POW-LESS BITCOIN WITH CONFIDENTIAL BYZANTINE POA*

Marco Benedetti, Francesco De Scalas, Marco Ferrara, Giuseppe Galano, Sara Gammasurra, Antonio Maci, Matteo Nardelli

Main Objective
Design and implement a certified Byzantine consensus algorithm for permissioned blockchains which exploits aggregation of Schnorr signatures to generate a block validity certificate while providing signers' quorum confidentiality. Also: reuse all of Bitcoin codebase but POW is called FBFT.

Contributions
FBFT (FROSTED-BFT) combines 3 ingredients:

> 1. Bitcoin < we forked bitcoin core to implement our adaptations

Why Bitcoin
1) Mostly focused on digital payments
2) Extensively tested for almost 15 years
3) Enables 2-layer payments
4) Open-source software

> 2. Frost <
To aggregate Schnorr signatures and produce a valid block solution

FROST-OUTSIDE FEATURES

1) Exchange public frost commitments (d, e)
2) Identity the set of signers before the signing

Future works
1) Experimental evaluation
2) Exploration of dynamic network federation, fairness, privacy, and scalability
3) All code available soon!! as open-source

Results
We modified and combined 3 sophisticated protocols (Bitcoin, Frost, and PBFT) to obtain a permissioned Bitcoin - derived but that guarantees:
1) Byzantine fault tolerance
2) Deterministic finality of transactions
3) Network configuration and quorum confidentiality

Signature share depends on nonce commitments and set of signers...

Future works
1) Experimental evaluation
2) Exploration of dynamic network federation, fairness, privacy, and scalability
3) All code available soon!! as open-source

*All views and opinions are those of the author(s) and do not necessarily reflect the position of Bank of Italy.*