Research and analysis of Blockchain security

Introduction

The blockchain technology was first described in 1991 by stuart haber and w.scott .they wanted to introduce a practical solutions for time stamping digital document so that they could not be backdated or tampered .Well this was the idea but blockchain was first introduced in 2008 in the form for blockchain . Then was the amazing thing blockchain was discovered

What is blockchain

Blockchain is the series of block that forms a chain a blockchain can be of 2 blocks to infinity blocks .

In a block there is data , previous hash , new hash . This 3 elements provide data and security to blockchain . Like steve jobs said keep it simple , when you get too complex you forgot the obvious thing you remember , “See it big .and keep it simple “ is said by steve jobs . In block you store data , Now you will say that if we change the blocks then the data can be changed but we can only change the blocks if it is some blocks but what if we have thousands of blocks attaching the block which we changed ,then comes the problem here we cant change thousands of blocks as it can take some years or even decades .This amazing feature of blockchain makes it nearly impossible to hack

Hash function – Hash functions is kind of a algorithm that is used in blockchain for getting a random sequence of 64 bit which is used in safe guarding the data There are many Hash functions like SHA – 256 ,SHA -1 etc

Properties of blockchain

1 Decentralised – Blockchain is decentralised where data is not stored with one person or one place

2 Time stamping - Every transactions , data storage , block creation gets time stamping . this feature provides transparency and full transactions history

3 Immutibilty – Data once stored in a block cannot be deleted or altered

4 Access and governance system - Every blockchain gets characterized through its access and government systems

\*

Blockchain security How is blockchain made

This is most interesting part of blockchain . Blockchain contains data ,previous hash and new hash , in first block data is inserted and then it is given a hash which is 64 bit sequence then the first block is chained with 2nd block , the hash of the first block is given to 2nd block where data gets stored it contains hash of 1st block and its new hash which is 64 bit sequence now the hash of 2nd block is given to 3th block as previous hash now 3thblock stores some data previous hash (hash of 2nd block)and it gets a new hash . That’s it how a blockchain is made .

Now you will say where is security in the above blockchain

If we try to access data in one block then the hash of that block changes with change of the first hash the next block also changes which causes domino effect where one is changed all is changed . one of features of blockchain is that when data is added it records the time and data and whenever there is change in hash or data it even records it which makes it kind of a permanent and unchangeable . So this feature of blockchains makes it amazing as if one person tampers one block then he has to change all the blocks that are connected to it which makes it very difficult for one person to hack it

We can divide blockchain in 2 parts :

1 private blockchain

2 public blockchain

Private blockchain - In this type of blockchain everyone is not equal as public blockchain but we have to make an organization .Then the organization how the structure of the network should be . In this users gets divided in roles as per organization . So how does blockchain security works in this , Here the blocks are made by the people having authority regarding this and when blocks need to be appended then a voting system is created where to approve the changes majority should be ok with it

Public blockchain – In this type of blockchain users are all same where no authority can stop .For example Bitcoins transactions , This is public blockchain where anyone can come and buy and sell Bitcoins .

Smart Contracts :

Smart Contracts allow for transactions to be made automatically and without the need to rely on a central party to adjust the operation of the contract terms . Smart Contract code can be written directly onto a block and is examinable by contracting parties ahead of time . just like legal contract

IF it is agrees to , then the smart contract will automatically execute its own term . This means releasing a payment following a certain trigger , running a software account or account an investment

Advantage of smart contract over legal contract is that they reduce the risk of fraud . With legal contract if contract is broken they enforce terms after the damage is done But , smart contracts prevent this as they operate on stated terms regardless the person . The contract will carry out only code

Conclusion :

By concluding this research paper we can say that blockchain is really good for security ,as it is decentralised , immutable , having time stamp features in it . We can say that blockchain is kind of a record where everything is stored . By , dividing blockchain into public blockchain and private blockchain we made a private security feature where one person must have a majority of votes to append a block .

The size limit of blocks can differ between varying blockchains. It depends on blockchain if user wants to keep all its file on chain or they have ti use off chain solutions like cloud or IPFS(Inter Planetary File system .When a file is made with the help of IPFS In relation with blockchain the chain only stores an associated hash that references to the actual file on IPFS (off chain solutions )

Blockchains also is used in many start ups but not in large scale . Some governments use it for voting system and some private companies like crowdfunding use blockchain

References

[https://www.frontiersin.org/articles/10.3389/fbloc.2019.00016/full](about:blank)

[https://www.techtarget.com/searchcio/definition/blockchain](about:blank)

[https://www.researchgate.net/publication/318131748\_An\_Overview\_of\_Blockchain\_Technology\_Architecture\_Consensus\_and\_Future\_Trends](about:blank)

[https://www.diva-portal.org/smash/get/diva2:1365314/FULLTEXT01.pdf](about:blank)

[https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf](about:blank)