Efficient and DoS-resistant Consensus for Permissioned Blockchains

Xusheng Chen[†], Shixiong Zhao[†], Ji Qi[†], Jianyu Jiang[†], Haoze Song[†], Cheng Wang[†¶], Tsz On Li[†], T-H. Hubert Chan[†], Fengwei Zhang[‡], Xiapu Luo[§], Sen Wang[¶], Gong Zhang[¶], Heming Cui[†*]
{xschen,sxzhao,jqi,jyjiang,hzsong,cwang2,toli2,hubert}@cs.hku.hk,zhangfw@sustech.edu.cn
csxluo@comp.polyu.edu.hk,wangsen31@huawei.com,nicholas.zhang@huawei.com,heming@cs.hku.hk,
[†]The University of Hong Kong, [‡]Southern University of Science and Technology,
[§]The Hong Kong Polytechnic University, [¶]Huawei Technologies.

ABSTRACT

Existing permissioned blockchain systems designate a fixed and explicit group of committee nodes to run a consensus protocol that confirms the same sequence of blocks among all nodes. Unfortunately, when such a system runs on a large scale on the Internet, these explicit committee nodes can be easily turned down by denial-of-service (DoS) or network partition attacks. Although recent studies proposed scalable BFT protocols that run on a larger number of committee nodes, these protocols' efficiency drops dramatically when only a small number of nodes are attacked.

We propose a novel protocol named Eges that leverages hardware trusted execution environments (e.g., SGX) to develop a new abstraction called "stealth committee", which effectively hides a committee into a large pool of fake committee nodes. Eges selects a different stealth committee for each block and confirms the same blocks among all nodes with overwhelming probability. Our evaluation shows that Eges is the first efficient permissioned blockchain's consensus protocol, which simultaneously satisfies two important metrics: (1) Eges can tolerate tough DoS and network partition attacks; and (2) Eges achieves comparable throughput and latency as existing fastest permissioned blockchains' consensus protocols. Eges's source code is available on github.com/hku-systems/eges.

1 MOTIVATION

A blockchain is a distributed ledger recording transactions agreed by a consensus protocol [7, 15, 18] with the consistency guarantee: nodes *confirm* the same sequence of blocks. A blockchain can be permissioned or permissionless. Compared to permissionless blockchains that use cryptocurrency mechanisms [10] to incentivize nodes to follow the protocols, permissioned blockchains running the mature Byzantine Fault-Tolerant (BFT) protocols [7, 15, 18] are more suitable for deploy general data-sharing applications.

Unfortunately, existing permissioned blockchains [1, 13] run their consensus protocols on a static and explicit committee, making them vulnerable [6, 16] to targeted Denial-of-Service and network partition attacks. With recent DoS attacks lasting for days [8], tolerating such attacks is crucial, yet challenging, for applications deployed on permissioned blockchains.

To this end, this paper aims to explore the new design point of building a permissioned blockchain's consensus protocol with the *unpredictable dynamic committee* merit to defend against targeted DoS or targeted partition attacks, and at the same time, achieves comparable efficiency as existing BFT protocols [7, 15, 18].

2 THE EGES CONSENSUS PROTOCOL

We present Eges[1], the first efficient consensus protocol that can tackle targeted DoS or targeted partition attacks for a permissioned blockchain. To defend against DoS or partition attacks targeting the committees, we leverage the integrity and confidentiality features of hardware Trusted Execution Environments (TEEs) to present a new abstraction called *stealth committee* with two new features. First, Eges selects a stealth committee without communication among nodes, and the selection progress is protected by TEE. This ensures that a committee node stays stealth before sending out its protocol messages. Second, when nodes in a committee are trying to confirm a block, Eges hides them into a large pool of fake committee nodes that behave identically as the real ones observed from outside TEE, so that an attacker cannot identify the real committees.

The key challenge faced by Eges it to efficiently ensure both consistency and reasonable liveness with dynamic stealth committees in an asynchronous network. Specifically, suppose a committee node x for the n^{th} block fails to receive the $(n-1)^{th}$ block after a timeout, x cannot distinguish whether it is because the committee for the $(n-1)^{th}$ block failed to confirm the $(n-1)^{th}$ block, or because x itself does not receive the confirmed $(n-1)^{th}$ block due to network problems. As the committee nodes for the $(n-1)^{th}$ block may be under DoS attacks and be unreachable, x must have a mechanism to distinguish these two scenarios in order to maintain both consistency and reasonable liveness in Eges.

Eges tackles this challenge by leveraging simple probability theory. Eges's committee for each block contains one proposer and n_A (e.g., 300) acceptors, randomly and uniformly selected from all nodes. The proposer broadcasts its block proposal to all nodes by P2P broadcasts and seeks quorum `ACK`s from the acceptors. Eges models the randomly selected acceptors as a sampling of the *delivery rate* of the proposal in the P2P overlay network [6]. In the previous example, Eges confirms the proposal for the $(n-1)^{th}$ block only if the proposal is delivered to a large portion of member nodes; if multiple rounds ($D = 4$ by default) of the sampling show that very few nodes have received that proposal for the $(n-1)^{th}$ block, nodes in Eges consistently confirm the $(n-1)^{th}$ block as an empty block (with an overwhelming probability).

*Heming Cui is the corresponding author.

[1] Eges stands for Efficient, GEneral, and Scalable consensus.

Protocol	DoS/part. resistance	With TEEs?	No. nodes	Tput (txn/s)	Lat. (s)
Eges	high	Yes	300	3226	0.91
			10K	2654	1.13
Algorand	high	No	10K	~727	~22
PoET	medium*	Yes	100	149	45.2
Ethereum	medium*	No	100	178	82.3
SBFT	low	No	62	1523	1.13
MinBFT	low	Yes	64	2478	0.80
BFT-SMaRt	low	No	10	4512	0.67
Tendermint	low	No	64	2462	1.31
HotStuff	low	No	64	2686	2.63
HoneyBadger	low	No	32	1078	9.39

Table 1: Comparison of Eges to baseline protocols. "DoS/part. resistance" stands for resistance to targeted DoS or network partition attacks; "Lat" stands for confirm latency. *PoET and Ethereum cannot ensure consistency on network partition attacks [11].

In sum, Eges efficiently enforces consistency and can defend against targeted DoS or partition attacks. Specifically, Eges defends against such attacks by (1) letting committee nodes stay stealth *before* they start achieving consensus for a block, (2) using fake committee nodes to conceal real committee nodes *while* they are achieving consensus for a block, and (3) switching to a different committee and consistently confirming a block even if the attacker luckily guesses most real committee nodes for this block. [5] describes Eges's protocol step by step with formal proof and security analysis.

3 KEY RESULTS AND CONTRIBUTIONS

We implemented Eges using the Ethereum codebase and compared Eges with nine consensus protocols for blockchain systems, including five state-of-the-art BFT protocols for permissioned blockchains (BFT-SMaRt [15], SBFT [7], HoneyBadger [9], and HotStuff [18]), two TEE-powered consensus protocols for permissioned blockchains (Intel-PoET [12] and MinBFT [17]), the default consensus protocol in our codebase (Ethereum-PoW [4]), and two permissionless blockchains' protocols that run on dynamic committees (Algorand [6] and Tendermint [3]). We ran Eges on both our cluster and AWS. The extensive evaluation results (Table 1) show that:

- Eges is robust. Among all consensus protocols for permissioned blockchains, Eges is the only protocol that can defend against targeted DoS and network partition attacks.
- Eges is efficient. Eges confirms a block with 3000 transactions in less than two seconds in typical geo-distributed settings, comparable to evaluated consensus protocols that cannot tolerate targeted DoS attacks.
- Eges's throughput and latency are scalable to the number of nodes. When running 10k nodes, Eges showed 2.3X higher throughput and 16.8X lower latency than Algorand.

Our contribution is three-fold. First, Eges leverages TEEs to explore the new design point of tackling DoS attacks while enforcing both consistency and reasonable liveness for a permissioned blockchain in the asynchronous Internet. Second, we designed the new stealth committee abstraction and implemented Eges's consensus protocol. Our third contribution includes an implementation of the Eges prototype and the extensive experiments of Eges and existing blockchain consensus protocols on diverse adversarial network conditions, including targeted DoS attacks, ubiquitous DoS attacks, and network partitions. Our paper reveals that, in addition to safety and performance, DoS resistance is also an essential evaluation metric for practical Internet-scale blockchain applications [2, 14].

ACKNOWLEDGMENTS

We thank our shepherd, Zhenhua Liu, and all anonymous reviewers for their valuable comments. This project was funded by Huawei Innovation Research Program Flagship 2018, Huawei Theory Lab Flagship 2021, HKU-SCF R&D funding scheme, HK RGC GRF (17202318, 17207117, 17201220), HK RGC ECS (27200916), Research Grants Council of the Hong Kong Special Administrative Region, China (No. PolyU15222320), and a Croucher Innovation Award.

REFERENCES

[1] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*. ACM, 30.

[2] Mathieu Baudet, Avery Ching, Andrey Chursin, George Danezis, François Garillot, Zekun Li, Dahlia Malkhi, Oded Naor, Dmitri Perelman, and Alberto Sonnino. 2019. State machine replication in the Libra Blockchain.

[3] Ethan Buchman. 2016. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. http://atrium.lib.uoguelph.ca/xmlui/bitstream/handle/10214/9769/Buchman_Ethan_201606_MAsc.pdf. Accessed: 2017-02-06.

[4] Vitalik Buterin. 2014. Ethereum: A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed: 2016-08-22.

[5] Xusheng Chen, Shixiong Zhao, Ji Qi, Jianyu Jiang, Haoze Song, Cheng Wang, Tsz On Li, TH Hubert Chan, Fengwei Zhang, Xiapu Luo, et al. 2021. Efficient and DoS-resistant Consensus for Permissioned Blockchains. *Performance Evaluation* (2021), 102244.

[6] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. 2017. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. Cryptology ePrint Archive, Report 2017/454. Accessed: 2017-06-29.

[7] Guy Golan Gueta, Ittai Abraham, Shelly Grossman, Dahlia Malkhi, Benny Pinkas, Michael K Reiter, Dragos-Adrian Seredinschi, Orr Tamir, and Alin Tomescu. 2019. SBFT: a Scalable Decentralized Trust Infrastructure for Blockchains. IEEE/IFIP International Conference on Dependable System and Network (DSN 2019).

[8] Oleg Kupreev, Ekaterina Badovskaya, and Alexander Gutnikov. 2019. DDoS attacks in Q2 2019.

[9] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. 2016. The honey badger of BFT protocols. https://eprint.iacr.org/2016/199.pdf.

[10] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. Accessed: 2015-07-01.

[11] Christopher Natoli and Vincent Gramoli. 2016. The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example.

[12] poet [n.d.]. https://www.hyperledger.org/projects/sawtooth.

[13] Ji Qi, Xusheng Chen, Yunpeng Jiang, Jianyu Jiang, Tianxiang Shen, Shixiong Zhao, Sen Wang, Gong Zhang, Li Chen, Man Ho Au, and Heming Cui. 2021. Bidl: A High-Throughput, Low-Latency Permissioned Blockchain Framework for Datacenter Networks. In *Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles CD-ROM* (Virtual Event, Germany) *(SOSP '21)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3477132.3483574

[14] Robert Riemann and Stéphane Grumbach. 2017. Distributed Protocols at the Rescue for Trustworthy Online Voting. arXiv:1705.04480.

[15] João Sousa, Alysson Bessani, and Marko Vukolić. 2018. A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. IEEE/IFIP International Conference on Dependable System and Network (DSN 2018).

[16] Saar Tochner, Aviv Zohar, and Stefan Schmid. 2020. Route Hijacking and DoS in Off-Chain Networks. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 228–240.

[17] Giuliana Santos Veronese, Miguel Correia, Alysson Neves Bessani, Lau Cheuk Lung, and Paulo Verissimo. 2013. Efficient byzantine fault-tolerance. *IEEE Trans. Comput.* 62, 1, 16–30.

[18] Maofan Yin, Dahlia Malkhi, Michael K Reiter, Guy Golan Gueta, and Ittai Abraham. 2019. Hotstuff: Bft consensus with linearity and responsiveness. In *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*. 347–356.