POW-LESS BITCOIN WITH CONFIDENTIAL BYZANTINE POA*

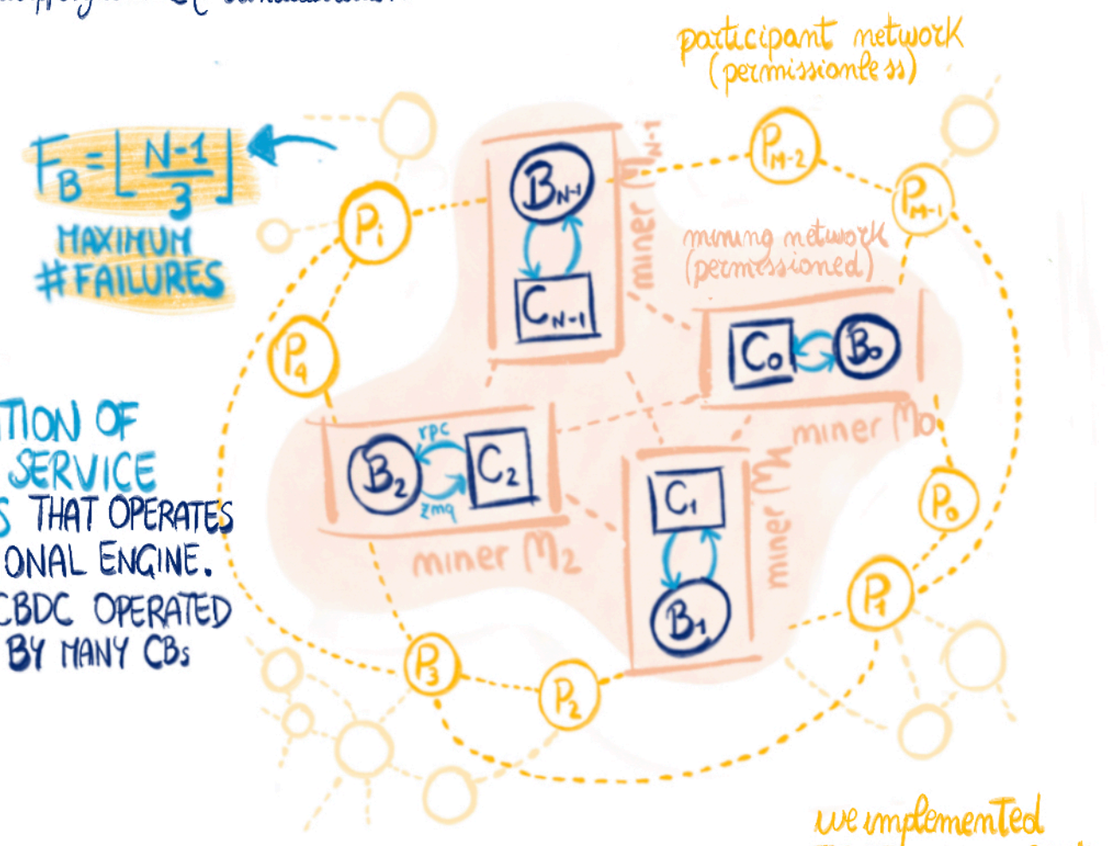
Marco Benedetti, Francesco De Sclavis, Marco Favorito, Giuseppe Galano, Sara Giammusso, Antonio Muci, Matteo Nardelli
{first name}.{last name}@bancaditalia.it, giuseppe.galano2@bancaditalia.it

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

→ CALLED FBFT

Target
A FEDERATION OF FINANCIAL SERVICE PROVIDERS THAT OPERATES A TRANSACTIONAL ENGINE.
EXAMPLE A CBDC OPERATED COOPERATEVELY BY MANY CBs



CONTRIBUTIONS

FBFT (FROSTED-BFT) COMBINES 3 INGREDIENTS:

>1 BITCOIN<

we forked bitcoin-core to implement our adaptations

Used as backbone protocol and architecture for maintaining our shared ledger

WHY BITCOIN

1) MOSTLY FOCUSED ON DIGITAL PAYMENTS
2) EXTENSIVELY TESTED FOR ALMOST 15 YEARS
3) ENABLES 2ND LAYER PAYMENTS → + SCALABILITY + PRIVACY
4) OPEN-SOURCE SOFTWARE → HUGE (FINTECH) ECOSYSTEM

→ PROOF-OF-WORK INDEPENDENT FEATURES

WHAT DID WE CHANGE

1) PROOF-OF-WORK IS DISABLED
2) BLOCKS ARE VALID IFF THEY INCLUDE A SOLUTION TO A SPECIFIC BLOCK CHALLENGE → AS IN THE BITCOIN SIGNET
3) BLOCK SOLUTION EXCLUDED FROM MERKLE ROOT HASH COMPUTATION
4) BLOCK INTERVAL SET TO 1 MIN
5) BLOCK SUBSIDY CAN BE SPENT IMMEDIATELY → COINBASE MATURITY = 0

>2 FROST<

we implemented FROST over secp256k1 from scratch

To aggregate Schnorr signatures and produce valid block solutions → BITCOIN COMPATIBLE

WHAT WE OBTAIN

- NETWORK CONFIGURATION AND QUORUM CONFIDENTIALITY
- PRIVATE QUORUM ACCOUNTABILITY
- FIXED SIZE SIGNATURE INDEPENDENT FROM #SIGNERS

>3 PBFT<

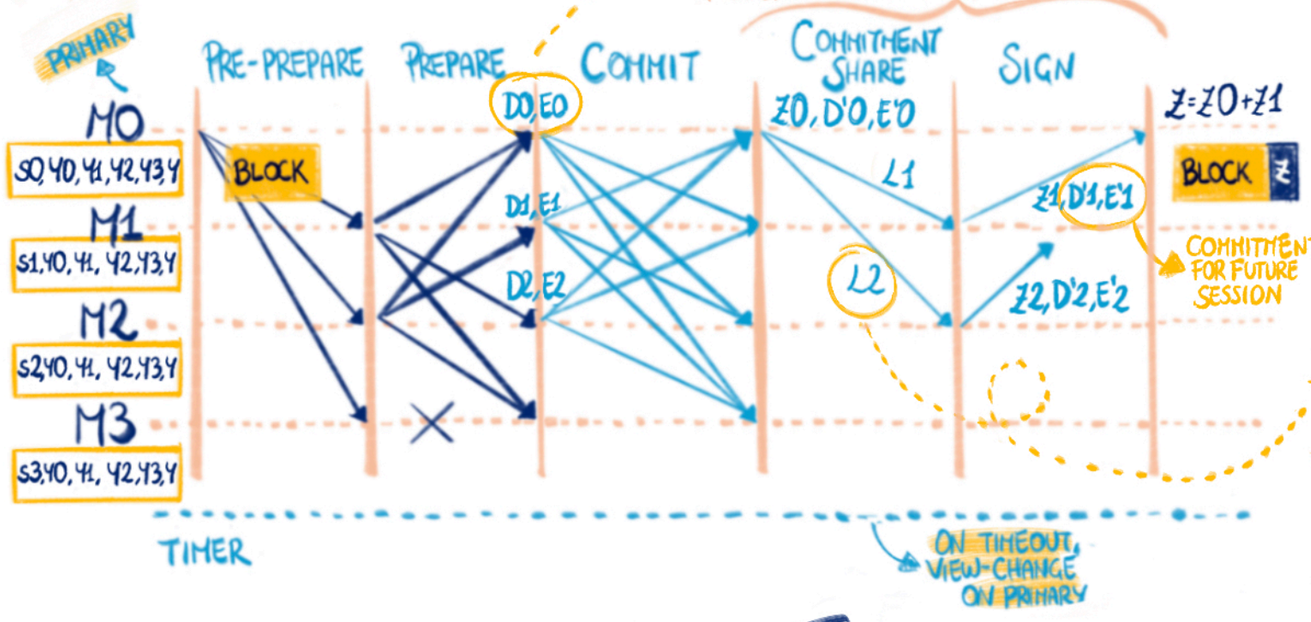
we reimplemented all of PBFT plus our additional rounds

To agree on next block

WHAT DID WE CHANGE

1) FROST COMMITMENTS AND SIGNATURE PROTOCOLS BLENDED INTO PBFT
2) ADDITIONAL ROUNDS TO GUARANTEE LIVENESS IN CASE OF BYZANTINE SIGNERS

Frosted-BFT



SETS OF K PARTICIPANTS:
- RESPONSIVE
- NOT STILL PENDING IN OTHER SESSIONS

TOGETHER WITH THEIR NONCE COMMITMENTS

SIGNATURE SHARE DEPENDS ON NONCE COMMITMENTS AND SET OF SIGNERS...

CHALLENGES:
1) EXCHANGE PUBLIC FROST COMMITMENTS (D_i, E_i)
2) IDENTIFY THE SET OF SIGNERS BEFORE THE SIGNING

RESULTS

WE MODIFIED AND COMBINED 3 SOPHISTICATED PROTOCOLS (BITCOIN, FROST, AND PBFT) TO OBTAIN A PERMISSIONED BITCOIN-DERIVED DLT THAT GUARANTEES:

1) BYZANTINE FAULT TOLERANCE
2) DETERMINISTIC FINALITY OF TRANSACTIONS
3) NETWORK CONFIGURATION AND QUORUM CONFIDENTIALITY

FUTURE WORKS

1) EXPERIMENTAL EVALUATION
2) EXPLORATION OF DYNAMIC NETWORK FEDERATION, FAIRNESS, PRIVACY, AND SCALABILITY
3) ALL CODE AVAILABLE (SOON!!) AS OPEN-SOURCE

BANCA D'ITALIA

A R T
Applied Research Team

IEEE ICBC DUBAI, 2023

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