SoK: Consensus Protocols in Blockchains

Shymaa M. Arafat
Associate Professor in CE/CS (independent)
shar.academic@gmail.com, shymaa.arafat@gmail.com

Abstract. When Nakamoto invented Bitcoin, the first generation of cryptocurrencies followed it in applying *POW (Proof of Work)* consensus mechanism; due to its excessive energy consumption and heavy carbon footprints, new innovations evolved like *Proof of Space*, *POS (Proof of Stake)*, *AI-based* consensus protocols, and a lot more with many variants for each. Furthermore, the emergence of more blockchain applications and kinds beyond just cryptocurrencies needed more consensus mechanisms that is optimized to fit requirements of each application or blockchain kind; examples range from *IoT (Internet of Things)* blockchains for sustainability applications that often use variants of *BFT (Byzantine Fault Tolerance)* algorithm, and consensus needed to relay transactions and/or assets between different blockchains in interoperability solutions. This paper tries to gather and organize all existing consensus protocols in the blockchain world with a focus on cryptocurrencies and interoperability solutions. We summarize the main consensus protocols with their academically recognized variants and collect other variants from white papers. We point out to existing surveys and systematic review papers, fill the gaps, and add the new; the aim is to introduce a comprehensive overview of the topic, along with the links to go deeper into every detail.
Keywords: Blockchains, consensus, BFT, POW, POS.

1 Introduction

Blockchains inherit the ***Byzantine Generals Problem*** from distributed information systems that is usually addressed using ***state machine replication*** approach; when a distributed information system replicates its servers to tolerate malfunctioning or malicious servers (referred to as *Byzantine*), it is supposed to answer enquiries and execute concurrent update requests to its replicated servers in a ***consistent*** and ***live*** manner [1,2]. That's quite similar to when block proposers each constructs a block with all needed certificates and references to previously delivered blocks and then compete to append their constructed block into the blockchain; choosing a certain block may change the Blockchain status in a way that render other competing blocks invalid.

The mechanism and criteria on which a block is selected from all proposed competing blocks is called the ***consensus protocol***. Typically, a consensus protocol involves a ***fair*** selection criterion between valid blocks (heaviest computation for POW and probabilistic stakes ratio for POS); also, a reliable message exchange

protocol[1] to negotiate the selection between participating nodes where a malicious node may broadcast a wrong message or not broadcast at all hoping to cause a DoS attack; finally, the usual *lock-commit* paradigm known in distributed databases [3] maybe mapped to forks handling strategies in single blockchains, but it **is** part of cross-chain consensus protocols when things get more complicated [4].

One may view blockchains as an asynchronous environment since there is no unified system clock, where deterministic consensus is impossible in the asynchronous setting[2]. Fortunately, blockchains are described as ***alpha synchronous*** (synchronization is achieved within time alpha) [5], since all Blockchains and their applications define a *finality time* after which most nodes have received (confirmed) the final block. The family of ***Byzantine Fault Tolerance (BFT)***, from 1999 [6], style protocols operate in *rounds* in this ***partially synchronous model*** , by *electing a round leader* to start the broadcast, and can tolerate (*guaranteed to terminate achieving a consensus*) within a maximum threshold of ***33%*** malicious or faulty (so called *Byzantine*) nodes; *Tendermint* [7] as depicted in Fig.1 is a classical blockchain era example, while *Honeybadger* [8] and [1] are consensus protocols that could work in an asynchronous setting. Seeking more efficiency (faster block production rate) than offered by Tendermint like protocols, blockchains deploy the ***finality gadget***[3] [9,10] concept where block production is decoupled from voting; i.e., nodes do not wait for the voting results, they just keep producing blocks over the last finalized (voted upon) block according to some chain selection rules between possibly resulting forks.

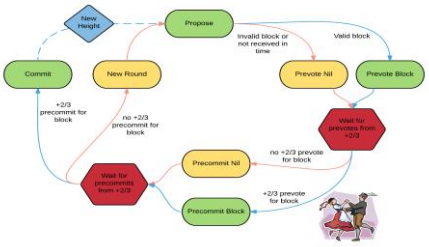

Fig1. The Tendermint protocol rounds (taken from [7])

[1] Although beyond the scope of this paper, the interested reader may find new research on theoretical bounds for *message exchange complexity*, and different *validity definitions* on https://arxiv.org/abs/2301.04920 (last version June 2023).

[2] M. J. **F**ischer, N. A. **L**ynch, and M. S. **P**aterson, Journal of the ACM, 1985, https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf; ***GRANDPA, G****host-based* ***R****ecursive* ***AN****cestor* ***D****eriving* ***P****refix* ***A****greement*, paper [10] proved in 2020 that the ***FLP*** impossibility result remains valid (still impossible) even with finality gadgets.

[3] Although the term *"finality gadget"* first appeared in the Casper FFG paper [9] 2017, one could view the 6 blocks escrow time for block confirmation in Bitcoin as the same idea; i.e., nodes just keep producing blocks and choose the heaviest chain when there are forks, GRANDPA in [10] elaborates more on the theoretical bases.

The dynamically varying, possibly large[4], number of participating nodes makes the consensus problem more complicated in blockchains [11, 5/lec9] since the committee that should agree upon a block is not predefined[5]; we cannot possibly guarantee a threshold ratio for Byzantine nodes if nodes can freely go on and off at any time (so called the ***Dynamically Available*** (***DA)*** setting). Therefore, either a new innovation is deployed, like *POW longest chain* consensus, or a strategic selection phase is first applied to select a committee (group) and then a proprietary *BFT* protocol is applied to the fixed size committee (we can roughly call the committee for now as working in the ***Quasi Permissionless***[6] (***QP***) settings); examples include the Helium blockchain [12] consensus protocol where nodes compete in submitting *Proof of Coverage* (internet coverage) [13] to select a group then a *Honeybadger BFT* variant is applied[7], and the use of the Tendermint protocol in Cosmos and Terra ecosystems [7].

Other challenges [14] in the blockchain environment consensus include, but not limited to, *time* and/or *bandwidth* especially with interoperability and cross chain applications when there are more than one blockchain involved [section2 in 15,16,17], the number of *compromised (Byzantine) nodes* the network could tolerate, and the degree of *fairness* and *decentralization* [18] in the committee selection. Hence, there are endless variants of consensus mechanisms out there, and the literature holds continuous innovations [19,20], general [21,22,23] and application specific [24,25] surveys and comparative studies [26]; the literature also holds theoretical contributions [27,28,29] and textbook style material [5,7,30].

In this paper we try to present a consolidated view of the complete picture, naturally focusing on only some of its details, and at the same time guiding the reader to all available material we have encountered. Section 2 summarizes most important consensus criteria used in different blockchain applications, while section 3 discusses design issues along with some examples of consensus in interoperability solutions; finally, section4 concludes the paper.

---

[4] Ironically, the small number of participating relay nodes in cross chain bridges and interoperability solutions is sometimes a problem (); we will elaborate more on this later on the paper.

[5] For a compact brief see (htttps://youtu.be/uWyJhNbJMn8)

[6] Theoretically, some protocols like *PosT* assume such settings (arXiv:2405.09173v1); practically, *Ethereum POS* imposes a penalty on committee members that go offline by slashing part of their stake (***inactivity leak***: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/, https://eth2book.info/capella/part2/incentives/inactivity/, and [9])

[7] This may have changed since the migration with Solana and hotspots stopped mining *HNT* tokens (switched to *IOT* tokens) and became NFTs on Solana (https://docs.helium.com/solana/migration/hotspot-operator/)

2 Main Types of Consensus Protocols Used in Blockchains

In this section we will try to cover the main consensus mechanisms in chronological order of their appearance along with their subvariants. Previous efforts include peer reviewed papers like [14,21,22,23], and an encyclopedia site [31].

1. ***Byzantine Fault Tolerant (BFT)***
   The traditional *BFT* [6], or a variant of it, remains suitable for private permissioned and consortium blockchains. For example, Estonia governmental *KSI* blockchain uses a proprietary *BFT* protocol [32,33]; also, ***Federated BFT*** [34] is used in payment-protocol-based blockchain platforms such as *Stellar*[8]; the default choice for sustainability applications blockchains is usually ***Practical BFT (PBFT)*** and could then be compared with other options [35]. In addition, as mentioned above, *BFT* style protocols are usually the second phase after committee selection in many blockchain applications, with ***Tendermint*** [7] being the most celebrated example.

2. ***POW***
   The basic idea originated in the 90's as a protection from spam and DoS attacks by performing some non-trivial amount of computation that outweighs the expected attack revenue; POW failed in spam email protection [36] but became a breakthrough in cryptocurrency consensus since Bitcoin 2008 [37] as the heavy computation can prevent (with overwhelming probability[9]) different attacks (double spending, selfish mining, sybil attacks)[10] unless attackers possess 50% of all existing computational power. Basically, miners compete to solve a cryptographic puzzle with a predefined difficulty level, combine it with their proposed block and try to append it to the chain; from the different possible future chains (new system state) nodes elect the longest chain (more accurately, the one with the heaviest computation) and the choice is considered finalized, escrow time, after 6 blocks. Despite all its merits, the high energy consumption along with its carbon footprint remains a significant argument against POW; attempts to

[8] Some material on the internet includes *Ripple* too as a federated BFT example, however (https://www.mdpi.com/1999-5903/12/3/53) explains in detail that only *Stellar*, which forked from *Ripple*, does and thus have the (<n/3) byzantine nodes threshold while Ripple consensus (RPCA) can tolerate only (<n/5).

[9] POW only provides *probabilistic finality*, while POS has *provable finality*.

[10] ***Double spending*** is trying to spend the same coins more than once, ***selfish mining*** is trying to mine several blocks secretly to produce a fork with a longer chain than the existing one (thus invalidates all TXs and mining rewards after the fork), and ***Sybil attack*** is for a single attacker to create a vision of multiple nodes creating a false majority (since it is a permissionless anonymous setting, nothing prevents from splitting your hash power into several addresses); however, the POW mechanism protects from all such attacks unless the attacker controls at least 50% of all available hash power worldwide.

decrease it by performing the computation only on certain key blocks include *Bitcoin-NG* [38].

3. ***Proof of Space/Capacity***
   In 2013, [39] suggested to dedicate a significant amount of memory or disk space as a greener alternative to POW computation. First crypto applications of proof of Storage include, [40], *Signum* (2014) and *Spacemint* (2015), while *Chia* (2018) deploys a variant called ***Proof of SpaceTime*** which necessitates reserving the storage for an amount of time[11]. Naturally, a variant of the latter is most suitable for distributed storage systems like ***Filecoin***[12] which has a 2-phase protocol (*Expected Consensus EC* [41]); a probabilistic Byzantine fault-tolerant consensus protocol runs a leader election among a set of storage providers to submit a block every time epoch, where the likelihood of being elected depends on how much provable storage a miner contributes to the network.

4. ***Proof of Activity***
   First suggested in 2014 paper with *Litecoin* Creator, Charlie Lee, as one of its authors and could be viewed as an improvement over POW. Miners solve an easier puzzle for empty blocks, then a set of validators from coin holders (an early variant of POS) verify the transactions part of the block and reward is split between miners and validators [42]; such an arrangement also harden the 51% hash power attack in POW to necessitate 51% malicious validators (coins holders) in addition. Proof of Activity is used in *Decred* and *Espers*[13]; a different variant that shares the same name, but targets incentivizing participation, appeared recently in *Fastex* [43] uses a smart contract deployed by validators to evaluate a user's activity level before granting the chance of being a validator or a block producer. *Proof of Contribution* introduced in 2021, [44], is a similar idea.

5. ***Proof of Burn (POB)***
   Instead of spending the money on energy consumption and mining devices, just remove it from circulation and increase coin scarcity (and hence its price) instead of increasing carbon emissions. The idea so called "burning" coins appeared in 2019 [45], and is used in *Slimcoin*[14]; infact, burning crypto got more popularity in burning tokens of different exchange tokens [46],

[11] Check appendix A, page 68, in [28] for a more theoretical enlightenment.

[12] Wikipedia includes *arweave* too (a distributed storage that follows a structure called *blockweave* similar to blockchains but not one); however, we have found that *arweave* used *Proof of Access* for some time (https://www.reddit.com/r/a:t5_67b622/comments/u37ldb/arweave_consensus_protocol_poa/) and seems to switched to another protocol inspired by *Perma coin* 7 months ago as shown in (https://github.com/ArweaveTeam/arweave-standards/blob/master/ans/ANS-103.md)

[13] https://decred.org, https://espers.io

[14] https://slimcoin.info

cross chain asset transfer, and of course burning ratio of the fees like in the *Near* protocol and Ethereum *EIP-1559*. Also, a recent 2024 paper [47] suggests upgrading cryptocurrencies with new tokens using *POB* via multi-currency auction.

6. Proof of Elapsed Time (PoAT)

Was originally developed by Intel engineers and contributed to *Hyperledger Sawtooth* [48] to replace the POW heavy computation by generating a random waiting time using a *trusted execution environment (TEE)* and select the least waiting time as the leader; ***Proof of Luck (PoL)*** [49] on the other hand chooses the one with highest random number as the leader. In 2017, [50] studied *PoET* under a theoretical framework and found that it can be attacked by θ(log log n/log n) fraction of the nodes[15], then [51] introduced a more practical simplified version (***ET***) of both *PoET* and *PoL* in 2021. *PoET*'s GitHub is now archived, and a following experimental *PoET2* was also archived [52]; *PoL* may capture the attention [53] from time to time since its first appearance 2016, but we also have not encountered any real implementation. However, the idea of leader selection based on randomly generated numbers, *Verifiable Delay Functions* and *Verifiable Random functions VRF*, is deployed in the consensus mechanisms of a number of layer-1 blockchains [54] including *Algorand*, *Cardano*, *Internet Computer*, and *Polkadot* to randomly select block producers; only those generate their random numbers in software code and are considered *POS* variants.

7. Proof of Stake (POS)

Although, *Peercoin* [55] claims to be the pioneer cryptocurrency using POS in 2012, the massive use of POS and its many variants started in 2017. The basic idea is that block selection is done probabilistically according to staked tokens; such an arrangement is more efficient (higher TX throughput) and consumes less energy, and also has introduced the possibility of ***slashing*** bad behavior (since stakes are registered, the evaluation smart contract mentioned in [43] proof of activity is possible). However, POS attacks are wider leading to more complicated and varying designs that can only tolerate only **27.8%**[16] malicious nodes in some cases [56]; a recent paper [57] proved that recovery through slashing at least *1/3* of the consistency violation stake can be possible with up to **5/9** Byzantine nodes in the *Quasi-Permissionless* settings (honest nodes cannot go offline), among other results[17]. Another example threat to start with is predicting the randomization process in selecting the block builder and a possible solution is to use *VRF*s as just mentioned above [54]. ***Nothing at stake*** attacks are named so because,

[15] That's less than 1/3 the nodes for n>10; i.e., worse than *BFT*

[16] Driven from "e" value (e=2.78)

[17] For example in their *PosT* protocol prevents consistency violation completely with <1/3 Byzantine nodes, as opposed to Hotstuff protocol that we will mention later where consistency violation are handled (but can happen) within this ratio.

unlike selfish mining in POW, forking and creating an alternative longer chain at any desired block in history costs nothing but simulating the randomization selection process. If *slashing* is the only defense, ***Long range attacks*** may wait enough to build a reputation and maybe withdraw their staked tokens before revealing the attack, some versions may even steal pretty old withdrawn keys with high credibility [58]; Cardano *Ouroboros*[18] protocol [59] use a *warm up epoch* and a *withdrawal epoch* where tokens remain locked without their owner being a candidate for selection; Ethereum *Casper FFG* [9] on the other hand assumes in addition that nodes will "log on" and gain a complete up-to-date view of the chain at some regular frequency ~ 1-2 months (*out-of-bound communication time* as called by [57] is roughly proportional to *cooldown*, withdrawal, delay), and then never revert a finalized block given so; finally, see videos 21&22 in [56] for details on how *VDF*s can be used to defend such attacks. Some criticize POS as more centralized and less democratized, since selection according to stakes could be viewed as "*making the rich richer*", we believe that hash power or mining devices in *POW*, space in *PoSpace*, internet coverage in *PoCoverage*,...etc. also costs money so it is nearly the same; however, some like *Axeler* [60] avoid vote monopoly by using a *quadratic voting* mechanism to slow down (by the square root) the growth of a validator voting power with the increase of his stake. Finally, POS has many variants that contains almost all what follows, ***Multi Token POS (MPOS***) [61] could be viewed as the multi-chain version; in nearly all versions, there is a group (committee) selection phase then there is a leader selection phase (not necessarily *BFT* style, although the most common[19]) among the group members.

8. Delegated Proof of Stake (DPOS)

In *DPOS* stake tokens are not physically transferred to another wallet, but instead are utilized through a staking service provider in a staking pool [62]. Most sites refer to Cardano *Ouroboros* protocol [59] as a *DPOS* example, also Aptos [63], and TRON [64]; EOS [65] consensus protocol, *EOSIO*, involves a *DPoS* phase to elect the active producers who will be authorized to sign valid blocks in the network, then the actual process of confirming each block until it becomes final (irreversible) is performed in an *asynchronous BFT* manner. Introducing staking pools in *DPOS*, like mining pools in POW, make things easier and increases the number of *Transaction Per Second (TPS)* compared to *POS*; could be viewed by some as allowing participation with less than the minimum stake, and by others as

[18] We will see in next section more variants of ouroboros deployed in interoperability solutions.

[19] Ethereum L2 for example combines longest chain voting LMD-Ghost with a PBFT protocol named Casper to achieve liveness and consistency.

concentrating power into staking service providers[20]. The authors in [66] suggest what they describe as a tweak to *DPOS*, ***Preferential delegated proof of stake (PDPoS),*** where block creators have to stake more tokens in order to validate or assemble TXs sent directly to mainnet, while TXs sent to L2 costs less to users, rewards less to block creators, and maybe delayed to 24hrs; an arrangement that seems like a city for the rich and a city for the poor is claimed to give much higher TPS. It's also worth mentioning that we found an 2024 paper [67] that deploys *DPOS* in an intelligent task scheduling system using blockchains.

9. Proof of Authority (PoAu)

Suggested by Ethereum founder Gavin in 2017 [68], a variant of POS, where [68,69,70] instead of choosing block miners based on their stakes in cryptocurrency tokens, a small group of authorities are selected as transaction validators by their identity or reputation[21] staked in the network. When it started, *Ronin* [71] used Proof of Authority consensus between limited validators to relay *Axie Infinity players* TXs through *Ronin-chains*; now it first selects a set of validators using *DPOS*, then validators take turns producing blocks in *PoAu* manner.

10. AI-Based Consensus

Instead of wasting computation and energy in solving puzzles, computation is used to achieve something useful like training neural networks or machine learning tasks; the first appearance of the idea we encountered was in 2018 [72] and 2019 [73], follow up variants include [20,74,75].

11. Application Specific Kinds

The literature, and the market, both hold enormous number of application optimized consensus innovations; we have mentioned Helium *Proof of internet Coverage* [12], this paper [76] defines *Proof of Absence* for its IoT blockchain system consisting of 10 devices at maximum, the survey in [14] mentions *Proof of Movement* used in healthcare blockchain systems, and there will always be a lot more. Also, Hyperledger Fabric as an example provides a variety of consensus protocols like Kafka [77], Raft [78], and PBFT, and allows for the integration of any desired consensus (the pluggable consensus feature) to extend its interoperability features [79,80]. Finally, it is worth mentioning that Wikipedia contains an "AI-generated" consensus protocol, [81], *Proof of Identity*.

12. DAG Consensus Protocols

---

[20] According to [66], EOS has only 21 validators and TRON has 27; also, staking pools in Ethereum (like *Lido*) allow participation with less than 32 ETH, and at the same time holds % of total stakes.

[21] The theme is similar whether it is called Proof of *Reputation/Activity/Authority*, it is some form of evaluation function coded in a smart contract.

This innovation [82] comes to replace the second phase, after choosing the set of validators in *POS* style protocols; instead of electing a round leader [5,6,7] to start the broadcast in traditional BFT variants, a *Directed Acyclic Graph (DAG)* is constructed to reflect the data dependency between Transactions (to guarantee *safety*) then all validators start to build and broadcast blocks in parallel to speed up the process. Round after round a *safe* total ordering is achieved (on a number of blocks instead of just one, and while still keeping the 33% byzantine threshold) either by excluding *equivocating* (contradicting) blocks or preventing their construction from the beginning [83,84]. DAG-based consensus protocols include DAG-Rider and Bullshark, and are currently deployed by many blockchain companies like Aptos [85] and Chainlink [86]; Aptos introduced the *Proof of Availability* idea in *Narwhal* where only meta data about the transactions are broadcasted till a consensus is reached to save bandwidth, while Chainlink removed the voting phase using lock before finalize (recall [3]) *BBCA* broadcast. Finally, as it might cross one's mind, on whether *DAG*-based total ordering schemes affect *MEV* (*Miner Extracted Value*), the Aptos lab discussed it [87] in light of their original paper [85], while chainlink also introduced their DAG-based protocol called *Fino* [88] that integrates MEV-resistance features into DAG-based BFT, before [86]

3 Consensus Across Chains in Interoperability Solutions

Reaching consensus in a multi-chain environment is much more complicated; for a start, safety involves more than one ledger like the simple combined (train-hotel) and (plane-hotel) reservation example in [4]; then selecting validators set or relay nodes is more complicated and involves more threats as depicted by the long history of cross chain attacks in their short lifetime [89].

3.1 Interoperability solutions classification

Most of the literature follow classifications presented in [90] that first divides them into ***heterogeneous*** solutions between different kinds of blockchains with Hyperledger as the most dominating example and we have just mentioned [77-80] how it offers flexibility by supporting pluggable consensus protocols in addition to *Raft* and *Kafka*. Then, there are ***Blockchain of Blockchains (BOB)*** solutions that provide a Cross Chain Communication extra layer blockchain to handle transactions between EVM like blockchains; famous contributors to the consensus literature like Chainlink [54,84,86], COSMOS [7], Polkadot [91], and Horizen [92] fall in this category, where innovations may include efficiency improvements like *DAG-BFT* approaches, and are most concentrated in choosing the validators committee in ways that provide enough rewarding incentives [71,93] and guarantee decentralization [54] and attack defense [60]. The last category, ***public connectors*** that include all notary systems like side chains and bridges have the same challenges of key leakage and

possible collusion more magnified since they can only provide smaller number of validators [94,15]. The authors in [95] examine in detail the security of many interoperability solutions including some that deploy POW instead of BFT consensus and some that use ***distributed private key control***; we have also mentioned *POB* interoperability solutions in [47], Metaverse specialized solutions in [16], and Axe-infinity game in Ronin [71].

3.2 Case Studies

We will go through some case examples in this subsection; the reader interested in more may check the consensus mechanism of interoperability solutions listed in [90,95,15].

- ***Polkadot***
  For a start Polkadot [91] uses *Nominated POS*, *NPOS*, where stakers can vote to nominate validators who are willing to dedicate the time and resources to run a validator node. Then a hybrid consensus (2 protocols) is applied to split block production protocol, BABE, from handling forks and guaranteeing finality protocol, GRANDPA. *Blind Assignment for Blockchain Extension (BABE)* is comparable to a recent *ouroboros* variant than Latus called *Praos* [96]; epochs are divided to slots (~6 secs) and validators are assigned to slots via a Lottery algorithm based on VRF[22], if more than one validator are selected to one slot they race to finish the block and if no validator is selected a backup round-robin validator selection is used[23]. *GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement)*, [10], where *GHOST* stands for *Greedy Heaviest Observed Subtree*, is run by validator nodes in parallel to reach provable finality through consecutive rounds of validators voting (on chains instead of single blocks); so *BABE* builds on the chain finalized by *GRANDPA* and if there are forks afterwards, it favors the chain with more primary blocks (generated thru VRF selection not round-robin). Finally, Polkadot supports a bridge, *BEEFY* (*Bridge Efficiency Enabling Finality Yielder*), to remote, segregated blockchains like Ethereum; *BEEFY* operates on top of *GRANDPA*, utilizing a consensus extension and a light client protocol[24].

- ***Bool Network***

[22] Note that each validator has an equal chance in this slots lottery; i.e. randomization is not based on stakes as in Cosmos [91/Polkadot comparisons] and many other POS variants.

[23] The videos in [56] points out that random number generation in POS systems will naturally lead to such cases and discusses different alternatives.

[24] BEEFY uses *Merkle Mountain Ranges (MMR)* as an efficient data structure for storing and transmitting block headers and signatures, which is almost the same Utreexo forest data structure introduced in Bitcoin as a stateless server providing worst case O(log n) Merkle proofs to stateless clients.

The original paper in 2022 [97] proposed a relay chain scheme that is based on secure multi-party computation and distributed private key management over an evolving hidden committee; the committee is elected using a *Ring verifiable random function (Ring VRF) protocol*, where the real public key of a VRF instance can be hidden among a ring. Furthermore, all the *key management procedures are executed in the TEE*, such as Intel SGX, to ensure the privacy and integrity of partial key components; although identities are hidden, committee members who behave maliciously can be detected and disqualified, and the cost of launching DoS or double-spending attacks is high. The (https://Bool.network/) site promotes itself as *a Bitcoin verification layer that turns all blockchains into Bitcoin layer 2*.

- ***Subsidy Bridge***

  A general and decentralized relay scheme with special incentive design similar to Bitcoin mining. The main idea, [98], is to keep utility of honest relayers (basic subsidy from target chain + transaction fee from cross-chain users) always positive even when users are temporarily inactive; it's worth mentioning that the designers of Latus [93] too, although a POS variant, emphasize that it is very important for the consensus security to continue issuing blocks, even if empty to keep the rewarding incentive. The authors calculated the Nash equilibrium conditions of the *subsidy bridge* game, and proved security under honest majority of relay developers with at least one honest relayer from the source chain; they also claim their design is flexible to support any source chain of any secure consensus, so can support Bitcoin efficiently in contrast with Polkadot and Cosmos and still support other blockchains if compared to BTC-Relay.

- ***Deterministic Cross-Blockchain Token Transfer (DEXTT)***

  All observer candidates use their private keys to sign the cross-chain transactions as soon as they discover it, *the observer the minimum signature value* [99] is considered the contest winner and thus broadcast the transaction and wins the witness reward; *VETO transactions* reporting double spending and penalizing bad behavior are subject to the same contest with a reward incentive. Finally, in their evaluation implementation the authors used three geth nodes in *Proof of Authority (PoA)* mode, creating three private blockchains, to ensure a reproducible and uniform ecosystem of blockchains.

- ***Practical AgentChain***

  Agentchain appeared in 2019 [100] and could be viewed as a *Proof of Reputation* consensus side chain that uses multi-signature schemes; trading operators can be combined as several decentralized trading groups by locking tokens to ensure credibility. Users choose a "*reputable*" trading group and deposit assets to the trading group's multi-signature address on the existing blockchain. Then the assets will be mapped to *AgentChain* by the

trading group, on which token fair exchange is supported. However, the design was in the conceptual stage with poor implementation; a follow-up paper introduced *Practical AgentChain* [101] in 2022 that introduced a complete system with more functionalities.

- ***Identity-Based Encryption (IBE-BCIOT)***
  Proposed electing proxy nodes according to a clustering algorithm based on density peaks [102]; aiming to elect nodes with efficient computing power, the algorithm assumes that if the cluster centers are surrounded by neighbor nodes with lower local density and the distance between any nodes is relatively large, then the clustering center will be defined as the local maximum of the data point density. Then, the elected proxy nodes are authenticated through a trusted cross-chain notary deploying an *Identity Based Encryption* (*IBE)* algorithm; this shares some resemblance with the AI generated *Proof of Identity* in [81]. Finally, selected nodes reach consensus using *PBFT*.

4 Conclusions & Future Work

We introduced in this systemization of knowledge paper a compact consolidation on blockchains consensus protocols trying to cover all aspects and point out to all significant work in the literature. The paper also shed some extra light on consensus schemes used in interoperability solutions. We hope this paper can be a starting point that provides the necessary reading material for researchers and developers, with enough guidance to go deeper.

References

1. https://decentralizedthoughts.github.io/2019-10-15-consensus-for-state-machine-replication/; last accessed 13/4/2024.
2. Sisi Duan et al., "*BEAT: Asynchronous BFT Made Practical*", ACM 2018, doi:10.1145/3243734.3243812, https://youtu.be/u0nypF5AIF4
3. https://decentralizedthoughts.github.io/2020-11-29-the-lock-commit-paradigm/; last accessed 13/4/2024.
4. https://anoma.net/blog/heterogeneous-paxos-and-multi-chain-atomic-commits; last accessed 12/10/2023.
5. Tim Roughgarden, "*Foundations of Blockchains*", lecture notes, Columbia University, 2021, https://github.com/timroughgarden/fob21/blob/main/l/l2-7-overview.pdf, https://timroughgarden.github.io/fob21/; last accessed 11/4/2024.
6. Miguel Castro and Barbara Liskov, "Practical Byzantine Fault Tolerance", In Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999, https://pmg.csail.mit.edu/papers/osdi99.pdf
7. https://cosmos-network.gitbooks.io/cosmos-academy/content/introduction-to-the-cosmos-ecosystem/tendermint-bft-consensus-algorithm.html; last accessed 12/4/2024.

8. Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song, "*The Honey Badger of BFT Protocols*", 2016, https://youtu.be/Qone4j1hCt8
9. V. Buterin and V. Griffith, "*Casper the Friendly Finality Gadget*", 2017, https://arxiv.org/abs/1710.09437
10. A. Stewart and E. Kokoris-Kogia, ***"A Byzantine Finality Gadget, GRANDPA, Ghost-based Recursive ANcestor Deriving Prefix Agreement***, 19 June 2020, https://github.com/w3f/consensus/blob/master/pdf/grandpa.pdf
11. J. Wu et al., "*SEGBFT: A Scalable Consensus Protocol for Consortium Blockchain*", ICBCT'22: The 2022 4th International Conference on Blockchain Technology, March 2022, Pages 15–2, https://doi.org/10.1145/3532640.3532643, https://dl.acm.org/doi/abs/10.1145/3532640.3532643
12. The Helium blockchain and its whitepaper, https://status.helium.com/; last accessed 11/4/2024.
13. https://www.telefonica.com/en/communication-room/blog/wi-fi-and-mobile-to-improve-coverage-enable-mobile-data-traffic-offloading/; last accessed 11/4/2024.
14. Y. Merrad, M. H. Habaebi, E. A. A. Elsheikh, F. E. M. Suliman, M. R. Islam, T. S. Gunawan, and M. Mesri, ''*Blockchain: Consensus algorithm key performance indicators, trade-offs, current trends, common drawbacks, and novel solution proposals*'', Mathematics, vol. 10, no. 15, p. 2754, Aug. 2022.
15. https://medium.com/@shymaa.arafat/blockchain-interoperability-part1-9d2e29da691b; last accessed 15/4/2024.
16. https://www.researchgate.net/publication/343730274_A_New_Consensus_Protocol_for_Blockchain_Interoperability_Architecture
17. Tianxiu Xie et al., "*RAC-Chain: An Asynchronous Consensus-based Cross-chain Approach to Scalable Blockchain for Metaverse*", Mar 2024, https://dl.acm.org/doi/10.1145/3586011
18. https://www.semanticscholar.org/paper/A-Truly-Decentralized-Blockchain-Consensus-Protocol-Wimal-Liyanage/200b1c126b3cccf88a92c6c4ed2d7139148dba40
19. Gai K, Hu Z, Zhu L, Wang R, Zhang Z, "*Blockchain meets DAG: a BlockDAG consensus mechanism*", In: Algorithms and architectures for parallel processing: 20th international conference, ICA3PP 2020, New York City, NY, USA, October 2–4, 2020, Proceedings, Part III, vol 20. Springer, pp 110–125, https://dl.acm.org/doi/abs/10.1007/978-3-030-60248-2_8
20. Mahmoud, H. H. M., Wu, W., and Wang, Y., "*Proof of Learning: Two Novel Consensus Mechanisms for Data Validation using Blockchain Technology in Water Distribution System*" in 27th International Conference on Automation and Computing (ICAC) (IEEE), University of the West of England, Bristol, UK, 1-3 September 2022.
21. S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, ''*A research survey on applications of consensus protocols in blockchain*'', Secur. Commun. Netw., vol. 2021, pp. 1–22, Jan. 2021.
22. Z. Hussein et al., "*Evolution of Blockchain Consensus Algorithms: a Review on the Latest Milestones of Blockchain Consensus Algorithms*", Cybersecurity 6, 30 (2023), https://doi.org/10.1186/s42400-023-00163-y
23. Yang Xiao, Ning Zhang, Wenjing Lou, and Y. Thomas Hou, "*A Survey of Distributed Consensus Protocols for Blockchain Networks*", IEEE Comm. Surveys & Tutorials, Vol. 22 Issue 2, 2020, https://ieeexplore.ieee.org/abstract/document/8972381/
24. "*Blockchain consensus mechanisms and their applications in IoT: A literature survey*", in Proc. Int. Conf. Algorithms Archit. Parallel Process. Cham, Switzerland: Springer, 2020,

pp. 564–579, https://slogix.in/blockchain-technology/blockchain-consensus-mechanisms-and-their-applications-in-iot-a-literature-survey/
25. M. Salimitari, M. Chatterjee, and Y. P. Fallah, "*A survey on consensus methods in blockchain for resource-constrained IoT networks*", Internet of Things, vol. 11, 2020; https://www.sciencedirect.com/science/article/abs/pii/S2542660520300482
26. A. Menon, T. Saranya, S. Sureshbabu, and A. Mahesh, ''*A comparative analysis on three consensus algorithms: Proof of burn, proof of elapsed time, proof of authority*'', in Computer Networks and Inventive Communication Technologies. Singapore: Springer, Jan. 2022, pp. 369–383.
27. Andrew Lewis-Pye and Tim Roughgarden, "*Byzantine Generals in the Permissionless Setting*", Jan 2023, https://arxiv.org/pdf/2101.07095.pdf
28. Andrew Lewis-Pye and Tim Roughgarden, "*Permissionless Consensus*", Nov 2023, https://arxiv.org/pdf/2304.14701v4.pdf
29. L. Nuzzi, K. Waters, and M. Andrade, "*Breaking BFT: Quantifying the Cost to Attack Bitcoin and Ethereum*", Mar 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4727999
30. Elaine Shi, "*Foundations of Distributed Consensus and Blockchains*", http://elaineshi.com/docs/blockchain-book.pdf
31. https://tokens-economy.gitbook.io/consensus/blockchain-consensus-encyclopedia-infographic; last accessed 12/4/2024.
32. "*Blockchains for Governmental Services: Design Principles, Applications, and Case Studies*", Dec 2017, https://www.ctga.ox.ac.uk/201712-CTGA-Martinovic-I-Kello-L-blockchainsforgovernmentalservices.pdf; last downloaded 9/4/2024.
33. https://www.reddit.com/r/Eesti/comments/olzmk5/can_someone_explain_how_the_estonian_government/; last accessed 9/4/2024.
34. https://tokens-economy.gitbook.io/consensus/chain-based-pbft-and-bft-based-proof-of-stake/federated-byzantine-agreement; last accessed 15/4/2024.
35. Y. Liu and C. Shang, "*Application of Blockchain Technology in Agricultural Water Rights Trade Management*", Sustainability 2022, 14(12), 7017; https://doi.org/10.3390/su14127017; https://www.mdpi.com/2071-1050/14/12/7017
36. Dwork, C., Naor, M. (1993), "*Pricing via Processing or Combatting Junk Mail*", In: Brickell, E.F. (eds) Advances in Cryptology — CRYPTO' 92. CRYPTO 1992. Lecture Notes in Computer Science, vol 740. Springer, Berlin, Heidelberg, https://link.springer.com/chapter/10.1007/3-540-48071-4_10
37. Satoshi Nakamoto, 2008, "*Bitcoin: a Peer-To-Peer Electronic Cash System*"; https://bitcoin.org/bitcoin.pdf
38. Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse, "*Bitcoin-ng: A scalable blockchain protocol*", In 13th USENIX symposium on networked systems design and implementation, NSDI'16, 45–59
39. Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak, "*Proofs of Space*", 2013, https://eprint.iacr.org/2013/796.pdf
40. https://en.wikipedia.org/wiki/Proof_of_space; last accessed 10/4/2024.
41. https://docs.filecoin.io/basics/what-is-filecoin/blockchain; last accessed 10/4/2024.
42. https://www.coinbureau.com/blockchain/proof-of-activity-explained-hybrid-consensus-algorithm/; last accessed in 9/4/2024.
43. https://cointelegraph.com/news/proof-of-stake-and-activity-posa-a-consensus-mechanism-for-the-new-era-in-web3; last accessed in 9/4/2024.
44. Hongyu Song, Nafei Zhu, Ruixin Xue, Jingsha He, Kun Zhang, and Jianyu Wang, "*Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual*

property protection", Information Processing & Management, Volume 58, Issue 3, May 2021, 102507, https://www.sciencedirect.com/science/article/abs/pii/S0306457321000170
45. Kostis Karantias, Aggelos Kiayias, and Dionysis Zindros, "*Proof of Burn*", September/2019, Financial Cryptography, https://doi.org/10.1007/978-3-030-51280-4_28, https://eprint.iacr.org/2019/1096.pdf
46. https://21shares.com/research/tokens-burns; last accessed 12/4/2024.
47. M. Rodinko et al, "*Decentralized Proof-of-Burn Auction for Secure Cryptocurrency Upgrade*", Vol. 5, Issue 1, March 2024, 100170, https://www.sciencedirect.com/science/article/pii/S2096720923000453
48. https://github.com/hyperledger-archives/sawtooth-poet; last accessed 9/4/2024.
49. https://mitar.tnode.com/post/proof-of-luck-consensus-protocol-and-luckychain/; last accessed 8/4/2024.
50. https://www.researchgate.net/publication/320246838_On_Security_Analysis_of_Proof-of-Elapsed-Time_PoET
51. Mic Bowman, Debajyoti Das, Avradip Mandal, and Hart Montgomery, "*On Elapsed Time Consensus Protocols*", 2021, https://eprint.iacr.org/2021/086
52. https://labs.hyperledger.org/labs/archived/sawtooth-poet2.html; last accessed 8/4/2024.
53. https://medium.com/@saimmoin64/exploring-the-pros-and-cons-of-proof-of-luck-pol-consensus-mechanism-in-blockchain-2cef9ada98c1; last accessed 8/4/2024.
54. https://chain.link/education-hub/verifiable-random-function-vrf; last accessed 9/4/2024.
55. *"Peercoin The Pioneer POS",* Whitepaper, 2012, https://www.peercoin.net/read/papers/peercoin-paper.pdf; last downloaded 7/4/2024.
56. Tim Roughgarden, "Lecture 12: *Proof of Stake*", 24 videos, Jun 2023, https://youtu.be/ZSqxGdsmLHs; last accessed 13/4/2024.
57. Eric Budish, Andrew Lewis-Pye, and Tim Roughgarden, "*The Economic Limits of Permissionless Consensus"*, May 2024, arXiv:2405.09173v1
58. https://ghoststaking.com/nothing-at-stake-long-range-attacks/; last accessed 13/4/2024.
59. Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov, "*Ouroboros: A provably secure proof-of-stake blockchain protocol*", CRYPTO 2017, Part I, volume 10401of LNCS, pages 357–388. Springer, Heidelberg, 2017.
60. https://docs.axelar.dev/learn/security; last accessed 14/4/2024.
61. https://www.researchgate.net/publication/343730274_A_New_Consensus_Protocol_for_Blockchain_Interoperability_Architecture
62. https://www.gemini.com/cryptopedia/proof-of-stake-delegated-pos-dpos; last accessed 7/4/2024.
63. https://aptos.dev/concepts/delegated-staking/; last accessed 7/4/2024.
64. https://developers.tron.network/docs/concensus; last accessed 7/4/2024.
65. https://developers.eos.io/welcome/v2.2/protocol-guides/consensus_protocol; last accessed 7/4/2024.
66. V. Bachani, and A. Bhattacharjya, "*Preferential delegated proof of stake (PDPoS)-modified DPoS with two layers towards scalability and higher TPS*", 2022, Symmetry 15(1):4, https://www.mdpi.com/2073-8994/15/1/4
67. O. Younis etc al., "*A Proposal for a Tokenized Intelligent System: A Prediction for an AI-Based Scheduling, Secured Using Blockchain*", March 2024Systems 12(3):84, DOI:10.3390/systems12030084,https://www.researchgate.net/publication/378790195_A_Proposal_for_a_Tokenized_Intelligent_System_A_Prediction_for_an_AI-Based_Scheduling_Secured_Using_Blockchain
68. https://en.m.wikipedia.org/wiki/Proof_of_authority; last accessed 7/4/2024.

69. https://www.sciencedirect.com/topics/computer-science/proof-of-authority#:~:text=The%20proof%20of%20authority%20(PoA,and%20efficiency%20of%20the%20network; last accessed 7/4/2024.
70. https://www.lcx.com/proof-of-authority-explained/; last accessed 7/4/2024.
71. https://docs.roninchain.com/basics/white-paper; last accessed 7/4/2024.
72. J. Chain et al., "*An AI-based Super Nodes Selection Algorithm in Blockchain Networks*", 2018, https://arxiv.org/abs/1808.00216
73. M. Salimitari et al., "AI-Enabled Blockchain: An Outlier-Aware Consensus Protocol for Blockchain-Based IoT Networks", IEEE 2019, https://ieeexplore.ieee.org/document/9013824
74. Qi Xiong, Nasrin Sohrabi, Hai Dong, Chenhao Xu, and Zahir Tari, "*AICons: An AI-Enabled Consensus Algorithm Driven by Energy Preservation and Fairness*", April 2023, https://arxiv.org/abs/2304.08128
75. https://flare.network/consensus-learning-harnessing-blockchain-for-better-ai/; last accessed 14/4/2024.
76. Alex Shafarenko, "*Indexing structures for the PLS blockchain*", 2021, https://doi.org/10.48550/arXiv.2107.08970
77. https://stackoverflow.com/questions/52605676/how-hyperledger-fabric-kafka-consensus-works; last accessed 14/4/2024.
78. https://raft.github.io/; last accessed 14/4/2024.
79. https://www.spydra.app/blog/hyperledger-fabric-consensus-mechanisms-exploring-the-options; last accessed 14/4/2024.
80. https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatis.html; last accessed 14/4/2024.
81. https://en.m.wikipedia.org/wiki/Proof_of_identity_(blockchain_consensus); last accessed 14/4/2024.
82. K. Gai, Z. Hu, L. Zhu, R. Wang, and Z. Zhang, "*Blockchain meets DAG: a BlockDAG consensus mechanism*", In: Algorithms and architectures for parallel processing: 20th international conference, ICA3PP 2020, New York City, NY, USA, October 2–4, 2020, Proceedings, Part III, vol 20. Springer, pp 110–125, https://dl.acm.org/doi/abs/10.1007/978-3-030-60248-2_8
83. Andrew Lewis-Pye, "*Directed Acyclic Graph (DAG)-based Consensus*", a16z group, Oct 2022, https://youtu.be/v7h2rXNtrV0
84. https://blog.chain.link/bft-on-a-dag/; last accessed 14/4/2024.
85. Alexander Spiegelman, Aptos Labs, "*DAG Meets BFT- The Next Generation of BFT Consensus*", Science and Engineering of Consensus Workshop An Affiliated Workshop of SBC'22, https://youtu.be/_lKfdHT6ZFU
86. Dahlia Malkhi, "*Break throughs in consensus research from chainlink labs*", SmartCon 2023, https://youtu.be/R8K48CgoCHs
87. https://hackmd.io/@0xtrojan/mev_meets_dag; last accessed 15/4/2024
88. Dahlia Malkhi and Pawel Szalachowski, "*Maximal Extractable Value (MEV) Protection on a DAG*", Dec 2022, https://arxiv.org/abs/2208.00940
89. https://www.chainalysis.com/blog/zetachain-security-halborn/, last accessed 8/9/2023.
90. R. Belchior et al., "*Survey on Blockchain Interoperability: past, present and future*", 2021, https://dl.acm.org/doi/10.1145/3471140
91. https://wiki.polkadot.network/docs/learn-consensus; last accessed 15/4/2024.
92. https://www.horizen.io/research/; last accessed 27/10/2023.

93. A. Garoffolo, D. Kaidalov, and R. Oliynykov, "*Latus Incentive Scheme: Enabling Decentralization in Blockchains based on Recursive SNARKs*", Mar 2021, https://arxiv.org/pdf/2103.13754.pdf
94. Dawn Song et al., "*zkBridge: Trustless Cross-chain Bridges Made Practical*",2022, https://arxiv.org/abs/2210.00264
95. H. Yuan, S. Fei, and Z. Yan, "*Technologies of blockchain interoperability: a survey*", Aug 2023, https://www.sciencedirect.com/science/article/pii/S2352864823001335
96. Bernardo David, Peter Gaˇzi, Aggelos Kiayias, and Alexander Russell, "*Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain*", April 2023, https://eprint.iacr.org/2017/573.pdf
97. Z. Yin, B. Zhang, J. Xu, K. Lu, K. Ren, "*Bool network: An open, distributed, secure cross-chain notary platform*", IEEE Transactions on Information Forensics and Security 17(2022), 3465–3478, https://ieeexplore.ieee.org/abstract/document/9903072; https://bool.network/
98. Y. Geng et al., "*Subsidy Bridge: Rewarding Cross-Blockchain Relayers with Subsidy*", Information and Communications Security (pp.571-589), Oct 2023, DOI:10.1007/978-981-99-7356-9_34
99. M. Borkowski, M. Sigwart, P. Frauenthaler, T. Hukkinen, and S. Schulte, "*Dextt: Deterministic cross-blockchain token transfers*", IEEE access 7 (2019) 111030–111042, https://ieeexplore.ieee.org/abstract/document/8794500
100. D. Li, J. Liu, Z. Tang, Q. Wu, and Z. Guan, "*Agentchain: A decentralized cross-chain exchange system*", in: 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (Trustcom/BigdataSE), IEEE, 2019, pp. 491–498, https://ieeexplore.ieee.org/abstract/document/8887310
101. Y. Hei, D. Li, Chi Zhang, J. Liu, Y. Liu, and Q. Wu, "Practical AgentChain: A compatible cross-chain exchange system", May 2022, https://doi.org/10.1016/j.future.2021.11.029
102. S. Shao, F. Chen, X. Xiao, W. Gu, Y. Lu, S. Wang, W. Tang, et al., "*IBE-BCIOT: An ibe based cross-chain communication mechanism of blockchain in IoT*", World Wide Web 24 (5) (2021) 1665–1690, https://link.springer.com/article/10.1007/s11280-021-00864-9