Improving the Scalability of Blockchain through DAG

Middleware 2019 Doctoral Symposium

Qin Wang, Swinburne University of Technology & CSRIO, Data61

Abstract

Current blockchain systems face the problems of poor scalability, low performance, and high cost. To address the previous bottlenecks, we plan to employ the DAG-based structure as the primary method and propose a concrete model, called *3D-DAG*, to improve the scalability. The model consists of two layers: mainchain and sidechain, which separately severs for maintaining the pivot sequence and improving the parallelism. Our expecting results should significantly improve the performance and scalability without compromising the security.

Keywords Blockchain, DAG, Mainchain, Sidechain

ACM Reference format:
Qin Wang, Swinburne University of Technology & CSRIO, Data61. 2019. Improving the Scalability of Blockchain through DAG. In *Proceedings of Middleware'19, UC DAVIS, USA, December 2019,* 2 pages.
DOI: 10.1145/3366624.3368165

Problem Statement Blockchain is a distributed protocol with the irreversibility, tampering resistance, and verifiability. Since Nakamoto published the Bitcoin paper in 2008 [12] and afterwards released Bitcoin system early 2009, Blockchain has quickly become popular in the IT industry, and subsequently spread over to other business sectors [13]. For a long-time development, Blockchain technology has evolved from Blockchain 1.0 (called the programmable virtual currency Bitcoin) to Blockchain 2.0 (called the programmable finance, the most important project is Ethereum [15]). The design of blockchain technology ensures that no single person can modify, delete, or even append any history to the ledger without the permissions and consensus from peers. The permanent history guarantee the immutability of records stored on chain. However, existing systems confront the problems of *poor scalability*, *low performance*, and *high cost*. In order to overcome the previous problems and other potentially serious threats, we start from analyzing the existing protocols and then propose a newly DAG-based blockchain model, called 3D-DAG. The proposed model, when successfully implemented, will greatly benefit the distributed applications on top of the blockchain platform.

Research Contribution After the analyses on current approaches, we conclude the reasons that cause the bottlenecks in three aspects, including the underlying consensus mechanism, system-level optimization, and fundamental structure. These three aspects mutually interact and lay the foundation of our systematic architecture. Our research goals are briefly going to achieve:

- Profound analyses in current research articles and open sourced projects, from the bottom of structure layers to the consensus layer and then to the application layer.
- The mechanisms of a suite of consensus protocols, and a series of architectures based on different structures.
- A prototype of proposed blockchain system, supporting over one hundred participants in the asynchronized environment with high throughput and performance.

Current Approaches Current methods to improve the performance of blockchain contains network sharding[11][8], consensus construction[7][6], and structure modification[3][2]. Sharding aims to divide the network into small zones, and each zone is self-governance, but the consensus is hard to achieve since different zones are asynchronized. Consensus construction focuses on the design of the protocol. Current prevailing protocols include BFT-style consensus (Paxos[9], PBFT[4], etc.), Nakamoto Consensus (PoW, PoS[14], DPoS[10], etc.) and Hybrid system (PoS+PBFT[1], PoW+PoS[6], etc.). However, the performance is still limited by the competition of blocks under the linear sequence. Hardware specification means improving the performance by specifying the algorithm into hardware, but it is too costly. Structure revolution aims to change the bottom structure of blockchain foundation, such as employing DAG-based or lattice-based structure.

Our Approaches Since the blockchain technology soared up, more and more participants join the game. The continuously increased traffic results in an unavoidably catastrophic congestion due to the block packaging process. Therefore, the linear structure of blockchain cannot avoid the problems of unscalability. We plan to focus on the graph-based structure, also know as *Directed Acyclic Graph (DAG)*, and propose an advanced DAG-based blockchain model supporting the network in large scale.

Why DAGs Different from the linear-chain topology in traditional blockchain, DAG-based blockchain removes the limitation of blocks, expanding the network through the directed acyclic graph. Newly generated transactions, without packing into blocks, directly establish the network in some directions by confirming the parent transactions to get a higher probability to be confirmed by the next transactions. Through several iterative rounds, the main graph is stably formed with a low probability of being reversed .

The advantages of a DAG-based model include greater scalability and lower transaction fees. Whereas linear-based blockchain slows down as the transactions increase, the DAG, on the contrary, works faster as they increases, making it very scalable. There is no mining on DAGs, so that it is no need to charge the participants with high transaction fees. DAGs can be used in many cases where blockchain would not be feasible. A prime example is the Nano-transactions between IoT devices and small sensors. Famous projects include IOTA's Tangle Network [3], Hashgraph [2], Byteball [5], etc.

Our DAG-based Model We are going to propose a DAG-based system, called 3D-DAG, to improve the scalability of blockchain. At a high-level description, 3D-DAG is a system, which consists of

Middleware'19, UC DAVIS, USA

DOI: 10.1145/3366624.3368165

one mainchain, and potential one or more sidechains in DAG-based structures. There are three dimensions in a 3D-DAG network. The first dimension of 3D-DAG is the basic asset-based mainchain to provide the assets transferring and exchanging, and technically it is based on PoW consensus to provide the high security with power guarantees. The second dimension of 3D-DAG is the state-based sidechain to provide the multiple utilities for a smart contract, and technically it is based on DAG-based structure combined with BFT-style consensus to provide parallel processing for high performance. The third dimension of the 3D-DAG is the cross-communication between the mainchain and sidechain, ensuring the inherent events smoothly and effectively flow between DAG and chain. Therefore the functions triggered by DApps can be integrated together.

The key design is to employ separate the workload into different level: the miners of the main chain is to secure all the block sequence, and the side chains is to take over the workload from practical scenarios. This design will offload the heavy workload from the main chain or side chains, to take advantage of the DAG's parallel strengths and improve the performance of DApps. Fundamentally, the smart contract execution is offloaded from the mainchain to sidechains, which reaches a relative balance between security and performance. From another viewpoint, our design point is to distinguish two different use cases in DApps. One is asset-based transactions, like bitcoin. The other use case is a state-based use case, which is relatively similar to Ethereum, realising various state transition through smart contracts. This kind of DApps can be modelled as a state transition DAG. We will use one single DAG for each DApp chain.

Guidelines of 3D-DAG Our 3D-DAG system follows several rules as guidelines, the details are presented below:

Claim 1. *3D-DAG consists of two layers of chains:* mainchain *and* sidechain. *The mainchain bases on UTXO-based chain to undertake the asset exchange, and the sidechain bases on DAG-based structure to provide the environment of state transition.*

Claim 2. *For consensus, the mainchain employs the mechanism called Proof of Useful Work (PoUW), while the sidechain uses modified BFT-style mechanism based on VRF.*

Claim 3. *For DAG network, the whole DAG network is divided into two layers to prevent the DoS attacks. The first layer is the Committee selected by the miners by the cryptographic sortition by VRF, to validate the transactions and maintain the DAG sequences. The second layer is the miners who vote for the committee.*

Expected Results For qualitative outcomes, the main properties for 3D-DAG is the consensus achievement, including agreement, validity and liveness. The definitions are listed below. Assume that the genesis unit of the DAG defines that it needs m miners to validate transactions, also up to b nodes are Byzantine nodes out of the m miners where $m > 3b$.

Aims 1 (Agreement)**.** *As long as each transaction receives $b + 1$ or $-(b+1)$ voting scores, all the non-faulty miners achieve an agreement that the transaction reaches finality status*

Aims 2 (Validity)**.** *As long as each transaction receives $b + 1$ voting scores, the transaction value comes from a non-faulty node.*

Aims 3 (Liveness)**.** *The 3D-DAG consensus mechanism should always reach an agreement after the finite rounds of consensus.*

For quantitative outcomes, the assumptions of the mainchain's throughput simulation are as follow: assuming that the transaction size as 512 bytes, block size as 1.0MB and block generation span as half minus. Ran 200 sub-DAG networks with 200 Transaction Output and 200 World State Transition, linked to the mainchain. The workload of each sub-DAGs varied from 500 to 8,000 TPS. The lasting time should be at least an uninterrupted 24-hour test. As for the expected results, the main chain should handle at least 1000 Tx/s to 2000 Tx/s, with supports subchains at least 1 million/s to 3 million/s of the total throughputs.

Conclusion Blockchain has been widely recognized as a trusted computing platform to support decentralized applications. However, the low performance and scalability of the existing Blockchains make the prospects unattainable. DAG-based model emerges as an alternative blockchain architecture to address the performance and scalability issue. However, DAG-based blockchain capacity still remains some concern, due to the lack of open-source implementations and published experimental results. We plan to propose a DAG-based model, called 3D-DAG, to address the bottleneck of performance. Technically, our 3D-DAG consists of two layers of chains: *mainchain* and *sidechain*. While our mainchain uses the classical blockchain data structure and PoW consensus mechanism to inherit the strong trust and security from Bitcoin for assets trading, DAG is used for constructing the sidechains to enable fine-grain parallel transaction processing. Our expecting results of our 3D-DAG should meet the challenging performance requirements which are expected by the decentralized applications without compromising security.

Acknowledgement Deepest appreciation to the technical inspiration and support of our team members, Joe Zou (Science and Technology Academy, China Institute Of Digital Asset), Yi Tang (Guangzhou University), Zhongli Dong (University of Sydney), Peng Zhuang (IBM), Wei Li (University of Sydney), and Albert Y. Zomaya (University of Sydney). The same appreciation to my supervisor Shiping Chen (CSIRO Data61) and Yang Xiang (Swinburne University of Technology).

References

[1] 2019. EOS. https://eos.io/
[2] 2019. Hedera Hashgraph. https://www.hederahashgraph.com/
[3] 2019. IOTA. https://www.iota.org/
[4] Miguel Castro, Barbara Liskov, et al. 1999. Practical Byzantine fault tolerance. In *OSDI*, Vol. 99. 173–186.
[5] Anton Churyumov. 2016. Byteball: A decentralized system for storage and transfer of value. *URL https://byteball. org/Byteball. pdf* (2016).
[6] Tuyet Duong, Lei Fan, and Hong-Sheng Zhou. 2016. 2-hop Blockchain : Combining Proof-of-Work and Proof-of-Stake Securely.
[7] Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, and Robbert Van Renesse. 2016. Bitcoin-NG: A Scalable Blockchain Protocol. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. 45–59.
[8] Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ewa Syta, and Bryan Ford. 2018. Omniledger: A secure, scale-out, decentralized ledger via sharding. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE.
[9] Leslie Lamport et al. 2001. Paxos made simple. *ACM Sigact News* (2001).
[10] Daniel Larimer. 2014. Delegated proof-of-stake. *Bitshare whitepaper* (2014).
[11] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. [n. d.]. A secure sharding protocol for open blockchains. In *2016 ACM SIGSAC Conference on Computer and Communications Security*.
[12] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system.
[13] Marc Pilkington. 2016. Blockchain technology: principles and applications. *Research handbook on digital transformations* (2016), 225.
[14] Pavel Vasin. 2014. Blackcoin's proof-of-stake protocol v2. *URL: https://blackcoin. co/blackcoin-pos-protocolv2-whitepaper. pdf* (2014).
[15] Gavin Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151 (2014), 1–32.