UNIVERSITY of NICOSIA

Session 8

Consensus

BLOC 514: Emerging Topics in Blockchain and Digital Currency

Objectives of Session

- Understand the need for, and challenges associated with, distributed consensus in cryptocurrencies.
- Explain the similarities and differences between the main mechanisms for achieving distributed consensus in cryptocurrencies.
- Review indicative protocols such as proof-of-work, proof-of stake, proof-of-burn, and proof-of-capacity.
- Review the need for proof-of-reserve along with the respective steps for audit
- Understand a framework that can be used for deciding about the "green profile" of the consensus needed in a broader IT solution/architecture

T

Agenda

- Distributed consensus
- Methods for achieving distributed consensus
  - Proof-of-work
  - Proof-of-stake
  - Proof-of-burn
  - Proof-of-capacity
  - Delegated proof-of-stake
- Proof-of-reserves
- Green consensus
- Conclusions
- Resources

Distributed Consensus

Introductions: distributed vs. decentralized systems

Introductory discussion

Distributed systems

vs.

Decentralized systems

The need for Distributed Consensus

- **Distributed Consensus, as the term is used in crypto-currencies, is a global agreement between many parties that do not know or trust each other.**
  - The reason this consensus is needed is the **double-spending** problem. A **distributed consensus** on transaction ordering achieves this: in the case of conflict, everyone agrees that the transaction which came first is valid, while all others are not.
  - In Satoshi Nakamoto's words, **"for the purposes of cryptocurrency, it is sufficient to achieve distributed consensus on the time-ordering of transactions (and nothing else)".**
- The Bitcoin blockchain is authenticated using a **dynamic-membership multi-party signature (DMMS)**. "Dynamic-membership" means that there is no fixed list of authenticating parties (anyone can participate).
  - This consists of an expensive to produce, but cheap to verify, computation which is performed continuously on the entire blockchain. This computation is called **proof-of-work (PoW).**
- Because PoW is computationally, and therefore thermodynamically, very expensive, **alternatives** have been proposed, which aim to be economically and environmentally more efficient.

Proof-of-Work

Proof-of-Work (PoW)

- **The proof-of-work concept was originally designed by Dwork and Naor in 1993 as a mechanism to combat junk emails.**
  - The main idea is: "*to require a user to compute a moderately hard, but not intractable, function in order to gain access to the resource, thus preventing frivolous use*".

- The same concept can be applied to numerous situations, in which **the goal is to prevent fraudulent or malicious use**.
  - Users are required to do some computational work (usually solve a mathematical puzzle) in order to gain access to an online service.
  - A key feature of such work is that it must be hard to compute (the difficulty level depends on the task at hand), but easy to verify.

- PoW is a way to **impose fees to users** when transacting with a service.
  - Users who try to abuse the service will be unable to do so, due to high costs.
  - However, in the long run, PoW alone might lead to low network security when block incentives decline over time.

Proof-of-Work Functions

- PoW schemes can be categorized, based on the underlying function they use, into:
  - **CPU-bound**, where the time to solve the puzzle is determined by the processing power. For example, Bitcoin uses SHA256, which is a CPU-bound PoW function.
  - **Memory-bound**, where the time to solve the puzzle depends on the amount of memory allocated. For example, Litecoin uses Scrypt, which is a memory-bound PoW function.
  - **Network-bound**, where the time to solve the puzzle is bounded by network latency/bandwidth.

Desirable PoW Properties

- Finding an appropriate mathematical puzzle is not trivial. Ideally, this puzzle should:
  - **Be feasible to compute in desired time**. The user should be able to compute the solution in a reasonable amount of time. If the given puzzle is not solvable, then the user would not be able to connect to the server and/or use the service.
  - **Be easy to verify the solution**. If the verification of the solution is difficult, then the server would not be able to handle a large number of users.
  - **Not be amendable to amortization**. The time for completing *n* puzzles should be proportional to *n* (i.e., linear relationship).
  - **Not easy to be computed after preprocessing**. If the problem can be reduced to another problem that requires less computational power, then users would be able to cheat and abuse the system.
- Popular proof-of-work puzzles include:
  - Integer square root modulo a large prime
  - Hashcash (used in Bitcoin)

Bitcoin and Proof-of-Work

- **Bitcoin uses the Hashcash proof-of-work mechanism**, proposed by Adam Back in 1997.
  - The original puzzle is "find x such that SHA(x) contains N high-order null bits". In Bitcoin, the mining process involves **double hashing**.
  - The number of leading zeros is determined by the **difficulty target** (the more leading zeros the more difficult to solve the problem). The target is automatically adjusted, every 2,016 blocks, so that blocks are produced approximately every ten minutes.
  - **Miners are incentivized** to provide their computational power through two types of rewards: transactions fees and newly minted coins.
  - This has created a **mining arms race**: from CPU to GPU to FPGA to ASIC mining. This race has raised concerns regarding the decentralization of the network.

- To avoid ASICs, many alt-coins have introduced different hashing algorithms and/or PoW schemes that are considered to be ASIC resistant.
  - However, this is not the case, as **ASICs can be designed to perform any hashing algorithm.**
  - ASICs will be developed when/if the total cost of production is less than expected profits.

Scrypt-based PoW

- In cryptography, **Scrypt is a password-based key derivation function** created by Colin Percival.
  - The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by **requiring large amounts of memory**.
  - A simplified version of Scrypt is used as a **memory-bounded** PoW scheme in various cryptocurrencies.
  - Scrypt was originally implemented as part of an alt-coin called **Tenebrix** and later served as the basis for coins like **Litecoin** and **Dogecoin**.
  - By requiring memory (instead of processing power) to perform the PoW, Scrypt was thought to make it impossible to mine with SHA-based ASICs – so, users would be able to mine using their CPUs and GPUs again.
  - However, when alt-coins gained enough popularity/value to make ASIC production and mining profitable enough, Scrypt ASICs were implemented, too.

Proof-of-Stake

Proof-of-Stake

- The Proof-of-Stake (PoS) consensus mechanism, introduced by King and Nadal in 2012, is perhaps the most popular alternative to PoW in digital currencies.
  - PoS is a method of securing a crypto-currency network and achieving distributed consensus by **requesting users to show ownership of a certain amount of currency.**
  - In PoS systems, **the probability to create a block is proportional to a user's ownership stake in the system.**
  - The rationale behind PoS is that users with highest stakes have the most interest to keep the network secure. Malicious users would need to acquire most of the currency, **making the attack very expensive.**
  - The main **advantages** are the absence of expensive computations and specialized hardware.
  - The main **disadvantage** is the initial distribution of the coins.

- Interesting debate between economist Yanis Varoufakis (former Greek finance minister) and blockchain developer Viktor Tábori including the argument that *"POS promotes oligarchy"*
  - At BrainBar 2022
  - Link to video

Proof-of-Stake: Ethereum 2

- (Before Merge) According to ethereum.org:
  - PoS *"is a consensus mechanism that is going to replace the proof-of-work system currently in place."*
  - *"Proof-of-stake is managed by the Beacon Chain."*
  - *"Ethereum will have a proof-of-stake Beacon Chain and a proof-of-work Mainnet for the forseeable future. Mainnet is the Ethereum we've been using for years."*
- Please frequently monitor ethereum.org as updates are rapidly announced/taking place
- Another important aspect is how one can be involved in the staking process
  - Many "details" are critical, e.g., see below

Solo staking

Rewards

- Maximum rewards - receive full rewards directly from the protocol
- You'll get rewards for batching transactions into a new block or checking the work of other validators to keep the chain running securely
- You'll also receive unburnt transaction fees for blocks you propose

Risks

- Your ETH is at stake
- There are penalties, which cost ETH, for going offline
- Malicious behavior can result in 'slashing' of larger amounts of ETH and forced ejection from the network

Staking as a service

Rewards

- Usually involves full protocol rewards minus monthly fee for node operations
- Dashboards often available to easily track your validator client

Risks

- Same risks as solo staking plus counter-party risk of service provider
- Use of your signing keys is entrusted to someone else who could behave maliciously

Pooled staking

Rewards

- Pooled stakers accrue rewards differently, depending on which method of pooled staking chosen
- Many pooled staking services offer one or more liquidity tokens that represents your staked ETH plus your share of the validator rewards
- Liquidity tokens can be held in your own wallet, used in DeFi and sold if you decide to exit

Risks

- Risks vary depending on the method used
- In general, risks consist of a combination of counter-party, smart contract and execution risk

- Paper on recent PoS-related attacks – Section 2 summarizes PoS Ethereum/Gasper

Proof-of-Stake

- Synopsis according to ethereum.org:

Proof-of-stake underlies certain consensus mechanisms used by blockchains to achieve distributed consensus. In proof-of-work, miners prove they have capital at risk by expending energy. Ethereum uses proof-of-stake, where validators explicitly stake capital in the form of ETH into a smart contract on Ethereum. This staked ETH then acts as collateral that can be destroyed if the validator behaves dishonestly or lazily. The validator is then responsible for checking that new blocks propagated over the network are valid and occasionally creating and propagating new blocks themselves.

Proof-of-stake comes with a number of improvements to the now-deprecated proof-of-work system:

- better energy efficiency – there is no need to use lots of energy on proof-of-work computations
- lower barriers to entry, reduced hardware requirements – there is no need for elite hardware to stand a chance of creating new blocks
- reduced centralization risk – proof-of-stake should lead to more nodes securing the network
- because of the low energy requirement less ETH issuance is required to incentivize participation
- economic penalties for misbehaviour make 51% style attacks exponentially more costly for an attacker compared to proof-of-work
- the community can resort to social recovery of an honest chain if a 51% attack were to overcome the crypto-economic defenses.

Hybrid PoW/PoS

- In hybrid systems, instead of relying solely on processing power, block generation relies also on the **concept of coinage**.
  - **Coinage is the amount of coins owned multiplied by the duration of ownership**. The more coinage a user owns, the more chances s/he will produce a valid block.
  - Usually, hybrid crypto-currencies use **PoW for the initial production/distribution of coins.**
  - Over time, PoS phases out PoW.
  - The main advantage of such systems is that they are environmentally friendly in the long run, while also avoiding the initial distribution problem of pure PoS.

Proof-of-Burn

Proof-of-Burn

- The idea of PoB is **that miners should show proof they burned some coins to increase their chances of mining a block.**
  - Coins are burned by sending them to addresses where they cannot be redeemed.
  - The probability of finding a block is proportional to the amount of burned coins.
  - The philosophy is similar to PoS (while also adding to coin deflation). The more you burn, the more you invest, hence the more incentive you (must) have to keep the network secure.
  - PoB is considered an expensive consensus mechanism, but it does not consume other resources (environmental friendly).
- **Counterparty** was the most popular crypto-currency that used PoB.
  - Participants received Counterparty tokens by providing proof they burned bitcoins (see here).
- But there is another angle to view/utilize burning
  - An action for reducing the supply in order to preserve/increase the demand (that is, increase scarcity)
  - Related example: LUNA

Proof-of-Capacity

Proof-of-Capacity

- PoC is **an implementation of an idea called "megabytes as resources".**
  - Instead of processing power (PoW SHA256) or memory **(PoW Scrypt), PoC utilizes HDD mining to validate blocks.**
  - The probability of finding a block is proportional to the hard disk space allocated.
  - It is an energy efficient consensus mechanism, which also offers botnet protection (as it is hard to steal a large portions of HDD from victims).
  - On the other hand, it does not solve the "nothing-at-stake" problem. For example, miners can use PoC to mine different chains simultaneously without spending more resources. It is also slower (it requires disk access, which takes significant time).

Delegated Proof-of-Stake

Delegated Proof-of-Stake

- A blockchain engineer named Daniel Larimer thought that Bitcoin mining was too **wasteful of energy.** Also he wanted to build a system that was capable of transaction speeds like **100,000 per second**. He invented and built a new system that used very little energy, was fast and also very secure: **the Delegated Proof of Stake, or DPOS.**
    - DPoS uses a **reputation system** and **real-time voting** to achieve consensus.
    - The DPOS algorithm is divided into two parts: **electing a group of block producers** and **scheduling production**. The election process makes sure that stakeholders are ultimately in control because stakeholders lose the most when the network does not operate smoothly.
    - All network parameters, from fee schedules to block intervals and transaction sizes, can be tuned via **elected delegates**. Deterministic selection of block producers allows transactions to be confirmed in an average of just **1 second**.
    - The consensus protocol is designed to protect all participants against **unwanted regulatory interference**.

Example of DPoS as Governance Model

- **System requires Trust, Efficiency, Effectiveness, Robustness and Speed**
- **Look at how Steemit is set up with Steem-Witnesses:**
  - Each Account holder has **Votes** for Steem-Witnesses. The witnesses function as **'delegates**' that are responsible for the overall vitality of the Network/blockchain.
  - Having a somewhat small concentrated number of delegates/witnesses, enables a high performance level of effectiveness in mining the blocks and general upkeep of the network/blockchain.
  - By having a focused amount of primary positions of responsibility for witnesses/delegates - trust can be created through a democratic practice. See it is in the delegates/witnesses interest to take care in doing best work as each witness/delegate has a vested interest in the overall communities best interest. This is a win/win. This works as a win/win because the incentives are effectively structured.
  - The voting process is a sort of 24/7 thing - meaning that each steemit user has so many votes and one can utilize their votes at any time. This is quite cool in regards to keeping things moving effectively as a showcasing of 'self-governance' (for the people by the people).

    (source)

Proof-of-Reserves

Proof of Reserves

- After the recent (Nov 2022) FTX collapse, the protection of investors finds its place within the "proof-of-*" family of measurements
- Indicative example: Binance

What Is Proof of Reserves and How it Works on Binance

Intermediate Updated Nov 30, 2022 5m

TL;DR

Crypto custodians use Proof of Reserves (PoR) audits to show they're holding users' funds in full. Binance conducts and publicly publishes internal audits, whereupon third-party auditors help to verify them using cryptographic techniques to prove users' funds are securely held in company reserves. Binance users can also independently verify that their account balances are included in these audits.

Proof of Reserves

- In general, Proof of Reserve apply to business entities that hold cryptocurrencies and have depositors
- Those entities need to prove their respective solvency (mainly to their depositors as well as others)
- The target solvency is achieved through audits
  - Should be conducted by trustworthy independent parties
- Disadvantages
  - Centralized
  - Require time
  - Require manual effort
- Alternative decentralized approach
  - Smart contracts
  - Combined with Oracles

Proof of Reserves

Basic steps of audit

- Generate shapshots of balances of interest
- All snapshots are packed into a Merkle tree
- The root of the Merkle tree is retrieved
- Collection of signatures held by the business entity under audit
  - Need to correspond to balances that can be verified
- Final check
  - Those balance should be equal or larger to the balances corresponding to the Merkle tree

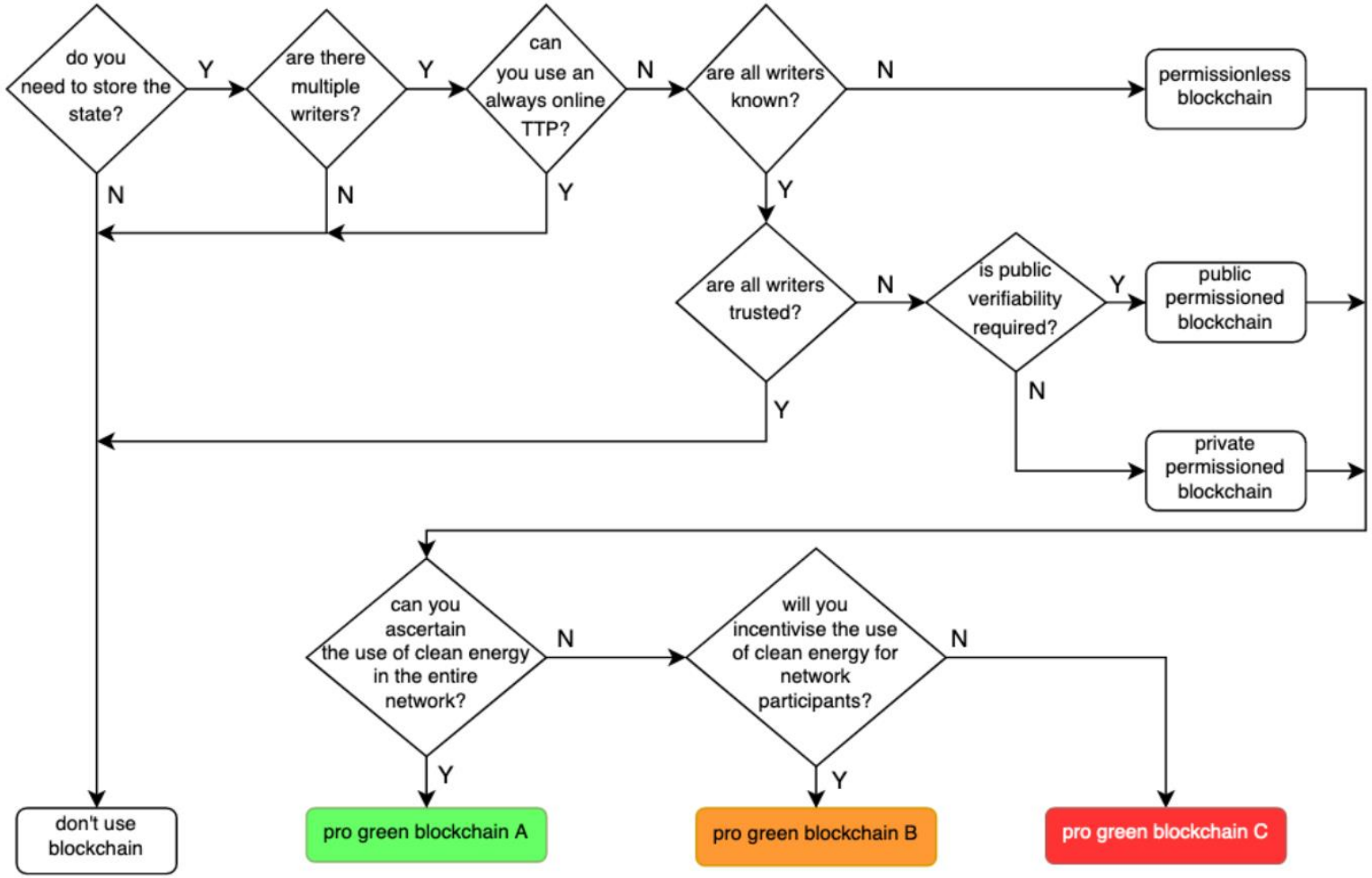
Source

Green Consensus

A Framework Towards Green Consensus

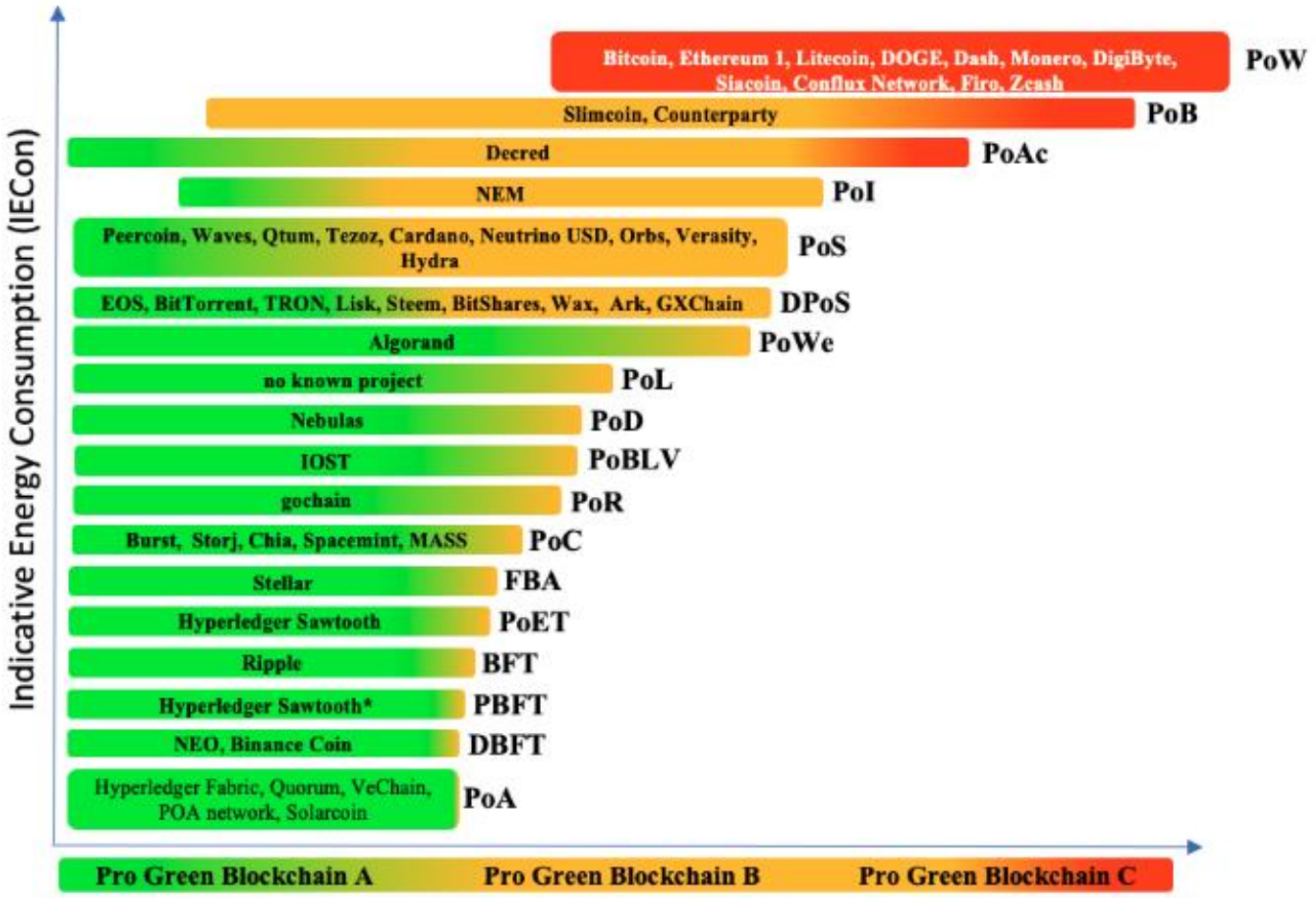
- Proposed in
  - "Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption" by A. O. Bada et al.
  - Link: https://eprints.bournemouth.ac.uk/36968/1/GREEN_BLOCKCHAIN.pdf
- Emphasis on Section IV
  - Extension of the classical framework enabling the decision regarding the incorporation of a blockchain component
  - Figure 1
  - Figure 2
    - Needed for interpreting the suggestions of Figure 1
- Also, this paper provides a high-level comparative analysis of several consensus protocols

A Framework Towards Green Consensus



Source

A Framework Towards Green Consensus



Source

Conclusions

Conclusions

- **How distributed consensus is achieved is critical** for the long-term success of digital currencies, especially as miners compete (**mining arms races**) and adoption scales.
- **Proof-of-work is the most popular mechanism** used today.
- However, it has serious environmental implications.
- Proof-of-stake is a promising alternative, especially when combined with PoW in **hybrid PoW/PoS** systems.
- Motivated by cases like FTX collapse (Nov 2022) other "Proof-of-*" are proposed/added meant for the protection of investors
- The "green" aspects of consensus attract great interest across numerous fronts (e.g., from research to practical considerations)

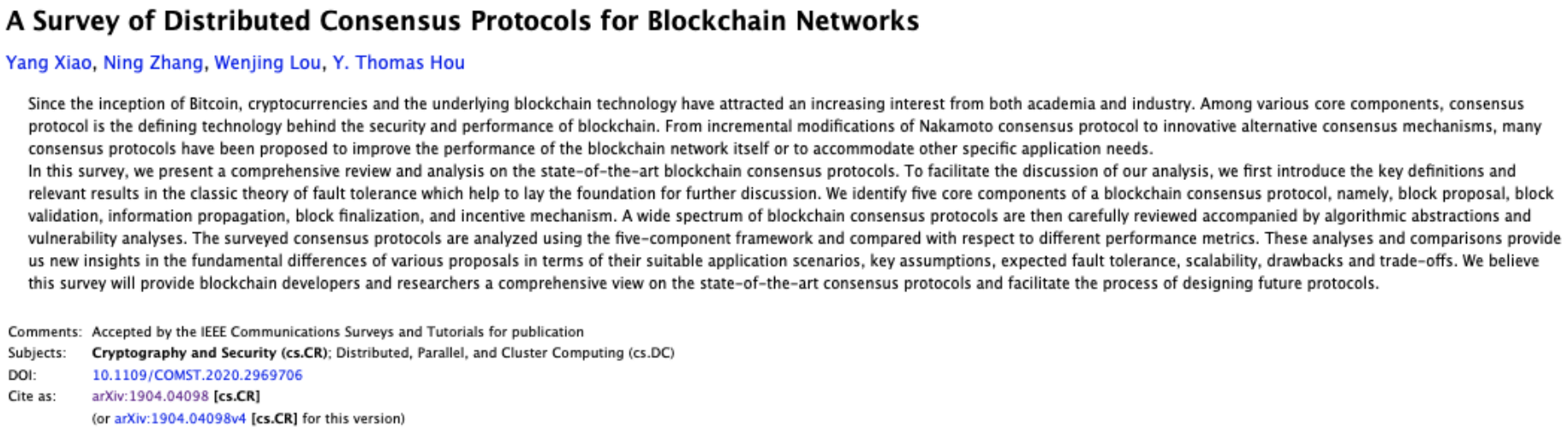
Resources

References

- Ismail and Materwala. **A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions**. Symmetry.
  - Section 5

References: Survey of Distributed Consensus Protocols

- Yang Xiao et al. **"A Survey of Distributed Consensus Protocols for Blockchain Networks"**
  - **Excellent** academic paper
  - *Note: High-level overview (Section I, IX, X) is sufficient. Technical content (rest sections) is optional.*



A Survey of Distributed Consensus Protocols for Blockchain Networks

Yang Xiao, Ning Zhang, Wenjing Lou, Y. Thomas Hou

Since the inception of Bitcoin, cryptocurrencies and the underlying blockchain technology have attracted an increasing interest from both academia and industry. Among various core components, consensus protocol is the defining technology behind the security and performance of blockchain. From incremental modifications of Nakamoto consensus protocol to innovative alternative consensus mechanisms, many consensus protocols have been proposed to improve the performance of the blockchain network itself or to accommodate other specific application needs.
In this survey, we present a comprehensive review and analysis on the state-of-the-art blockchain consensus protocols. To facilitate the discussion of our analysis, we first introduce the key definitions and relevant results in the classic theory of fault tolerance which help to lay the foundation for further discussion. We identify five core components of a blockchain consensus protocol, namely, block proposal, block validation, information propagation, block finalization, and incentive mechanism. A wide spectrum of blockchain consensus protocols are then carefully reviewed accompanied by algorithmic abstractions and vulnerability analyses. The surveyed consensus protocols are analyzed using the five-component framework and compared with respect to different performance metrics. These analyses and comparisons provide us new insights in the fundamental differences of various proposals in terms of their suitable application scenarios, key assumptions, expected fault tolerance, scalability, drawbacks and trade-offs. We believe this survey will provide blockchain developers and researchers a comprehensive view on the state-of-the-art consensus protocols and facilitate the process of designing future protocols.

Comments: Accepted by the IEEE Communications Surveys and Tutorials for publication
Subjects: **Cryptography and Security (cs.CR)**; Distributed, Parallel, and Cluster Computing (cs.DC)
DOI: 10.1109/COMST.2020.2969706
Cite as: arXiv:1904.04098 **[cs.CR]**
(or arXiv:1904.04098v4 **[cs.CR]** for this version)

- Link to arXiv (see the latest version: v4, Jan. 2020)

Additional Bibliography (Optional)

- Poelstra, A. **On Stake and Consensus** (source)
  - *A discussion of DMMS and a critique on PoS.*
- Mazieres, D. **The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus** (source)
  - *Stellar (https://www.stellar.org) is a proposed alternative D/C mechanism, based on FBA (Federated Byzantine Agreement).*
- Tromp, J. **Cuckoo Cycle: A Memory-Hard Proof-of-Work System** (source)
  - *Cuckoo is another proposal for a memory-hard PoW consensus mechanism.*
- Dr. Arati Baliga **Understanding Blockchain Consensus Models** (source)
- Zhang Ren, Preneel Bart **On the Necessity of a Prescribed Block Validity Consensus: Analyzing Bitcoin Unlimited Mining Protocol** (source)
  - *This paper addresses the necessity of a prescribed block validity consensus for cryptocurrencies.*

Additional Bibliography (Optional)

- Rafael Pass and Elaine Shi Hybrid Consensus: **Efficient Consensus in the Permissionless Mode** (source)
- Joseph Bonneau et al. **Research Perspectives and Challenges for Bitcoin and Cryptocurrencies** (source)

UNIVERSITY *of* NICOSIA

Instructor’s Email:
iosif.e@unic.ac.cy