International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 06 Issue 13
December 2019

Block Chain Technology using Machine Learning

V . Subhalakshmi[1], Dr.U.vidyasagar[2], Dr. P. Veereesh[3]
[1]P.G. Scholar, [2]Associate Professor, [3]Head of the Department
[1,2,3] St. John's College Of Engineering & Technology , Yemminagur
Email:- [1]subhareddy9848@gmail.com, 2engg.sagar@gmail.com

ABSTRACT

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof- of-work.

Keywords: - Bock chain, Machine Learning, cryptographic.

INTRODUCTION

Trade on the Internet has come to depend only on monetary foundations filling in as confided in outsiders to process electronic installments. While the framework functions admirably enough for most exchanges, despite everything it experiences the inborn shortcomings of the trust-based model. Totally non-reversible exchanges are not so much conceivable, since budgetary organizations can't abstain from interceding questions. The expense of intervention builds exchange costs, constraining the base down to earth exchange size and removing the likelihood for little easygoing exchanges, and there is a more extensive expense in the loss of capacity to make non-reversible installments for nonreversible administrations. With the plausibility of inversion, the requirement for trust spreads. Traders must be careful about their clients, bothering them for more data than they would some way or another need. A specific level of misrepresentation is acknowledged as unavoidable. These expenses and installment vulnerabilities can be maintained a strategic distance from face to face by utilizing physical cash, yet no component exists to make installments over an interchanges channel without a confided in gathering.

What is required is an electronic installment framework dependent on cryptographic evidence rather than trust, enabling any two consenting partakers to execute legitimately with one another without the requirement for a confided in outsider. Exchanges that are computationally unrealistic to switch would shield dealers from misrepresentation, and routine escrow components could without much of a stretch be executed to secure purchasers. In this paper, we propose an answer for the twofold spending issue utilizing a shared disseminated timestamp server to produce computational verification of the sequential request of exchanges. The framework is secure as long as legitimate hubs all in all control more CPU control than any coordinating gathering of assailant hubs.

Related Work

You may have heard the term 'block chain' and rejected it as a craze, a popular expression, or even specialized language. In any case, I accept block chain is a mechanical development that will have wide-arriving at suggestions that won't simply change the monetary administrations however numerous different organizations and businesses.

A block chain is a disseminated database, implying that the capacity gadgets for the database are not all associated with a typical processor. It keeps up a developing rundown of requested records, called blocks. Each block has a timestamp and a connect to a past block. Clients can just alter the pieces of the block chain that they "claim" by having the private keys important to keep in touch with the record. Cryptography guarantees that everybody's duplicate of the disseminated block chain is kept in sync.

Block chains are secure databases by structure. The idea was presented in 2008 by Satoshi Nakamoto, and after that actualized without precedent for 2009 as a component of the advanced piece coin money; the block chain fills in as the open record for all piece coin exchanges. By utilizing a block chain framework, bit coin was the primary computerized cash to tackle the twofold spending issue (in contrast to physical coins or tokens, electronic records can be copied and spent twice) without the utilization of a legitimate body or focal server.

Fig: 1.1 Block Chain Model

Shutter stock

The security is incorporated with a block chain framework through the dispersed time stepping server and distributed system, and the outcome is a database that is overseen self-rulingly in a decentralized manner. This makes block chains incredible for account occasions like restorative records exchanges, personality the board, and demonstrating provenance. It is, basically, offering the capability of mass disintermediation of exchange and exchange preparing.

1.2.1 How does block chain really Work

A few people have called block chain the "web of significant worth" which I believe is a decent similitude. On the web, anybody can distribute data and after that others can get to it anyplace on the planet. A block chain enables anybody to send esteem anyplace on the planet where the block chain record can be gotten to. In any case, you should have a private, cryptographically made key to alter just the blocks you "possess." Using your private key and another person's open key you can move the estimation of whatever is put away in that segment of the block chain. Along these lines, to utilize the bit coin model, keys are utilized to move blocks, which contain units of money that have budgetary worth. This fills the job of account the exchange, which is generally completed by banks. It likewise fills a subsequent job, building up trust and character, in light of the fact that nobody can alter a block chain without having the comparing keys. Alters not confirmed by those keys are dismissed by the system. Obviously, the keys like a physical cash could hypothetically be taken, yet a couple of lines of PC code can for the most part be kept secure at next to no cost. (In contrast to, state, the cost of putting away a reserve of gold in a famous Fort Knox.) This implies the significant capacities completed by banks confirming personalities to anticipate misrepresentation and afterward recording genuine exchanges can be done by a block chain all the more rapidly and precisely.

Why is block chain important

We are largely now used to sharing data through a decentralized online stage: the web. In any case, with regards to moving worth for example cash, possession rights, protected innovation, and so forth we are typically compelled to fall back on antiquated, brought together organizations or foundations like banks or government offices.

.

Block chain innovation offers the interesting probability of taking out this "go between". It does this by filling three significant jobs recording exchanges, building up personality and setting up agreements customarily did by the money related administrations part. This has colossal ramifications on the grounds that, around the world, the budgetary administrations market is the biggest segment of industry by market capitalization. Supplanting even a small amount of this with a block chain framework would bring about a colossal disturbance of the money related administrations industry, yet additionally a huge increment in efficiencies.

The third job, setting up agreements, opens up a fortune trove of chances. Aside from a unit of significant worth (like a piece coin), block chain can be utilized to store any sort of computerized data, including PC code. That bit of code could be customized to execute at whatever point certain gatherings enter their keys, along these lines consenting to an agreement. A similar code could peruse from outer information channels stock costs, climate forecasts, news features, or anything that can be parsed by a PC, truly to make gets that are naturally recorded when certain conditions are met.

These are known as "shrewd agreements," and the potential outcomes for their utilization are for all intents and purposes perpetual. For instance, your savvy indoor regulator may convey vitality utilization to a shrewd matrix; when a specific number of wattage hours has been come to, another block chain consequently moves an incentive from your record to the electric organization, successfully mechanizing the meter peruser and the charging procedure. Or then again, shrewd agreements may be put to use in the guideline of protected innovation, controlling how often a client can access, offer, or duplicate something. It could be utilized to make extortion evidence casting a ballot framework, restriction safe data dissemination, and considerably more.

Objective

An absolutely distributed rendition of electronic money would enable online installments to be sent straightforwardly starting with one gathering then onto the next without experiencing a budgetary foundation. Advanced marks give some portion of the arrangement, yet the primary advantages are lost if a believed outsider is as yet required to avoid twofold spending. We propose an answer for the twofold spending issue utilizing a distributed system. The system timestamps exchanges by hashing them into a continuous chain of hash-based confirmation of work framing a record that can't be changed without re-trying the evidence of-work. The longest chain not just fills in as confirmation of the succession of occasions saw, however verification that it originated from the biggest pool of CPU control. Up to a lion's share of CPU power is constrained by hubs that are not coordinating to assault the system, they'll create the longest chain and outpace assailants. The system itself requires insignificant structure. Messages are communicated on a best exertion premise, and hubs can leave and rejoin the system voluntarily, tolerating the longest confirmation of-work chain as evidence of what occurred while they were no more.

SYSTEM DESIGN

Introduction

Block chain, as the underlying technology of bitcoin, has entered the public eye. Block chain is a distributed book composed of data blocks based on cryptography. Each block contains a large amount of transaction information to verify the validity of the information. The prominent advantage of block chain technology lies in the decentralized design. Block chain system consists of a large number of nodes to form a point-to-point network. The rights and obligations of any node are equal. The data in the system is maintained by all nodes, and they are independent of each other. By using asymmetric encryption technology, timestamp, Merkletree, consensus mechanism and incentive mechanism, point-to-point transactions based on decentralized creditare implemented in independent node distributed networks.

Because of the high reliability and safety, lowcost and high efficiency of decentralization, the problems of centralization are solved. Block chain is not only a technological innovation, but also the opening of an era. Block chains make the big data more accurate, while big data make the data of block chain more valuable. The block chain can make the big data flow more safely and ensure the privacy of data. Considering the impact of block chains on accounting from the perspective of large data ensures the high security of accounting and the unalterable and traceability of data, which is conducive to the establishment of a new financial accounting system and sharing system.

The Core Technology of Block Chain

Distributed accounting method

Distributed accounting is a decentralized and decentralized accounting method. Transaction accounting is composed of nodes operating in different areas, and each node will make its information public, sothat everyone can see, can supervise each other, improve the legitimacy of transactions.

The database records the information of all traders, and everyone can make changes to the information, and the updated content is made public so that other participants can see it, and all participants can access the information publicly.

Asymmetric encryption and authorization Technology

In order to ensure the security of the transaction information, it is necessary to encrypt the information. In general, it is encrypted with a public key and a private key, and encrypted with a secret key, it needs to be decrypted with another secret key, for example, encrypted with a public key and decrypted with a private key. Public key generation is irreversible, that is, the private key cannot be deduced from the public key, onlythe decryptor can see, thus ensuring a high degree of confidentiality of information.

Consensus mechanism

Traders form a consensus through the POW, POS,DPOS, POOL mechanism to judge the accuracy of amessage, which can not only confirm the information butalso prevent information from being tampered with, toachieve the balance of efficiency and security.

Smart contracts

Intelligent contracts are self-executable contracts that not only execute the plan, but also manage the plan and its day-to-day work and transaction costs. In theta fang system, there are a variety of projects, some may become alternatives to the stock market, some may become a new democratic model, in which politicians will be more accountable to citizens. In the sector chain accounting industry, it is not only the processing and accounting of accounts, but also the analysis and collation of financial data.

Block chain core algorithm

POW is the abbreviation of English Proof of Work.POW has the following requirements for the format of theblock B submitted by the node.

$H(B) < target$

Where H is a hash algorithm, target is a fixednumber. That is, the hash value of the whole block is less than a given number target. Only when the block meetsthis condition is a legitimate block, which can beaccepted by other nodes. And when a node finds such alegitimate block, it is also this also solves thedecision-making problem of results without center and multi-node.

The whole network uses the data of the first node to find the legitimate block. The hash value generated by the hash function is random, and a small change to the original data can make the hash value completely different from the previous one. You can start accumulating from 1.The value of the target is automatically adjusted at intervals to ensure that the block generation time is basically fixed, such as the bit coin guarantees that a new block will be generated every 10 minutes. The probability of blocks is

$$\frac{Target}{HASH_{max}}$$

From this formula, we can see that the smaller the target, the smaller the probability that each attempt will find a legitimate block. In Bitcoin, the target value is adjusted every 2,2016 pieces (two weeks) by the following formula

$$Target\ now = \frac{T3016}{2\ weeks} * target$$

T2016represents the time it takes to generate the first2016 blocks. The shorter the time it takes, the smaller the final target value. The difficulty of building blocks can also be determined by the following formula

$$difficulty = \frac{target1}{Current\ target}$$

Transactions

We characterize an electronic coin as a chain of advanced marks. Every proprietor moves the coin to the following by carefully marking a hash of the past exchange and the open key of the following proprietor and adding these as far as possible of the coin. A payee can check the marks to confirm the chain of possession.

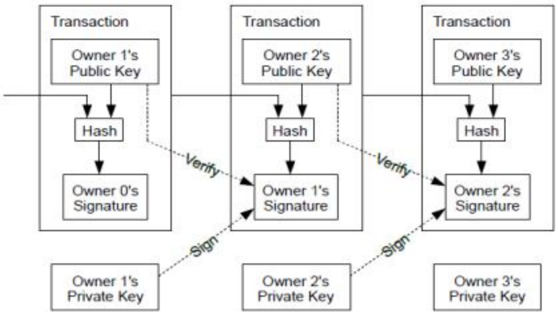


Fig.3.22: Transaction

After every exchange, the coin must be come back to the mint to give another coin, and just coins gave legitimately from the mint are trusted not to be twofold spent. The issue with this arrangement is that the destiny of the whole cash framework relies upon the organization running the mint, with each exchange experiencing them, much the same as a bank. We need a route for the payee to realize that the past proprietors didn't sign any previous exchanges. For our motivations, the most punctual exchange is the one that matters, so we couldn't care less about later endeavors to twofold spend. The best way to affirm the nonappearance of an exchange is to know about all exchanges. In the mint-based model, the mint knew about all exchanges and chose which showed up first. To achieve this without a confided in gathering, exchanges must be freely declared [1], and we need a framework for members to concur on a solitary history of the request wherein they were gotten. The payee needs verification that at the hour of every exchange, most of hubs concurred it was the main gotten.

Timestamp Server

The arrangement we propose starts with a timestamp server. A timestamp server works by taking a hash of a block of things to be time stepped and broadly distributing the hash, for example, in a paper or Usenet post. The timestamp demonstrates that the information more likely than not existed at the time, clearly, so as to get into the hash. Each timestamp incorporates the past timestamp in its hash, shaping a chain, with each extra timestamp strengthening the ones preceding it.

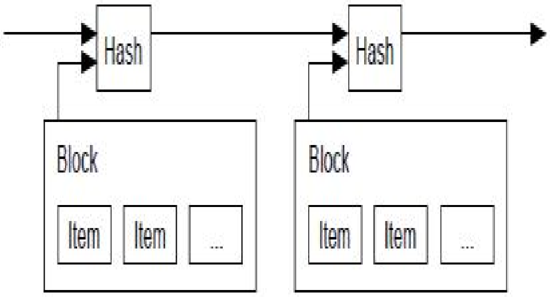


Fig.3.23: Time Stamp Server

Proof-of- Work

To actualize an appropriated timestamp server on a distributed premise, we should utilize a proof of work framework like Adam Back's Hash cash [6], as opposed to paper or Usenet posts.

The verification of-work includes filtering for a worth that when hashed, for example, with SHA-256, the hash starts with various zero bits. The normal work required is exponential in the quantity of zero bits required and can be confirmed by executing a solitary hash. For our timestamp organize, we execute the confirmation of-work by increasing a nonce in the block until a worth is discovered that gives the block's hash the necessary zero bits. When the CPU exertion has been exhausted to cause it to fulfill the evidence of-work, the block can't be changed without re-trying the work. As later blocks are chained after it, the work to change the block would incorporate re-trying every one of the blocks after it.

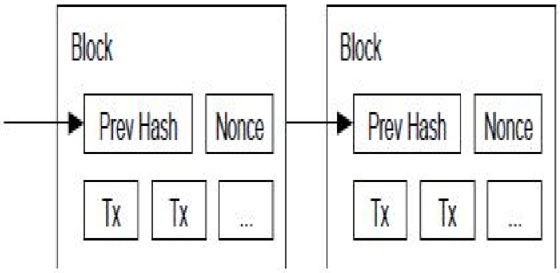


Fig.3.24: Proof of Work

The verification of-work likewise takes care of the issue of deciding portrayal in larger part basic leadership. On the off chance that the dominant part depended on one-IP-address-one-vote, it could be subverted by anybody ready to dispense numerous IPs. Confirmation of-work is basically one-CPU-one-vote. The lion's share choice is spoken to by the longest chain, which has the best evidence of-work exertion put resources into it. In the event that a lion's share of CPU power is constrained by legitimate hubs, the fair chain will become the quickest and outpace any contending chains. To change a past block, an aggressor would need to re-try the confirmation of-work of the block and all blocks after it and afterward make up for lost time with and outperform crafted by the genuine hubs. We will indicate later that the likelihood of a more slow assailant making up for lost time reduces exponentially as consequent blocks are included. To make up for expanding equipment speed and changing enthusiasm for running hubs after some time, the confirmation of-work trouble is dictated by a moving normal focusing on a normal number of blocks every hour. On the off chance that they're created excessively quick the trouble increments.

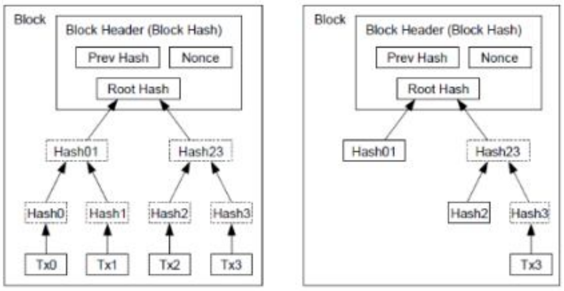
Incentive

By show, the principal exchange in a block is an exceptional exchange that starts another coin claimed by the maker of the block. This adds a motivating force for hubs to help the system, and gives an approach to at first disperse coins into dissemination, since there is no focal power to give them. The consistent option of a steady of measure of new coins is undifferentiated from gold excavators consuming assets to add gold to dissemination. For our situation, it is CPU time and power that is exhausted.

The motivator can likewise be financed with exchange expenses. In the event that the yield estimation of an exchange is not as much as its info esteem, the thing that matters is an exchange expense that is added to the motivator estimation of the block containing the exchange. When a foreordained number of coins have entered flow, the motivating force can progress totally to exchange expenses and be totally expansion free. The motivating force may help urge hubs to remain genuine. On the off chance that an insatiable aggressor can gather more CPU control than all the genuine hubs, he would need to pick between utilizing it to cheat individuals by taking back his installments, or utilizing it to produce new coins. He should think that its progressively beneficial to play by the guidelines, such decides that support him with more new coins than every other person consolidated, than to undermine the framework and the legitimacy of his own riches.

Reclaiming Disk Space

When the most recent exchange in a coin is covered under enough blocks, the spent exchanges before it very well may be disposed of to spare plate space. To encourage this without breaking the block's hash, exchanges are hashed in a Merkle Tree with just the root incorporated into the block's hash. Old blocks would then be able to be compacted by stubbing off parts of the tree. The inside hashes don't should be put away.



Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

Fig.3.25: Transactions Hashed in a Metric Tree

A block header without any exchanges would be around 80 bytes. On the off chance that we guess blocks are produced like clockwork, 80 bytes * 6 * 24 * 365 = 4.2MB every year. With PC frameworks ordinarily selling with 2GB of RAM starting at 2008, and Moore's Law foreseeing current development of 1.2GB every year, stockpiling ought not be an issue regardless of whether the block headers must be kept in memory.

Simplified Payment Verification

It is conceivable to confirm installments without running a full system hub. A client just needs to keep a duplicate of the block headers of the longest verification of-work chain, which he can get by questioning system hubs until he's persuaded, he has the longest chain, and acquire the Merkle branch connecting the exchange to the block it's time stepped in. He can't check the exchange for himself, yet by connecting it to a spot in the chain, he can see that a system hub has acknowledged it, and blocks included after it further affirm the system has acknowledged it.

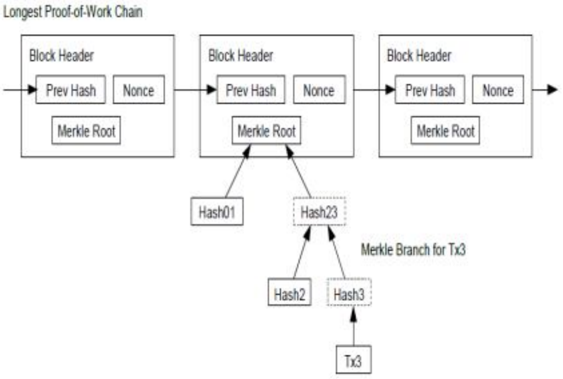
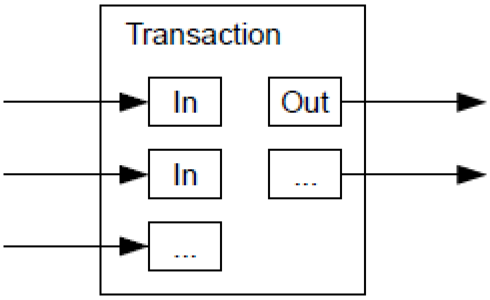


Fig.3.26: Simplified Payment Verification

In that capacity the check is dependable as long as legit hubs control the system, yet is increasingly helpless if the system is overwhelmed by an aggressor. While arrange hubs can confirm exchanges for themselves, the streamlined strategy can be tricked by an assailant's created exchanges for whatever length of time that the aggressor can keep on overwhelming the system. One system to secure against this is acknowledge cautions from system hubs when they recognize an invalid block, inciting the client's product to download the full block and alarmed exchanges to affirm the irregularity. Organizations that get visit installments will most likely still need to run their own hubs for progressively autonomous security and speedier check.

Combining and Splitting Value

Despite the fact that it is conceivable to deal with coins independently, it is cumbersome to make a different exchange for each penny in an exchange. To enable an incentive to be part and joined, exchanges contain different data sources and yields. Ordinarily there will be either a solitary contribution from a bigger past exchange or different sources of info joining littler sums, and at most two yields: one for the installment, and one restoring the change, assuming any, back to the sender.



It ought to be noticed that fan-out, where an exchange relies upon a few exchanges, and those exchanges rely upon some more, isn't an issue here. There will never be the need to separate a total independent duplicate of an exchange's history.

Privacy

The customary financial model accomplishes a degree of protection by restricting access to data to the gatherings in question and the confided in outsider. The need to report all exchanges freely blocks this strategy, however protection can in any case be kept up by breaking the progression of data in somewhere else: by keeping open keys mysterious. The open can see that somebody is sending an add up to another person, yet without data connecting the exchange to anybody. This is like the degree of data discharged by stock trades, where the time and size of individual exchanges, the "tape", is made open, yet without telling who the gatherings were.

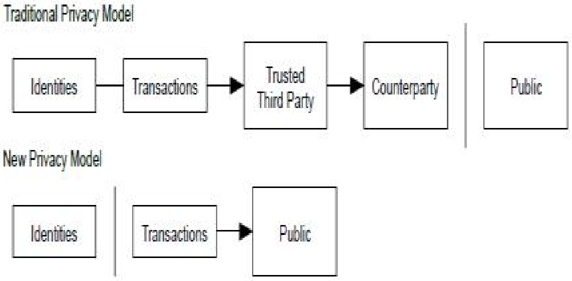


Fig.3.27: Privacy Model

As an extra firewall, another key pair ought to be utilized for every exchange to shield them from being connected to a typical proprietor. Some connecting is as yet unavoidable with multi-input exchanges, which fundamentally uncover that their data sources were possessed by a similar proprietor. The hazard is that if the proprietor of a key is uncovered, connecting could uncover different exchanges that had a place with a similar proprietor.

Application of Block Chain Technology in Accounting

Application status of block chain technology in accounting industry

With the further development of the block chain, its application field has developed from the initial digital currency to a deeper direction.

In December 2016, the State Council issued the "Thirteenth Five-Year Plan" for National Information. In this plan, the research of block chain technology will be brought into the national plan for the first time in China, which shows the important position of block chain technology in today's society. As of January 2018, there are not many achievements in the application of the block chain, and the related intellectual property rights and patents are blank. The block chain field is showing the development trend driven by technological and industrial innovation. Deloitte Encrypted Monetary Community, a group founded in 2014, has distributed members around the world to focus on the use of block chains in the accounting industry. After professional training of these members, Deloitte has made full use of block chain timestamps to ensure transaction time standards in auditing operations.

Confirmation, using hash function to ensure that it can not be tampered with modification, through Merkle to ensure the integrity of audit information, through asymmetric encryption technology to ensure that the data is open and transparent. Another company dedicated to block-chain technology and accounting is San Francisco Subledger, which provides businesses with a scalable, block-chain-based, dual-entry accounting book scheme that delivers real-time financial and performance data.

Construction of irreversible distributed financial system based on big data.

Block chains are run entirely by the public themselves. The connection of individual nodes can provide the huge computational power needed for computing. There is no control of central nodes in the network. Block chains can be used to build a new computational model - Block Chains as a Service.

Therefore, future large data can be built directly on the public block chain, and platform services can be provided directly on this public cloud. This mode can be called public chain as a service. Block chains can also be private or regional. Private chains or alliance chains are mainly used in enterprises or organizations, and local decentralized block chains are built through a limited number of hosts or distributed data centers. Developing distributed applications running on block chains or creating a new block chain requires a lotof manual development and powerful background computing capabilities to build and maintain distributed infrastructure.

Block Chain as a Service (BCS) can provide a large data infrastructure platform with a variety of developer tools by combining platform as a service, which makes it easier for users to develop block chain applications and greatly reduces the development effort. Security; also, can only combine infrastructure as a service, giving users the maximum development space to design their own block chain, large data services only provide the block chain infrastructure. Block Chain as a Service (BCS) transforms the infrastructure of large data and cloud computing, liberating closed data services and cloud computing infrastructure, allowing the public to operate their own infrastructure and provide rich distributed system features.

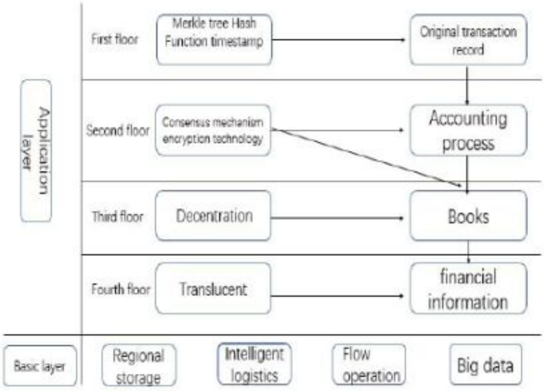


Fig.3.32: Distributed Financial

System Based on Big Data

Based on this, through the enterprise internal process reengineering, the block chain storage technology based on large data + Intelligent Internet of Things + distributed financial accounting system (as shown in Figure)

Will be an important application of accounting information and intelligence in the future. Distributed bookkeeping based on block chain technology is a network of bookkeeping organizations formed under the technical rules of block chain. The bookkeeping uses encryption computer algorithm-hash algorithm and collaborative maintenance to carry out digital distributed bookkeeping, while allowing users of multiple sites in different geographical locations to trade, assets and other wisdom. And it an share database.

In the specific operation, because of the characteristics of the block chain, an enterprise can establish an open and transparent enterprise financial system when it establishes an account book.

By guaranteeing the openness of financial information, it is conducive to the examination and examination of enterprise financial information from all walks of life, and only the private key can verify and share sensitive information. The security of enterprise secrets. The characteristics of block chain timestamp can ensure the accuracy of each transaction time, thus cannot change the time point, ensure that financial information cannot be tampered with, but also reduce the difficulty of audit. The essence of Distributed Accounting is a digital transaction record database based on a particular network(open or closed network), which contains all transaction information of all participants in that particular network.

Under the application of block chain technology, this transaction information can be tampered with, comprehensive and traceable. Every transaction participant can see all the information of the transaction and its real-time updated data situation, prevent the trader to do the data already completed by others, thus reducing the repeatability, avoiding the trader's waste of time and calculation, and need the agreement of all traders in the whole network before the information can be changed. It guarantees the safety and correctness of the system and reduces the financial risk. Block chain technology realizes the openness and transparency of the books, which not only ensures the safety and accuracy of the information and assets of the books, but also reduces the financial risks and transaction costs.

SIMULATION RESULTS

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent. The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.The probability of an attacker catching up from a given deficit is analogous to a Gambler’s Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows

p = probability an honest node finds the next block

q = probability the attacker finds the next block

qz = probability the attacker will ever catch up from z blocks behind

Given our assumption that p > q, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind. We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late. The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working onit continuously until he is lucky enough to get far enough ahead, then executing the transaction atthat moment. Once the transaction is sent, the dishonest sender starts working in secret on parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value.
$\lambda = z\frac{p}{q}$

CONCLUSION

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

REFERENCES

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no2, pages 99-111, 1991.
[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping, "In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.
[6] A. Back, "Hashcash a denial of service counter-measure,"http://www.hashcash.org/papers/hashcash.pdf, 2002.
[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security andPrivacy, IEEE Computer Society, pages 122-133, April 1980.
[8] W. Feller, "An introduction to probability theory and its applications," 1957.
[9] Fanning K, Centers D P. Blockchain and Its Coming Impacton Financial Services[J]. Journal of Corporate

Accounting &Finance, 2016, 27(5):53-57.

[10] Stanghellini E. Monitoring the Behavior of Credit CardHolders with Graphical Chain Models[J]. Journal of BusinessFinance & Accounting, 2010, 30(9-10):1423-1435.

[11] ChenQ, LewisTR, SchipperK, et al. Uniformvs.Discretionary Regimes in Reporting Information withUnverifiable Precision and a Coordination Role[J]. Journal ofAccounting Research, 2016, 55(1).

[12] May R G, Sundem G L. Research for Accounting Policy: An Overview[J]. Accounting Review, 1976, 51(4):747-763.

[13] Croman K, Decker C, Eyal I, et al. On ScalingDecentralized Blockchains[C]// International Conference onFinancial Cryptography & Data Security. Springer BerlinHeidelberg, 2016.

[14] Volonté, Christophe. Culture and Corporate Governance: TheInfluence of Language and Religion in Switzerland[J].Management International Review, 2015, 55(1):77-118.

[15] Cheng C, Eshleman J. Does the market overweight imprecise information? Evidence from customer earnings announcements[J]. Review of Accounting Studies, 2014,19(3):1125-1151.

[16] Frale C, Grassi S,Marcelino M G, et al. Euro Mind-C: A Disaggregate Monthly Indicator of Economic Activity for theEuro Area and Member Countries[J]. International Journal of Forecasting, 2015, 31(3):712-738.