Blockchain Technology Use on Transactions of Crypto Currency with Machinery & Electronic Goods

Apoorva Ganapathy

Senior Developer, Adobe Systems, San Jose, California, **USA**

E-mail for correspondence: apganapa@adobe.com

Received: Oct 02, 2016; **Accepted:** Nov 23, 2016; **Published:** Dec 25, 2016

Source of Support: Nil **No Conflict of Interest:** Declared

ABSTRACT

Blockchain technology used in transactions of cryptocurrency with machinery & electronic goods' deals with keeping the transactions secure by using blockchain technology so that machinery and electronic goods can be bought by cryptocurrencies. Currently, there are transactions from cryptocurrency based on blockchain networks that can be done securely. The name is coined from the arrangement of records. Single records are referred to as blocks. They are also connected in a list known as chains. Transactions on the blockchain network can be kept secure. Cryptocurrencies can be used just like the normal centralized currencies for any kind of transaction on the blockchain network.

Keywords: Blockchain, Cryptocurrency, Bitcoin, Hashgraph, Nodes

INTRODUCTION

Blockchain is becoming the hottest topic in technology, and it's not hard to see why. The technology, which was popularized after the emergence of Bitcoin in October 2009, provides a decentralized system for secure transactions that cannot be altered or deleted. With blockchain technology, companies have become interested in securing other types of transactions, from a simple contract to an international trade transaction. Blockchain technology's uniqueness is seen in certain features, including transparency, immutability/stability, decentralization, and trust.

The technology that blockchain offers has posed an enormous variety of benefits, especially in its role in cryptocurrency. Since the world has started to tilt towards the use of digital currency (cryptocurrency) in the purchase of products (machinery and electronic goods), it has become vital to discuss the security of transactions using blockchain technology.

What is Cryptocurrency?

Cryptocurrencies are unregulated and decentralized. This means that no central government agencies are issuing it. This is a point of attraction for major investors because its existence and transactions are not subject to government interference or influence (Ganapathy, 2015). In addition, it is based on blockchain technology.

Bitcoin and Ethereum remain the most popular cryptocurrencies, with also the most significant market capitalization. However, over 5,000 cryptocurrencies exist in the digital world today, and more are currently being created every day. Cryptocurrencies can be used just like regular Fiat currencies to purchase things, items, goods, and services online and in the real world. Most persons see cryptocurrencies are an investment like other property investments. I.e., just like investing in the stock market or investing in things like gold and other precious metal.

What is Bitcoin?

Bitcoin was launched in 2009 by an anonymous person called Satoshi Nakamoto and has since then grown in popularity. Bitcoin is a P2P (Peer-Peer) technology that has no central authority. Both the issuance of bitcoin and the management of transactions are done collectively across several networks. It is currently ranked as the dominant cryptocurrency in the world. In recent times, Tesla CEO Elon Musk officially announced that Tesla vehicles can now be bought in the US with bitcoins, the world's most popular cryptocurrency.

As much as bitcoin has high prospects, only a few countries have fully legalized transactions using bitcoins, while others are still skeptical. Some of these countries include the United States, Norway, Canada, El Salvador, Australia, Canada, and European Union.

Blockchain Alternatives

After the emergence of blockchain, other technologies that offer similar functionality have sprung up with promising features. Some of these blockchain alternatives are briefly explained below.

Hashgraph

Hashgraphs is alternative to blockchain that utilizes technologies. It uses consensus establishing information-sharing techniques known as gossip about gossip, which is completely different from the blockchain system, just like the usual gossip scenario where people talk to each other about something, spreading information and data. The Hashgrapgh system works similarly. Data is shared to several randomly selected nodes by a single node. New data and data gathered from other nodes on transactions will jointly be transferred by a close node to another randomly selected node. The first information goes round, and the process is repeated until all the participants get it (Vadlamudi, 2015).

BLOCKCHAIN TECHNOLOGY

Blockchain simply refers to a decentralized (that is, having none of its information stored in a central location) or a distributed record of digital transactions, called blocks connected and shared by an extensive network of participants. Blockchain emerged with one clear message, "NO MORE INTERMEDIARIES," which makes it almost impossible for existing records to be deleted or altered. As a result, financial intermediaries like banks can now be out of the picture thanks to blockchain technology. What makes blockchain so unique? The uniqueness of blockchain comes from a number of its key features:

Decentralization: Before the arrival of blockchain, all we had were fully centralized services. So, for example, the centralized system of banks had to be involved before you're able to get access to your money. Yes, these centralized systems made things better for several years, but there's room for advancement, right? For example, one problem these centralized systems continually face is how it shuts out anyone who needs to use it during an upgrade or change. Because the core of blockchain is decentralization, the complete information is hosted by each node in the network. By implication, every node contains a copy of the entire blockchain history. As such, third parties or intermediaries are not needed for interaction with data. This was one of the reasons bitcoin's popularity speedily skyrocketed. A simple way to relate it is this. No one but you is in charge of your money! This does not outrightly rule out the possibility of hacks in the blockchain. For example, there were 122 attacks in 2020, according to data collected by Slowmist Hacked. In general, however, the decentralized nature of blockchains makes it more difficult to hack compared to traditional infrastructures.

Trust: The addition of new information in blockchain is done by consensus. That is, new records can only be added upon approval by more than fifty percent of the various network participants after verifying that the information cryptographically transmitted is, in fact, correct. Thus, the authentication of information is done within short time spaces, and all participating networks receive the updated information.

Immutability or Stability: In blockchain technology, previously existing data receives new information. After this further information has been successfully added, it can no longer be altered, changed, or lost, making it a permanent historical record not subject to corruption. The stability of immutability that blockchain offers could be precious in the ideal world as far as financial security goes. It can help eliminate fraud while lowering operational risks and reducing administrative costs. In addition, it will become more difficult for people who fraudulently manipulate companies as the intermediaries will completely be eliminated.

Transparency: Transparency and privacy, which are two concepts that blockchain guarantees, seem to conflict, right? Like how is it possible to guarantee both privacy and transparency simultaneously? Here's how it is. This is achieved simply through the use of complex cryptography and public addresses. In cryptocurrencies, users can view all transaction history due to the transparency that blockchain offers. Each user possesses both public and private keys. The public key is shared with other users. Still, another user's private key is impossible to guess, which keeps user data private, which explains how blockchain ensures both transparency and privacy simultaneously.

Disintermediation: Simply put, there is no intermediary. The record of transactions is not maintained by any central entity but by a network of computers worldwide (Ganapathy, 2016). This implies that a transaction can be carried out between two parties without a third party or go-between.

HOW TRANSACTIONS WORK ON BLOCKCHAIN

A typical blockchain transaction is broken down into several applicable steps regardless of its use for either financial or product tracking.

- A record is made of each transaction. Each participant's digital signature is used for authentication of the record, which contains certain details of each participant.
- Each transaction is verified to ensure its validity. For verification, each computer connected to the network checks for the legitimacy of the transaction. The decentralized blockchain system ensures that verification can only be completed after every node in the network agrees.

- Once verified, each transaction is added to a block that gets hashed. Every block (basic groups of transaction records) is unique. Hash value or hash digest is a code appended on each block that helps in identifying each differently, revealing its position within the blockchain. The hash also ensures the integrity of the data to show that it remained the same without alterations since it was recorded on the block.
- After completion, the block is added to the end of the blockchain. The successful addition of the block to the end of the blockchain indicates the end of the transaction. Also, the completion of one block is usually followed by another within a short time.

Consensus Mechanisms

Blockchain consensus mechanisms can be divided into eight types:

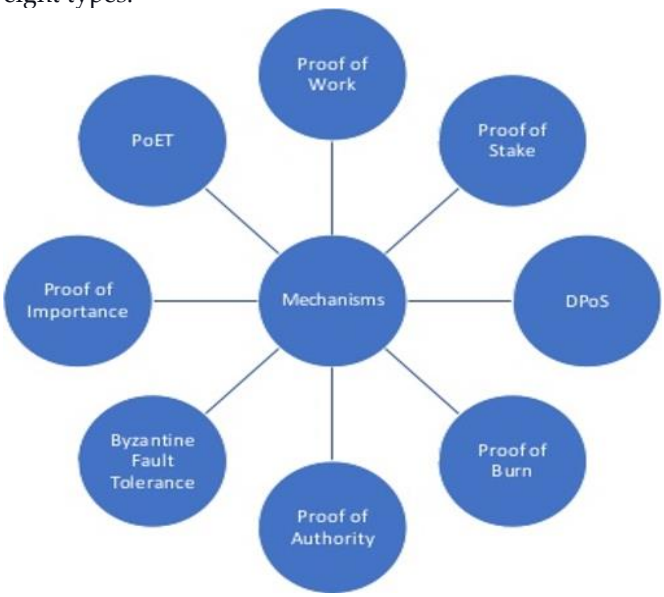

Figure 3: Blockchain Consensus mechanism (Source: slidesharecdn.com)

Proof of Work (PoW): This process is also known as mining, and the miners are nodes. Note that all miners are nodes, but not all nodes are miners and every node in the blockchain network is a potential miner. Miners solve complicated mathematical puzzles that require extensive computational power. Miners utilize multiple mining methods to solve mathematical puzzles. Some of these mining methods include CPU mining, GPU mining, FPGA mining, mining pools, ASIC mining, and more. The reward for being the first to successfully solve the mathematical puzzles is a block. You should also know that solving the puzzles is like a guessing game. Hence, miners require an increasing amount of computational power to find solutions quickly. As the speed at which the blocks are mined increases, the puzzle becomes more difficult. If the blocks are mined quickly, the puzzle gets difficult, and if they are mined slowly, it is easier to solve. Therefore, new blocks have to be created within a particular time frame to carefully adjust the difficulty level of puzzles. Bitcoin, among other popular cryptocurrencies, makes use of this process.

Proof of Stake (PoS): This consensus mechanism uses a randomized process to figure out who gets a chance to produce the next block. Validators have the same responsibilities as miners in proof of work, and they are selected based on the amount or quantity of coins (used as stakes) they can hold. This means that the miner has as much mining power as the coins he holds (Paruchuri, 2015). In this mechanism, transaction fees are used as rewards instead of the blocks used as rewards in proof of works. An alternative to this is the reward of validators with a specific amount of coins due to inflation. With this approach, the Proof of Stake method offers incentives to validators for maintaining the blockchain network. In addition, proof of Stake is more energy-efficient than other blockchain consensus mechanisms like Proof of Work.

Delegated Proof of Stake (DPoS): This consensus mechanism was developed in 2014 by Daniel Larimer and worked like a voting system where stakeholders select several delegates. It is often termed Technological democracy. The delegates (or witnesses as they are also called) that receive the highest number of votes produce new blocks and verify transactions on behalf of all nodes in the network. The voting power of stakeholders is as good as the number of coins or tokens they have. Like in the proof of stake consensus mechanism, transaction fees or a specific amount of coins are used as rewards for the delegates. Compared to Proof of Work and Proof of Stake, Delegated Proof of Stake (DPOS) mechanism is the fastest as it can process transactions per second. Also, delegates can be replaced if fraudulent activity is detected or the delegate fails to perform well, ensuring a continuous block creation process making it the most efficient and organized consensus mechanism.

Proof of Capacity (PoC): In proof of capacity consensus mechanism, miners dedicate digital storage spaces which would be used to store possible solutions to the cryptographic puzzles. The larger the storage space, the more possible solutions can be stored and the better the chance of finding a matching solution which can, in turn, earn the miner a block as a reward (Donepudi, 2015). This consensus mechanism consumes way less energy than the proof of work.

Proof of Elapsed Time (PoET): Proof of Elapsed Time is a consensus mechanism that Intel Corporation developed in 2016. This mechanism uses wait time instead of competition like in other consensus mechanisms to determine which miner or node produces a new block. A random wait time is allocated to each user, and the user with the shortest wait time produces a new partnership which is added upon verification.

Proof of Identity (PoI): Proof of Identity compares the private key of a user with an authorized identity. Proof of Identity is cryptographic evidence for a user's private access that is cryptographically attached to a specific transaction. Any identified user from a blockchain network can create a block of data presented to anyone in the network. Proof of Identity ensures integrity and authenticity of created data. Smart cities can adopt this consensus mechanism for the verification of their citizens' identities.

Proof of Authority: Proof of Authority mechanism is an algorithm that stakes identity (validators make their identity public). Thus, there is no competition and almost no need for computing power which equates to almost no electricity. Validators are selected based on reputation and not the number of tokens or coins they hold. These validators are responsible for verifying transactions and adding new blocks to the network. Validators are given incentives as rewards for staking their identities to preserve the blockchain network.

Proof of Activity (PoA): Proof of Activity consensus mechanism is a combination of proof of work and proof of stake. First, miners compete to solve a mathematical puzzle-like in PoW or mine a new block. The new block produced by the first miner would contain a header and his reward address. To validate the block, a group of validators or witnesses will be selected at random. After proper consideration of the new block, while taking the header details into account, the new block will be validated and added to the existing blockchain. Also, note that if most validators or witnesses do not sign in the new block, it will be discarded. The next winning block will be considered and validated by a new set of randomly selected validators. Also, a validator's likelihood of being selected to sign in a new block lies in how much coin (token) he holds. Both the winner, miner, and validators will be rewarded.

Types of Blockchain Technology

Public Blockchain: A public blockchain is ideal if the aim is to create an open blockchain closely related to bitcoin, which allows the participation of any and every one within the network. Participation in the core activities like reading, writing, and auditing the blockchain network is free in the public blockchain. The public network encourages new members to join to keep active by providing incentives. Public blockchains are permission less and truly decentralized, making it difficult to alteration of data. Some popular public blockchain includes Bitcoin, ethereum, and litecoin.

Private Blockchain: A private or consortium blockchain is ideal if the aim is to allow only a few to gain access and contribute to the network, just like how private businesses run. Imagine a party that can only be attended strictly by invitation. That's just how the private blockchain works, as there are restrictions on who can be participants in the network. The network operators or a well-structured protocol set up by the network also need to ensure accuracy and validity. The main variation between the public and private blockchain is a restriction of access and participation in the blockchain network to a selected few in a private blockchain. In contrast, the public blockchain is open to any and everyone. Furthermore, only a single or few entities control the blockchain network in a private blockchain, which technically makes it not decentralized.

Permissioned Blockchain: In permission blockchain, both public and private blockchain characteristics are featured, and it also allows room for customization. These incorporate permitting anybody to join the permissioned network after an appropriate check of their personality and distribution of select and assigned consents to perform just certain exercises on the network. Ripple is an illustration of permission blockchain as jobs are given to members by consent. Such blockchains are fabricated, so they award exceptional consents to every member. This permits members to perform explicit capacities like reading, access, and compose data on the blockchains. Organizations are progressively picking permissioned blockchain networks. This permits them to specifically put limitations while configuring the networks and control the exercises of the different members in the ideal jobs.

Permission less Blockchains: As the name implies, this type of blockchain has no restrictions on who could be a part and also contribute to the network. In simple terms, it is a decentralized ledger open to the public. The majority of cryptocurrencies, including the popular bitcoin, runs by permission less blockchain networks.

Security and Privacy Methods Used in Blockchain based Systems

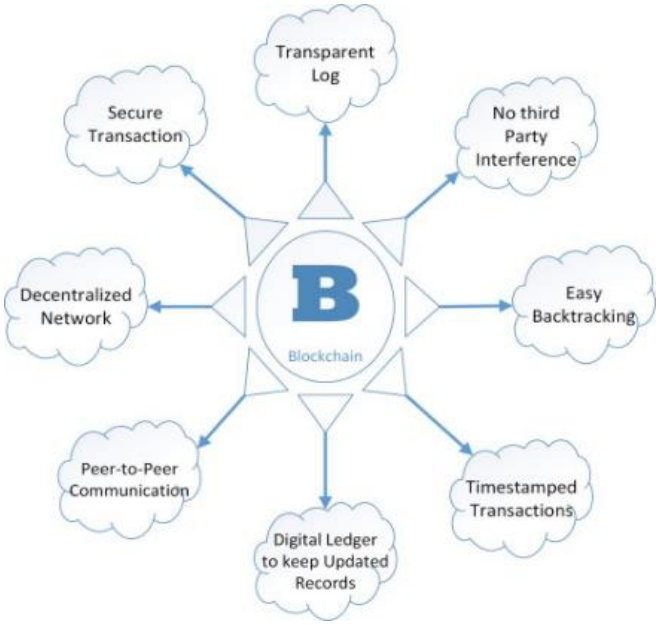

Figure 4: Blockchain Privacy (Source: ars.els-cdn.com)

Attribute-Based Encryption Algorithm: In attribute-based encryption, changes from cipher text to plain text (decryption) and vice versa (encryption) are based on attributes. Decryption can only be done when there is a match between attributes of the secret key and that of the encrypted data (ciphertext). Although researchers have proposed this method to ensure privacy and security on Blockchain, it has still not been implemented because of inadequate knowledge of both the concept and its implementation.

Anonymous Digital Signatures: Anonymous Digital Signatures are digital signatures that offer users privacy (Neogy & Paruchuri, 2014). Group signature and ring signature are two digital signatures that can improve the security and privacy of applications or systems that use blockchain.

Group Signature: In this case, a group of users is formed, and they share a public key while possessing individual private keys. So when a group member signs a message using a private key anonymously, the remaining members use the shared public key to verify the signature. During the verification process, only the membership of the signer is disclosed; the signer's identity remains secret. Also, the group has a leader responsible for resolving issues, if any. For example, the group leader can reveal a user's identity and remove and add members. This method can be used in consortium (private) Blockchain to enhance security.

Ring signature: This technique is similar to the group signature technique because any group member can sign a message on behalf of other members with his private key and verification done by other group members with their shared public key. But instead of group signature, there is no group leader, and users can form the group themselves. This method can be used in public Blockchain.

Mixing: To eliminate the possibility of having users trailed by their transactions and their identity revealed in blockchain, the concept of mixing was proposed. In this method, user transactions and assets that can be tracked are mixed, thereby obscuring the trail that can lead to the user.

Homomorphic Encryption Algorithms: The process of decrypting data from cipher text to plain text makes the data vulnerable to hackers. As such, a homomorphic encryption method was proposed. In this method, operations can be done on the ciphertext without decrypting it, thereby ensuring user privacy and security. Moreover, it likewise guarantees that when a similar activity is performed on similar encrypted information after decryption, i.e., returned to the plaintext, and the outcome produced is equivalent to the output created on the ciphertext (Vadlamudi, 2016). With no changes in the blockchain abilities, homomorphic cryptography can be effortlessly utilized on the information in the blockchain, which guarantees the protection of the information in the public blockchain and permits evaluating and overseeing the data in an encrypted structure were.

A system with Non-Interactive and Zero-Knowledge Proof: Non-Interactive Zero-Knowledge (NIZK) is an incredible technology for cryptography that protects the framework's security utilizing the idea of zero-knowledge pieces of evidence. The idea driving it's anything but a program can be executed with some obscure (private) input information and the yield (public), which is produced without uncovering some other insight regarding the information or clients; which implies a client can demonstrate about some case to be valid by establishing it without disclosing the truthful information. A variation of the NIZK framework recommended that zero-knowledge computational knowledge be accomplished without cooperation among the clients. A similar idea can likewise be utilized in a blockchain-based framework as the information inside the squares is put away after scrambling. Hence, a client can make the exchange by using the NIZK evidence without uncovering the authentic information.

Secure Multiparty Computation Protocol: This model hosts a protocol for various parties that assist in completing some joint calculations on the private information of those parties, and the output is given without spilling anything about their knowledge (maintaining privacy). At first, the protocol was intended for two parties in particular, which was then summed up for various parties, and it permits partaking cryptically. This summed-up form has been utilized for some MPC instruments for applications like voting, offering, sell-off, and so on. In addition, blockchain-based systems have received the MPC in the last few years for applications, such as a "multiparty lottery system" that guarantees reasonableness with no position.

CONCLUSION

The advancements in blockchain technology as attracted a lot of attention—several financial corporations and companies, are incorporating blockchain technology into their system for more security and transaction efficiency. Blockchain technology has evolved to accommodate several types of transactions. With the development and design of several new cryptocurrencies like bitcoin, stable coins, and altcoins, trades on the blockchain network need to be better secured to avoid hacks and security breaches. In times to come, cryptocurrency would become be widely used and generally accepted at a level higher than the current rate. Which would necessitate a better security network for blockchain.

REFERENCES

Donepudi, P. K. (2015). Crossing Point of Artificial Intelligence in Cybersecurity. *American Journal of Trade and Policy*, *2*(3), 121-128. https://doi.org/10.18034/ajtp.v2i3.493

Ganapathy, A. (2015). AI Fitness Checks, Maintenance and Monitoring on Systems Managing Content & Data: A Study on CMS World. *Malaysian Journal of Medical and Biological Research*, *2*(2), 113-118. https://doi.org/10.18034/mjmbr.v2i2.553

Ganapathy, A. (2016). Speech Emotion Recognition Using Deep Learning Techniques. *ABC Journal of Advanced Research*, *5*(2), 113-122. https://doi.org/10.18034/abcjar.v5i2.550

Neogy, T. K., & Paruchuri, H. (2014). Machine Learning as a New Search Engine Interface: An Overview. *Engineering International*, *2*(2), 103-112. https://doi.org/10.18034/ei.v2i2.539

Paruchuri, H. (2015). Application of Artificial Neural Network to ANPR: An Overview. *ABC Journal of Advanced Research*, *4*(2), 143-152. https://doi.org/10.18034/abcjar.v4i2.549

Vadlamudi, S. (2015). Enabling Trustworthiness in Artificial Intelligence - A Detailed Discussion. *Engineering International*, *3*(2), 105-114. https://doi.org/10.18034/ei.v3i2.519

Vadlamudi, S. (2016). What Impact does Internet of Things have on Project Management in Project based Firms?. *Asian Business Review*, *6*(3), 179-186. https://doi.org/10.18034/abr.v6i3.520

--0--

SOCIAL SCIENCE RESEARCH NETWORK

2171 Monroe Avenue, Suite 203, Rochester, NY 14618, USA

http://www.ssrn.com/en/

AJTP Link: https://www.ssrn.com/link/American-Journal-Trade-Policy.html