IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

NPTEL

BLOCKCHAINS

ARCHITECTURE, DESIGN AND USE CASES

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

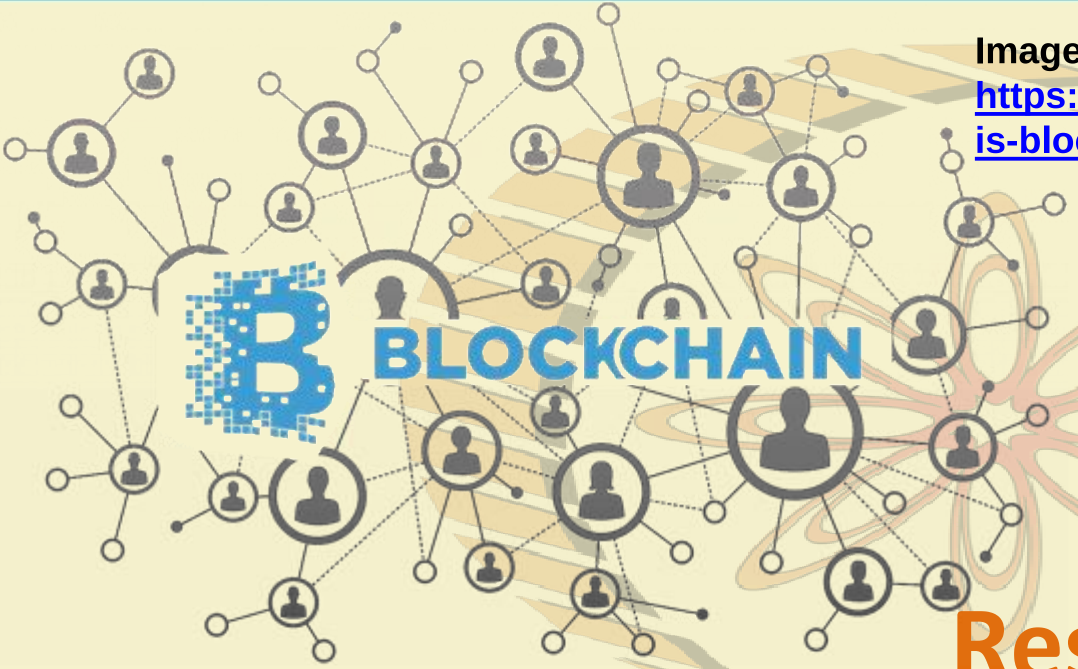


Image Source: https://steemit.com/blockchain/@tariq3njr/what-is-blockchain-technology

Research Aspects - II
Consensus Scalability

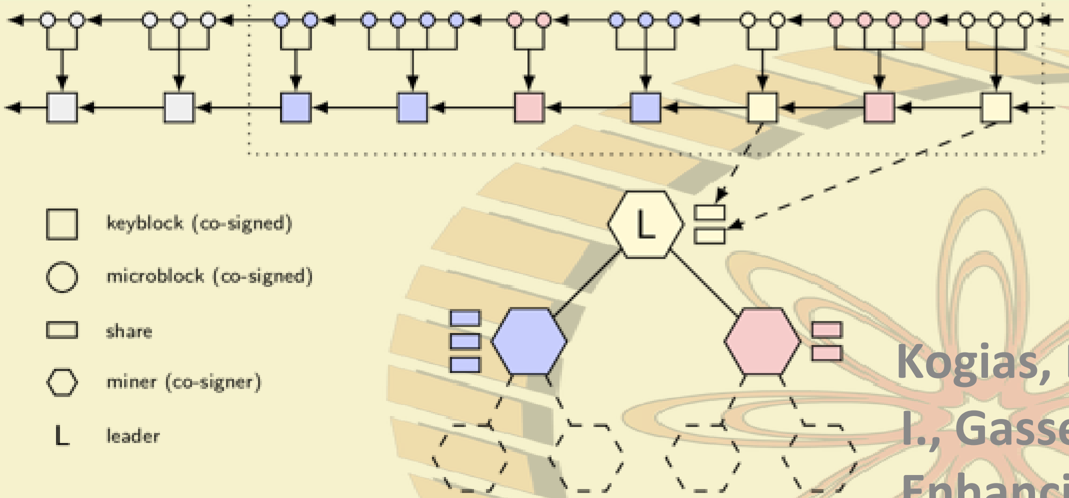


Image Source:
http://hackingdistributed.com/2016/08/04/byzcoin/

Kogias, E. K., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., & Ford, B. (2016, August). Enhancing bitcoin security and performance with strong consistency via collective signing. In *25th USENIX Security Symposium 2016*

Byzcoin

Requirements for Blockchain Consensus

- **Byzantine fault tolerant** – the system should work even in the presence of malicious users while operating across multiple administrative domains
- Should provide **strong consistency guarantee** across replicas
- Should **scale well to increasing workloads** in terms of transactions processed per unit time
- Should **scale well to increasing network size**

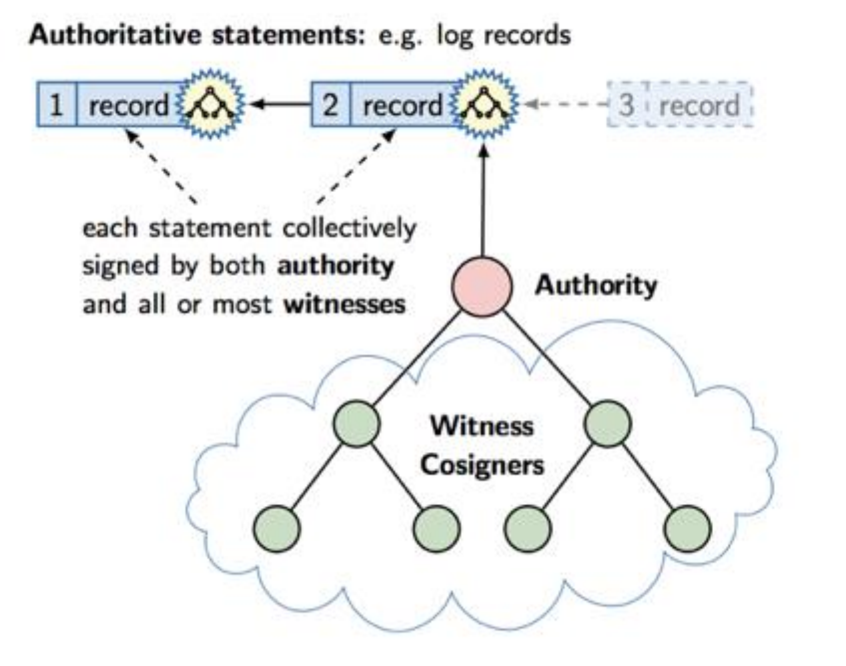
Some Background

- Collective Signing (CoSi)
  - Syta, Ewa, et al. "**Keeping authorities "honest or bust" with decentralized witness cosigning**" *2016 IEEE Symposium on Security and Privacy (SP)*, 2016.

Collective Signing (CoSi)

- Method to protect “authorities and their clients” from undetected misuse or exploits
- A **scalable witness cosigning protocol** ensuring that every authoritative statement is validated and publicly logged by a diverse group of witnesses before any client accepts it
- A statement *S* collectively signed by *W* witnesses assures clients that *S* has been seen, and not immediately found erroneous, by those *W* observers.

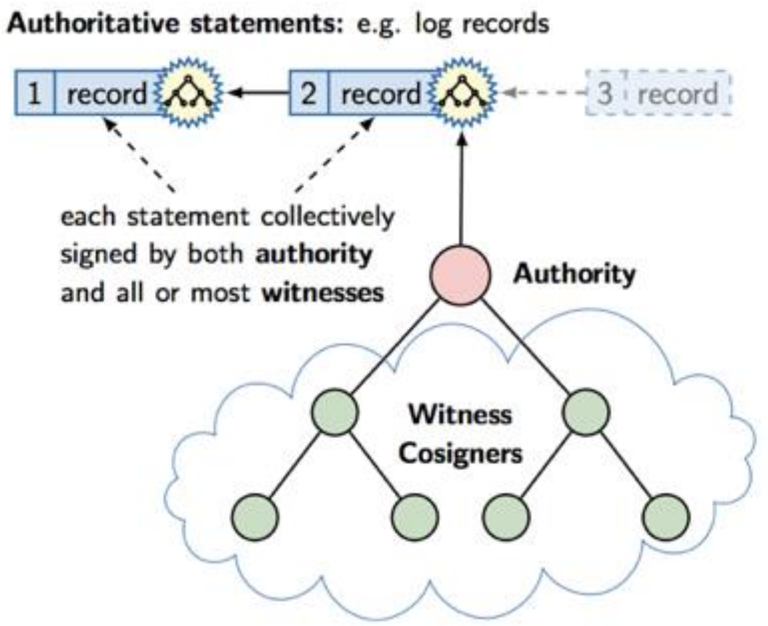
CoSi Architecture



- The leader organizes the witnesses in a tree structure – a scalable way of aggregating signatures coming from the children

- Three rounds of PBFT (pre-prepare, prepare and commit) can be simulated using two rounds of CoSi protocol

CoSi Architecture



- The basic CoSi protocol uses **Schnorr signatures**, that rely on a group *G* of prime order
  - *Discrete logarithmic problem is believed to be hard*

CoSi based on Schnorr Multisignature

- **Key Generation:**
  - Let G be a group of prime order *r*. Let *g* be a generator of G.
  - Select a random integer x in the interval $[0, r-1]$. x is the private key and g^x is the public key.
  - *N* signers with individual private keys $x_1, x_2, \ldots, x_N$, and the corresponding public keys $g^{x_1}, g^{x_2}, \ldots, g^{x_N}$

CoSi based on Schnorr Multisignature

- **Signing:**
  - Each signer picks up the random secret v_i, generates $V_i = g^{v_i}$
  - The leader collects all such V_i, aggregates them $V = \prod V_i$, and uses a hash function to compute a collective challenge $c = H(V||S)$. This challenge is forwarded to all the signers.
  - The signers send the response $r_i = v_i - cx_i$. The leader computes the aggregated as $r = \sum r_i$. The signature is (c, r).

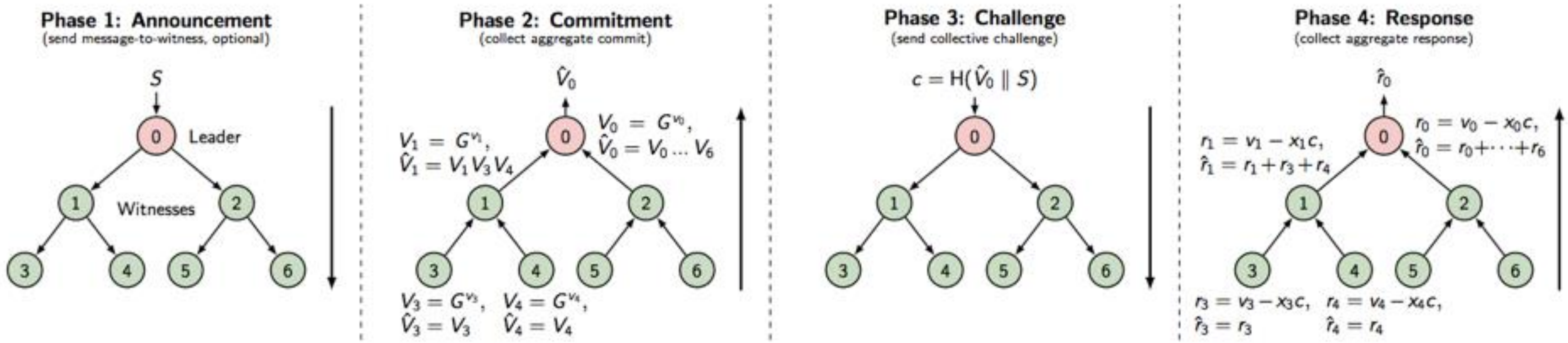
CoSi based on Schnorr Multisignature

- **Verification:**
  - The verification key is $y = \prod g^{x_i}$
  - The signature is (c, r), where $c = H(V||S)$ and $r = \sum r_i$
  - Let $V_v = g^r y^c$
  - Let $r_v = H(V_v||S)$
  - If $r_v = r$, then the signature is verified

CoSi based on Schnorr Multisignature

- **Proof:**
  - The verification key is $y = \prod g^{x_i}$
  - The signature is (c, r), where $c = H(V||S)$ and $r = \sum r_i$
  - $V_v = g^r y^c = g^{\sum(v_i - cx_i)} \prod g^{cx_i} = g^{\sum(v_i - cx_i)} g^{\sum cx_i} = g^{\sum v_i} = \prod g^{v_i} = \prod V_i = V$
  - So, $r_v = H(V_v||S) = H(V||S) = r$

CoSi Protocol



- One CoSi round to implement PBFT's pre-prepare and prepare phases
- Second CoSi round to implement PBFT's commit phase

Scaling CoSi Further

- Use **Boneh–Lynn–Shacham (BLS)** Signature

- Uses a **bilinear pairing for verification**, and **signatures are elements of an elliptic curve group**.

- Let $e: G \times G \rightarrow G_T$ be a non-degenarate, efficiently computable, bilinear pairing where G and G_T are groups of prime order *r*. Let *g* be a generator of G.

BLS Signature

- Let $e: G \times G \rightarrow G_T$ be a non-degenarate, efficiently computable, bilinear pairing where G and G_T are groups of prime order *r*. Let *g* be a generator of G.

- Consider an instance of the computational Diffie-Hellman (CDH) problem g, g^x, g^y
  - The pairing function *e* does not help us to compute g^{xy}, the solution of the CDH problem

BLS Signatures

- **Key generation:** Select a random integer x in the interval $[0, r-1]$. x is the private key and g^x is the public key.

- **Signing:** Let M be a message and $H(M)$ is the hash of M. Then the signature is $\sigma = H(M)^x$.

- **Verification:** Given a signature σ and public key g^x, we verify that
$$e(\sigma, g) = e(H(M), g^x)$$

Advantages of BLS

- **Signing is simple. We do not require two communication round trips similar to Schnnorr Multisignatures, a single communication round trip is sufficient.**

- **Key aggregation is simple.** Say x and y are private keys and g^x and g^y are corresponding public keys. Then,
  - Aggregated Private key: xy
  - Aggregated Public key: $g^x \times g^y = g^{xy}$

thank you!