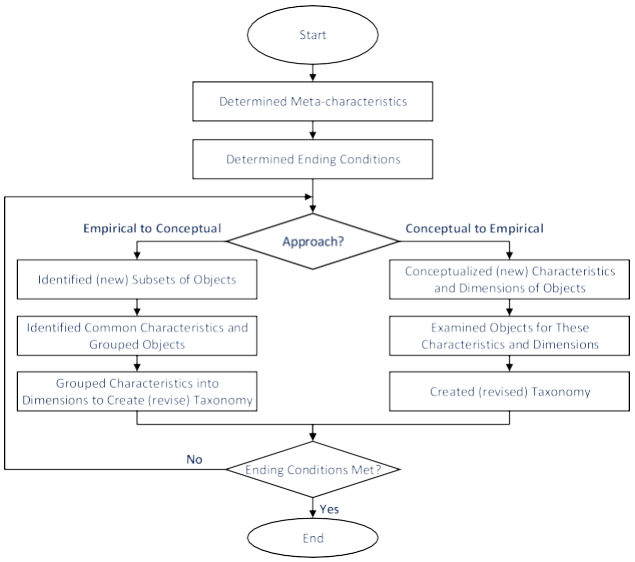


Fig. 1. Research method for taxonomy development [32].

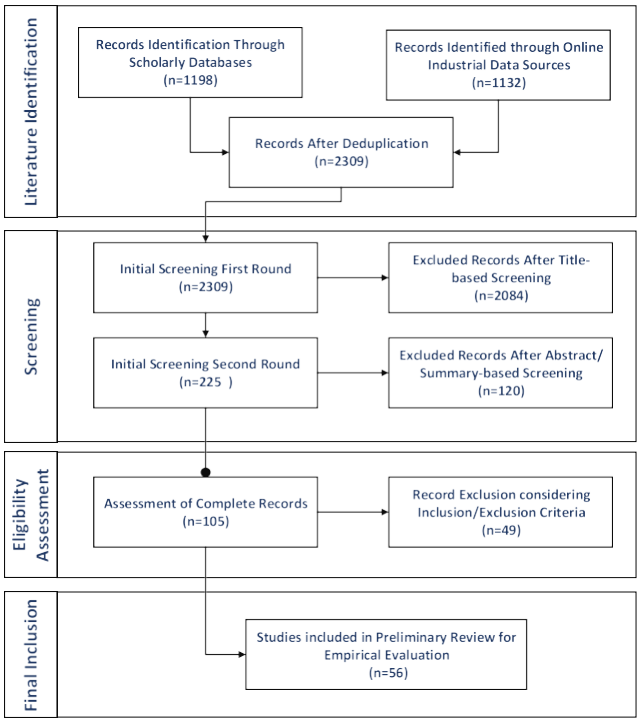


Fig. 2. Systematic literature collection and data analysis [33].

TABLE I
INCLUSION/EXCLUSION CRITERIA

	Inclusion Criteria (IC)
IC1:	Peer reviewed articles
IC2:	Articles discussing trust issues in cryptocurrency related blockchain systems
IC3:	Articles published by commercial blockchain operators on their web sites
IC4:	Technical white papers of blockchain developers
IC5:	Technical yellow papers of blockchain developers
IC6:	Inclusion of industry surveys and research reports with empirical data
IC7:	Inclusion of academic surveys and research reports with empirical data
	Exclusion Criteria (EC)
EC1:	Studies other than in English language
EC2:	Studies with abstracts only
EC3:	Articles discussing trust in fiat currencies, banking, and government regulating agencies
EC4:	Studies with proposal only without any validation or proof
EC5:	Studies with unclear reporting of results

TABLE II
QUALITY ASSESSMENT CRITERIA

QC1:	Context and environments are clearly stated
QC2:	Technical details of the ecosystem are provided
QC3:	The aims and objectives are clearly defined
QC4:	Contributions and limitations are stated
QC5:	Minimal biaseness in the study

we searched the web portals of the industrial contributors to find their white papers, code repositories, and technical specifications of the relevant cryptocurrency platforms.

2) Ending Conditions: we performed iterative analysis of the characteristics and further broke down these characteristics based on the semantic dissimilarity between the attributes in order to find the relevant literature and build the taxonomy. We ensured to come up with mutually exclusive and collectively exhaustive characteristics. These include cryptocurrency, blockchain, trust, stakeholders, wallets, exchanges, payment networks, miners, mining systems, regulators, governance, users, blockchain operators, service enablers, developers, and validators. The mutual exclusiveness was ensured through manual filtering, and ensuring, e.g., that a characteristic related to governance is not by mistake a characteristic that should be related to regulators, and vice versa.
3) Data Analysis: we iterated and combined top-down and bottom-up strategies to specify a unified taxonomy. While the published literature is diverse enough, for some characteristics, we found more data and for other characteristics only a few conceptual studies. Therefore, we conducted bottom-up analysis of the studies with enough data. Alternately, we performed top-down analysis of studies which had less supporting data.
4) Taxonomy Design: we explicitly checked if the subjective ending conditions are met at the end of each iteration. If we found enough data to meet the ending conditions, we included the relevant studies in the taxonomy; otherwise, we performed further iterations to find the empirical or conceptual data to meet the subjective ending conditions and updated the taxonomy. If we did not find enough data, we discarded the relevant characteristics under the observation.

Finally, the elicitation was done on 56 sources that contained data analyzed and evaluated in this article.

III. CRYPTOCURRENCY ECOSYSTEM

To analyze trust in the blockchain-based cryptocurrency ecosystem, we have to understand the key elements of the cryptocurrency ecosystem: cryptocurrencies, wallets, exchanges, mining systems, payment networks, blockchain systems, and key stakeholders.

A. *Cryptocurrency*

Dwyer [34] defines cryptocurrency as

> Bitcoin and similar digital currencies are called cryptocurrencies by some because the underlying algorithms and security are intimately related to digital cryptographic algorithms.

On top of security features, cryptocurrencies must ensure the basic three features of money, i.e., they must be exchangeable, measurable, and valuable. In addition, cryptocurrencies benefit by enabling extraneous features such as *pseudonymization* by hiding original identities of transacting stakeholders, *decentralization* by enabling multiparty transaction verification, *reduced transaction fees* as compared to traditional money transfer channels, *fast money transfer* by overcoming institutional and territorial hurdles, and *trustless* by eliminating third-party centralized trusted validators. Other desirable features include *convertibility* to other cryptocurrencies and fiat money, *irreversibility* that ensures that once a transaction is performed it cannot be rolled back, *rapid transaction settlement* by enabling quick value exchange between transacting parties, and *controlled supply* to maintain the right equilibrium and good intrinsic value. Despite having these advanced features, cryptocurrencies are still not mature enough to dominate the currency markets. A lot of efforts are needed in order to ensure trustworthy transactions between cryptocurrency stakeholders. There are more than 2100 active cryptocurrencies today. However, a few of them have gained in popularity. Table III presents key features of ten most widespread cryptocurrencies having almost 85% of total market capital [6], [35].

B. *Wallets*

Cryptocurrencies manage user identities using long random sequences of characters known as private keys (secret passwords) and public keys (public usernames). Wallets are software applications that are used to create, store, manage the keys, and to perform transactions. Cryptocurrencies come with their native wallets having the basic features, but the open-source community and commercial entities are releasing a variety of sophisticated wallets with enhanced security and feature-rich user

TABLE III
TOP-10 CRYPTOCURRENCY PLATFORMS

Cryptocurrency	Year of Launch	Maximun Supply	New Coin Creation Frequency	Tnx / Sec.	Network	Block Time	Consensu Mech-anism	Hashing Algo-rithm	Difficulty Ad-just-ment	Unit of Mea-sure-ment
Bitcoin [2]	2009	21 mn.	12.5 per block	7	NA	8 mins 40s	PoW	SHA256	2016 blocks	Satoshi
Ethereum [36]	2015	unlimited	3 per block	20	Ethereum	15 sec.	PoW	Sthash	1 block	Wei
Ripple [37]	2012	100 bn.	1 bn. per month	1500	RippleNet	near instant	NA	NA	1 blok	Drop
Bitcoin Cash [38]	2017	21 mn.	12.5 per block	60	NA	10 mins	PoW	SHA256	6 blocks	Satoshi
EOS [39]	2018	unlimited	upto 5%	2800	EOS.IO	0.5 sec.	DPOS	DPOS	NA	NA
Stellar [40]	2014	unlimited	upto 1%	1000	Stellar	5 sec.	NA	NA	1 block	Lumen
Litecoin [41]	2011	84 mn.	25 per block	56	NA	2.5 mins	PoW	Scrypt	2016 blocks	Photon
Tether [42]	2014	NA	NA	NA	NA	NA	NA	NA	NA	Tether
Bitcoin SV [43]	2018	21 mn.	12.5 per block	7	NA	10 mins 22s	PoW	SHA256	2016 blocks	Satoshi
Tron [44]	2017	100 bn.	NA	NA	NA	NA	DPOS	NA	NA	NA

interfaces for multiple cryptocurrencies. For example, privacy-preserving hierarchical deterministic (HD) wallets provide an extra layer of protection by allowing users to create mnemonics which are understandable and memorable phrases to replace long private keys [45]. In addition, HD wallets enable users to generate and associate multiple private keys with a single phrase in order to enhance security. Few other notable features include integrated currency exchange, linked credit and debit cards, key recovery services, zero-fee off-chain and on-chain transactions, insurance coverage, and support through email and SMS services. Due to these additional features, there exists a thin line between wallets and the cryptocurrency exchanges where most of the wallets offer overlapping features which were previously core features of the exchanges.

Wallets vary in the form of which type of storage they support: cold storage wallets and hot storage wallets. The cold storage wallets remain offline and they connect online only when a user needs to perform a transaction. These types of wallets include hardware wallets whereby a wallet software, private and public keys, and cryptocurrencies' balances are stored on the physical devices [46], [47]. Hardware wallets provide intrinsic security features and they can get online through any connected device. However, carrying and physically safeguarding these wallets is a challenge. Paper wallets are another type of cold storage wallets whereby users note their secret keys on a paper or generate and print the quick response (QR) codes of their secret keys. The destruction or loss of paper wallets is possible and therefore users tend to manage multiple copies of these paper wallets. Conversely, hot storage wallets normally remain connected to store online information. Hot storage wallets come in the form of mobile and desktop applications or these wallets are hosted on web and cloud servers. Mobile-based wallets store information in mobile applications and these wallets are considered to be highly insecure as compared to the other types of wallets [48]. Desktop-based wallets are used by downloading and installing the wallet applications on personal computers and these wallets are also considered to be insecure due to accessibility through the Internet [49]. Finally, cloud-based wallets are provided by third-party cloud service providers. Although these wallets operate in highly secure environments, handing over personal keys to cloud service providers is considered to be a risky decision [50].

Some additional types of wallets include multisignature wallets [51], simplified payment verification (SPV) wallets [52], and brain wallets [53]. The multisignature wallets are designed just like a joint account in traditional banking system whereby multiple account holders authenticate a transaction before it is processed by a bank. Similarly, multisignature wallets use multiple private keys before transferring money. Multisignature protocols are mostly used when multiple parties are involved in a transaction but they do not trust each other. In this case, multisignature wallets ensure agreement of majority before making any transaction [51]. SPV, on the other hand, are light-weight wallets and they operate without downloading the entire blockchain. SPV wallets rely on the their connected nodes which have full copy of the blockchain [52]. SPV wallets are fast and storage-efficient, and therefore these wallets are very useful for resource-constrained mobile devices. Finally, the brain wallets do not randomly generate complex cryptographic keys; instead, they ask the users to provide any random paraphrase and they create new combinations to generate private keys [53]. However, brain wallets are not as reliable as these wallets could be easily hacked. Most of the wallets charge from users in the form of either product fee, annual fee, or transaction fee in exchange for provision of quality services to the users. Table IV presents the comparison of the top 10 widely used cryptocurrency wallets. However, selection of wallets depends upon type and the amount of cryptocurrencies, frequency of usage, affordability of transaction fee, ability to carry physical wallets, privacy, security, and trust measures enabled by wallet providers.

C. Online Exchanges

Exchanges enable interplatform and cross-platform borderless transactions. Exchanges are categorized as brokerage services, order-booking exchanges, and trading platforms. The

TABLE IV
TOP-10 CRYPTOCURRENCY WALLETS

Wallet	Type	No. of currencies	Easy of use	Security level	Anonymity	Cold Storage	Fees/ Cost	User Control	Hosted	Decen.	Validation	HD	MFA	Open Source	Integrated Exchange
Ledger Nano S [46]	hardware	1000+	average	high	high	yes	70 USD	yes	no	yes	SPV	yes	2FA	yes	no
Ledger Blue [54]	hardware	1000+	easy	high	high	yes	270 USD	yes	no	yes	SPV	yes	2FA	yes	no
KeepKey [55]	hardware	50+	difficult	high	medium	yes	129 USD	yes	no	yes	SPV	yes	no	no	no
Jaxx [56]	mobile, desktop	80+	average	medium	high	yes	free	yes	no	no	centralized	yes	no	no	yes
Trezor [57]	hardware	9	average	medium	medium	yes	EUR 149	yes	no	yes	full node	yes	2FA	yes	no
Guarda [58]	mobile, desktop, web	38	easy	medium	high	no	free	yes	yes	no	SPV	yes	no	yes	yes
Exodus [59]	desktop	100+	easy	medium	high	no	free	yes	yes	no	full node	yes	no	yes	yes
Ethos [60]	mobile	150+	easy	high	medium	no	free	yes	yes	yes	SPV	yes	3FA	no	no
Paytomat [61]	mobile	18+	easy	high	high	no	various	yes	no	no	centralized	yes	no	no	yes
Coinomi [62]	mobile, desktop	500+	easy	high	medium	yes	free	yes	yes	no	spv	yes	no	no	yes

brokerage service exchanges are widely popular and they enable services to buy and sell cryptocurrencies. The order-booking exchanges provide services to use different cryptocurrency trading engines. The trading platforms provide interoperable services to connect multiple cryptocurrencies, national fiat currencies, and digital products and services. Depending on the size of an exchange, it operates either in one mode or in multiple modes. A market survey reports that small exchanges usually operate in one mode while large exchanges are providing services in two modes [63]. However, 22% of large exchanges and 4% of small exchanges are providing services in all three modes. The support for cryptocurrencies also varies in the exchanges. All of the surveyed exchanges support Bitcoin, followed by support of Ethereum and Litecoin by 43% and 35% of exchanges, respectively. Similarly, most of the exchanges (65%) support trading with USD followed by EUR (49%) and GBP (39%).

Despite being one of the main drivers of cryptocurrency ecosystem, exchanges face numerous operational challenges and need to consider many risk factors. Since small exchanges cannot ensure high monetary guarantee and user-base, large-scale banking institutions rarely rely on them. On the other hand, large exchanges put huge amount of users' money at risk, and therefore, the regulatory bodies closely observe and intervene in their operations. Security is the major risk factor since 73% of the exchanges keep users' private keys in their own custody [63]. Although the security is enabled by creating backup of users' keys using cold storage, the exchanges also use third-party security services for multisignature authentication. Large exchanges also hire specialized security staff for physical and virtual protection of the security setups but small exchanges mostly rely on the third-party security services. Despite all this, the risk of theft from internal security staff is always high and therefore exchanges enable two-factor authentication (i.e., verifying identities using passwords and pass-codes) and some exchanges use three-factor authentications by adding hardware-based digital identity verification mechanisms in the security setups.

D. Payment Networks

Payment companies operate as third-party bridging networks between cryptocurrencies and general economy. Payment networks are broadly categorized as payment rail (national currency-focused) and cryptocurrency payments (cryptocurrency-focused). The payment rail enables trade between the national currencies and cryptocurrencies at end-points (i.e., senders/receivers) using cryptocurrency exchanges in the middle of the networks. Payment rails are largely adopted to perform speedy cross-border transactions; however, due to pseudonymization of cryptocurrencies, these networks could not be easily monitored and regulated by governments. The payment rails provide money transfer services between individuals as well as business-to-business payments. Alternately, cryptocurrency payment networks ensure the use of cryptocurrencies at least at one end-point. These networks are used for merchant services to process payments for the merchants accepting cryptocurrencies. In addition, these networks could be used as general cryptocurrency platforms.

Recent market survey reports that 80% of payment networks use Bitcoin payment network [63]. The payment rails mix currencies in four ways: national-to-national (N2N) currency, national-to-cryptocurrency (N2C), cryptocurrency-to-national (C2N), and cryptocurrency-to-cryptocurrency (C2C). Majority of the transactions (67%) on the payment rails are either N2C or C2N, followed by N2N (27%) and C2C (6%). Another interesting fact was reported that cross-border transactions are generally higher value transactions which could be the reason that most cryptocurrency companies are operating from specific regions in North America and Europe. In the worst case, it could be the cases of money-laundering or illegal cross-border money transfers. It was also reported that consumers' payments to businesses normally account for low-amount transactions averaging US $210, followed by peer-to-peer (P2P) transfers averaging $351. The B2B transfers remained high and they averaged at about $1878. Despite the successful adoption by the individual users, consumers, and businesses, the payment

networks are facing difficulties in establishing working relationships with financial institutions and they need to bear the high cost of regulations. Sometimes, low liquidity in local markets also negatively impacts the payment networks.

E. Blockchain Technologies

We define blockchain as a *distributed and decentralized ledger technology spanning across peer to peer networks and ensuring immutability using complex mathematics of cryptographic functions.* The intrinsic value of a cryptocurrency is determined by the properties and functionality of the underlying blockchain system. Blockchain systems ensure the creation of the new currency coins since most of the top 10 cryptocurrencies use proof-of-work as the consensus mechanism but they also enable tamper-proof distributed ledgers to perform transactions without centralized intermediaries. Blockchain systems operate as permissionless (open, public blockchains) or permissioned systems (private, consortium, and cloud-based blockchains). We have discussed the details of these blockchains in our previous work [64].

A blockchain system must provide some basic features in order to ensure a foolproof and trustworthy platform for cryptocurrencies. These features include:

1) *trustless*—to prevent currency control and manipulation by centralized entities.
2) *decentralization*—to enable a decentralized system across P2P networks in order to delegate control to the users, to remove centralized points of failure, to reduce the chances of hacking by enabling complex mathematics of cryptographic functions, to ensure zero scams and frauds by enabling algorithmic approaches instead of designing people-oriented systems, and to ensure authenticity and transparency by designing open systems.
3) *distributed ledger technology*—to avoid malicious record changes, to ensure fair participation of users, to implement uniform participation rules across the network, and to provide updated local copy of the database at each node.
4) *tamper-proof environment*—to ensure the committed and verified transactions cannot be altered or deleted.
5) *security and privacy*—to use computationally complex cryptography algorithms and anonymization using hash keys.
6) *consensus mechanism*—to exercise the agreement between majority nodes in the P2P network.
7) *faster transactions*—to delegate system control to algorithms instead of users.

Blockchain technologies also benefit the cryptocurrency users by reducing the transaction processing fees as compared to centralized transaction processing systems such as banks, payment networks, and exchanges.

F. Mining Systems

Bitcoin has a self-adjusting distributed consensus protocol to maintain the distributed ledger in a decentralized manner [2]. In order to maintain the right supply of new coins in the system, Bitcoin introduced the concept of proof-of-work mining whereby validators are asked to randomly find the hash keys with particular properties in order to verify the new waiting transactions and add them in the next block. The validators with correct guess get rewarded with a specific amount of Bitcoins. Initially, in 2009, the mining was started with CPUs but due to the self-adjusting behavior, it became hard to guess the correct hash keys which required more sophisticated computing systems. Several new types of Bitcoin mining systems exist these days which include graphics processing unit (GPU) miners, field programmable gate array (FPGA) miners, application-specific integrated circuit (ASIC) miners, professional Bitcoin mining farms, large mining pools, cloud-mining, mobile mining, and remote-mining (via web-browser), to name a few. Each of these mining systems works differently and has its own advantages and disadvantages. However, it is quite hard to decide whether mining is profitable or not. The profitability of mining depends upon multiple factors, such as hash rate (the computing power to perform number of guesses in a specific time), block reward (the number of coins rewarded to successful miners), mining difficulty (the proportion of total computing power in the network and the desired new blocks to be generated in the cryptocurrency system), electricity rate, power consumption by mining systems, pool fees (the amount of coins charged to manage mining pool), price of coin, and how the difficulty will increase in the future.

G. Stakeholders

The main cryptocurrency stakeholders are as follows:

1) *Users*, persons, applications, or systems who send or receive coins.
2) *Service-enablers*, individual developers, or companies, who provide development and trading platforms for cryptocurrencies.
3) *Regulators*, executives, companies, representatives, or consortium, who design policies, operating frameworks, rules, and procedures for legal and ethical use of cryptocurrency systems.
4) *Validators*, the person(s) or companies who mine the cryptocurrencies and validate the transactions.

Table V presents a detailed risk analysis of the cryptocurrency ecosystem and its impact on the different stakeholders [63].

IV. Results

The term *trust* in the blockchain technology community has never been formalized or quantified. Different researchers tend to use this term from different perspectives, e.g., [65]–[68]. Considering cryptocurrencies, Wang [69] treats trust as a "synonym of consensus mechanisms in cryptocurrencies" and links it with privacy, scalability, and security of blockchain systems. Similarly, Pérez-Marco [70] presents blockchain as a "trust machine" for cryptocurrencies and highlights several Bitcoin-related blockchain features to enable trustworthy cryptocurrency ecosystem. Likewise, Gurguc and Knottenbelt [71] describe trust as the implication of data and system-related privacy issues in blockchain technologies. Although there are multiple facets of trustworthy cryptocurrency systems, the community has agreed on the fact that solving the inherent technical and nontechnical

TABLE V
RISK ANALYSIS OF THE CRYPTOCURRENCY ECOSYSTEM WITH RESPECT TO STAKEHOLDERS

Domain	Risk Factors	Stakeholders			
		Users	Service-enables	Validators	Regulators
Cryptocurrency	Loss/destruction of private key	high	no risk	no risk	no risk
	Cybersecurity risks including malicious activities	high	high	high	variab e
	Risks during P2P transactions	high	variab e	variab e	no risk
	Loss of confidence in digital currencies	variab e	high	high	no risk
	Regulations for cryptocurrencies	variab e	variab e	variab e	ow
	Taxation of cryptocurrencies	variab e	high	high	variab e
	Cryptocurrency momentum	variable	variable	high	variable
	Positive investor attention	variab e	no risk	no risk	no risk
	Negative investor attention	high	high	high	ow
	Crypto-volatility	variab e	high	high	no risk
	Currency-conversion	variab e	variab e	variab e	no risk
	Longevity of cryptocurrencies	ow	ow	ow	no risk
	Market manipulations	high	high	medium	no risk
	Exiting market	variab e	variab e	variab e	no risk
	Crypto-scams	high	variab e	ow	ow
	User address error	high	ow	no risk	no risk
	Failure of governance	high	variab e	variab e	high
Wallets	Regulations for wallets	variab e	variab e	no risk	no risk
	Spoofing payment information and phishing	high	variab e	no risk	no risk
	Loss of wallet file	high	no risk	no risk	no risk
	Hacking a wallet	high	no risk	no risk	no risk
	Destruction of paper wallet or Loss of hardware wallet	high	no risk	no risk	no risk
Exchanges	Risks during P2P transactions	variab e	variab e	variab e	medium
	Regulations for exchanges	variab e	variab e	no risk	no risk
	Hacking an exchange	high	high	variab e	no risk
	Exchange market manipulations	variab e	ow	variab e	variab e
	Detection of money-laundering	high	high	high	no risk
	Taxation	variab e	variab e	variab e	ow
	Financial services regulation	variab e	variab e	variab e	ow
Payment Networks	Hacking a payment gateway	variab e	high	ow	no risk
	Transaction processing time	variab e	variab e	medium	no risk
	Currency exchange risk	variab e	variab e	variab e	no risk
	Regulations	variab e	variab e	no risk	no risk
Blockchain Technology	Regulations for blockchain technologies	variab e	variab e	variab e	no risk
	Network performance	ow	high	high	no risk
	Forks	medium	high	high	no risk
	Security attacks	high	high	high	no risk
	Settlement issues Due to irreversibility	high	no risk	no risk	no risk
	Consensus and governance	no risk	medium	high	no risk
	Platform development/continuity/open source community	variab e	high	high	no risk
	Privacy compromises	high	high	variab e	no risk
	Legal issues	variab e	high	high	no risk
Mining Systems	Regulations for miners	no risk	high	high	no risk
	Power consumption	no risk	variab e	variab e	no risk
	Cost of hardware	no risk	variab e	high	no risk
	Reduction in mining rewards	ow	ow	high	no risk
	Miners leaving the networks	no risk	no risk	no risk	no risk
	Large pool size	no risk	no risk	high	no risk
	Unusual growth of miners	no risk	no risk	high risk	no risk
Overall Ecosystem	Jurisdiction of government entities	variab e	variab e	variab e	high
	Leading economists/industrialists/thought leaders' tendency	variab e	variab e	variab e	no risk
	Cyber-crimes and dark Web	high	high	no risk	high
	Impact of politics	variab e	high	high	high
	Uncertain regulatory frameworks	high	high	high	high
	Demand and supply of cryptocurrencies	variab e	no risk	variab e	no risk
	Failure to obtain, maintain, or renew licenses and permits	high	high	high	no risk
	Interference of government entities	ow	medium	variab e	no risk
	Burdens of applicable laws, regulations, and standards	high	high	high	no risk
	Consumer protection	no risk	variab e	variab e	no risk
	Unlawful or arbitrary government actions	high	high	high	ow

issues in cryptocurrency platforms can lead toward more trustworthy, inclusive, and participative cryptocurrency economy. Considering this notion, we performed a detailed analysis of the top 10 cryptocurrency platforms as presented in Table III. Fig. 3 presents the detailed taxonomy of the trust issues that we identified through the analysis of these 10 cryptocurrency platforms.

A. Price Manipulations and Volatility

Considering the basic properties of money, cryptocurrencies are a significant attraction for malicious stakeholders. Cryptocurrencies seem more vulnerable and easier accessible as compared to the physical currencies. To this end, cryptocurrencies face multiple monetary issues.

Since cryptocurrencies are traded in open, online, and unregulated environments, the equilibrium of supply and demand keeps changing continuously. The equilibrium moves positively when the quantity of bought cryptocurrency increases compared to sold cryptocurrency, and vice versa. However, the volatility in prices can remain high and traders can make or loose a lot of money fast. Different actors such as high-volume transacting users, exchange-level manipulators, and technology bots try

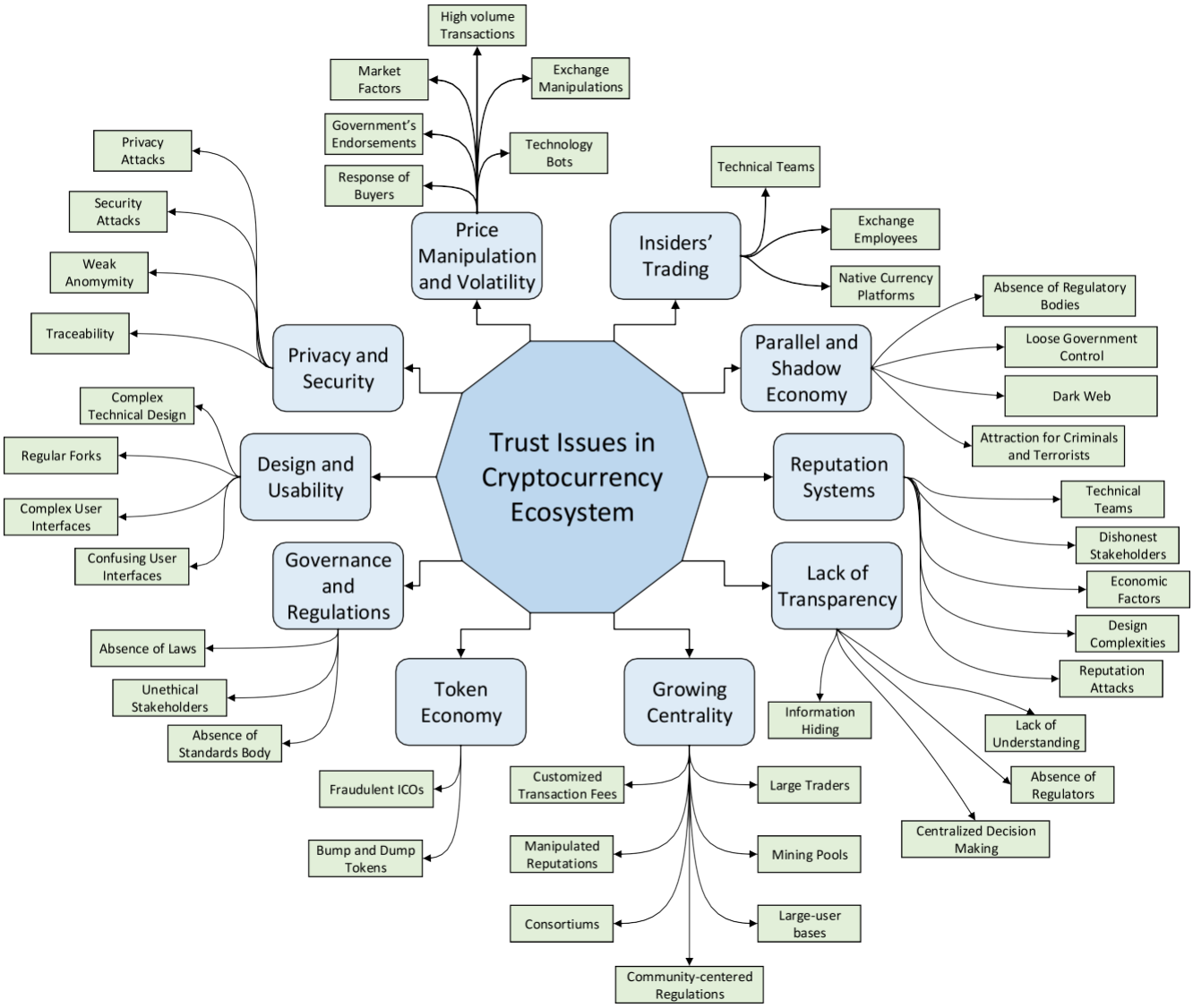


Fig. 3. Blockchain trust issues.

to manipulate the prices of the cryptocurrency [5], [72]–[74]. On the other end, different market factors, such as collective optimism that influence peers to trade cryptocurrencies, endorsements by government authorities, response of buyers to newly launched massively marketed cryptocurrencies, and the tendency of big investors toward a cryptocurrency, can drive up the prices of these cryptocurrencies.

Researchers started finding the potential reasons behind upsurge in Bitcoin's price which reached $19 783 USD in December 2017. Some believe that Bitcoin's price was mainly manipulated by cryptocurrency exchanges Bitfinex and Krakan who massively traded in a newly launched coin Tether [75]. Tether was said to be a stable coin because it was supposed to preserve $1 USD value in exchange for each Tether. However, this money was never tracked by auditors and law-enforcement agencies. The authors believe that the upsurge in Bitcoin's price happened due to a strong correlation between Tether and Bitcoin's mutual trade but interestingly the price of Tether remained almost unchanged while the price of Bitcoin increased from $1000 USD to $19 783 within 12 months. Despite these reservations, it is almost impossible to track price manipulation activities because of the absence of regulatory and legal enforcement bodies. These bodies could try to stop price manipulations by restricting cryptocurrency trade by putting a maximum limit for users or by enforcing high taxation and transaction fees, but both of these ideas are against the vision behind the cryptocurrencies. To address the issues of price manipulations and high volatility, a few alternate stable coins [76]–[78] were proposed by researchers but they did not received high attention from users and cryptocurrency community.

B. Insider Trading

When dealing with traditional economies, governments can protect the consumer rights and ensure the compliance of conflict of interests. Since cryptocurrencies are traded in open,

anonymized, and unregulated environments, they open an opportunity for technical development teams of public cryptocurrencies and employees of private and consortium blockchain-based cryptocurrencies development companies to proactively buy or sell coins and make profit [79]. The insider trading results in sudden hikes and downfalls of cryptocurrencies where regular customers loose their money. The insider trading could be stopped by some form of self-regulation of cryptocurrencies within the technical teams and general traders [80].

Exchanges, especially with cold storage, are an easy target for insider trading since the employees can access the transaction histories and uncover hidden patterns. In addition, early information about upcoming currency launch or listing or delisting at exchanges gives them an edge to perform early trades and manipulate the prices. Similarly, the employees of these exchanges can act proactively by considering early classified information from cryptocurrency companies and government agencies. A similar case was reported when Bitcoin Cash (which has branched from Bitcoin) saw an early hike in its prices [81]. The experts termed it as an insider's activity from a Coinbase (popular exchange) employee who was aware about Bitcoin Cash listing on their exchange and bought early tokens which resulted in sudden upsurge in coin's value [81]. The authorities investigated but no clue was found about such malicious activity.

C. Parallel and Shadow Economy

The centralized control results in well-regulated trade of fiat currencies considering ethical and legal boundaries of the societies. However, cryptocurrencies are opening up the parallel and shadow economies [82], [83]. In parallel economic systems, people prefer to use cryptocurrencies over fiat currencies in order to perform various financial transactions. Shadow economy is totally hidden from authorities and all the transactions and operations of cryptocurrencies run over the dark web. Since controlling the cryptocurrencies in the dark web is almost impossible, the shadow economies represent a relative challenge for governments to control. Governments are taking measures to control and regulate the parallel economies but there is insignificant progress so far to control the shadow economies.

D. Reputation Systems

The reputation of a cryptocurrency and its users plays a vital role in establishing trust in the cryptocurrency ecosystem [84]. The reputations could be derived from certain quantitative measurements such as supply of circulated coins, current market cap, age of currency (the number of years since its launch), new coins creation frequency, transaction processing time, and time to create new blocks. These reputation measures can help in the initial decision-making to select a cryptocurrency. There are multiple qualitative attributes that derive the reputation and trust among all stakeholders in a cryptocurrency ecosystem [84]. The reputation of the network operators (the company, consortium, or technical team running the underlying network) is a primary concern. Similarly, the reputation of traders, miners, wallets, and exchanges also play a critical role in building trust in the cryptocurrency ecosystem [85]. Likewise, the economic factors such as demand and supply of coins, stability, and volatility of the cryptocurrency also play a critical role in establishing reputation of cryptocurrencies. Designing a reputation system for traders on the basis of quantitative data is relatively simple but inclusion of qualitative attributes increases complexity and it becomes challenging to design a feature-rich high-quality reputation system.

Since majority of traders are the weakest participants, a bad reputation system can deteriorate the trust of traders in the cryptocurrency ecosystem. For example, Ethereum emphasizes that a reputation system must enable three functions: filtration of honest stakeholders in the ecosystem, incentive mechanism to reduce cheating, and a point-system for intrinsic value creation. Achieving these three functions is quite challenging [86]. First, traders and miners social backgrounds and preferences vary according to location, culture, political system, and government policies; therefore, filtering honest traders and miners is a challenging task. Second, currency reputation systems rate the users but do not penalize cheating stakeholders. Third, cryptocurrencies facilitate the miners to produce more coins but lack the encouragement for traders to consume the coins. This is the main bottleneck because the surplus of coins leads toward inflation and lowers the intrinsic value and vice versa. Since the reputations are opinion-based strategies, the manipulation of opinions is another challenge in reputation systems design.

Reputation systems also need to handle few attacks such as long-con attack whereby one person portrays to act honestly and slowly builds his reputation and suddenly starts performing the malicious activities that negatively impact the cryptocurrency ecosystem [30]. The Sybil attack is another form of attack where one trader creates multiple user accounts and performs trading among those users to increase reputation of the selected accounts. This fake reputation can help the attacker to act as a reputed stakeholder in the system. The market attack can also impact the trustworthiness of cryptocurrency whereby different users cluster themselves in order to provide fake reputations and take control of the reputation system. Finally, double use attacks are another issue with reputation systems. This attack happens when a user A pretends that she has to receive a certain amount X of money from another reputed user B having account balance Y. Since $X < Y$, B starts trading with other users on the basis of connection with highly reputed user A and runs away. Current cryptocurrencies do not address such fractional reserve challenges.

E. Lack of Transparency

The decentralization of cryptocurrency systems enables openness and transparency which ideally leads toward a more trustworthy system. However, the ability to understand the technical and nontechnical implications of a cryptocurrency system is a major bottleneck [87]. Users must be able to know about the technical and nontechnical details and teams behind cryptocurrencies, wallets, exchanges, etc. The reputation of major traders also plays a vital role in establishing trust of traders. The information about validators and to whom the money is being transferred to also increases trust among traders, miners,

and regulators. The information about technology infrastructure and the ability to provide security and privacy to traders lead to increased trustworthiness of cryptocurrency systems. The ability to understand trading costs, transaction prioritization mechanisms, transaction patterns, momentum of currencies, volatility rate, estimated transaction processing time, and awareness about trading rules and regulations on trading platforms ensure trustworthiness in the cryptocurrency ecosystem [88].

The transparency in the ecosystem is also achieved by providing the essential information about wallets and exchanges [89]. Wallet companies ensure to educate traders about the storage processes of public and private keys, the underlying security and privacy measures, the persons responsible for the keys management, keys backup plans, support of currencies, and additional features other than key and currency management [48]. On the other hand, exchange companies should educate traders about listed fiat currencies and cryptocurrencies, the conversion rate computation mechanisms, the conversion process from cryptocurrencies to fiat currencies and vice versa, big transacting traders, transaction patterns on exchanges, comovement in the value of multiple currencies, transaction fees, and the implications of policies enforced by regulators and government agencies [89]. Apart from the wallets and exchanges, the payment networks also need to provide information about their technical teams and infrastructures, currency exchange mechanisms, fees calculation formulas, and insurance to enable complete money transfer. Miners and mining systems should also be open enough to provide transparent and accountable information to all stakeholders about miners, their locations, big mining systems, mining pools, mining share distributions, miners-wise coin creation patterns, average transaction processing time by each mining node, system, and pool, and the amount of mining fees earned by miners. Most of the newer cryptocurrencies and their underlying blockchain systems are being controlled by private companies and their consortiums which rules out the involvement of open-source development communities in the critical decision-making activities [36], [37]. This lack of transparency not only leads to mistrust between cryptocurrency blockchain operators and the development communities, but it also brings centrality which is against the essence of original vision behind Bitcoin and similar cryptocurrencies. The decentralization of the critical decision-making activities and blockchain governance operations could help in addressing this issue.

F. Growing Centrality

The essence of cryptocurrency systems lies in true decentralization. However, the attraction of the monetary value is leading toward centralization from multiple perspectives. At the individual level, traders try to accumulate more wealth by trading in multiple cryptocurrencies to strengthen their portfolios [2]. The user control to offer customized transactions fees also effects negatively whereby specific users easily get their transactions processed while nonpaying users remain in the queue. Similarly, validators try to increase their reputation in order to effect the transaction processing mechanisms and grab mining fees as compared to small and nonreputed mining systems [90]. At the company level, different stakeholders form consortiums and launch new currencies to grab their share from cryptocurrency markets and also retain their traditional noncrypto trading [37]. Different mining groups and mining systems gather together to form large mining pools where most of the transaction fees go to these pools while individual and small miners not being able to get a reasonable share.

Wallets and exchanges also face a growing impact of centrality since these platforms try to support multiple cryptocurrencies and fiat currencies in order to increase their user base. This effort results in large user base at one end but it also increases the chances of security attacks and privacy compromises. Since most of the exchanges are operated by single companies having centralized infrastructure, this also leads to increased centrality. Although a few exchanges have proposed decentralized mechanisms, the level of centrality still remains high because of low adoption and immature technologies. The development communities and blockchain operators try to hide the information from other developers, which increases centrality in decision-making and blockchain governance. Governments and regulators also try to develop the policies to protect a large segment of society. Community-based regulations and policies can affect many individuals negatively. The launch of government-supported cryptocurrencies is another factor of centrality because general population tends to trust more on governments instead of public cryptocurrencies since governments have more resources to compensate losses due to various security and privacy problems.

G. Token Economy

Unlike fiat currencies that are printed, circulated, and controlled by government organizations, the value of cryptocurrencies is determined by the number of circulating tokens (coins) in crypto-markets. The fraudulent initial coin offerings (ICOs) and pump-and-dump strategies for cryptocurrency coins are two major issues in token economy [91].

The ability to create new tokens (launching new cryptocurrencies) on top of existing cryptocurrency platforms is a major attraction for fraudsters and thieves [92], [93]. For example, the ERC20 (a standard contract on Ethereum) enables us to create a new token on top of the Ethereum network and it can be listed and traded across all Ethereum-supporting wallets and exchanges. Many fraudulent ICOs emerged in recent years due to this easy creation and launch of new cryptocurrencies [94]. The fraudulent ICOs quickly collect money from traders by selling their tokens in exchange for other cryptocurrencies and suddenly disappear from the cryptocurrency market [95]. A recent study reports that 80% of newly launched ICOs in the year 2017 were scams [96]. These frauds happened because of the sudden upsurge in cryptocurrency market in year 2017 whereby almost all currencies gained momentum due to the Bitcoin's price hike. The study reports that more than 150 scammers were publicly identified whereby top 10 scams costed about $687.4 million USD to investors. These top 10 scammers included Pincoin, Plexcoin, Bitcard, Opair, Benebit, Bitconnect,

Confido, REcoin, Ponziecoin, and Karbon. Despite these scams, traders kept investing in ICOs in 2018—they invested about $7.8 billion USD in total—but the investments gradually decreased from $1.5 billion USD in January to $74.5 million USD in December [97].

Pumping and dumping of coin values is another major trust-related issue in the token economy. The pumping and dumping activities are usually performed by a group of individuals who try to manipulate the coin prices to maximize their profit during trading [98]. These groups are well organized and well connected behind the scene through social media channels and chat groups such as Telegram. First, they announce the schedule of their activities. They pump the price of coins by speed-buying (which occurs usually within the seconds of starting the scheduled time) and when the price reaches at a reasonably high level, they quickly sell the coins. Since most of them make early purchases, they end up selling their coins with a marginal profit. The span of pumping and dumping lifecycles is usually very short (up to a few minutes) and therefore these activities do not affect the large user base of cryptocurrency traders on the platform [99]. However, buying and selling during pump-and-dump lifecycle could become disastrous for some traders. Researchers analyzed different chat histories and social media groups and advised to minimize pump-and-dump activities by aggressive regulations at cryptocurrency trading platforms and at government levels [100]. However, they also conclude that due to deliberate involvements of some cryptocurrency exchanges in these activities, it will be hard to regulate cryptocurrency trade at the platform level. However, few efforts are being made at the government level [101].

H. Governance and Regulations

Most cryptocurrencies are envisioned to create an open trustworthy platforms for traders; however, this openness becomes a big attraction for malicious attackers and nonethical users. Considering these issues, governments and cryptocurrency developers are trying to create a legally and ethically compliant cryptocurrency ecosystem. The governance and regulation measures have two facets. The cryptocurrency ecosystem needs to be interoperable with various types of exchanges and payment networks without territorial considerations. However, each territory, even within a country, may have different regulations. Therefore, the complexity in governing the overall ecosystem is a big challenge. The inability to understand the technical implications of the technologies behind cryptocurrencies, the availability of platforms for everyone, the absence or limitations of the regulating laws, the reluctance of the main economic players such as banks and other financial institutions to fully adopt the cryptocurrency ecosystem, and the resistance from the public representatives to approve new laws and regulations are the pressing issues which need to be addressed in order to run a governable, trustworthy, and regulated cryptocurrency ecosystem. In addition to the core cryptocurrency-related trust issues, investors and traders should also consider social [102] and financial factors [103] for investments at both macro and micro levels.

I. Design and Usability

The design and usability are the key drivers of increasing trust of nonexpert participants in the cryptocurrency ecosystem. The current ecosystem is mainly benefiting the technical audience who have good understanding of the underlying technologies and their implications [104]. However, this technical audience is very limited so that it is increasing centrality and distrust. The issue arises when the users find technical issues or flaws in the cryptocurrencies and instantly try to fork the system. In addition, technically aware participants can try to manipulate cryptocurrencies by performing algorithmic changes in the underlying systems. Therefore, all cryptocurrency platforms need to train their participants to increase the trust as well as the usability [105].

Hiding technical details from the users and providing simple user interfaces are the basic design principles of technology-based systems. Considering the openness of cryptocurrency ecosystem where both data and source code are available for public use, it is almost impossible to implement these design principles. Therefore, almost all the cryptocurrencies provide complex user interfaces as compared to their traditional rivals such as banking institutions and currency exchanges [106]. Cryptocurrency traders cannot link their bank accounts or credit cards information with most of the wallets and the users have to understand most of the technical details before transacting on the networks. Traditional banking solutions provide an easier user interface to enhance user experiences. Wallets complement most of the usability requirements; however, most of the exchanges provide quite complex and confusing user interfaces and therefore nonexpert users do not fully trust these exchanges [89]. The major issues with exchanges include provision of multiple types of histories such as deposit history, withdrawal history, trade history, transfer history, marketplace history, and referral history to name a few. In addition, confusing instructions to manage public and private keys decrease reliability of the systems. Similarly, users do not know about the estimated time of transaction processing on majority of exchanges but have only a simple update notification with pending status. Despite these obvious problems, we have not found any research related to the design and usability issues of cryptocurrency exchanges.

J. Privacy and Security

The openness of cryptocurrencies on decentralized networks raises privacy concerns because neither the participants nor the transaction histories should be fully exposed. Considering current cryptocurrency networks, users could be relatively easily tracked through their transaction patterns, public keys, and IP addresses [107]. Therefore, privacy-preserving decentralized cryptocurrency networks are the main drivers of trust in the cryptocurrency ecosystem. In order to preserve privacy, a cryptocurrency must ensure that its users are untraceable and anonymous enough for potential security attacks and fraudulent transactions. Researchers presented a comprehensive survey on privacy-related issues in Bitcoin [16].

Privacy coins have been introduced to ensure the anonymity of users and to break the link between the senders and receivers.

Privacy coins follow the privacy-by-design principle whereby each possible privacy leakage issue is considered while designing the cryptocurrency systems. Few notable privacy coins include Zcash [108], Monero [109], and Dash [110]. Zcash is designed using a blockchain-variant of zero-knowledge proof algorithm [111] called zk-snarks [112]. The zk-snark solves the high computational complexity problem of conventional zero-knowledge proof algorithm by maintaining the privacy of senders. Monero uses a Ring Confidential Transaction protocol by enabling three privacy-preserving mechanisms: ring signatures to hide sender's identity, stealth addresses to protect users' IP addresses, and RingCT to hide transaction amounts. Dash uses CoinJoin method to combine individual payments against new hash addresses before performing transactions and it hides the information about individual users on the network [113]. Bulletproofs [114] are another variant of zero-knowledge proof algorithms which offer small proof size as compared to zk-Snark; however, it requires linear computation time as compared to logarithmic computation time of zk-snark. In addition, it relies on public-key cryptography which is a computationally expensive verification method. Researchers also used multiparty computation strategies for privacy preservation whereby they jointly compute function without revealing their input information [115].

Mixing services are another group of privacy-by-design strategies whereby the sender identity is obscured in order to stop the traceability of transactions [109]. Mixing services work both in centralized and decentralized settings. The centralized mixing services are run by currency operators who create new transactions, e.g., as it is in the case of Monero, but users have to trust the operators. Some operators offer accountable mixing services to develop the trust with the users. The decentralized mixing services (also known as n-party mix) are created and operated by anonymous users on the P2P networks [116]. Decentralized services provide more anonymity and user control, but finding the anonymous users for participation is a challenging task. Although mixing services are a feasible choice for users to preserve the privacy, these services also help enable trade on the dark web. Mixing services also need to address some research issues related to poor performance, Sybil attacks, incompatibility with Bitcoin, and denial of service.

Privacy and security are key requirements of trustworthy cryptocurrencies. Wallets and exchanges are perceived to provide secure environments for privacy-preserving tamper proof currency storage and transaction processing. However, the attackers can try to access these platforms to take the control of private keys and they also can try to change the security setup of these platforms [117]. In addition, they can try to manipulate transaction amounts and hash addresses during transaction processing. A number of security attacks have been reported in recent literature surveys [15], [17], [18], [118].

V. Evaluation and Threats to Validity

This section summarizes our findings through the gap analysis between state-of-the-art in academia and industry.

Ideally, the whole cryptocurrency ecosystem must run autonomously without any centralized entity in a fully trusted and dependable environment. The ecosystem must ensure the safe, secure, and equal-opportunity environment for all traders from small to big participants. At the cryptocurrency level, the companies need to ensure that their whole currency system is running autonomously without external and internal interference in technical infrastructures, their operations, and trading activities. However, considering the issues discussed in the previous section, the cryptocurrency ecosystem is still far away from the ideal vision. Table VI presents our comparison of the trust issues in the top 10 cryptocurrencies and Table VII presents our analysis of the open challenges toward increased blockchain trust in the cryptocurrency ecosystem.

Despite a significant total market cap, the mainstream traders and investors are still reluctant to adopt cryptocurrencies due to the trust issues including unavailability of data and internal information, lack of technical understandings, absence of laws and regulations, and lack of protection and insurance. Although the underlying blockchain technologies and infrastructures are capable to support user requirements, only a few cryptocurrencies have gained in popularity so far. This popularity has increased due to the Bitcoin upsurge in 2017 when Bitcoin's price hike lured the investors toward other altcoins which resulted in massive investments. At that time, a few altcoins such as Ether, Bitcoin Cash, and XRP also gained in popularity.

Considering the price manipulations and volatility, the cryptocurrencies are needed to ensure an adaptable coin supply instead of constant coin generations. The upper limit and fixed size generation of coins seem to be the major bottlenecks that result in a coin's upsurge and attraction of the malicious traders to perform pump and dump activities and insider trading. In addition to this, the regulatory frameworks and algorithmic interventions are needed to stop the price manipulations by exchange employees and technology bots. Lack of technical and financial understandings is another major concern which leads to lack of trust by the users.

The centralization and dishonesty are two major concerns in the cryptocurrency ecosystem which must be addressed. The strategies are needed to identify, penalize, and prevent dishonest traders, technical employees, miners, and fake coins. In addition, new algorithmic approaches are needed to stop the centralization efforts at all levels, from accumulation of massive amount of coins among a few users to keeping private keys at exchanges. This is necessary because, on one end, cryptocurrencies are neither inheritable nor recoverable, and on the other hand, these coins are exchanged with fiat money. Therefore, sudden death of cryptocurrency holder or loss of credentials leads to massive loss of wealth. New algorithmic approaches are needed to stop dishonest stakeholders from launching reputation attacks and taking control of cryptocurrency systems. In addition, dishonest stakeholders can affect the whole ecosystem at any level. They can accumulate wealth and use it for illegal trading on dark web or cash-out in exchange for fiat money which in turn leads to massive price hike to refrain future traders from buying that currency.

TABLE VI
COMPARISON OF THE TOP 10 CRYPTOCURRENCIES

Trust Issue	Bitcoin	Ethereum	Ripple	Bitcoin Cash	EOS	Steller	Litecoin	Tether	Bitcoin SV	Tron
Price manipulation activities	High	High	Medium	High	High	Low	High	High	High	High
Volatility	High	High	Low	High	High	Low	High	Low	High	High
Impacts of transaction amount	High	High	Low	High	Low	Low	Medium	NA	High	Low
Impact of transaction frequency	High	Medium	Low	High	Low	Low	High	NA	NA	NA
Transaction response time	Slow	Medium	Fast	Slow	Fast	Medium	Slow	NA	NA	NA
Ease of use	No	Yes	Yes	No	Yes	Yes	No	No	No	Yes
Frequency of reported theft cases	High	High	High	High	High	High	High	High	Low	Medium
Reputation in black market Reputation of technical teams	High NA	Low Good	Low Good	Low Good	Low Good	Low Good	Low NA	Low NA	Low NA	Low NA
Native blockchain platform	No	Yes	Yes	No	Yes	Yes	No	No	No	No
Potential for dishonest stakeholders	High	Low	Low	High	Low	Low	High	High	High	High
Design complexities Frequency of reputation attacks	High High	Low High	Low Low	High High	Low Low	Low Low	High High	High NA	High NA	High NA
Miners attacks	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
Security attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Privacy attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Customized transaction Fees	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No
Fraudulent ICOs	NA	Yes	Yes	Yes	Yes	Yes	No	No	NA	Yes
Reported bump and dump activities	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Chances of pairing with other currencies and exchanges	High	High	High	High	Low	High	High	High	Medium	NA

The dishonest wallets and exchanges could result in loosing traders' money; therefore, strict regulatory frameworks with guarantees are needed in order to operate wallets and exchanges. The dishonest miners can try to take control of the maximum hash rate in order to generate 51% attacks which can result in centralization and loss of other miners in the system. Current cryptocurrencies are trying hard to cope with this issue but more research and algorithmic approaches are needed to handle the 51% attack. Although cryptocurrency systems are trying to anonymize users data and devise new security and privacy strategies, these systems need to be updated in order to handle new attacks on the systems. New artificial intelligence and machine learning-based algorithmic approaches, therefore, are required to enable a fully private and secure trustworthy cryptocurrency ecosystem.

Recent interests of large corporations such as JP Morgan [8] and Facebook [7] are an evidence of the fact that cryptocurrency ecosystems will rise and stay for a long time. The pace of the industrial research is fast due to the direct involvement of monetary benefits. Most of the cryptocurrency ecosystem is based on the open-source projects and creating an opportunity for academic researchers to benefit from their development tools for active contribution. We believe that the industrial partners will play a leading role in the near future and, in order to maximize their commercialization benefits, the trust issues will remain as high priority. However, serious efforts are needed to minimize the gap between academic and industrial research through active collaborations and inclusive participation of all stakeholders in the cryptocurrency ecosystem.

A. Threats to Validity

Cryptocurrencies are one of the research areas lead by the industrial practitioners, and, therefore, there exists a significant gap between published peer-reviewed academic literature and technical specifications and availability of the empirical data by industrial practitioners. Considering this fact, the main threats to the validity of this review are the selection bias, data extraction and analysis, and reliability. However, we tried our best to cover the breadth and depth of research studies on blockchain trust in cryptocurrencies ecosystems. In order to ensure the validity, we used mixed method research by combining the research methods from [32] and [33]. In order to minimize the selection bias, we first defined the metacharacteristics [32], followed by a systematic literature collection [33] of empirical to conceptual analysis for taxonomy design. We then further expanded our manual research to redesign the taxonomy considering the ending conditions and ensure a comprehensive detailed taxonomy for this review. We ensured the minimal selection bias whereby one researcher collected the data and the other researcher examined it for correctness and validity. In addition, we extracted the data from relevant studies and provided references for each data source used in this study in order to ensure the reproducibility and reliability of this research work. However, considering the fast momentum of this research area, we believe that our presented taxonomy will only serve as a comprehensive starting point for the future improvements. Analyzing and including further metacharacteristics, and further expanding the ending conditions for detailed taxonomic discussions, will help further improve the understanding of trust in the cryptocurrency ecosystem.

Finally, with respect to the completeness, which is often an issue in the review studies, we have indeed not been able to cover more than top 10 currencies with respect to available systems to analyze as compared to the pure literature review which was much more comprehensive. We have ignored all the other failing cryptocurrencies, scam cryptocurrencies, etc. due to the positive focus of the study on the issues that provide trust. Future research can deal with the negative-focus type of the study that analyzes various scams and incentive mechanisms that break trust. Unfortunately, for this type of the study, the availability of research literature is even narrower.

TABLE VII
REQUIREMENTS AND POTENTIAL SOLUTIONS FOR TRUST ISSUES

Research Issues	Requirements	Immediate Solutions	Short Term Solutions	Long Term Solutions
High Value Transactions	The amount and frequency of transactions should not create an upsurge in the prices.	- Constant coin creation frequency - Upper limit on transaction amount - Instant notification to all stakeholders	Number of coins should be adjusted to maintain the right equilibrium between demand and supply to stop the upsurges in the prices	Growth in number of coins must be aligned with the proportion of time-lapse, transaction frequencies, and transaction amounts.
Exchange Manipulations	Exchanges should operate independently.	The exchanges should not keep user keys	Smart contract based decentralized exchanges	Proof of Stake based blockchain systems
Technology Bots	Rational technology bots	Algorithmic monitoring of bot activities	Algorithmic detection and stoppage of bot traders	AI and machine learning strategies are required for active prevention of malicious bot trading.
Market Factors	The prices of all coins must independently move	Cryptocurrency platforms should remove the complexities and highlight the strengths of technologies	The platform should provide complete documentations including user manuals, and source codes.	Cryptocurrency platforms should build a large community of traders, coders, and miners to come out of Bitcoin's influence.
Governments' Endorsements	Governments must regulate and endorse cryptocurrencies to increase pool of tax-payers	Governments should consider cryptocurrencies in their policy development and implementations	Government should enable regulatory frameworks for different application domains.	The establishment of working groups and policy making consortiums to each sector of economy is needed.
Trading by Technical Employees of platforms, wallets, and exchanges	Trading by technical teams must be transparent	The trades by technical teams should be highlighted	The companies must ensure to limit the transactions performed by technical teams	Separate transaction pools should be created for technical traders
Dark Web	All activities must be performed on public internet	All the websites trading on dark web should be blocked and banned	Algorithmic approaches are needed to detect the malicious dark web users	AI and machine learning based approaches are used to monitor, classify, and ban dark web users and websites
Dishonest Stakeholders	There should not be dishonest stakeholders	Stakeholders must be able to report about dishonest stakeholders	A reporting tool should be enabled in all cryptocurrency wallets, exchanges, and mining platforms	Need to monitor and identify dishonest traders, miners, nodes, and networks
Technical Design Complexities in Reputation Systems	Reputation systems should be well designed and calculate reputation scores on qualitative and quantitative information	The design complexities should be identified	Algorithmic approaches are needed to improve reputation mechanisms for traders, miners, nodes, and networks	The qualitative attributes-based reputation systems are needed for trustworthy stakeholders.
Reputation Attacks	There should be no reputation attack	Identify the attackers	Penalize the attackers	Intelligent monitoring tools
Lack of Understandings	The whole cryptocurrency ecosystem must be easily understandable	Provide all news and updates about technical and non-technical details	Users must be involved to provide feedback about their understanding about the system	All technical and non-technical information must be publicly available for discussion on platform's blogs
Information Hiding	Transparent Ecosystem	All information should be available	Algorithmic approaches are needed to analyze the information about stakeholders, currency momentum, and market factors	The analysis of all information should be integrated in to existing platforms
Large Traders	Large traders should not accumulate the maximum wealth	Traders should be monitored	The transactions should be limited by frequency and amount	Algorithmic incentive mechanism are needed to retain large traders
Mining Pools Centrality	All miners should be able to equally access and mine the coins	Detect the miners who are creating centralization	Develop tools to monitor the centralization attacks from miners	Algorithmic approaches needed to monitor mining pools, detect mining attacks, and create ASIC resistant mining rules and protocols
Manipulated Reputations	Stakeholders should not be able to manipulate reputations	Algotithmic approaches are needed to identity reputation manipulators	Incentive mechanisms are needed to ensure reputed stakeholders and networks	AI and machine learning based approarch are needed for continuous monitoring of stakeholders and networks
Fraudulent ICOs	There is no fraudulent ICO	Mechanisms are required to reverse transactions to fraudulent ICOs	ESCROW based or credit card based services should be used for ICOs	Early detection of fraudulent ICOs using intelligent algorithms
Pump and Dump Activities	There are no pump and dump activities	Finding pump and dump social media groups	Monitoring pump and dump activities	Banning users or creating delays in the systems to stop pump and dump activities
Privacy and Security Attacks	There is no privacy attack	Users must be aware of all types of privacy attacks	Algorithmic approaches are needed to handle privacy attacks	AI and machine learning approaches are needed for early detection and prevention of attacks

VI. Conclusion

The goal of achieving a highly trustworthy cryptocurrency ecosystem is not reachable within short time. There is a need to develop awareness among all stakeholders in order to fully develop and use decentralized cryptocurrency platforms. On the one hand, governments and regulators are needed to develop legal and regulatory frameworks for technology enablers and other financial services that are willing to adopt and develop cryptocurrencies. On the other hand, the underlying systems are needed to be even more secure, privacy preserving, and trustworthy to attract large user bases. This article presented a detailed discussion of the key trust issues in the entire cryptocurrency ecosystem and suggested multiple immediate, short-term, and long-term solutions. We envision that these trust issues, if resolved, will lead to the development of new generation of cryptocurrency systems whereby cryptocurrencies will be the main drivers of financial institutions and the mainstreams economy. However, all stakeholders from regulators to service-enablers, mining systems, and traders are needed to understand the technical and nontechnical implications of the cryptocurrency ecosystem in order to develop long-term and sustainable operating environment.

References

[1] J. Chiu and T. V. Koeppl, "The economics of cryptocurrencies–bitcoin and beyond," 2017. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3048124

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf, Accessed: May 21, 2019.

[3] D. Chaum and S. Brands, "'Minting' electronic cash," *IEEE Spectr.*, vol. 34, no. 2, pp. 30–34, Feb. 1997.

[4] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Proc. Conf. Theory Appl. Cryptography*, Springer, 1988, pp. 319–327.

[5] X. Li and C. A. Wang, "The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin," *Decis. Support Syst.*, vol. 95, pp. 49–60, 2017.

[6] "Crypto market capitalization." [Online]. Available: https://coinmarketcap.com/

[7] "Libra whitepaper." [Online]. Available: http://bit.ly/2MuBB3L

[8] "JP Morgan is rolling out the first us bank-backed cryptocurrency to transform payments business." [Online]. Available: https://cnb.cx/2IBQnVx

[9] D. Romano and G. Schmid, "Beyond Bitcoin: A critical look at blockchain-based systems," *Cryptography*, vol. 1, no. 2, p. 15, 2017.

[10] A. Berentsen and F. Schar, "A short introduction to the world of cryptocurrencies," vol. 100, no. 1, p. 16, 2018. [Online]. Available: http://dx.doi.org/10.20955/r.2018.1-16

[11] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies," in *Proc. IEEE Secur. Privacy Symp.*, 2015, pp. 104–121.

[12] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[13] M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in Bitcoin-like digital cash systems," *IEEE Commun. Surveys Tut.*, vol. 20, no. 3, pp. 2543–2585, Third Quarter 2018.

[14] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, 2018.

[15] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018.

[16] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Commun. Surveys Tut.*, vol. 20, no. 4, pp. 3416–3452, Fourth Quarter 2018.

[17] H. Hasanova, U.-J. Baek, M.-G. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *Int. J. Netw. Manage.*, vol. 29, no. 2, p. e2060, 2019.

[18] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, 2017, pp. 1–13. [Online]. Available: http://dx.doi.org/10.1016/j.future.2017.08.020

[19] F. Hawlitschek, B. Notheisen, and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," *Electron. Commerce Res. Appl.*, vol. 29, pp. 50–63, 2018.

[20] M. Berkhout, F. van den Brink, M. van Zwienen, P. van Vulpen, and S. Jansen, "Software ecosystem health of cryptocurrencies," in *Proc. Int. Conf. Softw. Bus.*, Springer, 2018, pp. 27–42.

[21] S. Boshuis, T. B. Braam, A. P. Marchena, and S. Jansen, "The effect of generic strategies on software ecosystem health: The case of cryptocurrency ecosystems," in *Proc. 1st Int. Workshop Softw. Health*, ACM, 2018, pp. 10–17.

[22] A. Aldweesh and A. van Moorsel, "A survey about blockchain software architectures," in *Proc. 32nd Annu. UK Perform. Eng. Workshop Cyber Secur. Workshop*, Newcastle University, 2016, pp. 1–13.

[23] S. Kim, Y. Kwon, and S. Cho, "A survey of scalability solutions on blockchain," in *Proc. Int. Conf. Inf. Commun. Technol. Convergence*, IEEE, 2018, pp. 1204–1207.

[24] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Commun. Surveys Tut.*, vol. 21, no. 2, pp. 1676–1717, Second Quarter 2019.

[25] M. Garriga, M. Arias, and A. De Renzis, "Blockchain and cryptocurrency: A comparative framework of the main architectural drivers," 2018, *arXiv:1812.08806*.

[26] S. Solat, "Security of electronic payment systems: A comprehensive survey," 2017, *arXiv:1701.04556*.

[27] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst.*, IEEE, 2017, pp. 1–5.

[28] R. Raju, M. SaiVignesh, and K. I. A. Prasad, "A study of current cryptocurrency systems," in *Proc. Int. Conf. Comput. Power Energy Inf. Commun.*, Mar. 2018, pp. 203–209.

[29] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," in *Proc. 27th Int. Conf. Comput. Commun. Netw.*, IEEE, 2018, pp. 1–11.

[30] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK)," in *Principles of Security and Trust*, New York, NY, USA: Springer, 2017, pp. 164–186.

[31] F. K. Maurer, "A survey on approaches to anonymity in Bitcoin and other cryptocurrencies," *Informatik*, vol. p-259, pp. 2145–2150, 2016.

[32] R. C. Nickerson, U. Varshney, and J. Muntermann, "A method for taxonomy development and its application in information systems," *Eur. J. Inf. Syst.*, vol. 22, no. 3, pp. 336–359, 2013.

[33] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, 2007.

[34] G. P. Dwyer, "The economics of Bitcoin and similar private digital currencies," *J. Financial Stability*, vol. 17, pp. 81–91, 2015.

[35] "Live cryptocurrency data." [Online]. Available: https://www.cryptocompare.com/

[36] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[37] Ripple, "The cost-cutting case for banks - the ROI of using ripple and XRP for global interbank settlements," *Vision Paper*, 2016. [Online]. Available: ripple.com/xrp-portal

[38] M. A. Javarone and C. S. Wright, "From Bitcoin to Bitcoin cash: A network analysis," 2018, *arXiv:1804.02350*.

[39] EOSIO, "EOSIO blockchain software architecture," 2019. [Online]. Available: https://eos.io/

[40] Steller, "Steller basics," 2019. [Online]. Available: https://www.stellar.org/how-it-works/stellar-basics/

[41] Litecoin, "Litecoin wiki," 2019. [Online]. Available: https://litecoin.info/index.php/Main_Page

[42] Tether, "Tether whitepaper," 2019. [Online]. Available: http://bit.ly/2nuc3eG

[43] BITC INSV, "Bitcoin SV," 2019. [Online]. Available: https://bitcoinsv.io/

[44] T. Tron, "Tron decentralized the web," 2019. [Online]. Available: https://tron.network/index?lng=en

[45] G. Gutoski and D. Stebila, "Hierarchical deterministic Bitcoin wallets that tolerate key leakage," in *Int. Conf. Financial Cryptography Data Secur.*, New York, NY, USA: Springer, 2015, pp. 497–504.

[46] Ledger, "Hardware wallets," *Ledger Nano S*. Accessed: Jan. 28, 2019. [Online]. Available: https://www.ledger.com/

[47] M. Gentilal, P. Martins, and L. Sousa, "Trustzone-backed Bitcoin wallet," in *Proc. 4th Workshop Cryptography Secur. Comput. Syst.*, ACM, 2017, pp. 25–28.

[48] D.-H. Shin, "Towards an understanding of the consumer acceptance of mobile wallet," *Comput. Human Behav.*, vol. 25, no. 6, pp. 1343–1354, 2009.

[49] T. Volety, S. Saini, T. McGhin, C. Z. Liu, and K.-K. R. Choo, "Cracking Bitcoin wallets: I want what you have in the wallets," *Future Gener. Comput. Syst.*, vol. 91, pp. 136–143, 2019.

[50] F. Karegar, D. Lindegren, J. S. Pettersson, and S. Fischer-Hübner, "User evaluations of an app interface for cloud-based identity management," in *Advances in Information Systems Development*, New York, NY, USA: Springer, 2018, pp. 205–223.

[51] S. Goldfeder *et al.*, "Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme," 2015. [Online]. Available: http://www.cs.princeton.edu/~stevenag/threshold_sigs.pdf, Accessed: May 21, 2019.

[52] P. K. Kaushal, A. Bagga, and R. Sobti, "Evolution of Bitcoin and security risk in Bitcoin wallets," in *Proc. Int. Conf. Comput. Commun. Electron. (Comptelix)*, IEEE, 2017, pp. 172–177.

[53] M. Vasek, J. Bonneau, C. K. Ryan Castellucci, and T. Moore, "The Bitcoin brain drain: A short paper on the use and abuse of Bitcoin brain wallets," in *Financial Cryptography and Data Security, Lecture Notes Comput. Sci.*, Springer, 2016, vol. 8975, pp. 44–61.

[54] T. Ledger, "Ledger blue," *Ledger Blue*. Accessed: Jan. 26, 2019. [Online]. https://www.ledger.com/products/ledger-blue

[55] T. Shapeshift, "Keepkey own your own bank," *KeepKey*. Accessed: Jan. 26, 2019. [Online]. https://shapeshift.io/keepkey/

[56] T. J. Liberty, "Jaxx liberty," *Jaxx*. Accessed: Jan. 26, 2019. [Online]. https://jaxx.io/

[57] T. Trezor, "Trezor," *Trezor*. Accessed: Jan. 26, 2019. [Online]. https://wiki.trezor.io/Developer_portal

[58] T. Guarda, "Guarda," *Guarda*. Accessed: Jan. 26, 2019. [Online]. https://guarda.co/

[59] T. Exodus, "Exodus," *Exodus*. Accessed: Jan. 26, 2019. [Online]. https://www.exodus.io/

[60] T. Ethos, "Ethos," *Ethos*. Accessed: Jan. 26, 2019. [Online]. https://www.ethos.io/

[61] T. Paytomat, "Paytomat," *Paytomat*. Accessed: Jan. 26, 2019. [Online]. https://paytomat.com/

[62] T. Coinomi, "Coinomi," *Coinomi*. Accessed: Jan. 26, 2019. [Online]. https://www.coinomi.com/en/

[63] G. Hileman and M. Rauchs, *Global Cryptocurrency Benchmarking Study*, vol. 33. Cambridge Centre for Alternative Finance, Cambridge, U.K., 2017.

[64] K. Salah, M. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, Jan. 2019.

[65] D. Gambetta *et al.*, "Can we trust trust," in *Trust: Making and Breaking Cooperative Relations*, vol. 13, Oxford, U.K.: Univ. Oxford, 2000, pp. 213–237.

[66] J. D. Lewis and A. Weigert, "Trust as a social reality," *Soc. Forces*, vol. 63, no. 4, pp. 967–985, 1985.

[67] C. F. Sabel, "Studied trust: Building new forms of cooperation in a volatile economy," *Human Relations*, vol. 46, no. 9, pp. 1133–1170, 1993.

[68] D. Good, "Individuals, interpersonal relations, and trust," in *Trust: Making and Breaking Cooperative Relations*, Oxford, U.K: Univ. Oxford, 2000, pp. 31–48.

[69] W. Wang, "A vision for trust, security and privacy of blockchain," in *Proc. Int. Conf. Smart Blockchain*, Springer, 2018, pp. 93–98.

[70] R. Pérez-Marco, "Bitcoin and decentralized trust protocols," 2016, *arXiv:1601.05254*.

[71] Z. Gurguc and W. Knottenbelt, *Cryptocurrencies: Overcoming Barriers to Trust and Adoption*. London: Imperial College, 2016. [Online]. Available: http://bit.ly/2MtmIih

[72] P. M. Krafft, N. Della Penna, and A. S. Pentland, "An experimental study of cryptocurrency market dynamics," in *Proc. CHI Conf. Human Factors Comput. Syst.*, ACM, 2018, p. 605.

[73] E. Jahani, P. M. Krafft, Y. Suhara, E. Moro, and A. S. Pentland, "Scamcoins, s*** posters, and the search for the next Bitcoin™: Collective sensemaking in cryptocurrency discussions," *Proc. ACM Human-Comput. Interaction*, vol. 2, no. CSCW, p. 79, 2018.

[74] T. Timothy, "How bots are manipulating cryptocurrency prices," 2019. [Online]. Available: http://bit.ly/2p9zJp4

[75] J. M. Griffin and A. Shams, "Is Bitcoin really un-tethered?" 2018. [Online]. Available: https://dx.doi.org/10.2139/ssrn.3195066

[76] J. I. Orlicki, "A stable coin with pro-rated rebasement and price manipulation protection," 2017, *arXiv:1708.00157*.

[77] Maker, "Dai stable coin," 2019. [Online]. Available: https://makerdao.com/en/

[78] F. M. Ametrano, "Hayek money: The cryptocurrency price stability solution," 2016. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2425270

[79] S. Sam, "Insider trading in cryptocurrency: Exploring new territory for the CFTC," 2018. [Online]. Available: https://cblr.columbia.edu/insider-trading-in-cryptocurrency-exploring-new-territory-for-the-cftc/

[80] D. C. Isaacs, C. Pendleton, and J. P. Gottlieb, "Insider trading and cryptocurrency: A primer for traders," *Big Law Bus.*, 2018. [Online]. Available: http://bit.ly/2ISs2ej

[81] W. Josiah, "Think coinbase employees engaged in insider trading? Deal with it," 2017. [Online]. Available: http://bit.ly/2Ms8huW

[82] R. Qin, Y. Yuan, S. Wang, and F.-Y. Wang, "Economic issues in Bitcoin mining and blockchain research," in *Proc. IEEE Intell. Vehicles Symp.*, IEEE, 2018, pp. 268–273.

[83] S. Naqvi, "Challenges of cryptocurrencies forensics: A case study of investigating, evidencing and prosecuting organised cybercriminals," in *Proc. 13th Int. Conf. Availability Rel. Secur*, ACM, 2018, p. 63.

[84] J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo, "Repucoin: Your reputation is your power," *IEEE Trans. Comput.*, vol. 68, no. 8, pp. 1225–1237, Aug. 2019.

[85] F. Gai, B. Wang, W. Deng, and W. Peng, "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network," in *Proc. Int. Conf. Database Syst. Adv. Appl.*, Springer, 2018, pp. 666–681.

[86] Ethereum, "Problems in eteherum," 2019. [Online]. Available: https://github.com/ethereum/wiki/wiki/Problems

[87] D. G. Birch and S. Parulava, "Ambient accountability: Shared ledger technology and radical transparency for next generation digital financial services," in *Handbook of Blockchain, Digital Finance, and Inclusion*, vol. 1. Cambridge, MA, USA: Elsevier, 2018, pp. 375–387.

[88] J. Biggs, S. R. Hinish, M. A. Natale, and M. Patronick, *Blockchain: Revolutionizing the Global Supply Chain by Building Trust and Transparency*. New Jersey, USA: Rutgers University, 2017.

[89] C. Y. Kim and K. Lee, "Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats," in *Proc. Int. Conf. Platform Technol. Service*, IEEE, 2018, pp. 1–6.

[90] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptology Conf.*, Springer, 2017, pp. 357–388.

[91] Ø. Bergesen and L. M. Palm, "An exploratory study of initial coin offerings: A better understanding of the ICO market and its fraudulent and unregulated nature," master's thesis, Dept. Econ. Finance, Fac. Bus Law, Univ. Agder, 2018.

[92] D. Boreiko and N. K. Sahdev, "To ICO or not to ICO–empirical analysis of initial coin offerings and token sales," [Online]. Available: 10.2139/ssrn.3209180

[93] D. A. Zetzsche, R. P. Buckley, D. W. Arner, and L. Föhr, "The ICO gold rush: It's a scam, it's a bubble, it's a super challenge for regulators," University of Luxembourg Law Working Paper, no. 11, 2017, pp. 17–83.

[94] S. C. Baum, "Cryptocurrency fraud: A look into the frontier of fraud," Honors theses 375, 2018. [Online]. Available: http://bit.ly/2olbu7E

[95] P. Cerchiello *et al.*, *ICOS Success Drivers: A Textual and Statistical Analysis*. Dept. Econ. Manage., Univ. Pavia, Pavia PV, Italy, 2018.

[96] Satis Data, *Cryptoasset Market Coverage Initiation: Network Creation*. Satis Group., 2018. [Online]. Available: http://bit.ly/2MsyZUb

[97] ICOData.IO, "ICO data-ICO 2018 statistics," 2019. [Online]. Available: https://www.icodata.io/stats/2018

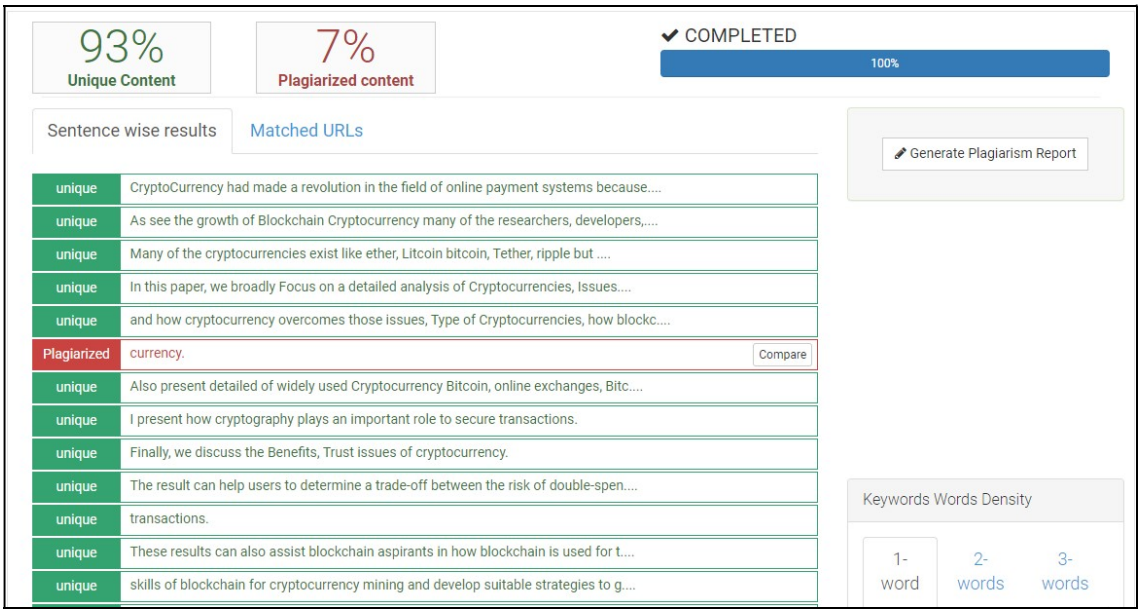
[98] J. Kamps and B. Kleinberg, "To the moon: Defining and detecting cryptocurrency pump-and-dumps," *Crime Sci.*, vol. 7, no. 1, p. 18, 2018.

[99] T. Li, D. Shin, and B. Wang, *Cryptocurrency Pump-and-Dump Schemes*. SSRN, 2018. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3267041

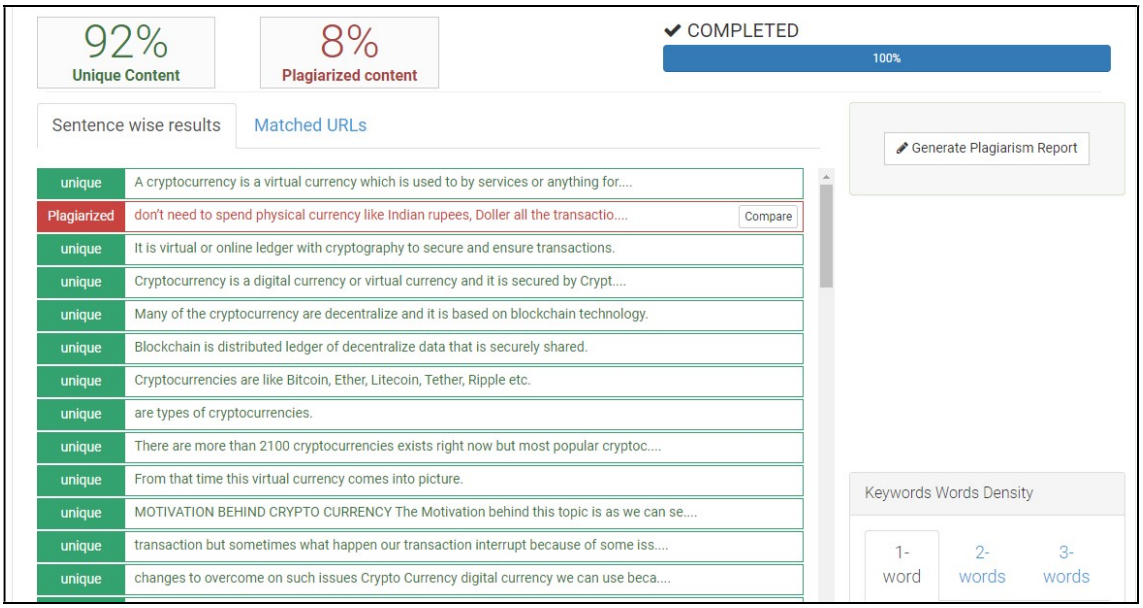
[100] J. Xu and B. Livshits, "The anatomy of a cryptocurrency pump-and-dump scheme," 2018, *arXiv:1811.101*

PLAGARISM REPORT

Plagiarism Report of Abstract



Plagiarism Report of Introduction and Literature



Plagiarism Report of System Architecture, Applications, Comparison and Conclusion