

Identity Based Consensus inspired by Delegated Proof-of-Stake

Data on a Blockchain is grouped in *blocks*, each of which contains multiple *transactions*. Blocks have to be resistant to replication over a 'Byzantine' network. On those networks, writers can act maliciously in different ways:

- Attempts to store incorrect/invalid transactions on the Blockchain
- Use one input state multiple times
- Censor the Blockchain by systematically withholding particular transactions

Participants on the network must ensure the blocks they are presented with contain feasible information. They must also understand which block to treat as correct under uncertainty (i.e. when they are presented with alternative blocks). How consensus is reached is the key differentiator between DLT protocols.

Proof-of-Work

The original 'Bitcoin' electronic cash system, the first occurrence of a blockchain protocol, records transaction by 'by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work' [Nakamoto2008].

Participants have to earn the right to add a block to the existing chain of blocks by solving a computationally expensive challenge based on the content of the previous block. The economic rationale behind this approach is to disincentivise distorting the blockchain by requiring participants to expend real resources (in the form of computing effort) [Ma2018].

Participant	Computing Power
Miner ₁	
Miner ₂	

The amount of the reward obtained for solving the challenge is encoded in the protocol and will be awarded exclusively to the miner who succeeded in solving it first. In the simplified example above, Miner₂ would contribute 10% of the system wide resources to 'mining' new coins, which would give them an expected reward of 10% of the total block reward on average.

There is no true finality in *Proof-of-Work*. The protocol dictates that clients accept the longest chain of blocks as the true representation of facts, but block creators can diverge at any given point by creating a 'fork' as long as they deliver proof of work. As such, finality is *probabilistic*, in that after a certain number of subsequent blocks have been created, a fork is considered to be very unlikely.





Proof-of-Authority

Using pre-approved *validator* nodes, permissioned Blockchain systems using PoA can operate quicker by letting those nodes take turns approving transactions in blocks. This approach requires a nominated and approved con-

sortium of validators to operate. It is thus akin to a distributed database ran by multiple trusted third parties.

Proof-of-Stake

Here, as opposed to relying on solving computationally expensive tasks, the protocol will probabilistically determine who has the right to create the next block based on their *stake* in the network. PoS commonly define stake as holding coins on a particular blockchain [Saleh2018]. This materialist rationale makes it applicable to financial use cases. It is, however, hard to generalise it.

Participant	Holdings
Owner ₁	
Owner ₂	
Owner ₃	
Owner ₄	

Applying a naïve protocol to the holdings shown in the table would give Owner₁ a ~53% chance of being given the right to create a new block, Owner₂ would merely have a ~6.6% chance.

Delegated Proof-of-Stake



DPoS is an extension to conventional PoS, where stakeholders vote for *validators* to which they want to delegate block creation. Validators with the most votes will then be promoted to *delegates*, who will in turn create new blocks. Voting power is commonly aligned with the stake held by the voter.

Contribution: Proof-of-Identity

Neither method is democratic in nature as they depend either on ownership of assets (PoS, dPoS), on access to compute resources (PoW) or on pre-approval (PoA). I propose an extension to the 'Proof-of-Personhood' protocol [Borge2017] that uses a coloured coin approach to assign identity assertion levels to participants on the network.




Consider two hypothetical entities that have knowledge of the identity details of persons: **Issuer_A** and **Issuer_B**.

Consider a Blockchain system in which **Issuer_A** is the primary identity provider. Assume Person₁ and Person₂ are recognised by **Issuer_A**. This means they each hold an identity token issued by **Issuer_A**.




Participant	Identity Assertion
Person ₁	
Person ₂	

This identity assertion values now give the same rights to participate in consensus that 'stake' does in *Proof-of-Stake*. This means that both persons would have stake value 1 and would thus each have a 50% chance to create the next block. One of the novel aspects of the protocol is, that

the set of allowed identity issuers is subject to on-ledger voting. Assuming that a vote is cast to add **Issuer_B** and that this vote is successful (i.e. both Person₁ and Person₂ voted for it), persons with identity tokens issued by **Issuer_B** could join the system.

Participant	Identity Assertion
Person ₁	
Person ₂	
Person ₃	

Furthermore, Participants can express mistrust towards individual issuers. For example, in situations where they suspect the identity issuer is acting maliciously. Assuming Person₃ expresses mistrust towards **Issuer_A** through on-ledger voting, this would impact the value of all tokens issued by them in the amount of the share of network participants that expressed mistrust. In the above example that means that both identity assertion values for Person₁ and Person₂ would be negatively impacted. Going forward, they would only have stake value ~0.666 at their disposition.

Participant	Identity Assertion
Person ₁	
Person ₂	
Person ₃	

This simple example shows how an identity-based protocol could combine the benefits of a fully permissioned systems with those of a Proof-of-Stake based system. Various entities could serve as identity issuers in networks ranging from small to very large.

Use cases for Proof-of-Identity

- Use cases that require reliable consensus but are not materialist in nature (i.e. have no backing currency)
- Use cases that are tied strongly to individual identity, such as basic electronic voting and more advanced approaches such as liquid democracy
- Use cases that require some form of governance, but it is not clear from the outset which governance model is suitable

Nakamoto, S.
Bitcoin: A peer-to-peer electronic cash system
2008

Ma, J.; Gans, J. S. & Tourky, R.
Market Structure in Bitcoin Mining
National Bureau of Economic Research
2018

Saleh, F.
Blockchain Without Waste: Proof-of-Stake
SSRN Electronic Journal, Elsevier BV
2018

Borge, M.; Kokoris-Kogias, E.; Jovanovic, P.; Gailly, N.; Gasser, L. & Ford, B.
Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies
1st IEEE Security and Privacy On The Blockchain
2017