A Brief Discussion on Two Different Cryptocurrency: BITCOIN & ETHEREUM

Srinjoy Mahato[#1] Tanmoy Khatua[#2] Ankan Das[#3] Mr. Tathagata Roy Chowdhury[#4]

[#1] *Student, Dept. Of BCA, Techno India University*
[#2] *Student, Dept. Of Computer Sc. & Engineering, Brainware group of Institutions-SDET*
[#3] *Student, Dept. of Computer Sc. & Engineering, University of Engineering & Management, Kolkata*
[4] *Asst. Professor. Dept. of Computer Sc. & Engineering, Elitte College of Engineering*

Abstract: *Here, we discuss different cryptocurrencies which are extremely important in the network security market. As we know, Cryptocurrencies are digital assets which can be designed to work as an exchange that can use strong cryptography to protect all the transactions. Here the two most popular aspects of it, Bitcoin and Ethereum, is discussed with their all functionalities, their methods of work, their advantages over each and other and moreover their concepts of architecture.*

Keywords: *Cryptocurrency, Bitcoin, Etherium, SHA algorithm, Ethash algorithm, Type of Cryptocurrency*.

I. INTRODUCTION

A cryptocurrency is a digital or virtual currency which utilizes cryptography for security purposes. A cryptocurrency is tough to counterfeit owing to this security feature. Several crypto currencies are unit decentralized systems supported block chain technology, a distributed ledger implemented by a disparate network of computers. A shaping characteristic of a cryptocurrency, and arguably its biggest allure, is that it is organic; it's not under the command of any central authority, rendering it in theory proof against government interference.

The first blockchain-based cryptocurrency was Bitcoin, and it remains the most fashionable and most used. Today, there are several alternate cryptocurrencies with varied functions and specs. Quite a number of these are clones of Bitcoin whereas others are forks or new cryptocurrencies that split far from a pre-existing one. Cryptocurrencies are systems that provide the secure payments of online transactions that are denominated in terms of a virtual "token," representing ledger entries internal to the system itself.

The word "Crypto" refers to the fact that varied encoding algorithms and cryptographical techniques, like elliptical curve encoding, public-private key pairs, and hashing functions, are unit utilized. Here we shall discuss two commonly used Cryptocurrencies: Bitcoin and Ethereum

A. BITCOIN :

Bitcoin is a digital currency founded in January 2009. It pursues the ideas declare in a white paper by the mysterious Satoshi Nakamoto, whose true identity has yet to be verified. Bitcoin offers the commitment of base transaction fees than customary online payment procedures and is administered by a decentralized authority, unlike government-issued money. There is no tangible bitcoin. An extensive amount of computing power verifies only balances recorded on a public ledger in the cloud, along with all Bitcoin transactions. Despite not being legal tender, Bitcoin has skyrocketed in popularity and has triggered the launch of several other cryptocurrencies collectively referred to as Altcoins.

a) CHARACTERISTICS OF BITCOIN

i. Decentralized

One of Satoshi Nakamoto's primary objectives while creating Bitcoin was the network's noninterference from any governing authorizations. It is designed such that every person, business, as well as each machine involved in mining/ verification of transactions, becomes part of a vast network.

ii. Anonymous

Nowadays, banks know almost about everything regarding their customers: credit history, addresses, phone numbers, spending habits.

In Bitcoin, it is difficult as the wallet isn't there to be associated with any personal information. Moreover, while some people frankly don't want their finances to be tracked by any government agency, others might debate that drug trade, some illegal and unhealthy activities can be conducted in this relative support.

iii. Transparent

In every single BTC, the transaction is stored in Blockchain in relative support. When our wallet address

is publicly used, we know exactly how much money is in it by studying blockchain ledger. However, tracing a specific Bitcoin address to a person is still quite an impossible feat. Those who prefer to stay anonymous with their transaction can take measures to stay under the radar. These types of wallets that can prioritize security and cryptology can be used by multiple addresses and can't send a massive amount of money to a single wallet or record.

iv. Fast

The Bitcoin payment process is almost so quick, it generally takes a few minutes for someone to receive the money from the other side of the world, but general bank transfers can take a few days.

v. Non-repudiable

Once we send our Bitcoins to someone, there is no way we can get them back, unless the recipient would want to return it. This ensures the acquisition of payment, meaning that whomever we're trading with can't scam us by claiming that they never received the money.

b) EXPLANATION OF SHA ALGORITHM

- SHA 256 algorithm, a part of encryption technology, is used in Blockchain to get a constant hash of 256 bits every time.
- In the figure below, we see the prototype of an algorithm containing some data called IV, which is of 256 bits.
- The extensive input is broken in size of 512 bits which may not always be a perfect multiple of 512 bits, so some part of the input can be left.
- To this input residue, we do concatenation with 10* bits before doing padding. So now we get perfect multiple of 512 bits input which is added with 256 bits IV to get a total of 768 bit, which passed through a compression function 'c' to get an output of 256 bits only.
- This output 256 bit is freshly merged with 512 bits input from block B2. Again the total is passed through the compression function to yield a 256-bit output. This loop goes on till the last block (block n).

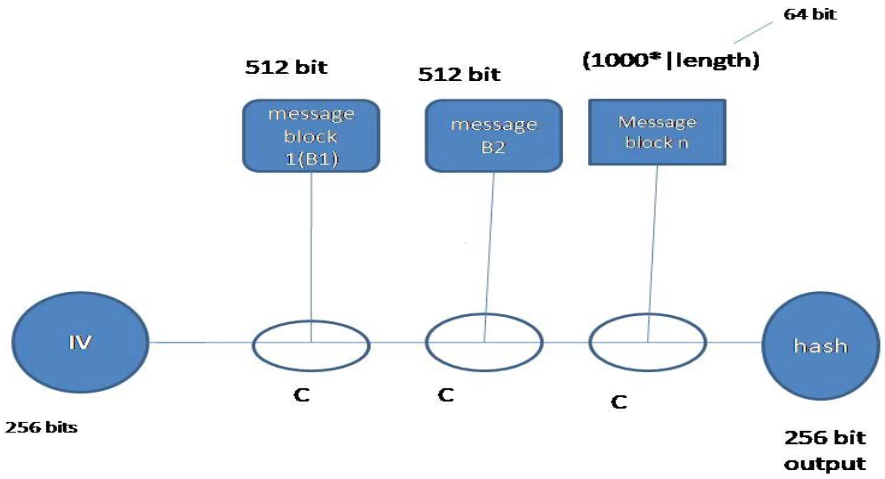

Fig 1: If c is collision-free, then SHA-256 is collision free

c) ADVANTAGES OF BITCOIN

1. Freedom

Bitcoin was designed aiming for freedom from governing authorities regulating the transactions, imposing fees and being in charge of people's wealth. When it comes to purchasing things, cryptocurrency became just as legitimate as flat currency recently, and considering the existence of numbers of deep-web markets that only accept Bitcoin payments, you may be able to buy some things much more comfortably with BTC than any other currency.

2. High portability

One of the main characteristics of money is it can be used and hold everywhere where we want. As Bitcoin is entirely digital, practically any sum of money can be stored in a flash drive or online.

3. Choose your commission

Another undeniable benefit of the Bitcoin network is the opportunity of choosing the amount you want to pay as a transaction fee or choosing not to pay it at all. The miner receives the transaction fee after a new block is

created with a successful hash. Generally, the sender pays the full fee, and deducting this fee from the recipient could account to an incomplete payment.

4. Safety and Control

Bitcoin users are capable of monitoring their transactions; no one can withdraw money from my account without my knowledge or agreement, which at times happen with other forms of payment, and no one can steal your payment information from merchants.

5. Transparent and neutral

Each transaction or every single data about all transactions, which can always be available for everyone in the Blockchain can be used in a real-time environment. The BTC protocol is protected, that's why no one can alter the data within the organizations, no one can control it, and the network is already decentralized. That's why the Bitcoin is always neutral.

6. It can't be counterfeited

One of the most popular paths of simulating in the digital world is using the same money twice, rendering both transactions deceptive. It is called 'double spend.' Bitcoin, just like most other cryptocurrencies, uses Blockchain technology as well as the various consensus mechanisms built into BTC algorithms.

B. ETHEREUM

Launched in 2015, Ethereum is one of the leading programmable blockchains available in the world. It is a decentralized, distributed, and open-source computing platform, with a Turing complete contracting language that allows us to create smart contracts and develop decentralized applications. The original Ethereum development team consisted of VitalikButerin, Mihai Alisie, Anthony Di Iorio, and Charles Hoskinson. Like other cryptocurrencies, Ethereum has its virtual currency token known as Ether.

Ethereum is primarily made up of three main layers. The first, primary layer that is the framework/backbone is a vast network of computers that process transactions and keep a shared database updated over time (the Blockchain). The second, on top of it, is the software layer. It helps in running programs called "smart contracts" on the Ethereum blockchain, made using a javascript-like programming language called "Solidity." The topmost layer is the collection of all the applications that offer various services to Ethereum users. The benefit of using Ethereum is that the applications that are built using Ethereum are entirely decentralized. Therefore they have no central point of connection and the chances of failure, if ever, are slim to none. It is also thereby free from government control as the ledger is independently present on each of the nodes.

a) LAYERS OF ETHEREUM

- Blockchain:

Almost all websites on the internet are hosted on a server in a data centre located in various places around the world. When we attempt to connect to a website, our computer connects to the servers and downloads the content requested by the user via the computer. This works completely fine when the internet was meant for connecting a single host to several entities, such as our computers. Nowadays, we require the client computers to be connected to other client computers as well directly (Web 2.0). A peer-to-peer network is this vast network of interconnected computers passing information to each other.

The Ethereum hardware layer is a pure peer-to-peer network of computers that compute transactions and keep the transactions in the order in a shared ledger. Each computer in this network is known as a node; it validates the new transactions and organizes them into blocks that are broadcasted to the entire Ethereum network. The transaction can contain both value and information. The value part is the digital currency of the Ethereum platform, called Ether. Moreover, the information is the code that can pass data and trigger actions.

- Software Layer: Solidity:

The Ethereum software layer has been built to overcome the currency-based limitation of Bitcoin. Ethereum can help in any transaction, from currency to a house purchase. To serve this purpose, a new programming language called Solidity was built to make programs called "Smart Contracts" that define the logic or flow of a particular transaction(s). Solidity is inspired by C++, Python, and JavaScript and is designed to target the Ethereum Virtual machine (EVM). A smart contract is an auto-executing, programmed agreement that is recorded on the Ethereum blockchain.

"Smart contracts are applications that exactly run as programmed without any possibility of downtime, censorship, fraud, or third-party interference."- Ethereum Foundation.

Ethereum makes it quite easy to create new digital currencies, called tokens, that can be transacted within the entire Ethereum community. This makes transactions in shopping centres much more accessible and secure. All Ethereum source code is open source and therefore readily available to the public. This has helped to grow a community of users/developers for fixing the bugs and add new features. Therefore, the

process is entirely transparent. The codebase is always being mutated to make it better, an ever-evolving platform.

The code behind every smart contract is public, so we can always be sure the transaction is going to happen correctly. The fact that it is public, the fact that it is free of government control makes it a much viable option for businesses, eliminating huge transaction fees as A well.

- Application layer: DApps

Third-party apps run on the hardware and software layers of the Ethereum network. The DApps are not only finance based, as previously established. There are over 2200 DApps as of the time of writing, almost 1500 of them live. Many developers are working on DApps because of the open and transparent nature of the Ethereum platform. The number of DApps has almost doubled since last year.

A few points about Ethereum that can be noted are:

i. It is Transparent: The codebase is open to view by anyone, from anywhere. All transactions are public and tracked, as well as the manner in how the transaction occurred.

ii. It is Strong: It's practically impossible to stop all the computer/nodes running on the Ethereum platform, and as it is a shared ledger, it is very impractical to even think about taking the entire Ethereum network down.

iii. Flexible code: The open-source nature of Ethereum makes the code much more changeable. As the code is publicly available, any bug or exploit needs to be immediately fixed as it becomes much easier to be exploited as hackers are always looking out for exploits, and it only makes their job more open-handed as the code is readily available to them.

b) ETHASH ALGORITHM

•Ethash Proof-of-Work Algorithm

ETHASH is based on a Proof-of-Work Algorithm constructed by the Ethereum network and cryptocurrencies based on Ethereum. In spite of being formed over the previous Dagger-Hashimoto algorithm, it has advanced enough to be considered an entirely new algorithm.

ETHASH uses Keccak-256 and Keccak-512 hash algorithms, and it creates confusions over the simultaneous development of SHA-3, also known as the Secure Hash Algorithm. SHA-3 is a standard part of Keccak. With ETHASH, the output created during the hashing procedure must result in a hash value, which is below a particular threshold. This system is known as difficulty, and its purpose is to increase or decrease the threshold of the Ethereum network to control the rate of the number of blocks that are mined on the network. Therefore, if too many blocks are mined in a short amount of time, the network automatically increases the difficulty, i.e., it is going to lower the network threshold, resulting in reducing the number of valid hashes that can be found. Precisely the opposite happens when the rate of mined blocks decreases. The network threshold increases to produce increasing numbers of correct hash values that can be found. This system of difficulty is essential for getting rid of an ideal situation where the time required to create new blocks drastically decreases, thus proportionally increasing the rate of payouts in the reward system. With the Ethereum Algorithm, the difficulty gets dynamically adjusted in such a way that, on an average, one block is generated by the network every 12 seconds.

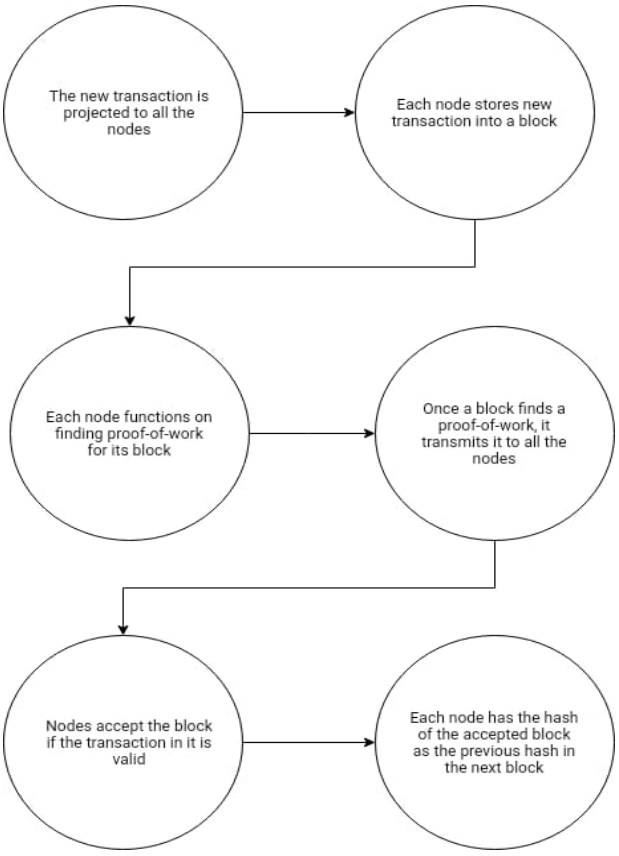

Fig 2: ETHASH algorithm working procedure

- **Proof of Stake Algorithm**

Ethereum is advancing towards a major upgrade around January 2020, named as Ethereum 2.0, which is expected to radically change the way how the billion-dollar network produces blocks and verifies transactions. Dubbed as phase Zero, the first phase is

supposed to launch Ethereum's new Proof-of-Stake algorithm strictly. Proof-of-Stake is based on consensus algorithms for public blockchains that rely on the validator's economic stake in the network.

Here are some essential characteristics of the algorithm:

i. Stake –

Only a select number of people who deposit money as a security deposit in the Ethereum network is going to be allowed to work on checking transaction blocks.

Therefore, the more money potential validators deposit into the Ethereum network, the higher his/her chances to be allocated a block that needs to be verified. The block rewards are to be delivered in proportion to the amount of money staked. The only way to increase the reward is to increase the stake deposit.

ii. Penalty –

The validators are going to receive a penalty if their work is found to be fraudulent, which shall be deducted from the money they deposited. This helps the users of Ethereum to find trust in the working of the network and also the validators.

iii. Decentralization –

As the algorithm is not up and running yet, we still do not know how decentralized it can make the network, but to launch a 51% attack, the people planning on that have to rely on extreme monetary holding instead of computational power. The more money kept as a stake in the network, the higher the chances to be selected as a validator. It is yet to uncover how the factor of penalty plays in stopping such attacks. It is believed that the code can be modified to create economic incentives that discourage the formation of groups that can launch the 51% attack. It has to be understood how the introduction of penalty plays into stopping such attacks, as any fraudulent activity shall be detected in the network and result in loss of ethers, and the only way to launch attacks is to acquire new ethers.

iv. Cheap –

If appropriately decentralized, this can prove to be a much cheaper way to mine/validate ethers than the traditional Proof-of-Work algorithm, as expensive mining equipment need not be required.

v. Backup –

In case a validator fails to turn up for the job, it can easily be assigned to anyone from a list of backup validators available.

c) EXPLANATION OF ETHASH ALGORITHM

The ETHASH algorithm is dependent on a randomly generated 1GB Dataset known as a DAG(Directed Acyclic Graph). The DAG is updated once every epoch(30000 blocks). The size of the DAG is going to continue to grow as the Blockchain keeps increasing.

- The block header which is derived from the latest block and the current nonce are combined using the Secure Hashing Algorithm to create the 128-byte mix.
- The mix is used to compute which 128-byte page from the DAG needs to be retrieved. The Get DAG Page block represents it.
- Then the mix is combined with the DAG page that has been retrieved. This is achieved using a specific mixing function of ethereum to generate another mix. Let's name it as mix 1.
- The steps two and three are repeated 64 times on mix 1, which yields another 64-byte mix.
- The 64-byte mix is further processed into a shorter 32-byte mix. This is the final mix. This mix is compared to the predefined 32-byte target threshold. If the final mix is less than or equal to the target threshold, the current nonce is considered successful, and it shall be broadcasted onto the ethereum network. Otherwise, the current nonce shall be held invalid, and the algorithm has to be rerun using a different nonce, either by increasing its value or by picking a value at random.

d) ADVANTAGES OF ETHEREUM

Apart from providing the general benefits that an ordinary blockchain possess, Ethereum has more to offer. Here are some benefits that are listed below.

1. Immutable:

All transactions on the Ethereum blockchain is immutable once the data has been verified and written into the ledger. Nobody is allowed to edit any data or transaction information once it has been uploaded.

2. Decentralized:

The validity of the transaction depends on the consensus mechanism due to which Blockchain thrives. This means there has to be no trusted intermediary to perform the actions. Smart contracts are self-executed, and each transaction is verified by a validator before being uploaded into the Ethereum blockchain. The proof of stake algorithm that is going to be implemented in the upcoming Ethereum 2.0 or Ethereum Constantinopole as a hard fork is expected to make the blockchain network more decentralized. It is an entirely new algorithm, and theoretically, it has overcome several cons that the Proof-of-Work algorithm faced, which is used in Bitcoin.

3. Fast Transactions:

There is no block limit on the Ethereum blockchain. The number of transactions that are written into a block depends on the work of the miners. Currently, in an

average, each block in Ethereum is mined is 10-20 seconds, and the number of transactions per second is around 15.

4. Currency and much more:

While Bitcoin and Ether are both digital currencies, unlike Bitcoin, the primary purpose of the Ethereum blockchain is not to establish itself as a payment alternative. The Ethereum algorithms are used by developers to build and run DApps or Decentralized Applications. These applications run on distributed computing systems and are popularized by distributed ledger technologies.

5. Secure:

All transactions on the Ethereum network are secured using cryptographic algorithms. Ethereum has approximately three times more nodes than Bitcoin verifying its transactions. A node is a computer that is connected to the Ethereum network which enforces the consensus rules of Ethereum. Therefore this implies that there are almost three times more miners on the Ethereum blockchain available to verify transactions.

6. Turing Completeness:

Ethereum is written with a code that suffices Turing completeness. A software or a program is considered to be Turing complete/computationally universal if it can run any universal code, provided enough resources. This takes away the problem of having specific software or computers that can only run particular codes. Ethereum, therefore, gets an edge over Bitcoin as Bitcoin uses an algorithm that is Turing incomplete and can only perform a limited set of functions.

7. Rich Statefulness:

VitalikButerin describes Ethereum's ability to remember and maintain more state at the blockchain level by using this term. Bitcoin is considered stateless as it is only able to deal with transactions. On the contrary, Ethereum can deal with contract code and data on top of keeping a balance.

8. Cheap:

With the introduction of Ethereum and smart contracts, transactions of money (which was already done by Bitcoin) along with transferring information and other things, for example, buying and selling houses, etc., has become cheaper as a decentralized system cuts out the use of a middle-man. On top of eliminating the risk of any potential malicious scam that could be conducted by the middle-man, the fees of hiring him/her are also deducted. The only fee the creator of the contract might have to pay is gas.

Gas is defined as the fee that is required to run the code for a smart contract on the ethereum network. The more gas you prefer to pay, the faster the transaction is going to be validated because the validators/miners prioritize contracts/transactions that offer more gas. The computational costs and the rewards for important transactions are made public to the miners. This gas is paid by the use of monetary tokens of Ethereum known as Ether.

9. Decentralized Autonomous Organization:

A Decentralized Autonomous Organization(DAO) is defined as an organization represented by using encoding rules of a computer program, controlled by shareholders and is uninfluenced by any central controlling body. There are several inherent advantages to such a system. As it is a transparent transaction system, there is no place for fraudulent business conduct. There is no physical body where employees have to reach to work. Therefore, work can be done from home, and people can be employed from around the world.

10. Solidity:

Solidity is a programming language, with a similar syntax to JavaScript designed to compile code and run on the Ethereum Virtual Machine. This is how users form codes that match their intention and run it using the hashing algorithms of Ethereum. Smart contracts are constructed by coding it on Solidity. Ethereum, being a worldwide platform, makes Solidity accessible to everyone. This allows the whole world to pour in their ideas and make applications by coding on this platform. Github is a popular network where coders gather and have a social platform to converse about new ideas. This makes Ethereum a much more versatile technology than Bitcoin, as nobody knows the limitations to which people can use their innovative ideas to build applications on top of the Ethereum using Solidity.

11. ASIC Resistant:

ASIC stands for Application-Specific Integrated Circuit. ASIC is a sort of hardware specialization whose purpose is to do only a single particular job, with exponential efficiency. This creation of a hardware specialization allows the CPU to perform specific actions without using the rest of its functions that have no use while working on a specific job. Therefore miners can develop this to mine coins from the Blockchain much faster than an ordinary piece of hardware (e.g., Graphics Card). Apart from creating an unfair advantage for ASIC users, this cuts out a lot of other people who use general pieces of hardware for mining. This defeats the purpose of decentralization and if done widely enough, can result in a 51% attack. Thus, Ethereum improved their algorithm to eliminate the incentive to create specialized hardware by making the payoff similar to the ones using general hardware. ETHASH achieves ASIC resistance by the use of

pseudo-random data set initialized according to the length of the Blockchain. Moreover, acquiring several pieces of such hardware can prove to be very expensive. This gives an average level playing field for everyone who wants to mine Ether, thus making it more decentralized. Bitcoin, on the other hand, is not ASIC-Resistant.

II. ADVANTAGE OVER EACH OTHER

When it's related to both cryptocurrencies which we are comparing here, special attention is needed for the way the mining works for both. Bitcoin's mining is based on proof of work algorithm where Ethereum's mining is going to be changed to proof of stake. Here, in PoW every miner competes with other miners using computational power whereas in PoS, the block validator receives the network fees and there is no other competition.

Ethereum has faster block time, whereas the Bitcoin has a longer block time. Also, in cryptocurrency investing, Bitcoin has managed to outperform Ethereum.

III. CONCLUSION

Now, as we can see, there are plenty of things to know about both Bitcoin and Ethereum, as they are the two largest cryptocurrencies now at the field. In the world of cryptocurrencies, it is vital to know the fundamental differences, characteristics, architectures and their advantages. Now in the market of networking projects, they are two of the most well-known projects where there are over two thousands different ones, and they have their identification. There are already many types of limitation existing, where Bitcoin's legal status varies dramatically in different countries. In some countries, the usage and trade of BTC are encouraged, while in others it is banned.

There have been several concerns regarding Bitcoin's legitimacy; several media outlets have falsely outright claimed that its value depends on the black market and illegal trade. Bitcoin decreased in value when the silk road was shut down. Still, we tried to gather all the data that we can achieve from all the sources and books. We want to help all the students like us who can use this data for their analysis. That's why we prepared the list of all the details that can help the reader and reviewer for their future projects or enhance their knowledge.

IV. ACKNOWLEDGEMENT

Here, we would like to express our sincere respect to our mentor Mr. Tathagata Roy Chowdhury, Assistant Professor, Department Of CSE, Elitte College of Engineering. We also gratefully acknowledge all the authors of our group without whose co-operation this paper will not proceed.

V. REFERENCES

[1] Paul Vigna, Michael J. Casey , 'Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order', Publisher – Vintage; latest edition

[2] Kiana Danial ,'Cryptocurrency Investing For Dummies' , Publisher – For Dummies, 1 edition

[3] Harsh Agarwal ,'Holding – A Bitcoin Wallet Handbook' , Publisher – Kindle edition

[4] Andreas M. Antonopoulos,Gavin Wood, 'Mastering Ethereum' ,Publisher – O'Reilly

[5] Andreas M. Antonopoulos ,'Mastering Bitcoin', Publisher – O'Reilly

[6] Arvind Narayanan, Joseph Bonneall, Edward Felten, Andrew Miller, Steven Goldfeder,'Bitcoin and Cryptocurrency Technologies : A Comprehensive Introduction'. Publisher – Princeton University Press

[7] William Mougayar, VitalikButerin;,'The Business Blockchain: Promise, Practice and Application of the Next Internet Technology ',Publisher -Willey; 1 edition

[8] Saifedean Ammous 'The Bitcoin Standard: The Decentralized Alternative to central Banking'; Publisher – John Wiley & Sons ; 1 edition

[9] Don Tapscott, Alex Tapscott,'Blockchain Revolution: How the Technology Behind Is Changing Money, Business, and the World'; Publisher – Portfolio.