R210 Essay: Blockchain

Chongyang Shi (*cs940*)

March 8, 2018

1 Summaries of research

The 2017 survey paper by Bano et al. [1] summarised state-of-art approaches to the consensus problem in blockchain systems. Starting with an overview on shared focuses of recent blockchain research, the authors categorised existing solutions based on their permission and transaction properties. These properties in turn constrained how consensus leaderships can be established with computational proofs in each solution. The authors then studied blockchain solutions using each consensus model for their liveness and safety properties, as well as their efficiencies. The traditional proof-of-work consensus was found to perform poorly on aspects of scalability, fair incentivisation, and majority attack resistance. Consensus approaches relying on stakes or capacity proofs generally improved on these aspects, but still suffered from poor network-wide consistency. Hybrid approaches with one or more consensus committees could achieve strong network-wide consistency, at the cost of reduced tolerance against malicious nodes and increased messaging complexity. Better consensus protocols addressing some or all of the issues were suggested as a direction of future work.

Bitcoin requires six or more new blocks to be mined before the probability of a prior double-spending attack becomes negligible, resulting in a long confirmation delay. ByzCoin by Kokoris-Kogias et al. [2] sought to address this by integrating an improved Practical Byzantine Fault Tolerance (PBFT) algorithm. As PBFT suffered from limited scalability due to static consensus group sizes and MAC-based $O(n^2)$ communications, the adapted solution resolved these by introducing scalable collective signing with the CoSi protocol [3] and $O(n)$ signature-based peer authentications. Along with the introduction of $O(\log n)$ communication trees and transaction-consensus separation, under simulation ByzCoin achieved multi-fold increases in throughputs and under-one-minute confirmation times as compared to Bitcoin. However, the reduced tolerance against malicious nodes (from 51% majority to 33% plurality) can be problematic with significant computation power imbalances in the network, especially with an uncertain window size that could not be confidently determined for real workloads.

Chainspace by Al-Bassam et al. [4] was proposed as a more scalable alternative to Ethereum [5] for decentralised ledgering with smart contracts. Under Chainspace, transactions under contracts were represented by general-purpose procedures and side-effect-free checkers, providing high descriptive power and low verification costs. With all computations processes (other than local secrets for privacy) publicly ordered and verifiable, linear capacity growth was achieved through *infrastructure sharding*. Consensus in Chainspace was assured with the S-BAC distributed commit protocol, ensuring liveness, consistency, validity and audibility of faults. Chainspace's vastly superior performance in evaluation against Ethereum was discussed, along with some possible use cases. However, the evaluation conducted was simulated and limited in scale, with the practical performance of S-BAC's optimistic concurrency untested under an Ethereum-level network workload.

2 Key themes of research

2.1 Decentralised consistency: performance and scalability

With all but a few blockchain systems adopting a decentralised supply and processing model [1, VIII. A.], practicalities of realising cryptocurrencies depend on the performance and scalability of their consensus models, which were the key metrics measured across the publications. By reducing communication and authentication complexities, most committee-based consensus solutions evaluated by Bano et al. [1] achieved near-linear network scaling, with ByzCoin [2] as an example. ByzCoin also achieved [2, 4.3] the highest relative throughput among proof-of-work consensus blockchains; while the flexible Chainspace [4, Sec. VII] significantly outperformed Ethereum in processing smart contracts.

2.2 Building strong DoS and forgery resistance in blockchain protocols

Without a centralised management, another important goal for blockchain systems is to be resilient against abuses, which can be malicious attacks aiming to damage public confidence in a blockchain system by denying its use or conducting fraud. Extensive efforts have been made in different blockchain systems to prevent selfish mining [1, VI. E.], open-access-flooding sybil attacks [6], and Byzantine failures caused by malicious leaders [1, VIII. B.]. ByzCoin [2, Sec. 1] left the Byzantine DoS degradation vulnerability unresolved, but its tree-based communication pattern can fall back to flat-layout on DoS attacks [2, 3.7.1]. Chainspace [4, VI. A.] implemented mechanisms to automatically exclude misbehaving shards in networks.

2.3 The fairness problem in blockchain incentivisation

Block chain networks require honest consensus-forming nodes (e.g. miners [2, 3.6.2], committee members [1, VII. D.] and verifying shards [4, IV. B.]) to satisfy their security assurances, therefore it is necessary to incentivise participating nodes fairly. Traditional Nakamoto consensus implemented probabilistic mining successes, which in turn encouraged computational imbalance through pooled mining [1, Sec. V]. ByzCoin [2, 3.3] improved this with stake-based reward sharing to encourage active participation in consensus groups. Chainspace [4, Sec. VIII] implemented a flat-fee system for validating smart contract transactions, with Ethereum-like variability as a development direction.

3 Ideas in current context

In discussing alternative consensus proofs, Bano et al. [1, VI. C.] mentioned the possibility of proof-of-elapsed-time (PoET) with secure platform modules such as Intel SGX. Bano et al. also raised concerns about compromises of such trusted hardware. In a more recent work, Chen et al. [7] demonstrated that due to the chronological nature of the competition, compromising hardware of $\theta(\frac{\log \log n}{\log n})$ nodes was sufficient for an attacker to simulate being the fastest node on the network – a relatively trivial scale requirement. Chen et al. further recommended some design changes to Resource-Efficient Mining to mitigate this vulnerability.

Bano et al. [1, IX. D.] also noted the difficulties in maintaining user privacy in a decentralised and permissionless open ledger system. These difficulties are also present in smart contract systems such as Chainspace [4, II. A.], in which case while local secrets are kept out of verifications by shard nodes, transaction metadata remains public. Several privacy-enhancing overlays [8] have been suggested to improve cryptocurrency privacy, with the most recent tumbler-based approach [9] sufficiently efficient and usable for practical deployment.

Implications of Bitcoin's temporary inconsistencies and block size limitations as suggested by Kokoris-Kogias et al. [2, 2.1] materialised during the recent transaction fee surge [10], making the cryptocurrency unusable for small transactions. As Bitcoin started to encounter performance issues under the 1MB block size limit, the signature block was detached from transactions to reduce resource utilisation [11] (known as *SegWit*). Users dissatisfied with the limited relief provided by SegWit eventually performed a hard fork on the cryptocurrency, creating Bitcoin Cash with 8MB-sized blocks [12].

4 Literature review

Analogical to the survey on blockchain consensus systems by Bano et al. [1], various literature surveys have been conducted on other aspects of the technology. These include an extensive study on security risks and attack surfaces of blockchain systems [13]; a study on applying blockchain designs for security and privacy protection in Internet of Things environments [14]; and a survey on applying blockchain architectures to improve the performance of traditional banking systems [15].

The weakly-synchronous PBFT consensus design of ByzCoin [2] inspired the design of a fully asynchronous BFT mechanism by Miller et al. [16], yielding high performance over poor-reliability networks. In designing a new hybrid blockchain consensus protocol, Pass and Shi [17, Sec. 5] raised the weakness in ByzCoin's committee selection design allowing selfish mining attacks without controlling the required $\frac{1}{3}$ of malicious nodes. In developing a blockchain benchmarking system, Dinh et al. [18] raised the limitations of ByzCoin's consensus-only performance improvement, drawing attention to wider influences on blockchain performance.

Ren and Erkin [19] warned that sharding-based smart contract solutions such as Chainspace [4] will compromise validity when used for value transfers (such as to compensate for validating transactions), and proposed a locally executable validation scheme as an alternative. Building on realistic use cases proposed in the original Chainspace paper, Sonnino et al. have since developed a smart contract library [20] for efficient implementations of additional applications, in addition to offering Ethereum-compatibility.

(1175 words according to texcount.)

References

[1] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Consensus in the age of blockchains," *arXiv preprint arXiv:1711.03936*, 2017.

[2] E. Kokoris-Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing Bitcoin security and performance with strong consistency via collective signing," in *25th USENIX Security Symposium (USENIX Security 16)*, 2016, pp. 279–296.

[3] E. Syta, I. Tamas, D. Visher, D. I. Wolinsky, P. Jovanovic, L. Gasser, N. Gailly, I. Khoffi, and B. Ford, "Keeping authorities" honest or bust" with decentralized witness cosigning," in *Security and Privacy (SP), 2016 IEEE Symposium on*. Ieee, 2016, pp. 526–545.

[4] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis, "Chainspace: A sharded smart contracts platform," *arXiv preprint arXiv:1708.03778*, 2017.

[5] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[6] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.

[7] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," in *Stabilization, Safety, and Security of Distributed Systems*, P. Spirakis and P. Tsigas, Eds. Cham: Springer International Publishing, 2017, pp. 282–297.

[8] S. Meiklejohn and C. Orlandi, "Privacy-enhancing overlays in bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 127–141.

[9] S. Meiklejohn and R. Mercer, "Möbius: Trustless tumbling for transaction privacy," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 2, pp. 105–121, 2018.

[10] L. Bershidsky, "Bitcoin's high transaction fees show its limits," November 2017. [Online]. Available: https://www.bloomberg.com/view/articles/2017-11-14/bitcoin-s-high-transaction-fees-show-its-limits

[11] P. W. Eric Lombrozo, Johnson Lau, "BIP-141, bitcoin improvement proposals," December 2015. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[12] P. Rizzo, "Bitcoin cash hard forks in bid to ease mining difficulties," 11 2017. [Online]. Available: https://www.coindesk.com/bitcoin-cash-hard-forks-blockchain-bid-ease-mining-difficulties/

[13] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[14] M. Atzori, "Blockchain-based architectures for the internet of things: a survey," 2016.

[15] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innovation*, vol. 2, no. 1, p. 24, 2016.

[16] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of bft protocols," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 31–42.

[17] R. Pass and E. Shi, "Hybrid consensus: Efficient consensus in the permissionless model," in *LIPIcs-Leibniz International Proceedings in Informatics*, vol. 91. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

[18] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data*. ACM, 2017, pp. 1085–1100.

[19] Z. Ren and Z. Erkin, "A scale-out blockchain for value transfer with spontaneous sharding," *arXiv preprint arXiv:1801.02531*, 2018.

[20] A. Sonnino, M. Al-Bassam, S. Bano, and G. Danezis, "Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers," *arXiv preprint arXiv:1802.07344*, 2018.