ALPH Ecosystem

This paper provides an architectural overview of the first release of the Alph ecosystem, codenamed Alph Network. For details on the economics of the native token, labeled $ALPH, we guide the reader to the accompanying token dynamics paper.

Disclosure: The information described in this paper is preliminary and subject to change at any time.
Furthermore, this paper may contain "forward-looking statements.

Alph Foundation (Network)

Contents:

Legal Disclaimer	***Mechanism Work*** **Proof-of-Work Algorithm** I. *Features of Proof of Work system* II. *Main issues with the Proof-of-Work consensus* *III. Cryptocurrencies using PoW*
Introduction	**Proof-of-Stake Algorithm** I. *What is Proof-of-Stake* II. *Advantages of PoS* *III. Weakness of a PoS mechanism* *IV. Blockchains using Proof-of-Stake*
CLIQUE	**Proof-of-Authority Algorithm** *I. Working of PoA* *II. Consensus and common attacks* *III. Advantages of PoA consensus* *IV. Application of PoA consensus*
Aura *I. Parameters* II. Finality III. Empty steps IV. Node Configuration V. Wishlist	**Running the authority nodes** **Useful RPCs** I. Connect the deployed nodes II. Create accounts III. Validate the blocks

PoA Implementations • *Smart contracts*	**A Sundry Ecosystem** *I. Enterprises* *II. Startups* *III. Community* *IV. Research partners* *V. Institutional partners/regulators*
Executive Summary	**How do we support the builders?**
Why Are We Making ALPH Network?	**Next-generation Proof of Authority will introduce**
How Proof of Authority consensus works in Alph *I. Validating nodes* *II. The leader node* *III. Generation of new blocks*	**Conclusion**
Forks	**Glossary**
Background *I. Speed and Volume* *II. Energy Consumption* *III. Decentralization* *IV. Secure and strict contracts*	**References**

Legal Disclaimer

This document is a technical white paper that presents the current status and future plans for the ALPH platform and ecosystem of ALPH Foundation Ltd (ALPH).

Nothing in this White Paper is an offer to sell, or the solicitation of an offer to buy, any tokens. Alph is publishing this White Paper solely to receive feedback and comments from the public. If and when Alph offers for sale any tokens (or a Simple Agreement for Future Tokens), it will do so through definitive offering documents, including a disclosure document and risk factors. Those definitive documents also are expected to include an updated version of this White Paper, which may differ significantly from the current version.

Nothing in this White Paper should be treated or read as a guarantee or promise of how Alph's business or the tokens will develop or of the utility or value of the tokens. This White Paper outlines current plans, which could change at its discretion, and the success of which will depend on many factors outside Alphs control, including market-based factors and factors within the data and cryptocurrency industries, among others. Any statements about future events are based solely on Alph's analysis of the issues described in this White Paper. That analysis may prove to be incorrect.

The sole purpose of this document is to provide information and is not to provide a precise description of future plans. Unless explicitly stated otherwise, the products and innovative technologies organized in this document are still under development and are yet to be incorporated.

ALPH does not provide a statement of quality assurance or affidavit for the successful development or execution of any of such technologies, innovations, or activities described in this document. Also, within legally permitted scope, ALPH rejects any liability for quality assurance implied by technology or other methods. No one possesses the right to trust any contents of this document or subsequent inference, and the same applies to any mutual interactions between ALPH's technological interactions that are outlined in this document. Notwithstanding any mistake, default, or negligence, ALPH does not have legal liability for losses or damages that occur because of errors, negligence, or other acts of an individual or group in relation to this document.

Introduction

Cryptocurrency and smart contracts are changing the world economy. From a currency perspective, what was previously impossible in most of the world transferring money globally in an instant – is now not only possible, it's safe, fast, easy and almost frictionless. .The way that people are now exchanging value is with the blockchain, decentralized trading platforms and smart contracts. What started as a need for digital cash in the 1990s has blossomed into an entire decentralized economy supported by an ecosystem of cryptocurrency wallets, exchanges, applications and services. Bitcoin was just the beginning.Cryptocurrency has changed global economics forever.

We first dive into the mechanisms of Proof of Authority protocols. Both Aura and Clique follow the basic idea of BFT-style consensus, where only one authority leader determines the block with instant finality. The differences lie in two aspects: (i) the ways to elect this leader; and (ii) the methods to agree on the block with peers.

Mission

Alph mission is to bring together an ecosystem of blockchain management solutions with high degree of automation, standardisation and compatibility.

CLIQUE

First of all, Clique is embedded inside Geth client for Ethereum, so it is designed in order to follow the mechanisms of the Ethereum blockchain. For example, the Clique is based on epochs, where each epoch is defined by a special sequence of blocks and every time a new epoch starts a special *TRANSITION BLOCK* is broadcasted containing mainly the set of authorities who are going to participate in consensus for that epoch. (1)

Step and Leader are calculated following a certain formula something that basically use the modulo operator among the number of authorities in order to have a unique leader for each round.
The Byzantine flavour of the algorithm comes now into account, since in Clique for each step there is not just one "leader" which might be byzantine and hence unreliable.

So for each step there is no just one leader but few authorities are allowed to publish and broadcast too their blocks together with the leader of that particular round. The leader formula allows each authority to send a block

only every (N/2 +1) blocks so for each step N-(N/2+1) authorities are allowed to propose a block. This, again, is designed in order to backup the leader if it might be faulty/malicious, sending for each round at least one block. I know, this can lead to forks since more than one block can be propagated per round, but fear not, the algorithm is designed in order to cooperate with the **GHOST** protocol of Ethereum chain where the canonical path of the chain is the one with the highest summed score.
Note that Clique assigns for each round a score to each block, where the leader has the highest score of the round and if two blocks are propagated in a single round, the one with the lowest score will be discarded.

In order to better understand how does this work and why this is byzantine tolerant we have to define that for each step, N-(N/2+1) authorities (leader counted) are allowed to propose their blocks, but among them, everyone except the leader will propagate its block only after a random time delay in order to avoid deterministic or sistematics forks.
So if the leader is up, it broadcast its block with the highest score, else, one among the round selected authorities will shoot its block, likely the one with the lowest random time delay.

Aura

Aura *(Authority Round)* is one of the Blockchain consensus algorithms available in OpenEthereum.Aura (Authority Round) is the PoA algorithm implemented in OpenEthereum (formerly Parity), the Rust-based Ethereum client. The network assumes that all authorities are synchronised within the same. Authorities maintain two queues locally, one for transactions and one for pending blocks. Each issued transaction is collected by authorities in the transaction queue. For each time step, the leader includes the transactions in the transaction queue in a block and broadcasts it to the other authorities. Then each authority sends the received block to the others (round block acceptance). If it turns out that all the authorities received the same block, they accept the block by adding it in the block queue. Any received block sent by an authority not expected to be the current leader is rejected. The leader is always expected to send a block; if no transaction is available then an empty block has to be sent. (2)

Parameters:

- n , the number of nodes
- f , the number of faulty nodes
- t, the step duration in seconds

Time is divided into discrete steps of duration t, determined by. $\frac{UNIX\ time}{t}$

At each step s, a *primary* will be assigned. Only the primary at a step may issue a block. It is misbehaviour to produce more than one block per step or to produce a block out of turn.

The primary for a step s is the node with index: *s* mod n.
The protocol contains a chain scoring rule SCORE(C) for a given chain C.

On each step, each honest node will propagate the chain with the highest score it knows about to all other nodes. Honest primaries will only issue blocks on top of the best chain they are aware of during their turn.

Finality

Under the assumption of a synchronous network which propagates messages within the step duration t, let SIG_SET(B) be the set of signatures from all authors in the set of blocks B:

$SIG\_SET(B)=\{a|\exists b\in B:AUTHOR(b)=a\}$
If there is a valid chain C ending with *C[K..]*, where $|SIG\_SET(C[K..])|>\frac{n}{2}$, then *C[K]* and all of its ancestors are finalized.

This definition of finality stems from a simple majority vote. In this setting, $2f+1\leq n$, so the faulty nodes cannot finalize a block all on their own.

Empty steps

In order to reach finality in a timely fashion it is necessary for the nodes to keep sealing blocks even when there are no transactions. To reduce blockchain bloat while still maintaining the same finality guarantees the nodes can sign and broadcast an *EmptyStep*(step, parent_hash) message instead of producing an empty block. All of the nodes accumulate the broadcasted empty step messages and they are included and rewarded in the next non-empty block.

The empty step messages included in blocks are also taken into account for finality.

To enable empty step messages set the emptyStepsTransition to enable it at the given block number. You can also specify a maximum number of empty steps with *maximumEmptySteps* in your chain spec.

Node Configuration

This consensus requires a *ValidatorSet* to be specified, which determines the list of n blockchain addresses at each height h which participate in the consensus. (3)

A node can represent a validator when it is run with --engine-signer *VALIDATOR-ADDRESS*.

The consensus can be run with --force-sealing which ensures that blocks are produced even if there are no transactions. This is necessary for blocks to reach finality in a timely fashion.

Wishlist

- Apply to step back off after skipping primaries, not before. Exponential backoff may allow for a weakly synchronous network without failure.
- Faster finality by broadcasting signed GOOD(Hash) messages where Hash is a block hash of a block with a number multiple of some epoch length. GOOD messages can be included in the seal.

Proof of Authority Implementations

About DPOA

DPOA is an L2 protocol built on ALPH, combining scalability, superior transaction speed, and cost-savings with Ethereum's security.

We provide two mainstream Proof of Authority implementations. In particular, we emphasize mechanisms from a block's proposal to verification. Aura (Authority Round) is implemented in Parity.

The network in Aura is assumed to be synchronous, and all authorities are assumed to hold the same UNIX time T.

The leader of each step is deterministically calculated by duration and the number of authorities $|sealers|$, which is represented as $i = T\,duration \bmod |sealers|$.
Each authority executes an infinite loop that periodically checks whether i equals her position index. If it does, this au will propose a block and broadcast it to other authorities.

If the received block is not produced by the current leader with the correct difficulty diff, it will be rejected.

This is achieved by the verification algorithm. Otherwise, if the block is valid, the authorities will send received blocks to others. The leader is always expected to produce a block with correct difficulty, even if no transactions are available.

Smart contracts are also rapidly changing the way business is done.

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

The potential uses of cryptocurrency and smart contracts via the blockchain are revolutionary and have the potential to disrupt almost every industry and institution imaginably. But, there are problems in making this vision a reality. The largest and most immediate problems are that blockchain in its current form is not scalable and uses absurd amounts of energy that are not sustainable.

We intend to fix those problems with our programs

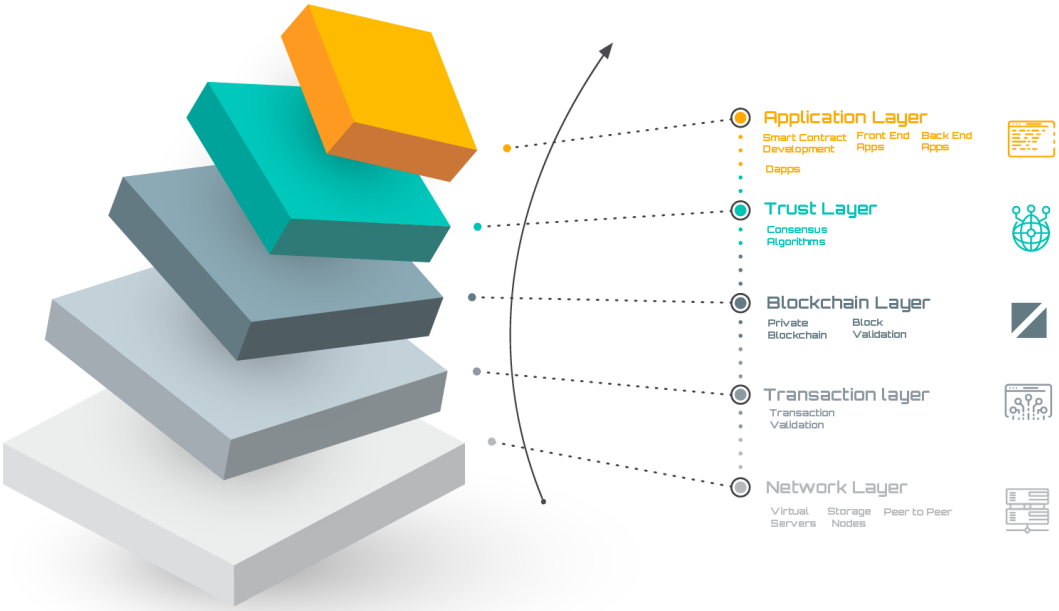
- Executive Summary

ALPH Network, a standalone blockchain, is a next-generation smart contract platform. It's built upon an improved Ethereum codebase that solves the scaling problem with immediacy.

Vitalik Buterin, one of the founders of Ethereum, has labelled scalability a trilemma where all 3 problems need to be solved simultaneously:

1. Scalability
2. Decentralization
3. Security

Motivated by the above-mentioned challenges, the Alph Network proposes a consensus protocol that focuses on the following key strategies:



● Double Validation to strengthen security and reduce likelihood of forks.
● Randomization to guarantee fairness and prevent handshaking attacks.
● Fast confirmation time and efficient checkpoints for finality or rebase.
● Self-KYC layer while setting up Network Node.
● run subnets

- Why Are We Making ALPH Network?

The vision of ALPH Network is to grant compatibility between all transaction bodies around the world using fast Proof of Authority technology that can be deployed at scale in the real world and to create a new infrastructure with high reliability that allows for real-time transactions and data sharing.

ALPH Network has the intention of being used on a large scale in various industry verticals, such as telecommunication, finance, logistics, electric vehicle provision and others. The ALPH Network Foundation intends to create the ALPH platform along with a new Smart Contract-based ecosystem that can be used by all current and future partner companies around the world.

To facilitate consistent global transactions with high accuracy and reliability, the ALPH Network Foundation will lead the next generation of distributed ledger technologies.

The platform intends to be open-source: used and changed by the community, and to provide various application support tools that can be used to create decentralized applications (DApps). (4)

- How Proof of Authority consensus works in Alph

Blockchains in Alph ecosystem are secured by the validating nodes that are arbitrarily selected as trustworthy entities.

Validating nodes

In Alph, only selected nodes called *validating nodes* can generate new blocks. These nodes maintain the blockchain network and the distributed ledger.

The list of validating nodes is kept in the blockchain registry. The order of nodes in this list determines the sequence in which nodes generate new blocks.

The leader node

The following formula determines the current *leader node*, a node that must generate a new block at the current time.

leader = ((time - first) / step) % nodes

LEADER
Current leader node.

time
Current time (UNIX).

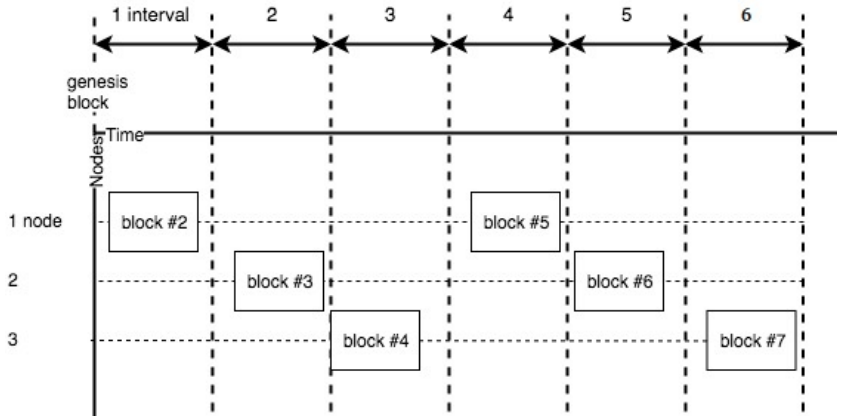
first
First block generation time (UNIX).

step
Number of seconds in the block generation interval.

nodes
Number of nodes at the current block generation interval.

Generation of new blocks

The new block is generated by a leader node of the current time interval. At each time interval, the leader role is passed to the next validating node from the list of validating nodes.



A new block is created

The leader node generates the new block as follows:

I. Collects all new transactions from its transaction queue.

II. Executes transactions one by one. Transactions that are invalid or cannot be executed are rejected.
III. Checks compliance to block generation limits.
IV. Creates a block with valid transactions and signs it with node's private key (ECDSA algorithm).
V. Sends this block to other validating nodes.

The new block is validated

Other validating nodes:

1. Receive the new block and validate that:
    - The new block was generated by the leader node of a current interval.
    - There are no other blocks generated by the leader node of a current interval.
    - The block is generated and signed correctly.

2. Execute transactions from the block one by one. Check that transaction are executed successfully and within block generation limits.

3. Add or reject the block, depending on the previous step:
    - If block validation is successful, add the new block to the node's blockchain.
    - If block validation failed, reject the block and send a *bad block* transaction. If the validating node that created this invalid block continues to generate such blocks, it can be banned or excluded from the list of validating nodes.

Forks

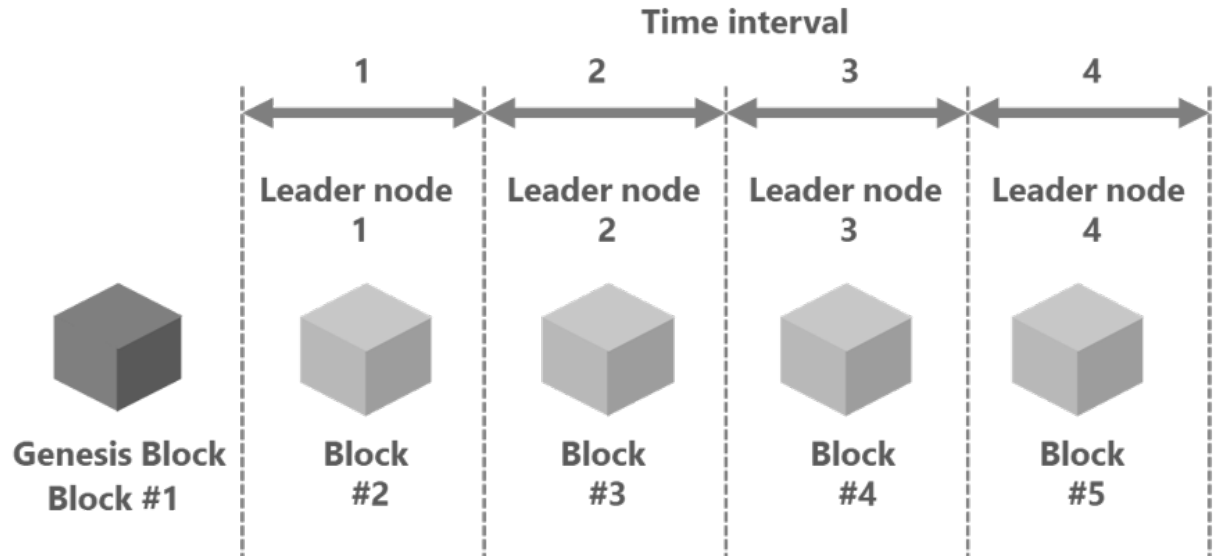
A *fork* is an alternate version of the blockchain. A fork contains one or more blocks that were generated independently from the rest of the blockchain. (5)

Forks usually occur when a part of the network becomes desynchronized. Factors that influence the probability of forks are high network latency, intentional or unintentional time limits violation, time desynchronization at nodes. If network nodes have a significant geographic distribution, block generation interval must be increased.

Forks are resolved by following the *longest blockchain* rule. When two versions of the blockchain are detected, validating nodes rollback the shorter version and accept the longer one.

Proof of Authority implementation based on Alph Network proof of consensus algorithm For the Decision Blockchain we chose the Alph Network proof of consensus algorithm that is described in more detail in the official documentation of Alph Foundation.

The consensus protocol of any blockchain must contain the following mandatory information: the timestamp when the block was produced and the identity of the entity that generated the block.



Background

- *Speed and Volume.*

Public, decentralized cryptocurrencies suffer from slow transactions and low transaction volume. Bitcoin can only process 7 transactions per second, and Ethereum can only process 13 per second. Additionally, the time to verify transactions can range from several minutes to several hours depending on the current volume In contrast, Visa, Inc. averages 150 million transactions every day and is capable of handling more than 56,000 transactions per second. Public cryptocurrencies are too slow for real-world processing by 4 orders of magnitude.

- *Energy Consumption.*

The process of mining blocks uses enormous energy because of a consensus algorithm called Proof-of-Work (PoW). (6)
PoW requires non-trivial computational work by mining nodes which, in turn, makes it cost prohibitive for a bad actor to perform malicious acts. This computational workload requires energy.

As of today, 3.5 million US households could be powered with the energy used to run the Bitcoin network, while Ethereum uses the equivalent power of 1 million households. This is unacceptable and unsustainable.

- *Decentralization.*

Decentralization is a central tenant of cryptocurrencies. It ensures no one company or government can control it. However, in practice, most mining has moved to China where electricity is cheapest .75% of all blocks are mined by large Chinese mining companies. This is true of Bitcoin, Bitcoin Cash, Ethereum and top cryptocurrencies.

In the event of company collusion or government privatization, 51% attacks would be possible.

- *Secure and strict contracts.*

Ethereum provides a unique feature called smart contracts. These smart contracts allow users to write small, unmodifiable programs that ensure all involved parties are committed to a set of rules with absolute certainty. This has been so successful that nearly every ICO in the past year has run on Ethereum's smart contract system. These smart contracts, however, are not smart at all. They are extremely rigid contracts that are unable to adapt to changes like real-world contracts would. Parties involved in a contract have no ability to upgrade their contract if necessary to adjust terms or to fix bugs in contract code.

Mechanism of Work

In the continue reviews well-known families of consensus algorithms for both permissionless and permissioned blockchains.This includes Proof-of-Work (PoW), Prof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS),Proof-of-Activity (PoW/PoS-hybrid), Proof-of-Burn (PoB), Proof-of-Validation (PoV), Proof-of-Capacity (PoC or Proof-of-Storage), Proof-of-Importance (PoI), Proof-of-Existence (PoE),Proof-of Elapsed Time (PoET), Ripple Consensus Protocol and Stellar Consensus Proto-col (SCP). Although each algorithm is briefly described, they lack of any form of analysisin presence of Byzantine nodes under an eventual synchronous model. (7)

Blockchain works via a multistep algorithm process, which in simple terms happens as follows:

Proof-of-Work Algorithm.

The idea for Proof of Work(PoW) was first published in 1993 by Cynthia Dwork and Moni Naor and was later applied by Satoshi Nakamoto in the Bitcoin paper in 2008. Proof of Work consensus is the mechanism of choice for the majority of cryptocurrencies currently in circulation. The term "proof of work" was first used by **Markus Jakobsson** and **Ari Juels** in a publication in 1999.

The Proof of Work consensus algorithm involves solving a computationally challenging puzzle in order to create new blocks in the Bitcoin blockchain. Colloquially, the process is known as 'mining', and the nodes in the network that engages in mining are known as 'miners'. The incentive for mining transactions lies in economic payoffs, where competing miners are rewarded with 12.5 bitcoins(at the time of writing this article; this reward will get reduced by half its current value with time) and a small transaction fee.

Features of Proof of Work system:
There are mainly two features that have contributed to the wide popularity of this consensus protocol and they are:

- It is hard to find a solution for the mathematical problem
- It is easy to verify the correctness of that solution

Main issues with the Proof-of-Work consensus:

The Proof-of-Work consensus mechanism has some issues which are as follows:

- **The 51% risk**: If a controlling entity owns 51% or more than 51% of nodes in the network, the entity can corrupt the blockchain by gaining the majority of the network.
- **Time consuming**: Miners have to check over many nonce values to find the right solution to the puzzle that must be solved to mine the block, which is a time consuming process.
- **Resource consumption**: Miners consume high amounts of computing power in order to find the solution to the hard mathematical puzzle. It leads to a waste of precious resources(money, energy, space, hardware). It is expected that the 0.3% of the world's electricity will be spent to verify transactions by the end of 2018.
- Transaction confirmation takes about 10–60 minutes. So, it is not an instantaneous transaction; because it takes some time to mine the transaction and add it to the blockchain thus committing the transaction.

Cryptocurrencies using PoW:

- Litecoin
- Ethereum
- Monero coin
- Dogecoin

Proof-of-Stake Algorithm.

Proof-of-Stake (PoS) is another consensus algorithm which pseudo-randomly chooses validators based on their stake in the network. The idea is that those with the most coins in circulation have the most to lose so they are positioned to work in the interest of the network.

What is Proof-of-Stake:

As understandable from the name, nodes on a network stake an amount of cryptocurrency to become candidates to validate the new block and earn the fee from it. Then, an algorithm chooses from the pool of candidates the node which will validate the new block. This selection algorithm combines the quantity of stake (amount of cryptocurrency) with other factors (like coin-age-based selection, and randomization process) to make the selection fair to everyone on the network.

- *Coin-age-based selection:*
  The algorithm tracks the time every validator candidate node stays a validator. The older the node becomes, the higher the chances of it becoming the new validator.

- *Random Block selection:*
  The validator is chosen with a combination of 'lowest hash value' and 'highest stake'. The node having the best weighted combination of these becomes the new validator.

Advantages of PoS:

- **Energy-efficient:**
  As all the nodes are not competing against each other to attach a new block to the blockchain, energy is saved. Also, no problem has to be solved(as in case of Proof-of-Work system) thus saving the energy.
- **Decentralization:**
  In blockchains like Bitcoin(Proof of Work system to achieve distributed consensus), an extra incentive of exponential rewards are in place to join a mining pool leading to a more centralized nature of blockchain. In the case of a Proof-of-Stake based system(like Peercoin), rewards are proportional(linear) to the amount of stake. So, it provides absolutely no extra edge to join a mining pool; thus promoting decentralization.
- **Security:**
  A person attempting to attack a network will have to own 51% of the stakes(pretty expensive). This leads to a secure network.

Weakness of a PoS mechanism:

- **Large stake validators:**
  If a group of validator candidates combine and own a significant share of total cryptocurrency, they will have more chances of becoming validators. Increased chances lead to increased selections, which lead to more and more forging reward earning, which lead to owning a huge currency share. This can cause the network to become centralized over time.
- **New technology:**
  PoS is still relatively new. Research is ongoing to find flaws, fix them and making it viable for a live network with actual currency transactions.
- **The 'Nothing at Stake' problem:**
  This problem describes the little to no disadvantage to the nodes in case they support multiple blockchains in the event of a blockchain split(blockchain forking). In the worst-case scenario, every fork will lead to multiple blockchains and validators will work and the nodes in the network will never achieve consensus.

Blockchains using Proof-of-Stake:

- Ethereum(Casper update)

- Peercoin
- Nxt

Proof-of-Authority Algorithm.

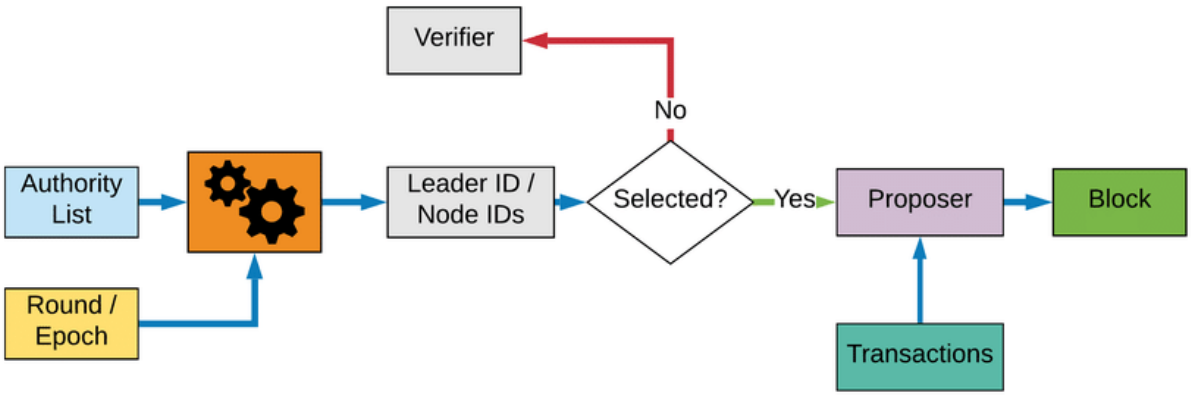
Proof-of-Authority is a new consensus algorithm where trusted set individuals provide all transaction processing.

This trust allows transaction processing speed to improve significantly by skipping the PoW hash computation. A few networks exist but they currently only focus on private networks or do not focus on performance as a goal.(8)

In blockchain platforms, consensus mechanisms can be divided into permissionless (eg., Ethereum, Bitcoin) and permissioned (eg Hyperledger, Ethereum Private). Unlike permissionless blockchain where anyone can become node, in permissioned blockchain all nodes are pre-selected. This allows using of consensus types with high scalability and bandwidth.

One of these consensus types is **Proof-of-Authority (PoA) consensus** which provides high performance and fault tolerance. Term was proposed in 2017 by co-founder of Ethereum and Parity Technologies Gavin Wood.

Working of PoA :



- In PoA, rights to generate new blocks are awarded to nodes that have proven their au ity to do so. These nodes are referred to as **"Validators"** and they run software allowing them to put transactions in blocks. Process is automated and does not require validators to be constantly monitoring their computers but does require maintaining the computer uncompromised. PoA is suited for both private networks and public networks, like POA Network, where trust is distributed.
- PoA consensus algorithm leverages value of identities, which means that block validators are not staking coins but their own reputation instead. PoA is secured by trust on the identities selected.

PoA consensus and common attacks :

I. **Distributed Denial-of-service attacks(DDos) :**
A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. An attacker sends large number of transactions and blocks to targeted network node in an attempt to disrupt its operation and make it unavailable.PoA mechanism makes it possible to defend against this attack because network nodes are pre-authenticated, block generation rights can be granted only to nodes that can withstand DoS attacks.

II. **51% attack :**
In Proof of Authority consensus, 51% of attack requires an attacker to obtain control over 51% of network nodes. This is different from 51% attack for the Proof-of-Work consensus types where an attacker needs to obtain 51% of network computational power. Obtaining control of the nodes in permissioned blockchain network is much harder than obtaining computational power. With PoA, individuals earn right to become validators, so there is an incentive to retain position that they have gained. Validators are incentivized with reputation which lets them retain their au it as a node. PoA only allows non-consecutive block approval from anyone validator, meaning that the risk of serious damage is centralized to the authority node. (9)

III. **Conditions for PoA consensus** :

Proof of Authority consensus may vary according to different implementations but generally, they are applied through the following conditions :

- Validators need to confirm their real identities.
- A candidate must be willing to invest money and put his reputation at stake. A tough process reduces the risks of selecting questionable validators and incentivizes long-term commitment to the blockchain.
- The method for selecting validators must be equal for all candidates.

- The identity of validators must be verified to maintain the integrity of blockchain. Some sort of process should be there to select honest validators.

Advantages of Proof of Authority consensus :

- High risk tolerance as long as 51% of the nodes are not acting maliciously.
- Interval of time at which new blocks are generated is predictable. For PoW and PoS consensuses, this time varies.
- High transaction rate.
- Far more sustainable than algorithms like Proof of Work which require computational power.

Quantum Mechanism

The advent of quantum computing poses a significant threat to traditional cryptographic algorithms, such as RSA and ECC, which are widely used in blockchain systems. Our blockchain introduces a quantum mechanism that integrates quantum-resistant algorithms and quantum-enhanced decentralization.
Quantum-Resistant Algorithms:

We employ post-quantum cryptographic algorithms, such as lattice-based cryptography, to secure transactions and smart contracts. These algorithms are designed to withstand attacks from both classical and quantum computers.
Quantum-Enhanced Decentralization:

Alph Network blockchain leverages quantum key distribution (QKD) to enhance the decentralization of transactions and contracts. QKD uses the principles of quantum mechanics to securely distribute encryption keys, ensuring that transactions and contracts are protected against quantum attacks.
Key Benefits:

Future-Proofing: Protects against the threat of quantum computing, ensuring long-term security.

Enhanced Security: Quantum-resistant algorithms and QKD provide unparalleled security for transactions and contracts.

Decentralization: Quantum-enhanced decentralization ensures that no single entity can compromise the network.

Consensus Mechanism

Alph Qchian employs a hybrid consensus mechanism that combines Proof of Authority (PoA) with a quantum-resistant Byzantine Fault Tolerance (qBFT) algorithm. This hybrid approach ensures high throughput, low latency, and robust security against quantum attacks.

1.2 Quantum-Resistant Ledger

The ledger is secured using lattice-based cryptographic algorithms, which are resistant to attacks from both classical and quantum computers. Each transaction is signed using a quantum-resistant digital signature, ensuring the integrity and authenticity of the data.

1.3 Quantum Key Distribution (QKD)

QKD is integrated into the network to securely distribute encryption keys between nodes. This ensures that even if a quantum computer were to break the encryption, the keys would remain secure due to the principles of quantum mechanics.

1.4 Smart Contract Execution

Smart contracts are executed on a quantum-enhanced EVM, which is optimized for performance and security. The EVM is compatible with existing Ethereum tools and libraries, making it easy for developers to migrate their dApps.

Use Cases

Decentralized Finance (DeFi)

Alph blockchain provides a secure and scalable platform for DeFi applications, including lending, borrowing, and trading. The quantum mechanism ensures that financial transactions and contracts are protected against quantum threats.

Supply Chain Management

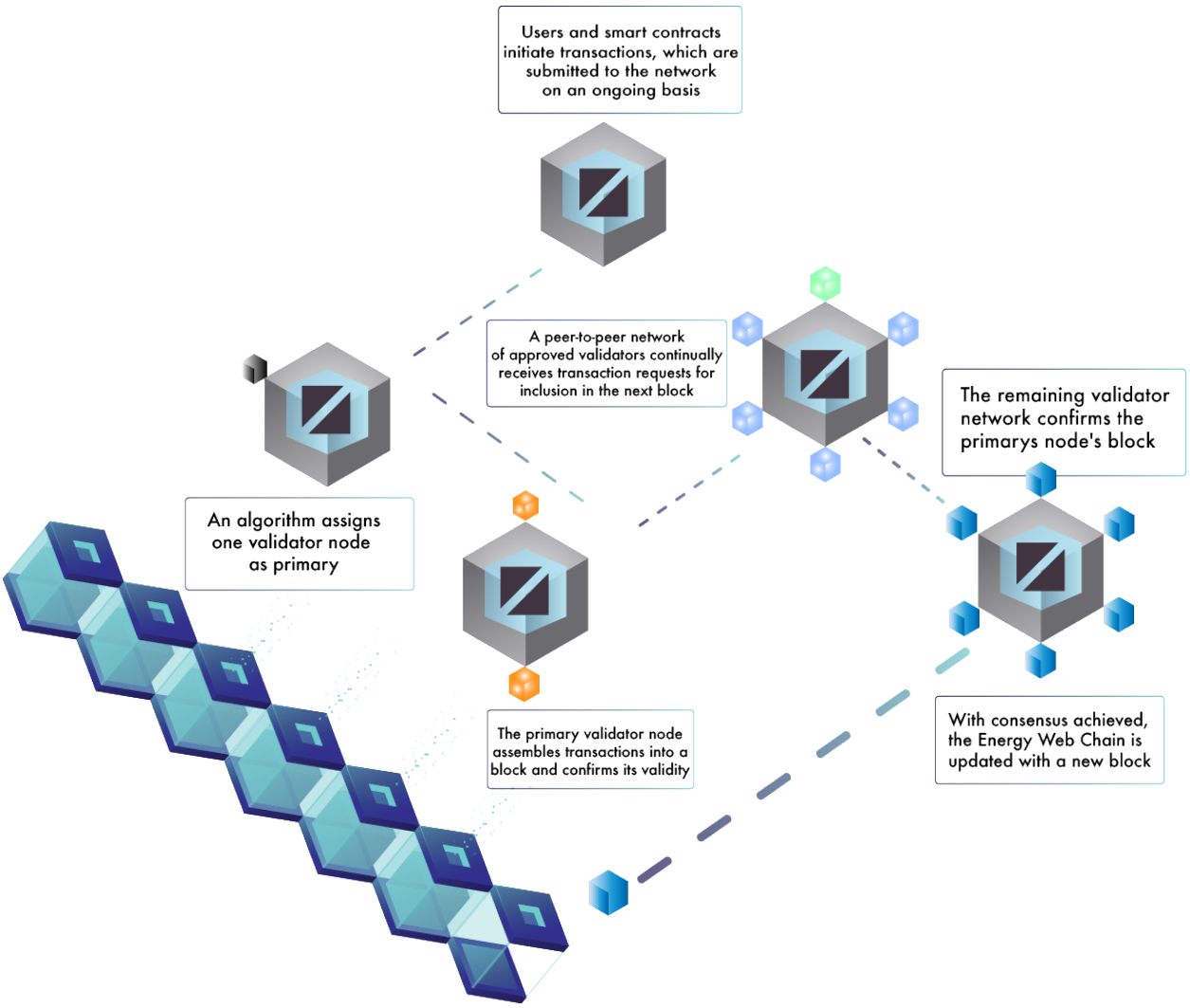
The transparency and immutability of our blockchain make it ideal for supply chain management. Smart contracts can automate and enforce agreements between parties, while the quantum mechanism ensures the security and integrity of the data.

Healthcare

In the healthcare industry, Alph blockchain can be used to securely store and share patient data. The quantum mechanism ensures that sensitive information is protected against quantum attacks, while smart contracts can automate processes such as insurance claims and patient consent.

Government and Public Sector

Alph Network blockchain can be used to create transparent and secure systems for voting, identity management, and public records. The quantum mechanism ensures that these systems are protected against quantum threats, while smart contracts can automate and enforce government processes.



Application consensus :

Proof of Authority consensus algorithm may be applied in a variety of scenarios and is deemed a great option for logistical applications such as supply chains.

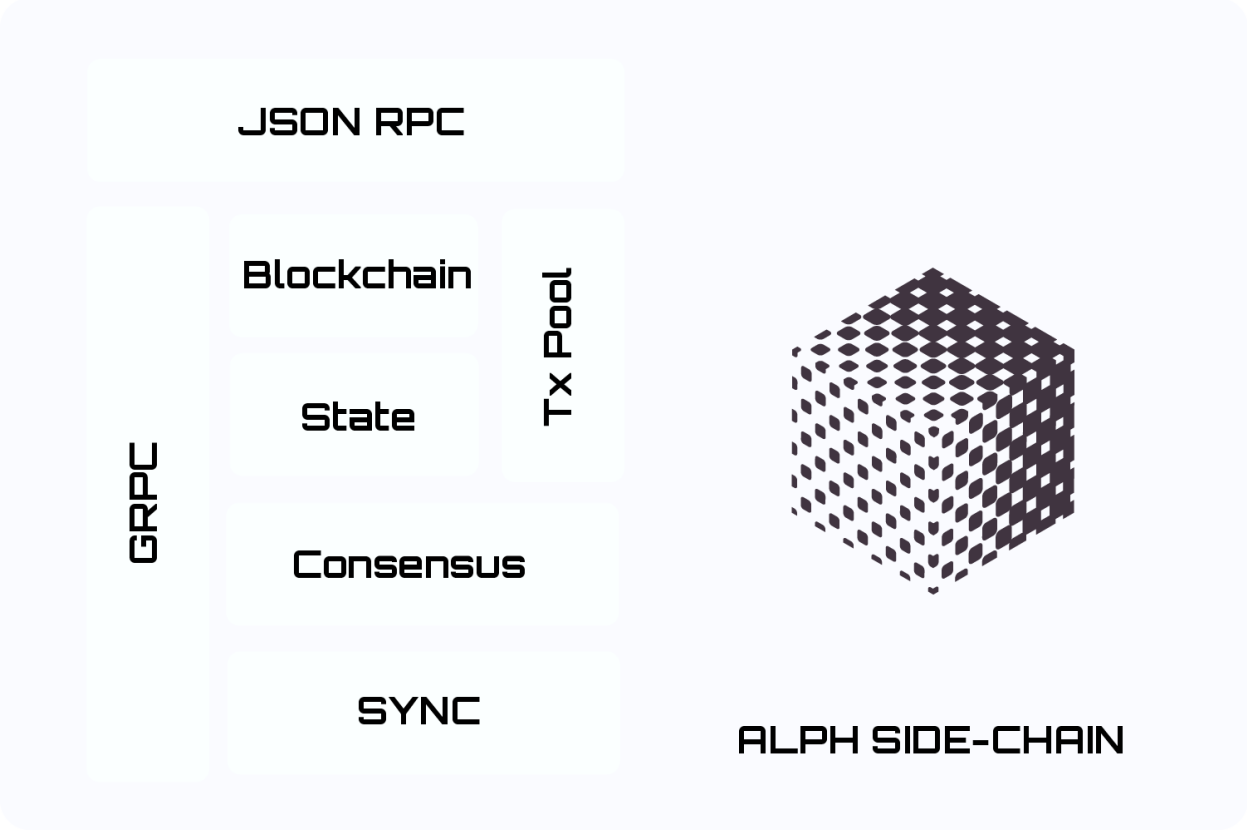
Proof of Authority model enables companies to maintain their privacy while availing benefits of blockchain technology. Microsoft Azure is another example where Proof of Authority is being implemented. Azure platform

provides solutions for private networks, with system that does not require native currency like ether 'gas' on Ethereum, since there is no need for mining. Azure nodes are pre-selected.(11)

Running the authority nodes

Each node on the network should run its node with chain spec JSON file provided to `--chain` option. Format of such file depends on the consensus `Engine` used and is described on the Chain specification page.

If you're expecting to issue blocks, make sure you have `--engine-signer` set to an account address



(`0xADDRESS`) listed in the engine configuration under `authorities` and password file for that account is provided to `--password`. OpenEthereum has a separate directory for each chain, so make sure that the account is visible on the specified chain (create an account with `--chain`, import the keys or use `--keys-path`). You should ensure anyone else you want issuing on the network is similarly configured. Each authority

can only run a **single node** and to utilize the full network capacity each authority should run a node. To make the transactions free, authority nodes can run with `--usd-per-tx 0`. The configuration can also be done via the config file with the following fields:

```
[parity]
chain = "/path/to/json/spec"

[account]
password = ["/path/to/password"]

[mining]
engine_signer = "0x37f93cfe411fa244b87ff257085ee360fca245e8"
reseal_on_txs = "none" // Authorities reseal automatically
usd_per_tx = "0" // Allows for free transactions.
```

Useful RPCs

Connect the deployed nodes:

- `parity_enode()` returns enode of the particular instance
- `parity_addReservedPeer(enode)` adds enode to the list of reserved peers (run with `--reserved-only` to avoid other connections)

Create accounts:

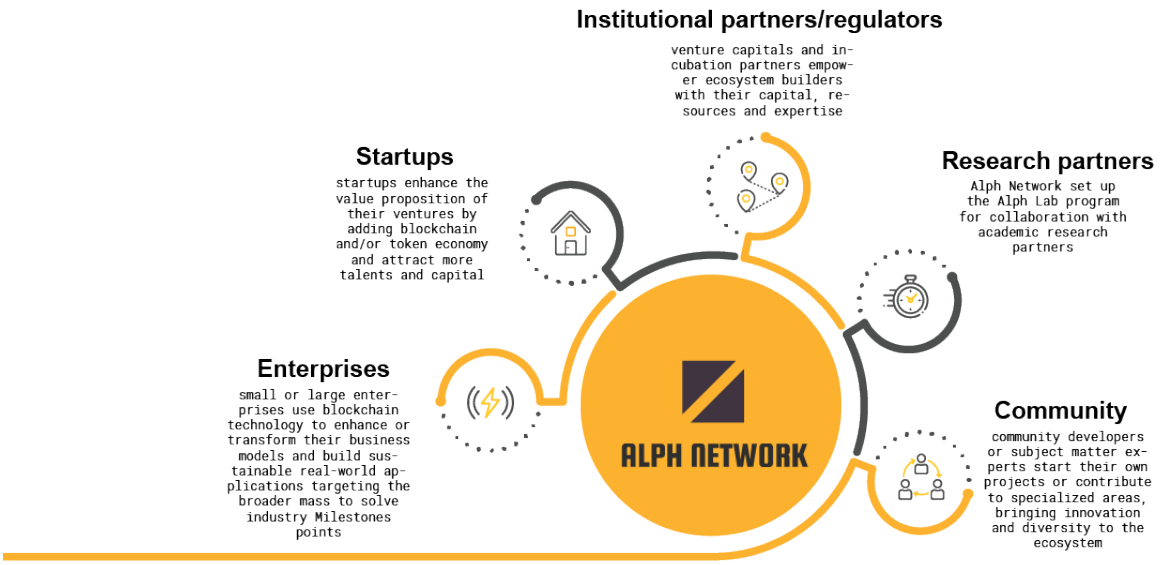
- `personal_newAccount(password)` creates new account and returns its address
- `parity_newAccountFromPhrase(phrase, password)` creates an account deterministically and returns its address (always the same for a given input)

Validate the blocks:

- `parity_setEngineSigner(address, password)` set this to one of authority addresses in order to participate in the consensus

A Sundry Ecosystem

Although enterprises are critical for mass adoption, built on top of the Alph Network public blockchain, the Alph Network ecosystem is open for various types of participants to collaborate and the open platform could significantly help reduce the friction across organizations and industries. While most enterprises seek ways to



Sundry Ecosystem

integrate blockchain into or transform their existing business models and systems, many startups or community projects are building their businesses around blockchain from the start. Because they are usually more nimble, it puts them in a better position to apply disruptive thinking from the ground up to create new business models or value chains than established businesses. (10)

As the enabler of the ecosystem, Alph Network is committed to working with the ecosystem participants to solve real-world economic problems and create value with blockchain technology. Alph Network connects the resources, supports and opportunities to the right participants with the goal to create value for the ecosystem holistically.

Alph Network - the enabler of the ecosystem, focusing on building the underlying technology, infrastructure utilities and services.Alph Network holds a significant reserve to support the ecosystem growth.

- **Enterprises** - small or large enterprises use blockchain technology to enhance or transform their business models and build sustainable real-world applications targeting the broader mass to solve industry Milestones points

- **Startups** - startups enhance the value proposition of their ventures by adding blockchain and/or token economy and attract more talents and capital to the ecosystem. Identify and test viable solutions that larger organizations may then adopt on a wider scale, forming a symbiotic relationship that drives continued blockchain innovation

- **Community** - community developers or subject matter experts start their own projects or contribute in specialized areas, bringing innovation and diversity to the ecosystem

- **Research partners** - following the real needs of ecosystem applications, Alph Network works closely with research partners to improve the underlying technologies to support the ecosystem. Alph Network set up the Alph Lab program for collaboration with academic research partners

- **Institutional partners/regulators** - venture capitals and incubation partners empower ecosystem builders with their capital, resources and expertise; Regulators provide well-defined and blockchain-friendly legislation for projects to thrive

How do we support the builders?

Alph Network has an unparalleled track record in the public blockchain space in helping established businesses build blockchain solutions that are used as part of daily business and add sustainable value.

Similar to a public cloud platform, enterprises and startups who may or may not have blockchain expertise or development capabilities will tend to choose the blockchain platform with comprehensive tools, services and support.

Enterprises

- The Alph Network data BaaS platform is a powerful tool for enterprises to quickly adopt blockchain technology for the existing business without investing in the in-house blockchain development capability

- With technology infrastructure, business acumen and a strong business partner network, Alph Network is well positioned to be a trusted technology partner in enterprises' digital transformation journey to create new business models and value chain

- The Alph Network public blockchain, development tools, turnkey solutions, as well as comprehensive technical support, makes it the most feasible public blockchain platform for enterprises to develop applications on

Startups

- Alph Network developed a wide range of open source tools, BaaS and turnkey solutions to help startups integrate and develop blockchain without the need to start everything from scratch. In addition to the technical documentation, startups can get direct access to the Alph Network tech team

- Startups will have the opportunity to work with our incubation partners to find the right business model and be prepared for investment. Since blockchain and crypto is a new space, we can help you explore and avoid pitfalls in areas such as legal, accounting and compliance

- As the startup scales the business, Alph Network can bring business opportunities by facilitating collaboration between ecosystem builders and partners. Startups will also have the opportunity to raise public awareness and exposure of the business with our global community, media and events

Community

- Alph Network helps entrepreneurs in the community turn ideas into projects with funding support and advisory services

- Developers can get technical support, join our developer channels or claim the bounty programs

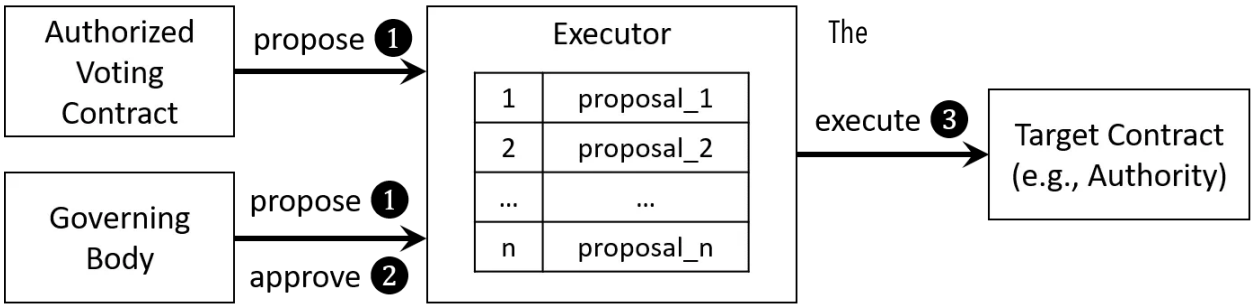
- Alph Network matchmakes community projects with contributors that share the same vision

- Alph Network provides the latest updates about the ecosystem and arranges events to engage with the community

Join the Alph Network ecosystem and learn more information at alph.network/start.

Next-generation Proof of Authority will introduce

Summary



I. A committee-endorsing mechanism that significantly lowers the possibility of a node manipulating his right to produce a new block and results in faster converging probabilistic finality
II. block-finality mechanism that grants absolute safety guarantee to blocks (as well as the included transactions) that qualify certain criteria

It can be seen that both probabilistic and absolute finality will be allowed to coexist by the consensus protocol, providing different levels of security guarantee for applications running on the blockchain platform. In general, the higher security is required, the less efficient the application will be, and vice versa. Consequently, enterprises will be able to select the correct security guarantee that best suits their needs to maximize application performance.

Conclusion

In this paper, we discussed the architecture of the alph ecosytem. Compared to other platforms today, which either run pos-style consensus protocols and therefore are inherently non-scalable, or make usage of pow-style consensus that is inefficient and imposes high operating costs, the ALph is lite-base chian EVM compatible ,
more scalable ,and more secure, and efficient.
The native token, which serves for securing the network and paying for
various infrastructural costs is simple and backwards compatible. $ALPH has capacity beyond other proposals to achieve higher levels of secured-chain, resist attacks, and scale to millions of nodes without any quorum or assembly election, and hence without imposing any limits to participation.

Glossary

Bonding: A key concept in PoS networks that can translate as building up a strong “binding” relationship with a PoS network. You express your commitment to the network by locking a defined amount of your network token for a specific period.

Collator: Collators maintain a full node. Their primary task is to aggregate transactions into a block (or block candidates) and provide proofs for validators on the relay chain.

Consensus Mechanism: A method of authenticating and validating a value or transaction on a blockchain or a distributed ledger without the need to trust or rely on a central au ity. Consensus mechanisms are central to the functioning of any blockchain or distributed ledger.

Cryptographic key: A cryptographic key is a string of data used to lock or unlock cryptographic functions, including authentication, au ization and encryption. Cryptographic keys are grouped into cryptographic key types according to their functions.

Cryptographic signature: Also known as a digital signature, it is a cryptographic value that is calculated from the data and a secret key known only by the signer.

A decentralized application (dApp): Decentralised applications are digital applications or programs that exist and run on a blockchain or peer-to-peer (P2P) network of computers instead of a single computer. DApps are outside the purview and control of a single au ity. DApps can be developed for various purposes, including gaming, finance, technology integration, and social media.

Digital Twin: A new form of a digital ledger for record-keeping and data exchange.

Ethereum state channel: State channels refer to the process in which users transact with one another directly outside of the blockchain, or "off-chain", and greatly minimize their use of "on-chain" operations. EU EIDAS scheme: Electronic Identification, Authentication and Trust Services. The eIDAS Regulation established the framework to ensure that electronic interactions between businesses are safer, faster and more efficient, no matter the European country they take place in.

Executor: Executors are the ones who conduct transactions on Supplain parachains.

Fisher: Fishers are responsible for cross-checking collators' work and providing an additional layer of security. Given a proof of authority consensus for private parachains, the fisher's role may only be required for public parachains.

Floating token: The opposite of a stablecoin, a token with a value that is subject to outside forces and therefore susceptible to higher levels of volatility.

Immutability: The ability for a blockchain ledger to remain a permanent, indelible, and unalterable history of transactions.

Initiator: Initiators are the original data owners that start each private parachain and most transactions. The initiator's typical objective is to transfer particular data or physical goods to recipients, using the assistance of executors.

Merkle tree hash: In cryptography and computer science, a hash tree or Merkle tree is a tree in which every "leaf" (node) is labelled with the cryptographic hash of a data block, and every node that is not a leaf (called a branch, inner node, or inode) is labelled with the cryptographic hash of the labels of its child nodes. A hash tree allows efficient and secure verification of the contents of a large data structure. A hash tree is a hash list and a hash chain generalization.

Metadata: Higher-level data that describes or annotates a data set, like tags in a programming code that describe the hierarchical structure and the relationships among discrete pieces of data.

Nominated Proof of Stake: The process of selecting validators to be allowed to participate in the consensus protocol. NPoS is a variation of Proof-of-Stake and is used in Substrate-based Blockchains such as Kusama, Edgeware or Polkadot.

Nominator: One of two main actors who are involved in a blockchain network that uses the nominated proof-of-stake (NPoS) consensus algorithm, the other being validators.

In regular proof-of-stake (PoS) networks, the power of an entity mining or validating network transactions is solely reliant on the number of network tokens they hold. The more tokens of that network are held by the miner or validator, the more mining power they have. This same power is also used in other types of decision-making scenarios. It is popularly used in governance functions, with validators voting on proposals for the future development of the network, for example.

Parachain: A parachain is an application-specific data structure that is globally coherent and validatable by the validators of the Relay Chain. They take their name from the concept of parallelised chains that run parallel to the Relay Chain.

Polkadot: A network protocol that allows arbitrary data—not just tokens—to be transferred across blockchains. Polkadot is a true multi-chain application environment where things like cross-chain registries and cross-chain computation are possible.

Private Blockchain: Private blockchain is developed and maintained by a private organization with authority over the mining process and consensus algorithm. The private organization decides who can join the network and download the nodes.

Proof of Authority: An algorithm used with blockchains that deliver comparatively fast transactions through a consensus mechanism based on identity as a stake.

Proof of Stake: A blockchain consensus mechanism for processing transactions and creating new blocks in a blockchain. A consensus mechanism is a method for validating entries into a distributed database and keeping the database secure. In the case of cryptocurrency, the database is called a blockchain—so the consensus mechanism secures the blockchain.

Protocol: A set of rules governing the format of messages that are exchanged between computers.

Public Blockchain: In a public blockchain, anyone is free to join and participate in the core activities of the blockchain network. Anyone can read, write, and audit the ongoing activities on the public blockchain network, which helps a public blockchain maintain its self-governed nature. The public network operates on an incentivizing scheme that encourages new participants to join and keeps the network agile. Public blockchains offer a precious solution from the point of view of a truly decentralized, democratized, and au its-free operation.

R3 Corda's shared fact: "To establish the architecture for an open, enterprise-grade, shared platform for the immutable recording of financial events and execution of logic".
See: https://www.corda.net/

Recipient: A recipient is at the end of each transaction the one to whom the data or the physical goods should reach.

Relay Chain: The Relay Chain is the central chain used by the Supplain network.

Settlement: The act or state of settling a transaction.

Smart contract: A self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

Splinter's private circuit: Splinter is a privacy-focused platform for distributed applications that provides a blockchain-inspired networking environment for private communication and transactions between organizations.

Stablecoin: Any cryptocurrency designed to have a relatively stable price, typically through being pegged to a commodity or currency or having its supply regulated by an algorithm.

Staking: The process of locking up crypto holdings to obtain rewards or earn interest.

Substrate Blockchain Framework: A framework for building customized blockchains. These blockchains can be run entirely autonomously.

Supply Chain: The entire process of making and selling commercial goods, including every stage from the supply of materials and the manufacture of the goods through to their distribution and sale.

Timestamping: A timestamp is a sequence of characters or encoded information identifying when a specific event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second. Transaction fees: Fees charged by the transaction facilitator.

Validation Rewards and Penalties: The act of giving or slashing tokens to a validator based on their completion of a task.

Validator: Also called a "blockchain verifier," validators are computers that maintain the blockchain's integrity by constantly computing the linkage from the first block to the last.

Decentralized Identifiers (DIDs): DIDs are a new type of identifier that enables verifiable, decentralized digital identity.

Zero-Knowledge Proof: An encryption scheme whereby one party (the prover) can prove the truth of specific information to another party (the verifier) without disclosing any additional information.

References Endnotes:

1. EIP-225: Clique proof-of-authority consensus protocol
https://eips.ethereum.org/EIPS/eip-225

2. PoA implemented by Ethereum clients
https://forum.openzeppelin.com/t/proof-of-authority/3577

3. Consensus Mechanism
https://docs.neo.org/v2/docs/en-us/basic/technology/dbft.html

4. Decentralized Applications (dApps)
https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp

5.Fork (blockchain)
https://en.wikipedia.org/wiki/Fork_(blockchain)

6. PROOF-OF-WORK (POW)
https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/

7. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain
https://www.academia.edu/36593920/PBFT_vs_Proof_of_Authority_Applying_the_CAP_Theorem_to_Permissioned_Blockchain

8. Proof of authority
https://en.wikipedia.org/wiki/Proof_of_authority

9. The Attack of the Clones against Proof-of-Authority
https://www.researchgate.net/publication/331397046_The_Attack_of_the_Clones_against_Proof-of-Authority

10. Exploring Blockchain Technology and Enterprise Resource Planning System: Business and Technical Aspects, Current Problems, and Future Perspectives

https://mdpi-res.com/d_attachment/sustainability/sustainability-14-07633/article_deploy/sustainability-14-07633-v2.pdf?version=1655962066

11. Rocket, T.: Snowflake to Avalanche: A novel metastable consensus protocol family for cryptocurrencies. IPFS425 (2018)

2022/10/13