BLOCKCHAIN TECHNOLOGIES

Najiya Hannath[1], Muhammed Shaheen.C.K[2], Faheem Anwer[3]

B.tech III Year, Dept of Computer Science and Engineering

Abstract-Block chain, the foundation of Bit coin, has receivedextensive attentions recently. Block chain serves as an immutable ledger which allows transactions take place in a decentralized manner.The first time blockchain used for bitcoin concept. It envisages an independent secure database without the help of an administrator. Blockchain has been described as the technology of the future and the new internet. Experts certify that there are many opportunities in this new technology. The accelerated blockchain development program is being implemented by the Kerala State Development and Innovation Strategy Council (K-DISC).Blockchain is also described as the backbone of the new type of internet

Blockchain is a distributed database. Block chain is the backbone of the cryptographic currency. Each module in the concept of the bitcoin is closely related with the blockchain.Each transaction in the bitcoin is stored stacks in the block chain .This constantly updating database is extremely safe with no more edits and glove.

Keywords- *Blockchain;Bbitcoin;Hashing; Delegation; Ledger; Cryptocurrency*

1. INTRODUCTION

In the early 1990s, the internet was like that with block chain technology. But the truth is that there is no obvious clarity. Bit coin and crypto currency is not a way connected, just like the email e commences and the social network is connected to the internet. Block chain is another technology like the internet. This has brought about a lot of changes in the world in the last 20 years and also the block chain technology will make even more changes in the next 20 years. Block chain is not bit coin and crypto currency; these are both usages that block chain technology uses. The block chain is considered as a ledger.The concept of block chain came in the 1991. Satoshi Nakamoto brought the concept of bit coin to block chain, that's when a big change took place

Block chain is mean that the collection of single blocks. Each single block is considered as an individual unit. It consists of data, hash and previous hash. . It consists of data, hash and previous hash. Data can be either information about the transaction, land information etc. Hash is similar to finger print. Each block is recognizes with finger print and its value is converted into set of codes. E ach block has hash code. Previous hash means, that is blockchain, each block will put its code in order to identify which block link with it.

While there are dissagreement about Nakamoto's true identity, one is for sure: he brought something revolutionary to the world, and it is up to the users to decide what they want to do with it. Some will take this opportunity and enlarge their own application for solving various problems in the society, others will invest money in those ideas or simply trade with ups and downs of the cryptocurrencies' values at the market.

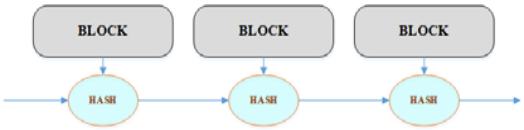
In this paper, we thought of assist a small introduction to the matter of blockchain and cryptocurrencies. We begin with a quick retroactive of some of the most famous solutions for decentralized digital money before Bitcoin, and then we go into the very core of its function, together with Ethereum. These two cryptocurrencies grasp majority of the cryptocurrency market capitalization. Of course, as it happens with new technologies, some limitations and problems materialized, and we described them as well.

2. BLOCKCHAIN TECHNOLOGY AND BITCOIN

A.Proof-of-work in block chain

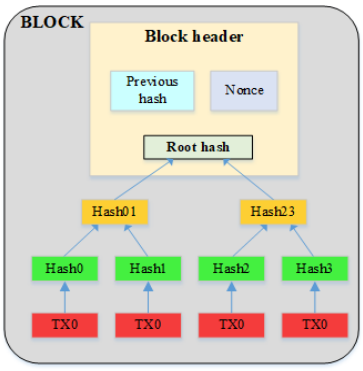
These situations are eliminated (or minimized) in Bit coin network by momentous a proof-of-work from each node that verifies the transaction. The nodes have to do some heavy estimation to prove that they are valid members of the network. As long as the

total computational power of the honest nodes is greater than the computational power of the attacker, the system will remain consistent and all legalized transactions will occur. A set of transactions, together with the hash of the previous block and a nonce, proclaims a block.A timestamp server makes a hash of a block and publicly introduces it, thus proving that the data inside the block must have been alive at the time of hashing. The timestamp server has to confirm that the timestamp of the block is greater than the timestamp of the preceding block in chain and less than two hours into the future. These hashes are associate in a chain and this is called a blockchain, as shown in Fig



The proof-of-work hashing scheme Bitcoinuses is alike to Hashcash [14] and based on SHA-256 hash function [15]. The proof-of-work is done by adding a nonce in the block until the value is produced that has the need number of zero bits at the beginning of the block hash. Once it is done, it cannot be undone without do again the computations. If it is somehow changed by a spiteful attacker, then all the following blocks would have ailing hashes. The rule is that the longest chain that has the majority harmony in the network is the correct one, so if the attacker wishes to change a block, he needs to have adequate computational power to overcome the voting of the majority of honest nodes, thus entering the contest problem.

The transactions inside a block are hashed in a Merkle tree [16], [17]. A Merkle tree is a type of binary tree with numerous leaf nodes, and a root of the leaf nodes is a hash of its children.



B. Bit coin

Bit coin is a decentralized currency that falls under the category of crypto currency. This digital currency is known in the cyber world as bit coin. Crypto currency is a non-physical currency system based on cryptography. This currency system is based on the use of cryptographic techniques and the creation of new coins to verify and validate transactions. Bit coin operates on cryptographic technology that is far safer than using other banking systems. Moreover, transactions are recorded in multiple places, so mistakes are never made. Bit coin is also be mined, as metals such as gold and silver are mined. This term is referred as hashing.

In the case of bit con, there is no central organization or person. Transactions information is sent to all computers where bit coin network is present. Here the public electronic ledges known as a block chain is used to record transaction information

C.Bitcoin network and mining

The first transaction in a block generates a new coin which is possessed by the creator of the block [12]. This gives spur to nodes to confirm transactions, and puts coins into circulation,

since there is not a central authority that issues them. This transaction is known as coinbase transaction. With this approach, the nodes are inducement to stay sincere. The Bitcoin network is deliberate to produce one block in around ten minutes [13]. Since the computational power increases in time, the block time is endure somewhat constant by gradually increasing the difficulty of generating new blocks.

The Bitcoin network begins with new transactions being broadcasted to all nodes. Each node congregate transactions into a block and works on finding proof-of-work, after which it broadcast its block to the network. The nodes in the network agree to receive the block as valid only if all transactions within it are correct and not already spent. If the block is accepted by the network, the chain is being continued by generated the next block and incrementing the hash of the previously added block to it [12].

Beside the reward based on the block creation, the nodes are rewarded with coins and by checking transactions. The procedure of adding new blocks to the blockchain is called mining [7]. The beginning block reward was set to 50 coins (50 BTC) and was deliberate to be gradually split in half with every 210,000 blocks. The initial block in the block chain is the genesis block and is used to supply the initial 50 BTC to the network. The halving of the block creation reward will continue until the reward let fall below one stash, which is the minimal unit of Bit coin and is equal to 10^{-8} BTC [7].

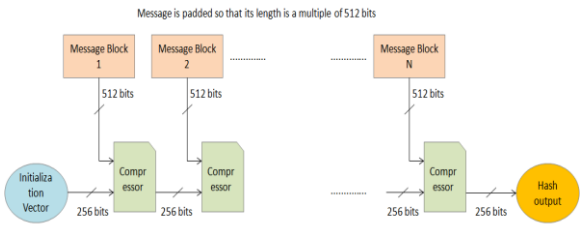
D.Bitcoin extensible problem

With a block size of 1MB, Bitcoin has grevious scalability issues. The number of transactions that can be supported with this block size is less than seven transactions per second (tps) [19]. In contrast, the payment network Visa achieved 47,000 tps during the 2013 holidays, and currently averages with hundreds of millions per day [20]. To attain such rate on Bitcoin network with 1MB block size, assuming that the transaction is 300 bytes in size, it would require a throughput of 8GB per Bitcoin hunk every ten minutes, which would lead to over 400TB of data per year [19]. This would highly centralize the Bitcoin network to support only those nodes with such storage capacities, and this is the very opposite of what Bitcoin and blockchain are intended for. Several solutions were suggested in order to tackle this issue efficiently. As a consequence, number of soft and hard forks of Bitcoin occurred. A soft fork is any change that is backward compatible, i.e. enabling the old software to recognize newly created blocks as valid. A hard fork, on the other hand, is a software update initiating a new rule to the network, thus rendering the old software unable to recognize new blocks

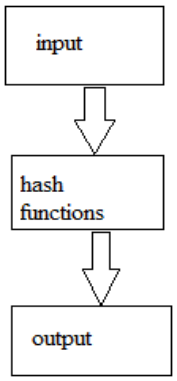
E.Hashing

Basically hash function is a mathematical function which takes an arbitrary length of numerical data and converts it to a fixed length of numerical data. The input may any length but the output is fixed length. For the same input, same is to get the actual input from the hash value.

Hash value is obtained even if there is small change in text it will change in the hash value. It is not possible to get the actual input from the hash value. Hashing is not an encryption. It is impossible to get data back when hashing is done. This output hash value is used in the block chain. Now the people are moving to Secured Hash Algorithm (SHA). Normally SHA2 is used in the block chain technology. This SHA is made by NSA (National Security Agency). SHA has two popular version one is SHA 256 and another one is SHA 512.These number are represent the output bit value



Hashing can be imagined as a machine. A hash of a data will always be same, but if it get its original data will never be found. Any changes to a block will change the value of hash

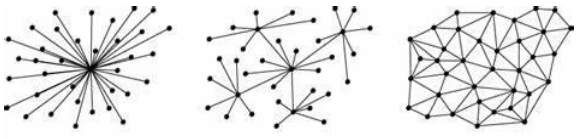


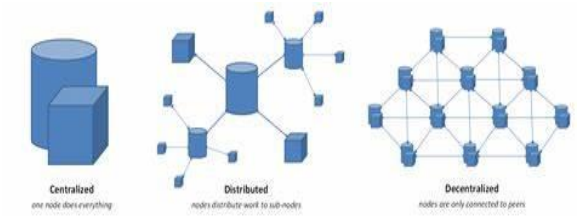
F. Bit coin software

Bit coin app is free, open source software that runs peer to peer protocol like applications like u torrent, bit torrent. B it coin software is available on windows, Linux, Blackberry android platforms. Bit coin software known as the bit coin wallet, it is a wallet that keeps bit coin secure. E ach wallet will have a unique address, such as email, which can be sent to other bit coin customers. Like the email account, the password belongs to the bit coin wallet owner. There are three types of bit coin wallet: software wallet, web wallet, and mobile wallet. If the bit coin wallet is lost, it is impossible to recover. If you lose your wallet or forget your password, you lose your money on the bridge. But the difference here is that the bit coins that are lost cannot be used by others without the owner's wallet key

G.Delegation

In general decentralizationis nota new concept and also we had human civilization for ten thousand years. In these years we had many examples of centralized things. In 2009 Satoshi Nakamoto has found a new concept behind bit coin. He referred it as a peer to peer electronic cash system. It is taken from a white paper in 1962 by Paul Baran. This white paper s called distributing computer network. This graphics is taken from Ethereum Stack Exchange.





This graphics is completely opposite of first graphics. This centralized in first graphics is match with the distributed in the second graphics. The distributed in the first graphics is actually matched with the second graphics. In block chain there is three type of decentralization

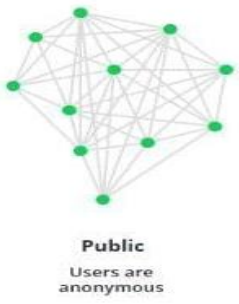
- Artificial Decentralization
- Political Decentralization
- Logical Decentralization

H.Ledger

Ledger is a kind of database where confirmation transaction are recorded

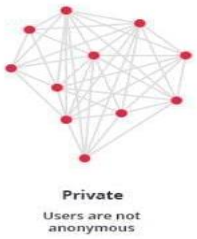
- Distributed ledger
  Block chain platforms don't use a centralized database instead each node has a copy of the ledger. Crypto currencies such as bit coin only stores balance information in the distributed ledger. Block chain platforms such as Ethernum can store any kind of information such as identity information, patient information, real estate information etc…in the distributed ledger.

- Public ledger/Permission less ledger
  When there is no central authority managing access to the ledger, this ledger is called a public ledger or permission less ledger



- Private ledger/ Permissioned ledger
  When there is a central authority directing access to the ledger ,this ledger is called a private ledger or a permissioned ledger

  Bit coin and Ethernum nodes have copies of the ledger but the ledger should correctly depicted the way



I. Cryptography

- Cryptography convert data into particular form so that only those for who it is intended can read end process it. The converted data is however unreadable for an unauthorized user
- In cryptography the fictional characters Alice, Bob, Carol, Dave and Eve used to make it easier for people to understand certain cryptography implementation
- The character Eve ids often used to represent an eavesdropper

J. Encryption and Decryption

- Encryption converts a readable message into unreadable message
- Decryption converts an unreadable message into readable message

2. RELATED WORK

The idea of digital currency is not comparatively new one, but not until recently has it been successfully implemented. In his paper, Chaum hand over an idea of untraceable electronic mail, return addresses, and digital pseudonyms, based on public key cryptography [1]. His technique didn't need a trusted authority and the correspondents could be unnamed. Law et al. presented with an idea of electronic cash also with public key cryptography, but their approach was deliberate for use with banks as central trust authorities [2].

Dwork and Naor [3] proposed a system for utilization in combat against junk mail, by demanding the user to provide a computation of a relatively hard pricing function. This was one of the first ideas of on condition that a proof-of-work as a system for exchanging digital commodities. In the same

manners, authors of b-money [4], reusable proof-of-work [5], and bit gold [6] represented ideas of using computational power as an asset with actual and usable value, comparing it with a precious metal or a minted coin [7].

Vishnumurthy et al. put forward a system for secure peer-to-peer (P2P) resource sharing, KARMA [8]. They distribute with the problem of having nodes in P2P networks that use more network resources than they contribute. With each contribution, a node's karma is incremented, and with each consummation, it is decreased. A set of nodes is in control for keeping records of each node's karma.

However, these approaches either need a trusted party in the form of banks or didn't quite solve the double-spending problem. In the centralized solution, banks or other trusted authorities can control the attempt of parallel issuance of two transactions, but in decentralized system, as in cryptocurrency, this problem carries great importance [7]. Also, since the central authority doesn't exist, the users have to maintain a compatible state of the P2P network, thus disabling the possible attackers to compromise the system with false data.

One of the possible solutions to these problems was the establishment of quorum systems [9], [10]. In these systems, the possibility of having incorrect information and malevolent entities in the network is assumed as true, but the concept of voting is supposed to surpass them [7]. If the majority of nodes in the network is assent about some information, they have the control of the network. However, this approach is susceptible to Sybil attack [11], where hostile node(s) could manipulate many peers with incorrect information, thus overcoming the election and injecting false information.

3 ETHEREUM

A. Overcoming Bitcoin's limitations

Ethereum was initiate in VitalikButerin's paper [29] and convey several limitations of the Bitcoin's scripting language. The main benefaction is full Turing-completeness, meaning that Ethereum supports all types of computations, including loops. Then Ethereum hold up the state of the transaction, as well as several other improvements over the blockchain structure.

Ethereum speak for a blockchain with a built-in Turing-complete programming language. It provides an abstract layer authorize anyone to generate their own rules for ownership, formats of transactions, and state transition functions. This is done by necessitating smart contracts, a set of cryptographic rules that are executed only if certain conditions are met [29].

The concurrence in the Ethereum network is based on modified GHOST protocol (Greedy Heaviest Observed Subtree) [30]. It is generated to tackle the issue of stale blocks in the network. The stale blocks can occur if one group of miners amalgamate in a mining pool has more computing power than the others, meaning that the blocks from the first pool will contribute more to the network, thus creating the centralization issue. GHOST protocol includes those stale blocks into computations of the longest chain.

The centralization problem is detached through providing block rewards to stales, where the stale block receives 87.5% of the reward, and the nephew of that stale block receives the remaining 12.5% of the reward. In this way, the miners are still recompensed even if their block didn't become the part of the main blockchain (those blocks are called uncles). Ethereum uses the moderation of the GHOST protocol which includes uncles up to seven generations [13].

B.Ethereum accounts

The Ethereum state is constitute of accounts, where each account has a 20-byte address and state transitions. The world state is depict between addresses and account states [31].

Ethereum carry two types of accounts: externally owned and contract accounts. An Ethereum account is fantasied four fields: nonce, ether balance, contract code hash, and storage root [30], [31].

Nonce imdicates the number of transactions sent from particular address or the number of contract creations made by an account and is used as a guarantee that each transaction can only be processed once. Ether balance is the number of Wei owned by this address (Wei represents the smallest fraction of Ether, one Ether – ETH, Ð, being equal to 10_{18} Wei). Ether is used for indemnifying transaction fees. Contract code hash is the Keccak-256 hash of Ethereum Virtual Machine (EVM) code of the account, which is executed if an address receives a message call. Storage root is the 256-bit hash of the root node of a Merkle Patricia tree that indicates the content of the account [31]. Merkle Patricia trees (tries) are worn for storage of all (key, value) bindings in Ethereum ecosystem. The block header consists three roots from three tries representing state, transactions, and receipts [32].

C. Ethereum transactions and messages

A transaction is a single instruction that is cryptographically inscribed. There are two types of transactions depend on their products (ones that result in message calls and ones that create new accounts). The transaction is defined as a signed data package dispatched from an externally owned account. Each transaction be composed of the recipient of the message, a signature identifying the

sender, amount of Ether to be sent, an optional data field, STARTGAS, and GASPRICE values [13], [31].

STARTGAS and GASPRICE fields are essential in the combat with attackers on the network. “Gas” is a basic unit of computation. Each transaction needs certain amount of computations, and the STARTGAS field denotes the maximum number of computational steps the transaction is allowed to consume.

Since the miners are remunerating more if they process the transaction with higher GASPRICE, the sender has to choose carefully the GASPRICE value if he wants his transaction to be processed. On the other hand, miners also have to accept some minimal GASPRICE under which they refuse to process a transaction [31].

The Ethereum state transition function, which changes states of the sender and the recipient by accomplishing a transaction, starts with verifying the correctness of the transaction

4 CONCLUSON

Bitcoin and Ethereum today are the most known and treasures cryptocurrencies. They are based on blockchain technology that is deliberated to promote a trust mechanism in a peer-to-peer network based on the consensus of the majority of the nodes. We have shown in this paper a short chronological survey of the early stages of the digital money implementation, as well as the foundations of blockchain technology, and it’s most popular implementations, Bitcoin and Ethereum.

In the past few years, there has been a expeditious growth of numerous cryptocurrencies, hashing algorithms, and consensus agreements in the networks. Some of the cryptocurrencies worth indicating are Ripple, Cardano, NEO, Stellar, Litecoin, EOS, IOTA, Dash, Monero, TRON, Qtum, Lisk, Tether, Stratis, Zcash, Steem, Siacoin, Verge, Electroneum, Nxt, Dogecoin, and many more.

5 REFERENCES

[1] Chaum, “Untraceable electronic main, return addresses, and digital pseudonyms,” in Communications of the ACM, vol. 24, no. 2, pp. 84-88, February 1981

[2] Law, S. Sabett, and J. Solinas, “How to make a mint: the cryptography of anonymous electronic cash,” American University Law Review, vol. 46, no. 4, pp. 1131-1162, 1996

[3] Dwork and M. Naor, “Pricing via processing or combatting junk mail,” in 12th Annual International Cryptology Conference, pp. 139-147, 1992

[4] Tschorsch and B. Scheuermann, “Bitcoin and beyond: a technical survey on decentralized digital currencies,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, March 2016

[5] Vishnumurthy, S. Chandrakumar, and E. G. Sirer, “KARMA: A secure economic framework for peer-to-peer resourse sharing,” 1st Workshop on Economics of Peer-To-Peer Systems, 2003