BLOCKCHAIN TECHNOLOGY

Dr. A. Meena Kabilan, [2]Sneha Srikanth, [3]Nandhitha.R

[1]Professor, [2,3]UG Scholar

Dept. of Computer Science & Engineering

, Sri Sairam Engineering College, Chennai

Abstract

A growing list of records which are linked using cryptography is called a Blockchain. These lists of records are called blocks. Every block in the chain contains three things: a cryptographic hash of the previous block, a timestamp, and the transaction data. By natural design, any block in the blockchain is resistant to any modification of the data. It is an open distributed ledger that can record the transferred data between any two parties efficiently. It is a verifiable, irreversible and permanent way. This blockchain is a technology that is typically managed by a peer-to-peer network that collectively adheres to a protocol for inter-node communication and validation of new blocks to be added to the chain. The blockchain technology was mainly believed to be invented for the usage of virtual money transactions. Bitcoin is a crypto currency which is a form of electronic virtual cash that offers a decentralized digital currency system. Being driven by the process that happens at the background of the Bitcoin blockchain, this paper mainly focuses on the usage of blockchain technology for voting process. Blockchain voting is also similar to analogue voting. Though, every nascent technology is viewed as a double-ended sword and has its own pros and cons. This paper highlights the ways in which voting can become more effective and more liable by involving the participation of every citizen.

Keywords: Cryptography, Blocks, Bitcoins, Transaction, Vote, Trust.

1. INTRODUCTION

The blockchain is a set of growing records that has no single administrator. This technology is a peer to peer network in which blocks are linked using suitable cryptography techniques. The blockchain is an open distributed ledger of records which is immutable and involatile. The blockchain technology was widely used for the Bitcoin, the first digital currency to solve the double-spending problem without the need of a trusted authority or any central authority. The blockchains provide a platform which is readable by the public and nowadays used as a payment gateway. Private blockchains have opportunities to develop business.

2. BITCOIN BLOCKCHAIN

Bitcoins was first registered under the domain name "bitcoin.org" on 18 August 2008. These bitcoins was invented by an unknown person or group of people using the pseudonym 'Satoshi Nakamoto'. Later in November 2008, a paper was posted to a cryptography mailing list which was authored under the name 'Satoshi Nakamoto' which was titled Bitcoin: A Peer-to-Peer Electronic Cash System. The bitcoin software was implemented and available as an open source code and it was released in January 2009. The identity of Nakamoto remained unknown and he was known to be the first person who mined the first block of the bitcoin blockchain, known as the genesis block. Nakamoto handed over the network alert key and control of code to Andersen who decided to make the technology decentralized and public. The first bitcoin transaction was initiated by a person named Hal Finney, in 2004.

3. MINING

The blockchain is a public ledger which records all type of transactions which is peer to peer between any two nodes or parties. This technology is implemented

as a chain of blocks. Each block of the chain contains a hash of the previous block up to the genesis block of the chain. The maintenance of the chain is performed by a network of communicating nodes (computers that have high computational power) running the software. Mining is a technique that is used for record-maintaining service that can be done through computer processing power. Mining is also referred as a distributed consensus system that is used to confirm the pending data updates by including them in the block chain. This system enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the transmitted data. The blockchain is kept consistent, complete, and unalterable

by the miners. They repeatedly group the newly broadcast data into a block, which is then broadcast to the network and verified. Each block contains a SHA-256 (type of hashing technique) cryptographic hash of the previous block, thus linking it to the previous block and giving the blockchain its name. To be accepted by the whole network, a new block must contain a so-called proof-of-work (PoW). The PoW algorithm requires miners to find a number called a nonce, such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's difficulty target. This proof is easy to verify for any node in the network, but it is extremely time-consuming to generate. This is due to the fact that for a secure cryptographic hash, miners must try many different nonce values before meeting the target. The proof-of-work algorithm makes modifications of the blockchain extremely hard, as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted. As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks increases.

Fig. 3.1.

4. DATA TRANSMISSION

In Blockchain, the data transmissions are defined using a Forth-like scripting language. This scripting language is based upon stack based computer programming. These transmissions may consist of one or more inputs and one or more outputs. In case of the bitcoin blockchain the transactions take place in the form of 'payer

X sends Y bitcoins to a payee Z'. When a user wants to send bitcoins, the user designates the receiver address and the amount of bitcoin being sent to that address as the input. The blockchain network uses public-key cryptography, in which there are two cryptographic keys, public key and private key. At basic, a wallet is a collection of both of these keys.

5. WORKING OF BITCOINS USING THE BLOCKCHAIN

A wallet is something that stores the information necessary for transaction of digital data. Wallets are more often described as a place to hold or store assets. A better way to describe a wallet relating to the bitcoin blockchain is something that "stores the digital credentials for your bitcoin holdings" and allows one to access them. Once a Bitcoin wallet is installed on the computer or mobile phone, it will generate the first Bitcoin address and one can be created whenever necessary. The address of the wallet can be disclosed to the contacts in your personal list so that they can pay you or vice versa. In fact, this process is pretty similar to how an email works, except that the bitcoin address can be used only once.

Fig. 5.1.

A transaction refers to the transfer of any digital value or data between the wallets that gets included in the block chain. Bitcoin wallets assigns a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof. All transactions are broadcast to the network and usually begin to be confirmed within 10-20 minutes, through a process `called mining.

6. PROPERTIES OF BLOCKCHAIN

1. Irreversible: After adding a block into the chain, it can not be reversed by nobody. And nobody means nobody. Not you, not the miners, or anyone else who views the data on the chain. Once the data is added it remains permanent and immutable.

2. Pseudonymous: Neither the money nor the accounts used in blockchains applications like the bitcoin are connected to real world identities. A person receives Bitcoins on so-called addresses, which are randomly seeming chains of around 30 characters (alphabets and numbers).

3. Fast and global: The mining process which is at most essential for the blockchain is propagated nearly in an instant and is confirmed in a couple of minutes. Since they happen through a global network of computers they are completely indifferent of the physical geographical location.

4. Secure: The data in the blocks are safely secured using a public key. For validation, the transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent the modification of previous blocks because doing so would invalidate all the other subsequent blocks. This ensures that no group or individual can control what is included in the blockchain or replace

parts of the block chain to roll back their own spends or modify it based on their needs.

7. ELECTION AND ELECTORAL FRAUD

An election, by definition is a formal group decision-making process by which the people in the country choose an individual to hold public office. In simple words, an election can be any process in which the head or leader of an organization is to be elected. Sometimes, elections do not take place in a fair manner and subjected to certain malpractices known as electoral fraud. This illegal interference is not encouraged and it may tend to change the opinion and decisions for which the election is conducted. These malpractices can include confusing or misleading voters about how to vote, violation of the ballot, ballot stuffing, tampering with voting machines, voter suppression, voter registration fraud, fraudulent tabulation of results and many more. Nowadays, electronic voting machines are widely adapted for voting. Though this is an effective and trusted method to count votes, all voting systems face threats of some form of electoral fraud. To prevent such kind of fraud, new methods can be adopted for voting. One such trusted and effective method can be the usage of blockchain technology. Inorder to cast a digital vote, a democratic citizen would need to register and prove their citizenship that is associated with their user key.

8. POWER OF BLOCKCHAIN IN VOTING

In its most basic form, blockchain is a public digital ledger. This technology runs based on the power from peer to peer networks or interconnected nodes to verify, process and record data. Blockchain's database is incorruptible and easily verifiable due to its encryption and decentralization features. It also has its unique advantage that it cannot be taken down or influenced by a single party because it does not exist in one place alone. Blockchains are not

only used for financial transactions, but any kind of data transmission. Hence, this kind of infrastructure can be extremely beneficial

for voting as votes are small piece of high value data. Online voting methods are also prone to hacking and tampering. To resolve most of these encountered problems, a blockchain based voting application can offer high security. Voters can submit their vote without revealing their identity or political preferences to the public. Officials can count votes with absolute certainty and security. Each id can be attributed to only one vote.

In this method, the voters will be able to log in to an application which ensures the voters real identity via biometric information that is already available in the government's database. This can be done through a mobile phone or a personal computer from anywhere and it ensures that the citizen is eligible to cast a vote. Once the person's identity matches with that in the authentic database of the government, then the voter can proceed to register the vote of his choice. The idea to verify that the person

who submitted the citizenship documents is as same as the person who is active at the computer or mobile during the time of vote.

On the blockchain, the information about the sender has to be hidden which can be accomplished by various methods such as zero knowledge proofs, ring transactions, or any other encryption techniques. This vote gets transformed into a block and gets added to the chain after validation by the miners. After which the officials can arrive at the outcome based on the data stored in the blockchain. There can be no manipulation, recording errors o tampering.

9. POSSIBLE IMPLICATIONS

1. Increased transparency: Transparency is the biggest benefit of blockchain voting method. In the current voting system, we do not know what happens to the vote once it is casted. On

the blockchain it is possible to track and it remains history.

2. Reduced fraud & Election rigging: The chance of fraudant votes gets reduced. The result could be the real opinion of the people in the democracy.

10. CONCLUSION

Blockchain is becoming recognized as a technology that can pave way for a direct democracy, where people can decide the course of policy themselves, rather than relying on representatives.

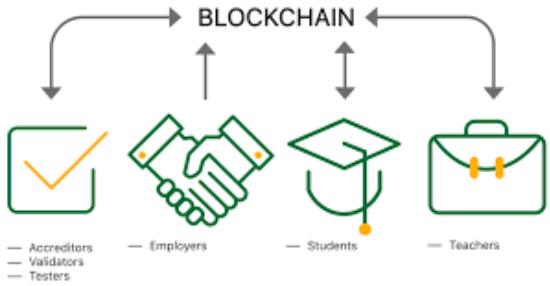

Fig. 10.1.

REFERENCES

1. https://www.google.co.in/search?source=hp&ei=RR1vW7zQNYzMvwSS-72QAQ&q=cryptocurrency&oq=crypoto&gs_l=psy-ab.1.0.0i10k1l10.862.3101.0.6233.8.7.0.0.0.0.200.432.1j1j1.3.0....0...1.1.64.psy-ab..5.3.429.0..0.0.AcZbPc8Kd5U
2. Jonathan john's "Transaction using bitcoins"
3. https://en.wikipedia.org/wiki/Cryptography
4. Siddique Ahemed's working of bitcoins in brief