Information Propagation on Blockchains: Analysis,Method and Evaluation

----Solutions for Block Expansion

葛波利 5120309578

Preface

- Blockchain is a distributed system node that can be spread around the world, furnishing an innovative and pratical approach to solve the problem of trust and value delivery. Recent two years blockchains experience mushroom growth leading large number of institutions or enterprises engaged in research at home and abroad.
- New concept and products emerged such as Lightning Network, Ethereum, and Hyperledger Fabric. 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 crowdfunding, guarantees and other supply chain finance, notarization and medical service.

FEATURES

- Distributed
- Reliable
- Irreversibility
- Smart Contract

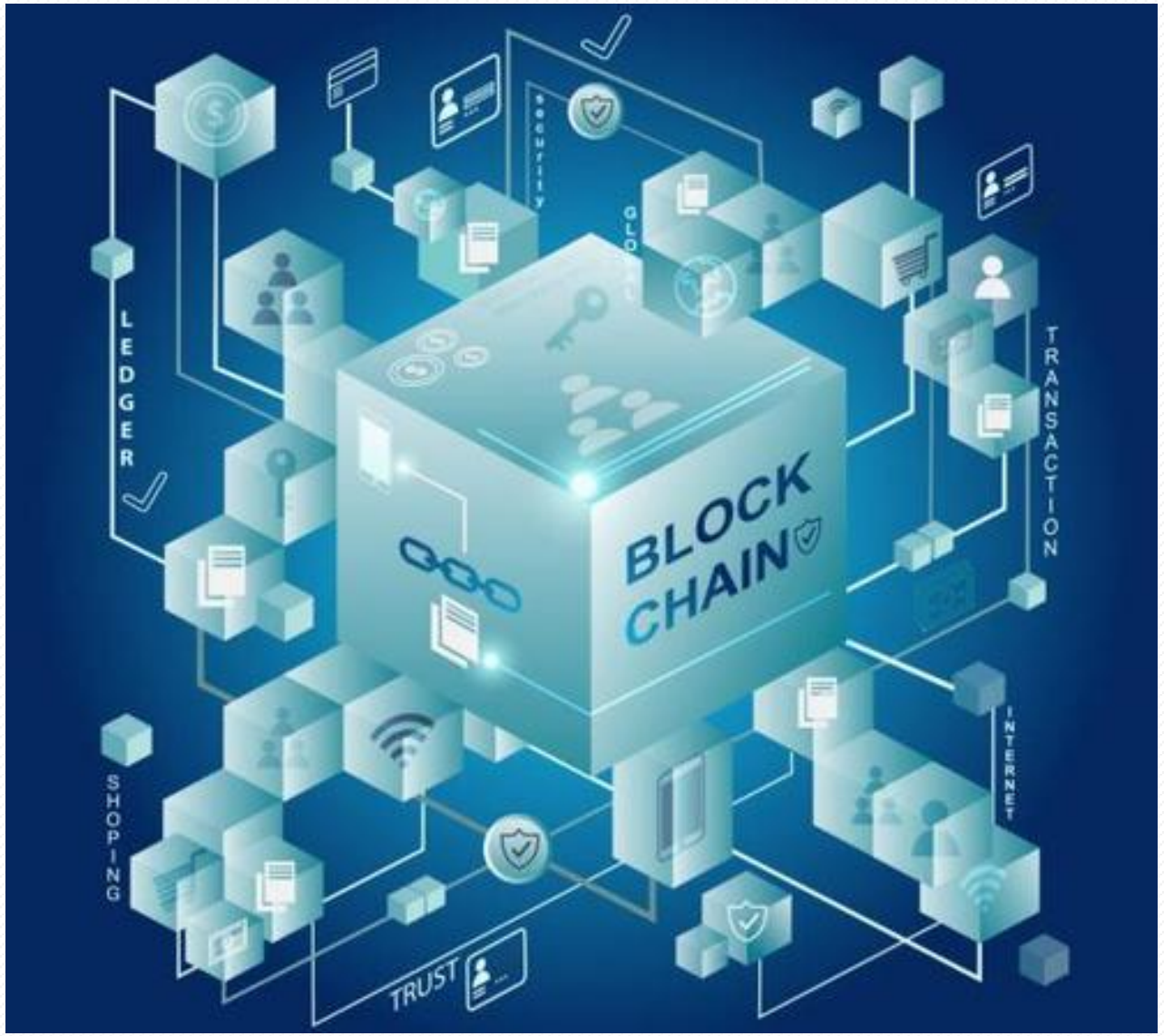
Problems of Blockchain

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 and expose various kinds of shortcomings.

In the last few years, the blockchain did expose those problem in practice, even some security accident.

- soft bifurcation and hard bifurcation
- 51% forced attack
- the ductility of the deal
- validation delay
- block expansion

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.



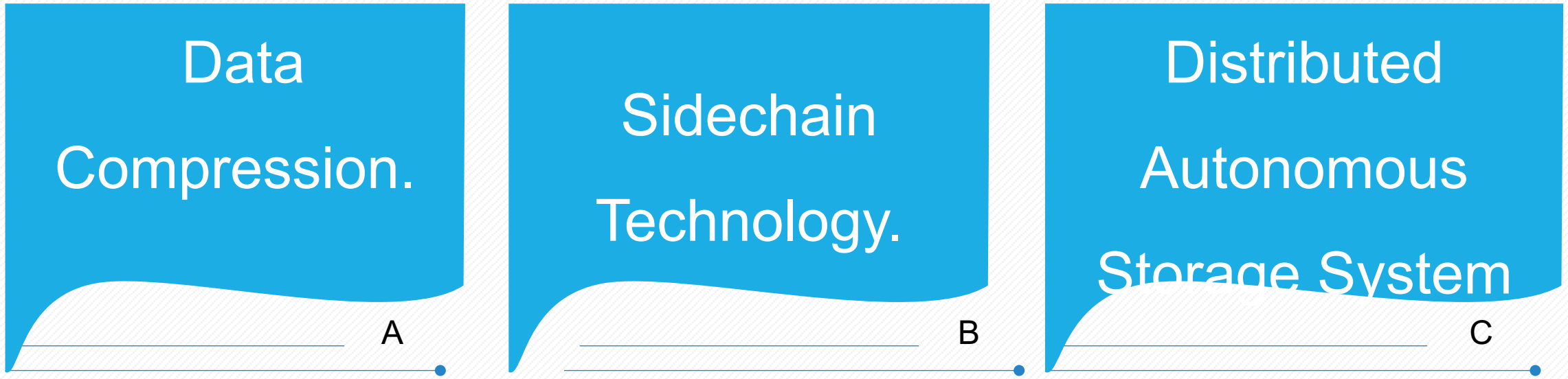
Block Expansion

In July 2016, the size of ledger of bitcoin blockchain was about 80GB, and by July 2017 it was 130GB. 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 3 years owing to a large number of smart contracts.

Block Expansion

Engineers have been trying to extend the distributed 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 stands still. It must be integrated into the consensus of collective to solve the problem.

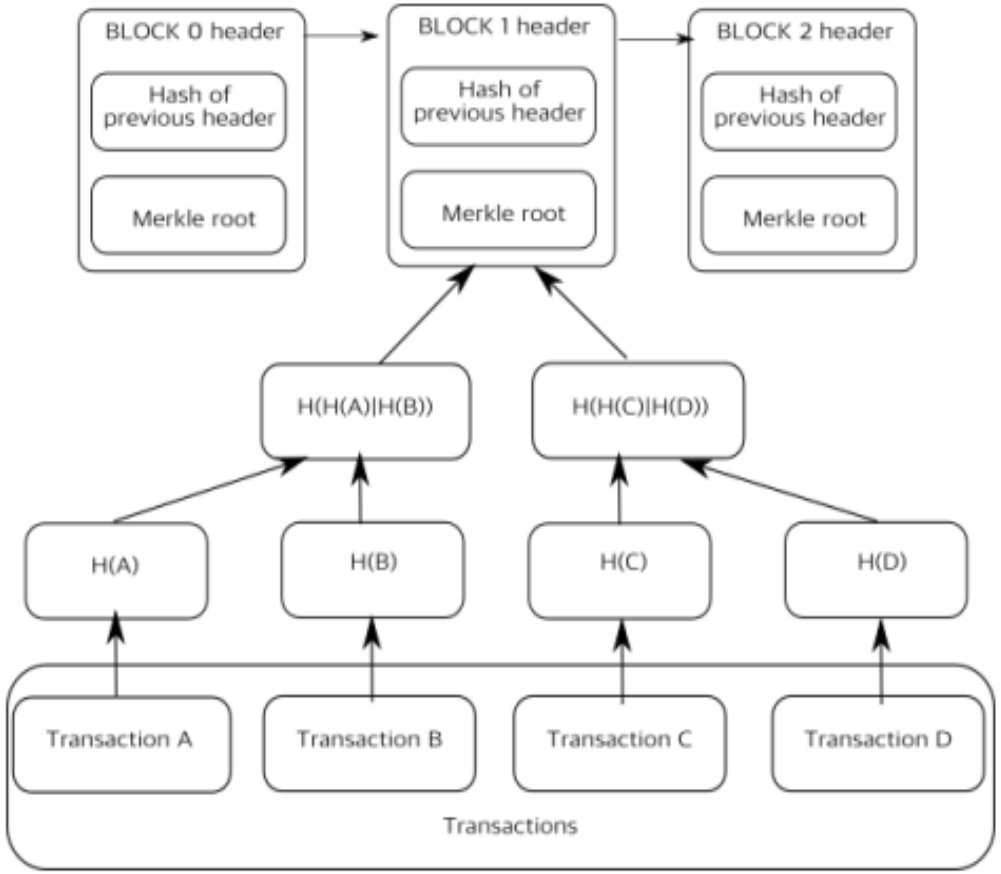
Three Basic Solutions



Basic Solution A

Data Compression.

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.



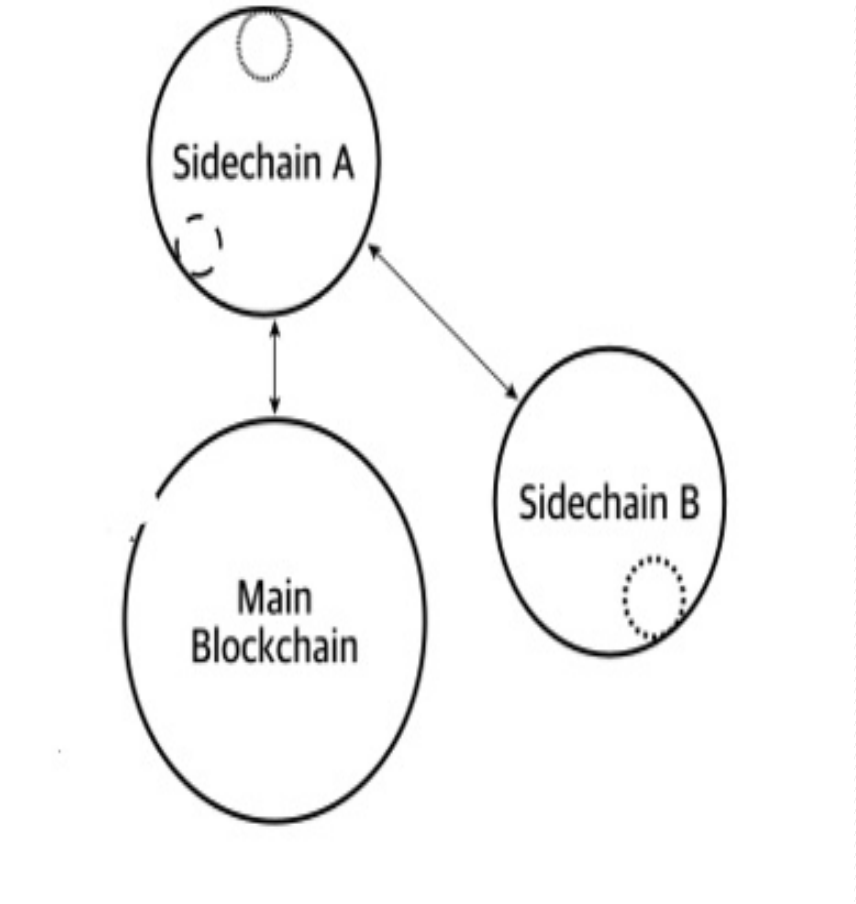
As we know, the hash value is calculated as the identity of the block when generated. In addition to the hash value of the block header, each affair in the block is also calculated into a hash value, known as the thing hash, which eventually forms data structure of a hash tree. The root of this hash 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.

- 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's. As the length of the chain growing up, the tamperation of the block data comes more difficult.
- If the number of complete blockchain nodes in the network decrease, 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.
- 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.

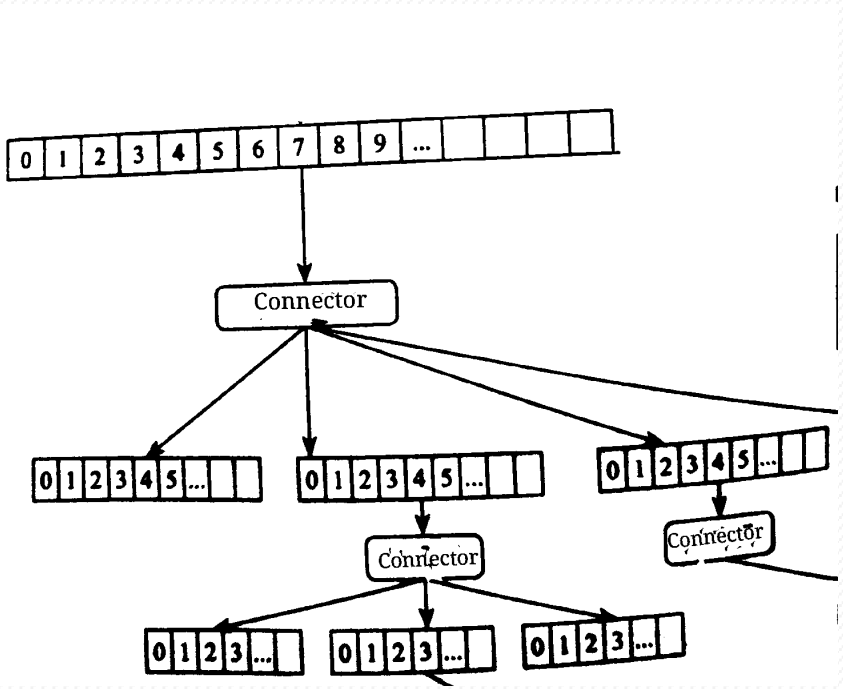
Basic Solution B

Sidechain Technology.

Bitcoins and other ledger assets can be transferred between multiple blockchains of different characteristics and technical architecture.



The corresponding asset transferred between the main chain and the sidechain will be freezed in advance and then activated on the 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.



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.

Basic Solution C

Distributed Autonomous Storage System.

A decentralized and distributed autonomous storage system, which storage block data in different nodes according to certain classification.We will test the node credibility and the corresponding redundancy can be carried out flexibly according to the online scenario of the node.

- 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.
- 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.

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.

The progress of science and technology is not always smooth, sometimes it is 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.

Thank you for watching