Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing

Context

ByzCoin, a novel Byzantine consensus protocol that leverages scalable collective signing to commit Bitcoin transactions irreversibly within seconds.

ByzCoin achieves Byzantine consensus while preserving Bitcoin's open membership by dynamically forming hash power-proportionate consensus groups that represent recently-successful block miners. ByzCoin employs communication trees to optimize transaction commitment and verification under normal operation while guaranteeing safety and liveness under Byzantine faults, up to a near-optimal tolerance of f faulty group members among 3 f + 2 total. ByzCoin mitigates double spending and selfish mining attacks by producing collectively signed transaction blocks within one minute of transaction submission. Tree-structured communication further reduces this latency to less than 30 seconds. Due to these optimizations, ByzCoin achieves a throughput higher than Paypal currently handles, with a confirmation latency of 15-20 seconds.

Bitcoin Issues

Bitcoin is a decentralized cryptocurrency providing an open, self-regulating alternative to classic currencies managed by central authorities such as banks. Bitcoin builds on a peer-to-peer network where users can submit transactions without intermediaries. Special nodes, called miners, collect transactions, solve computational puzzles (proof-of-work) to reach consensus, and add the transactions in form of blocks to a distributed public ledger known as the blockchain.

The key problem is that Bitcoin's consensus algorithm provides only probabilistic consistency guarantees.

Bitcoin's decentralized consensus and security derive from an assumption that a majority of the miners, measured in terms of hash power or ability to solve hashbased proof-of-work puzzles, follows these rules and always attempts to extend the longest existing chain.

Bitcoin's security is guaranteed by the fact that this majority will be extending the legitimate chain faster than any corrupt minority that might try to rewrite history or double-spend currency. However, Bitcoin's consistency guarantee is only probabilistic, which leads to two fundamental problems.

- First, multiple miners might find distinct blocks with the same parent before the network has reached consensus. Such a conflict is called a fork, an inconsistency that is temporarily allowed until one of the chains is extended yet again.
- Second, the Bitcoin block size is currently limited to 1 MB. This limitation in turn results in an upper bound on the number of transactions per second (TPS) the Bitcoin network can handle, estimated to be an average of 7 TPS. For comparison, Paypal handles 500 TPS and VISA even 4000 TPS.
- Temporary forks due to nearsimultaneous keyblock mining, or deliberately introduced by selfish or malicious miners, can still throw the system into an inconsistent state for 10 minutes or more.

Byzcoin improvements

ByzCoin addresses four key challenges in bringing PBFT's strong consistency to cryptocurrencies:

1. Open membership,
2. Scalability to hundreds of replicas
3. Proof-of-work block conflicts
4. Transaction commitment rate.

ByzCoin builds PBFT atop CoSi, a collective signing protocol that efficiently aggregates hundreds or thousands of signatures. Collective signing reduces both the costs of PBFT rounds and the costs for "light" clients to verify transaction commitment.

PBFT normally assumes a well-defined, closed group of replicas, conflicting with Bitcoin's open membership and use of proof-of-work to resist Sybil attacks.

ByzCoin addresses this conflict by forming consensus groups dynamically from windows of recently mined blocks, giving recent miners shares or voting power proportional to their recent commitment of hash power.

Lastly, to reduce transaction processing latency it adopts the idea from Bitcoin-NG to decouple transaction verification from block mining.

Experiments with a prototype implementation of ByzCoin show that a consensus group formed from approximately the past 24 hours of successful miners (144 miners) can reach consensus in less than 20 seconds, on blocks of Bitcoin's current maximum size (1MB). A larger consensus group formed from one week of successful miners (1008) reached consensus on an 8MB block in 90 seconds, showing that the systems scales both with the number of participants and with the block size. For the 144-participant consensus group, with a block size of 32MB, the system handles 974 transactions per second (TPS) with a 68-second confirmation latency.

These experiments suggest that ByzCoin can handle loads higher than PayPal and comparable with Visa.

Practical Byzantine Fault Tolerance Algorithm

The Byzantine Generals Problem refers to the situation where the malfunctioning of one or several components of a distributed system prevents the latter from reaching an agreement.3 f +1 participants are necessary to be able to tolerate f faults and still reach consensus

The Practical Byzantine Fault Tolerance (PBFT) algorithm was the first efficient solution to the **Byzantine Generals Problem** that works in weakly synchronous environments such as the Internet.

Every round of PBFT has three distinct phases:

1. In the first, pre-prepare phase, the current primary node or leader announces the next record that the system should agree upon.

2. On receiving this pre-prepare, every node validates the correctness of the proposal and multicasts a prepare message to the group. The nodes wait until they collect a quorum of (2 f +1) prepare messages and publish this observation with a commit message.

3. Finally, they wait for a quorum of (2 f + 1) commit messages to make sure that enough nodes have recorded the decision.

PBFT relies upon a correct leader to begin each round and proceeds if a two-thirds quorum exists; consequently, the leader is an attack target. For this reason PBFT has a view-change protocol that ensures liveness in the face of a faulty leader.

PBFT has its limitations:

1. It assumes a fixed, well-defined group of replicas, thus contradicting Bitcoin's basic principle of being decentralized and open for anyone to participate.

2. Each PBFT replica normally communicates directly with every other replica during each consensus round, resulting in O(n)2) communication complexity: This is acceptable when n is typically 4 or not much more, but becomes impractical if n represents hundreds or thousands of Bitcoin nodes.

3. Third, after submitting a transaction to a PBFT service,a client must communicate with a super-majority of the replicas in order to confirm the transaction has been committed and to learn its outcome, making secure transaction verification unscalable.

CoSi Protocol

CoSi is a protocol for scalable collective signing, which enables an authority or leader to request that statements be publicly validated and (co-)signed by a decentralized group of witnesses.

Each protocol run yields a collective signature having size and verification cost comparable to an individual signature, but which compactly attests that both the leader and its witnesses observed and agreed to sign the statement.

For each message to be collectively signed, the leader then initiates a CoSi four-phase protocol round that require two round-trips over the communication tree between the leader and its witnesses:

1. **Announcement**: The leader broadcasts an announcement of a new round down the communication tree. The announcement can optionally include the message M to be signed, otherwise M is sent in phase three.

2. **Commitment**: Each node picks a random secret and uses it to compute a Schnorr commitment. In a bottom-up process, each node obtains an aggregate Schnorr commitment from its immediate children, combines those with its own commitment, and passes a further-aggregated commitment up the tree.

3. **Challenge**: The leader computes a collective Schnorr challenge using a cryptographic hash function and broadcasts it down the communication tree, along with the message M to sign, if the latter has not already been sent in phase one.

4. **Response**: Using the collective challenge, all nodes compute an aggregate response in a bottom-up fashion that mirrors the commitment phase.

The result of this four-phase protocol is the production of a standard Schnorr signature that requires about 64 bytes, using the Ed25519 elliptic curve, and that anyone can verify against the aggregate public key nearly as efficiently as the verification of an individual signature.

ByzCoin Design

ByzCoin is designed for untrustworthy networks that can arbitrarily delay, drop, re-order or duplicate messages.

To implement PBFT Byzcoin does the following:

1. It uses Bitcoin's proof-of-work mechanism to determine consensus groups dynamically while preserving Bitcoin's defense against Sybil attacks.
2. It replaces MAC-authenticated direct communication with digital signatures to make authentication transferable and thereby enabling sparser communication patterns that can reduce the normal case communication latency from O(n2) to O(n).
3. It employs scalable collective signing to reduce perround communication complexity further to O(logn) and reduce typical signature verification complexity from O(n) to O(1).
4. It decouples transaction verification from leader election to achieve a higher transaction throughput.

Byzcoin employs a mechanism already suited to the Sybil attacks: proof-of-work mining. Only miners who have dedicated resources are allowed to become a member of the consensus group. This is called a proof-of-membership.

This mechanism maintains the "balance of power" within the BFT consensus group over a given fixed-size sliding share window. Each time a miner finds a new block, it receives a consensus group share, which proves the miner's membership in the group of trustees and moves the share window one step forward.

At a given moment in time, each miner wields "voting power" of a number of shares equal to the number of blocks the miner has successfully mined within the current window.

This mechanism limits the membership of miners to recently active ones, which prevents the system from becoming unavailable due to too many trustees becoming inactive over time, or from miners aggregating many shares over an extended period and threatening the balance in the consensus group.

Decoupling Transaction Verification from Leader Election

By adopting digital signatures for authentication, Byzcoin is able to use sparser and more scalable communication topologies, thus enabling the current leader to collect and distribute third-party verifiable evidence that certain steps in PBFT have succeeded.

Even with signatures providing transferable authentication, the need for the leader to collect and distribute and for all nodes to verify – many individual signatures per round can still present a scalability bottleneck.

Although ByzCoin so far provides a scalable guarantee of strong consistency, thus ensuring that clients need to wait only for the next block rather than the next several blocks to verify that a transaction has committed, the time they still have to wait between blocks can, nevertheless, be significant, up to 10 minutes using Bitcoin's difficulty tuning scheme

As in Bitcoin-NG, we use two different kinds of blocks. The first, microblocks or transaction blocks, represent transactions to be stored and committed. The current leader creates a new microblock every few seconds, depending on the size of the block, and uses the CoSi based PBFT protocol above to commit and collectively sign it. The other type of block, keyblocks,are mined via proof-of-work as in Bitcoin and serve to elect leaders and create shares in ByzCoin's group membership protocol.

Microblocks: A microblock is a simple block that the current consensus group produces every few seconds to represent newly-committed transactions. Each microblock includes a set of transactions and a collective signature. Each microblock also includes hashes referring to the previous microblock and keyblock: the former to ensure total ordering, and the latter indicating which consensus group window and leader created the microblock's signature. The microblock's hash is collectively signed by the corresponding consensus group.

Keyblocks: Each keyblock contains a proof-of-work, which is used to determine consensus group membership via the sliding-window mechanism discussed earlier, and to pay signers their rewards. Each newly-mined keyblock defines a new consensus group, and hence a new set of public keys with which the next era's microblocks will be collectively signed

Performance Evaluation

To simulate consensus groups of up to 1008 nodes,there were 36 physycal machines oversubscribed and ran up to 28 separate ByzCoin processes on each server. Realistic wide-area network conditions are mimicked by imposing a round-trip latency of 200 ms between any two machines and a link bandwidth of 35 Mbps per simulated host. Note that this simulates only the connections between miners of the consensus group and not the full Bitcoin network. Full nodes and clients are not part of the consensus process and can retrieve signed blocks only after consensus is reached. Since Bitcoin currently is rather centralized and has only a few dozen mining pools, we assume that if/when decentralization happens, all miners will be able to support these rather constrained network requirements. The experimental data to form microblocks was taken by ByzCoin clients from the actual Bitcoin blockchain. Both micro- and keyblocks are fully transmitted and collectively signed through the tree and are returned to the clients upon request together with the proof.

Regarding Consensus group size comparison ByzCoin achieves acceptable latency, as long as the consensus group size is less than 200. After this point the cost for the leader to broadcast the block to everyone incurs large overheads.

Regarding Transaction throughput the 144 node configuration can achieve close to 1000 TPS, which is double the throughput of Paypal, and even the 1008-node roster achieves close to 700 TPS. Even when the tree fails, the system can revert back to 1 MB microblocks on the flat and more robust variant of ByzCoin and still have a throughput ten times higher than the current maximum througput of Bitcoin.

Defence against Bitcoin attacks that Byzcoin covers

1. 0-confirmation Double-Spend Attacks
2. N-confirmation Double-Spend Attacks
3. Eclipse and Delivery-Tampering Attacks.
4. Selfish and Stubborn Mining Attacks.
5. Transaction Censorship.

Conclusion

ByzCoin is a scalable Byzantine fault tolerant consensus algorithm for open decentralized blockchain systems such as Bitcoin. ByzCoin's strong consistency increases Bitcoin's core security guarantees—shielding against attacks on the consensus and mining system such as N-confirmation double-spending, intentional blockchain forks, and selfish mining—and also enables high scalability and low transaction latency. ByzCoin's application to Bitcoin is just one example, though: theoretically, it can be deployed to any blockchain-based system, and the proof-of-work-based leader election mechanism might be changed to another approach such as proofof-stake. If open membership is not an objective, the consensus group could be static, though still potentially large. We developed a wide-scale prototype implementation of ByzCoin, validated its efficiency with measurements and experiments, and have shown that Bitcoin can increase the capacity of transactions it handles by more than two orders of magnitude.