Blockchain Improvement Suggestion–Solutions for Block Expansion

Ge Boli 5120309578

May 23, 2018

Abstract: Bitcoin has brought blockchain technology into the eyes of world as an identity of currency with a sense of mystery. Since then blockchains experience mushroom growth and new concept and products emerged such as Lightning Network, Ethereum, and Hyperledger Fabric. In addition blockchain has been operating in the supply chain finance, notarization and medical and so on. Blockchains furnish an innovative and practical approach to solve the problem of trust and value delivery.

1 Introduction

The core of Lightning Network, Ethereum, Hyperledger Fabric and other blockchains are of course the blockchains in bitcoin, developed to solve specific problems and applications. We know that the Internet itself doesn't have a value protection mechanism and it is even more troublesome to trade around the world because of involving different laws, different value rules and different terms of payment. Nonetheless blockchains can create such trust mechanism in the absence of a third party trust environment with trading process greatly simplified. Since blockchain is a distributed system node that can be spread around the world, it can realize the value transfer of borderless. Various financial activities can be realized through smart contracts on the blockchain. Blockchains can also support more complex programming of financial commercial contracts, such as crowd funding and guarantees. Features of blockchain, distributive, reliable, unfalsified and smart contract, will definitely show great advantages in the process of combining with traditional technology.

Whether you believe it or not, encryption economy changes the production relationship over the next 100 years.With the new trade cold war exploding, the collapse of the traditional real economy and the general antipathy towards technology giants, it has embarked on a sweeping journey. Everyone wants to go back to a more primitive and simpler way of life.This is the global village of blockchain. It's not about simplicity rather than being developed.The platform will disappear, you can't fight with the future. But fatalism is also naive because it naturally overestimates the speed of the revolution and underestimates

the depth.The speeding change does not mean that the resistance will diminish.In fact, the development of the blockchain in the past two years rises up leading large number of institutions or enterprises engaged in research at home and abroad.But it is undoubtfully that many people are overoptimistic about blockchain technology. Many desire to extensively apply blockchains to manufactory usage. In the long term, I believe that all of this will be accomplished depending on the technological progress of the blockchain platform, especially around trading and expansion.

Actually there won't be any perfect system,which is tested by various problems. As different types of software have their own problems, blockchain as a kind of software system is no exception. Blockchain itself can be regarded as a kind of application design experiment. Similar to the middle process product of competition soft bifurcation and hard bifurcation, 51 percent forced attack, the ductility of the deal, congestion problem of validation delay network and block expansion. In the last few years, the blockchain did expose those problem in practice, even some important security accident. Blockchain technology must be reliable if it is to be applied in such areas as financial payment and business witness. Once there are problems in the service, not only will people not accept but it even devastates blockchain technology.

2 Problems

2.1 Exchanges and Mines

As we know,ASIC mining machine is certainly more efficient than GPU mining, but it still burns energy. Blockchain consuming too much energy is original sin. Whereas Exchanges are a big failure of the blockchain, a double whammy of regulators and hackers. As bridges between the old financial system and the emerging industries, they are vulnerable to legal and technical attacks.We need a universal digital currency exchange agreement.In today's financial world, every step from trading, custody to asset inheritance should happen in the program itself without a third party.

2.2 Assignment

Communism does not inspire anyone to possess the resources within the system.The blockchain, however, takes into account the duality of human beings both selfish and selfless.The ecology of the blockchain does not mean a complete equality of distribution, nor does it mean that people cannot start businesses, trade or do other things to make more money.It is the only revolutionary economic model in history to deliver programmable assets to people directly so that people can create more economic benefits online.

2.3 Transaction Performance

At present the blockchain of bitcoin can only support about 7 businesses per second. It is generally believed that an-hour waiting time is necessary to confirm security for large quantity transaction. The throughput is slightly higher in Ethereum but poor performance is considered a major bottleneck in blockchain technology.

2.4 Block Expansion

Block expansion is what we will discuss in the following. Engineers have been trying to extend the distributive system. Traditional system structure adopts linear expansion and the more servers are added, the larger the capacity is. Nevertheless, no matter how many servers are added in blockchain, the performance of storage capacity stand still. It must be integrated into the consensus of collective to solve the problem. This paper studies the last problem mentioned above, summarizing the solutions proposed and giving a new framework.

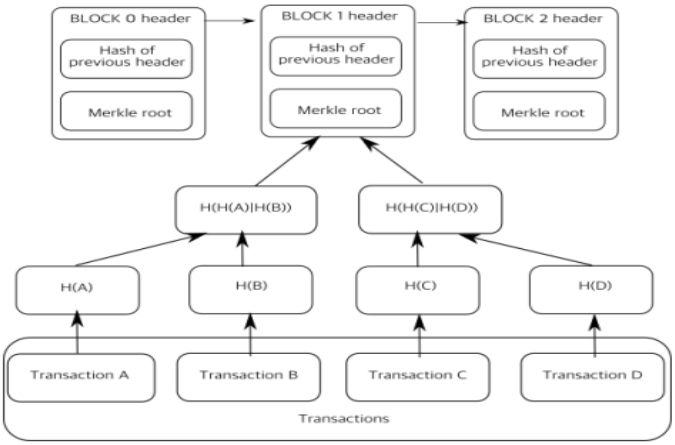
3 Settlement to Block Expansion

In July 2016, the size of ledger of bitcoin blockchain was about 80GB, and by July 2017 it was 130GB. Although the hard disk capacity is very large and 1TB is also easy to accommodate this capacity. But what is reflected here is the astonished growth speed of the block. It takes a long time to fully synchronize these nodes on another machine. As for Ethereum the volume has exceeded over 200GB within 3years owing to a large number of smart contracts.This paper proposes three feasible ideas.

3.1 Data Compression

It is possible to delete some early transaction data and preserve the block header. The hash value in the block header won't break and the block will be effectively compressed. As we know, the hash value is calculated as the identity of the block when generated. In addition to the hash value of the block header, each affair in the block is also calculated into a hash value, known as the thing hash, which eventually forms data structure of a hash tree. The root of this hash tree is called the Merkle root. Through this Merkle root, you can constrain all the affairs in the block. As long as the data in the block changes, Merkle root will change. This feature can be utilized to ensure the integrity of the blockchain data. The block data retained by the node should be simplified up to down and each node can obtain data from other nodes in parallel. In the blockchain system, data produced by a node or changed data will be broadcast to other nodes in the network to accept verification. The other nodes won't accept a tampered data because the data can not match with local data. As the length of the chain growing up the tamperation of the block data comes more difficult. Therefore, only small block header can be reserved in convenience of

specific transaction. Digging nodes need to retain entire copy of the data. And other nodes participating in digging, relying on the whole nodes must reserve the whole data. The node keeping complete blockchain data is very important.



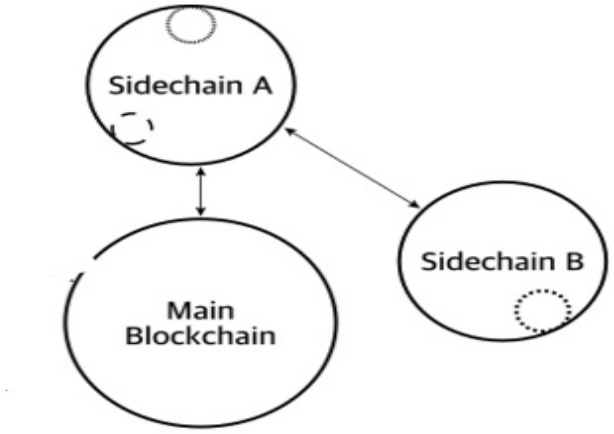
A merkle tree connecting transactions to a block header merkle root.

If the number of complete blockchain nodes in the network becomes less and less, will the stability and security of the network be affected? Performance and security will be reduced. But with the increasing number of nodes, even if the proportion of intact nodes is limited, the absolute number is still considerable. When trying to modify the historical block information, it will inevitably result in the different values of Merkle root or different block header hash values, which cannot be passed in the verification of the network node. Besides although the transaction history information is concentrated in the hands of only a few people, it seems to violate the decentralized principle. In fact, it is not possible to achieve absolute decentralization. For instance, deciding which chain as the main chain when the bifurcate occurs and software upgrading, important events are still decided and voted by the community and mineral pool who owns giant calculative power. It is a relatively decentralization to guarantee the fairness and stability.

3.2 Sidechain Technology

We propose a new technology, pegged sidechains, which enables bitcoins and other ledger assets to be transferred between multiple blockchains of different characteristics and technical architecture. This gives users access to new and innovative cryptocurrency systems using the assets they already own. We refer to the first blockchain as the parent chain, and the second simply as the sidechain. The sidechain is not the part of parent chain, but an independent blockchain interconnectively anchoring with the parent chain. Sidechain is relative to the parent chain of the concept. In some models, both chains are treated symmetrically, so this terminology should be considered relative. In general,

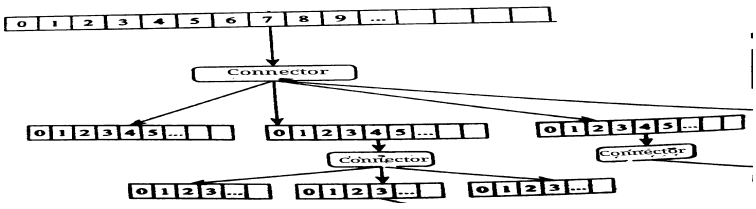
sidechain should ideally be fully independent, with users providing any necessary data from other chains. Validators of a sidechain should only be required to track another chain if that is an explicit consensus rule of the sidechain itself.



Pegged sidechains allow parties to transfer assets by providing explicit proofs of possession in transactions.

In order to transfer the asset from the main chain to the sidechain, the asset is frozen on the main chain and then activated on the sidechain. It is also possible to control the frozen assets on the main chain through a multi-signature address, similar to a smart contract. Parties agree on a notarial custody contract, which increases security and makes the sidechain protocol more smooth than the previous.

As shown in the figure, the corresponding asset transferred between the main chain and the sidechain will be freezed in advance and then activated on the sidechain. A transaction is initiated by the asset owner to lock the asset from the main chain address and then sent to a special address on the sidechain. The main chain needs to provide workload proof and be recognized by the sidechain. Assets once locked on the main chain will not be deleted, the fair has a waiting time for confirmation until enough random node confirmed.It can effectively prevent the counterfeit and attack. Because of the sidechain has agreed as the side chain of the main chain, sidechain will generate equivalent assets and set appropriate ownership. This process is carried out entirely according to the rules of sidechain. This transfer is equivalent and symmetry. Assets which are moved to sidechains should be able to be moved back by whomever their current holder is, and nobody else.



Multichain interaction

We think out a model of interconnected chains inspired by the sidechain. At present various blockchain system constantly emerge, some for digital currency, some for smart contracts. The chains can be classified into public chain, private chain and allied chain. If we connect these chains together, we will have a new level of intelligence in the society and our civilization will have a profound impact.Different systems can interconnect and complement each other as blockchain technology develops to the end. Each chain has its own advantages and disadvantages, which can be complemented by functions and be verified and opened to each other greatly enhancing the reliability and performance of the system.

3.3 Distributed Autonomous Storage System

Different from that all the nodes save the same data, we utilize blockchain technology to realize a decentralized and distributed autonomous storage system, which storage block data in different nodes according to certain classification. The file will be stored in form of shards, and then build decentralized cloud storage. We will test the node credibility and the corresponding redundancy can be carried out flexibly according to the online scenario of the node. At the same time, because that data is divided into small pieces, the space occupied is also small. And hence the upload and download speed will be vary fast and the integrity of the file can be guaranteed. Such a system does not exist a data center. Once the data is generated and entered in, anyone can obtain the data anywhere quickly and efficiently. This process means that when a node breaking down it will not affect the other storage of the node even to the end of the human society. Since the blockchain adopts a fair consensus mechanism, all participants have equal responsibility and equal ability. Therefore, it retains the characteristics of the decentralization of the blockchain and no one can control the distributed storage system of the blockchain. When looking for content, content-based addressing will replace traditional domain-based addressing. We don't need to care about the location of the server, regardless of the name and path of the file store. The hash value directly reflects the contents of the file, even if only one bit is modified the hash value will be completely different. When downloading a file, request a file hash value, it will use a distributed hash table to find the node where the file resides and then fetch the file and validate the data.

The download can be obtained from multiple nodes simultaneously. Such a

design can well share all kinds of data, including image, video stream, distributed database. Here list 3 advantages. Simple operation is easy to handle for node participants and complex technical logic is transparent to users. Furthermore construction of storage pool can form from distributed storage nodes of a certain scale, making the storage network more stable. Last, we can create a free storage space to share the trading market. Via making good use of idle resources, everyone shares their free hard storage drives and attain gains. Finally, in full competition of market, everyone can use the absolute safe decentralization storage at very low prices.

4 Conclusion

Via compressing data block, adopting sidechains, and constructing distributed storage system can effectively settle capacity expansion in blockchains.These technologies can solve block expansion without losing the decentralization and untampering of the blockchain. Distributed features retain good security and performance of the blockchain. Of course, the concrete implementation is still to be explored, here is just to give an design. For blockchain technology, it is not only a technology but a kind of ideology or value. The blockchain will shift from demonstration to production and emerge in variety of pilot projects and production systems. Of course, just as the early pistols easy to blow up, the operation easy to get infected, a technology with huge development prospects need constant discovery, improvement and settlement. The progress of science and technology is not always smooth, sometimes it is even impossible to judge whether the direction is correct. Only by constantly going forward, can we find the treasure in front. Believe that in the future, it will not be very far away to realize the true decentralized autonomous programmable society with blockchains.

REFERENCES

[1]Johnny Dilley, Andrew Poelstra, Jonathan Wilkins, Marta Piekarska, Ben Gorlick, Mark Friedenbach, 'Strong Federations: An Interoperable Blockchain Solution to Centralized Third-Party Risks'
[2]Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', www.bitcoin.org
[3]Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timn, Pieter Wuille, 'Enabling Blockchain Innovations with Pegged Sidechains', 2014-10-22 (commit 5620e43)
[4]Joseph Poon, Thaddeus Dryja, 'The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments', January 14, 2016, DRAFT Version 0.5.9.2