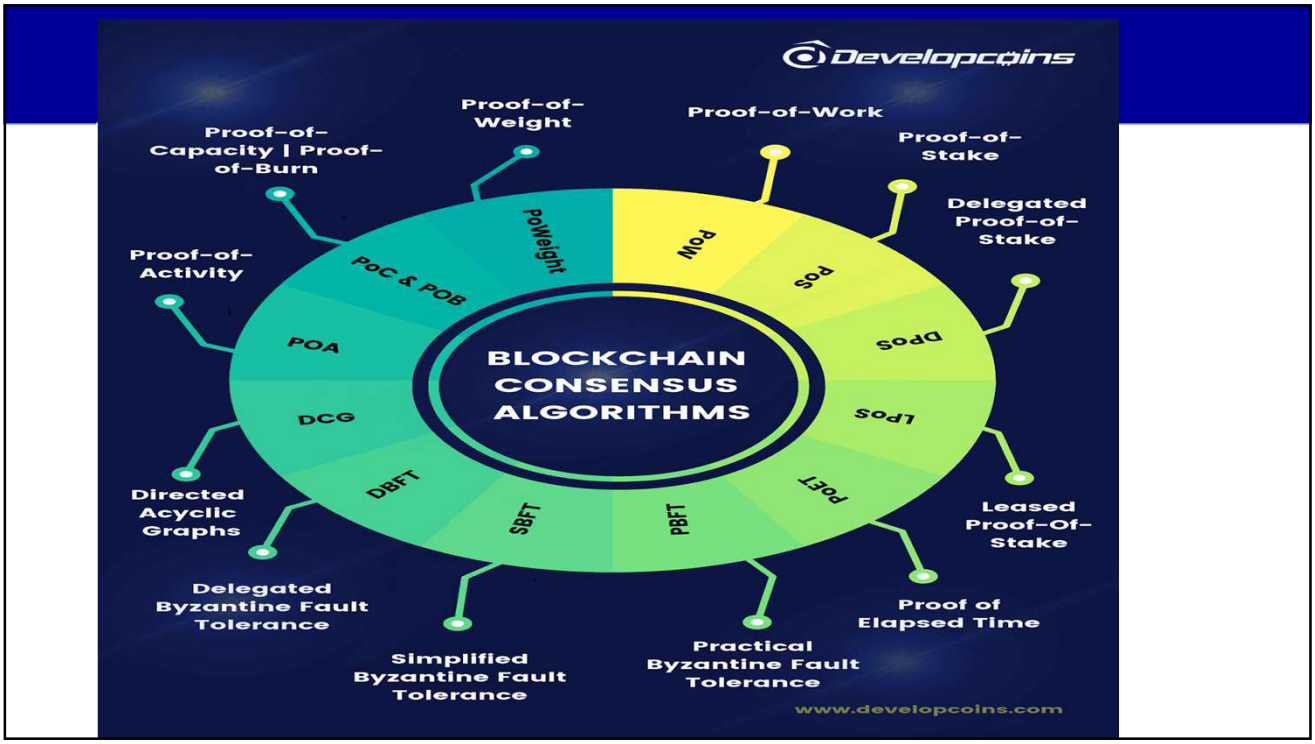
consensus protocols

other promising consensus protocols

- numerous other promising protocols for specific application scenarios
- Majority of them make use of established PoW , PoS and BFT schemes
- many other promising mechanism addresses just one or two components of the block chain consensus protocol
- a consensus method gives the power to nodes (small and designated number of nodes) to validate transactions or interactions with the network and to update



Consensus mechanisms

- In blockchain platforms, consensus mechanisms can be divided into
  - *permissionless* (Bitcoin, Etherium) and
  - *permissioned* (Apla, Etherium Private).
- In a permissioned blockchain, all nodes are pre-authenticated.
  - This allows to use consensus types that provide high transaction rate

Proof of Authority (PoA)

- an alternative to PoW and PoS coined by Ethereum co-founder Gavin Wood
- PoA is a replacement for PoW, which can be used for both public and private chain setups.
- PoA is a special case of PoS scheme
  - This consensus mechanism based on identity as a stake ie. own reputation
  - In this scheme a validator stakes with its identity instead of monetary tokens
- To become fit as a PoA validator in the consensus group,
  - a participant build up its authority for which he needs to go through a mandatory certification process
- Proving authority generally involves
  - having the unique identity verified formally,
  - demonstrating the ability to contribute consistently to the consensus and
  - making all certification documents publicly available

Proof of Authority (PoA)

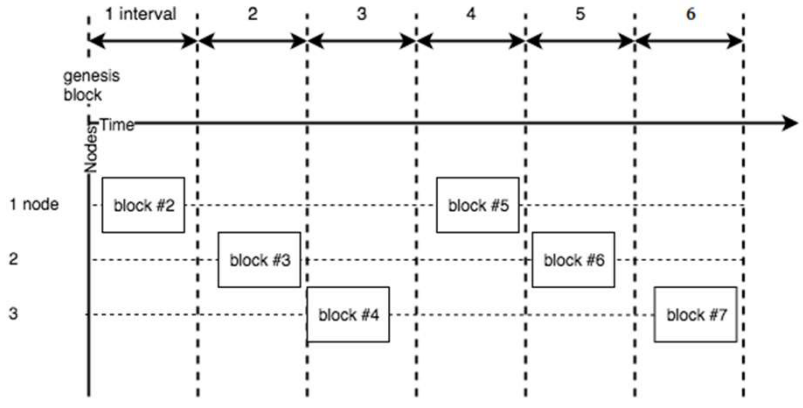
- There is no mining involved to secure the network with PoA,
  - relies on trusted 'Validators' to ensure that valid transactions are added to blocks, processed and executed by the Ethereum Virtual Machine (EVM) faithfully
- consensus group should be stable and small in size, and
- publicly scrutinized so that users can entrust the consensus group for reliable transaction processing and blockchain curation
- In case a validator shows incompetence in such tasks or misbehaves,
  - it will be discredited by users and peer validators
- deployed in Ethereum's Rinkeby (2017) and ethereum testnet- Kovan (2017), and POA Network (2018)
- Other most notable platforms using PoA are VeChain, Bitgert, Palm Network and Xodex
- it provides high performance and fault tolerance, High transaction validation rate, limited number of block validators makes it a scalable system

- **In Apla** blockchain platform; 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.
- To determines the current *leader node*, a node that must generate a new block at the current time may be using

```
cur_leader = ((cur_time – First_bloc_time) / step) % nodes
```

new blocks generation in Apla

- 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.



PoA's Security analysis

- It's small but trusted consensus group features makes it a good example of trading decentralization for security and performance
- In PoA consensus, the 51% attack requires an attacker to obtain control over 51% of network nodes.
  - Obtaining control of the nodes in a permissioned blockchain network is much harder than obtaining computational power as in PoW
- fault tolerance of a PoA depends onconsensus protocol used by the consensus group
  - BFT protocols with 1/3 fault tolerance threshold, Nakamoto-style protocols(such as Parity's AuthorityRound (AuRa)) can also be used to tolerate up to 50% of conspiring validators
- Denial-of-service attacks:
  - attacker may sends a large number of transactions and blocks to a targeted network node in an attempt to disrupt its operation and make it unavailable.
  - To defend DoS : Grant block generation rights only to nodes that can withstand DoS attacks.
    - exclude from validators node list, If a node is unavailable for a certain period
- To prevent validators from collusion
  - they are required to operate independently
  - constantly monitored by users.

Proof of Elapsed Time (PoET)

- developed by Intel Corporation(2016) which
  - enables permissioned blockchain networks to determine block winners and mining right
- consensus mechanisms are based on Byzantine Fault Tolerance
  - primarily focus on reducing the energy inefficiencies associated with proof of work's mining intensive process.
- PoET is now the consensus model of choice for **Hyperledger Sawtooth's** modular framework and
  - a popular tool for implementing and experimenting with distributed ledger systems.

Proof of Elapsed Time (PoET)

- PoET simulates the time that would be consumed by PoW mining instead of undergoing the hashing intensive mining
- In this every node randomly backs off for an exponentially distributed period of time before announcing its block
- For ensuring that the local time truly elapses,
  - PoET requires the back-off mechanism to be carried out in a trusted execution environment (TEE),
    - TEE is an isolated memory area that provides integrity and confidentiality to the program running inside, against a compromised hosting platform
    - Specially, the program enclosed in a TEE is called an "enclave".

Proof of Elapsed Time (PoET)

- This algorithm is for **permissioned** blockchain networks
  - Thus, a special verification is required from a node when it tries to *join* the network.
  - This verification is achieved using Intel's **Software Guard Extension (SGX)** technology (introduced in 2015)
  - **SGX** creates an *attestation* for a piece of code and protects the code from external access.
- Intel SGX and Arm TrustZone are the two major TEE solutions.
- Among other utilities, TEE provides an integrity proof of enclave program through remote attestation,
  - which essentially helps the network establish trust on consensus participants.

Working of PoET: Hyperledger Sawtooth's

Works in two phases for every participating node i:

Phase -1: TEE setup:

- Node i first obtains the PoET protocol program from a trusted source and instantiates the program on its SGX machine wherein the random back-off routine runs inside an enclave.
- The trusted program generates a signing **key pair (PKi ,Ski)** for node i and
  - starts the attestation process which results in sending an attestation report to the network.
- The attestation report contains the public key **PKi** and the enclave measurement signed by the Intel Enhanced Privacy Identification (EPID) private key inside the enclave.
- Other nodes in the network will validate the **node i's** hardware authenticity through Intel Attestation Service (IAS) and validate the attestation report before accepting **node i**

Working of PoET: Hyperledger Sawtooth's

Phase-2: Participating in consensus:

- The consensus process is similar to Nakamoto except for block generation and validation.
- For each block cycle, node i waits for a period dictated by the random back-off routine running in the enclave before producing a new block.
- The enclave then generates a certificate of back-off completion signed by node i's private key SKi which is broadcast to the network along with the new block.
- Upon receipt of the new block, other nodes validate the block content and the back-off completion certificate with node i's public key PKi .
- A block shall be appended to the blockchain if it passes validation and the finalization rule.

PoET

- PoET was initially proposed to substitute the PoW for block proposal without touching on the longest-chain rule,
- However, the usage of hardware-assisted public key cryptography actually enables the use of more efficient BFT algorithms for block finalization.
- The hybrid **PoET-BFT** idea is currently used by Sawtooth PBFT which is a sub-project of Hyperledger Sawtooth

Security analysis :PoET

- tolerate up to 50% TEE nodes being malicious.
  - Since every TEE node runs the same random back-off routine in its enclave,
- but a player can shorten its expected back-off time by running multiple TEE nodes,
    - which is susceptible to Sybil attacks.
- If more than 50% of TEE devices collude or are controlled by an attacker,
  - they can ultimately win the block race and keep extending the malicious chain.
- Therefore, PoET is most suited for permissioned blockchains, where every participant is authenticated and runs one TEE node.

Security analysis :PoET

- For Hyperledger Sawtooth,
  - Intel is the sole TEE hardware vendor and attestation service provider,
    - which poses a single point of risk to the network.
  - The validity of remote attestation depends on the integrity of SGX implementation and the availability of Intel Attestation Service(IAS)
  - posing a security threat at the hardware level
    - Recent attacks such as cache attacks ,
      - Foreshadow and Foreshadow-NG have demonstrated the ability to extract the Enhanced Privacy ID (EPID) protocal private key from hardware exploiting side channels and speculative execution
    - Enhanced Privacy ID (EPID) protocol allows systems to be identified as genuine SGX platforms without revealing their identity in the process

Proof of TEE-Stake (PoTS)

- another protocol in combination with TEE and blockchain consensus [2019]
- A PoTS node i follows the same setup procedure as in PoET
  - to bootstrap a TEE enclave,
  - generate the signing key pair (SKi ,Pki), and
  - attest the setup to the network.
- Instead of simulating the would-be elapsed time of PoW mining,
  - the enclave program of PoTS is similar to Algorand's cryptographic sortition scheme that randomly selects a committee according to the stake distribution
- PoTS additionally uses cryptographic techniques also to prevent grinding attacks and protect against posterior corruption

Proof of TEE-Stake (PoTS)

- Every node in the committee is eligible to propose a new block for the coming block cycle.
- To prove the block proposal eligibility to the network,
  - the block also includes the eligibility proof signature ,σ^{ep}_{SKi} ,
    - which is produced by the enclave program of the block generating node i.
  - Once other nodes receive this block, they validate the block content as well as signature σ^{ep}_{Ski} using node i's public key PKi .
  - The longest-chain rule is then used to determine whether to accept this block into the blockchain or not

Security analysis: PoTS

- It can tolerate up to 50% of all stake value at TEE nodes being maliciously controlled, the same as the fault tolerance of chain-based or committee based PoS.
- the incorporation of staking gives PoTS higher robustness against Sybil attacks compared to PoET
  - which implies its applicability to permission less blockchains .
- Furthermore, the security offered by public key cryptography and TEE certified execution of committee selection helps PoTS counter the stake-bleeding and stake-grinding attack.
- The single point of risk in TEE hardware vendor still exists

Proof of Retrievability (PoR)

- PoR was originally proposed as a cryptographic building block for a semi-trusted distributed archiving system in 2007
- The core feature of PoR is to allow a file owner to check if its online files or file fragments are securely stored and retrievable through a challenge-response protocol.
- The retrievability of a target file F at a remote node ni can prove ni indeed spends the required amount of storage resources on F.
- Due to the space requirement behind retrievability, also known as **proof of space.**
- similar to proofs of work (PoW), except that instead of computation, space is used to earn cryptocurrency.

Proof of Retrievability (PoR)

- In the role of a consensus protocol, PoR was first used by the cryptocurrency Permacoin, proposed by Miller et al. in 2014.
- It was designed as a mining-free alternative to PoW.
- First, a central dealer publishes a target dataset F and computes the digest of F (the Merkle hash tree root of all segments of F).
- Then each participant stores some random segments of F per its storage capability, and computes the digest of these segments.
- For every block cycle, the dealer initiates a lottery game with a random puzzle.
- Then every participant derives a lottery ticket consisting of a fixed number of PoR challenges from its locally stored segments, public key, and the puzzle.
- Participants with more segments stored have higher probability of winning the lottery and thus being eligible to generate a block.
- All PoR challenges are stored in the new block and verified by the whole network.

- Permacoin also implements a signature scheme to discourage participants from outsourcing the storage task.
- Aside from PoR, Permacoin inherits Bitcoin for other consensus components.
- PoR has two economical advantages over PoW
  - First, file storage consumes far less energy than brute-force mining, and storage space as a resource can be recycled.
  - Second, PoR can be re-purposed for meaningful storage tasks.
    - For example the target dataset can be some extremely large but useful public dataset.
  - In fact, the latter advantage is not seen in any other proof-of-X schemes

Security analysis

- the block winning rate of a participant is proportional to its local storage space, hence
  - PoR can tolerate up to 50% of gross storage being held up by the malicious party.
- Although this still can trigger an arm race of storage resources, it downplays the efficacy of ASICs (application-specific integrated circuit) and encourages a wider variety of mining participants.
- Meanwhile, the 50% threshold depends on the job of the randomness of the central dealer.
- To ensure the diversity of lottery tickets across all participants and increase the randomness of the lottery, the target dataset should be large enough so that participants stores almost non-overlapping segments.
- This assumption can be undermined if the dealer chooses a dataset not large enough or deliberately distributes overlapped segments.

Ripple Consensus Protocol/Algorithm (RCPA)

- proposed as the underlying protocol for Ripple in 2014
  - a global payment and gross settlement network operated by the Ripple company
- Unlike public blockchains(such as Bitcoin and Ethereum), Ripple treats individual transactions as the ledger's atomic items, similar to a transaction log
- In Ripple network, only validator nodes can participate in consensus
- Nodes collect transactions from clients and propose them to peer nodes for consensus.

RCPA (contd…)

- In initialization, every node establishes a unique node list (UNL)
  - which identifies the nodes it can trust and directly exchange messages with.
- A UNL relationship is reciprocal.
- We call a group of nodes that are fully connected by UNL relationships a UNL clique

Algorithm : RPCA (validator node)

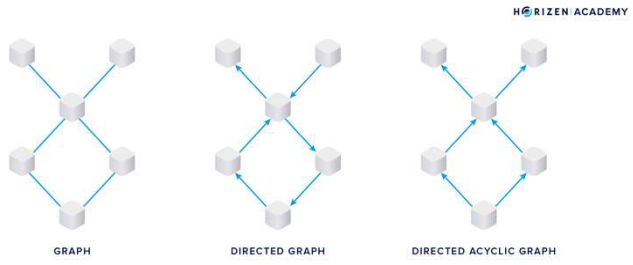
```
1  Joining Ripple network as a validator;
     /* Main loop */
2   for new epoch do
3          Collect valid transactions (new or leftover from previous epochs) ⇒ CandidateSet;
4       for r = 1 → MaxRound do
5           Broadcast CandidateSet to UNL peers;
6           After receiving transactions from UNL peers, add
                them to CandidateSet and broadcast a vote on the veracity (yes/no) of every transaction;
7         After receiving votes from UNL peers, discard transactions from CandidateSet whose
              yes- votes fall short of a threshold T Hr
                 (T HMaxRound = 80%);
8        end
9      The remaining transactions in CandidateSet are  accepted into the ledger;
10 end
```

Security analysis RCPA

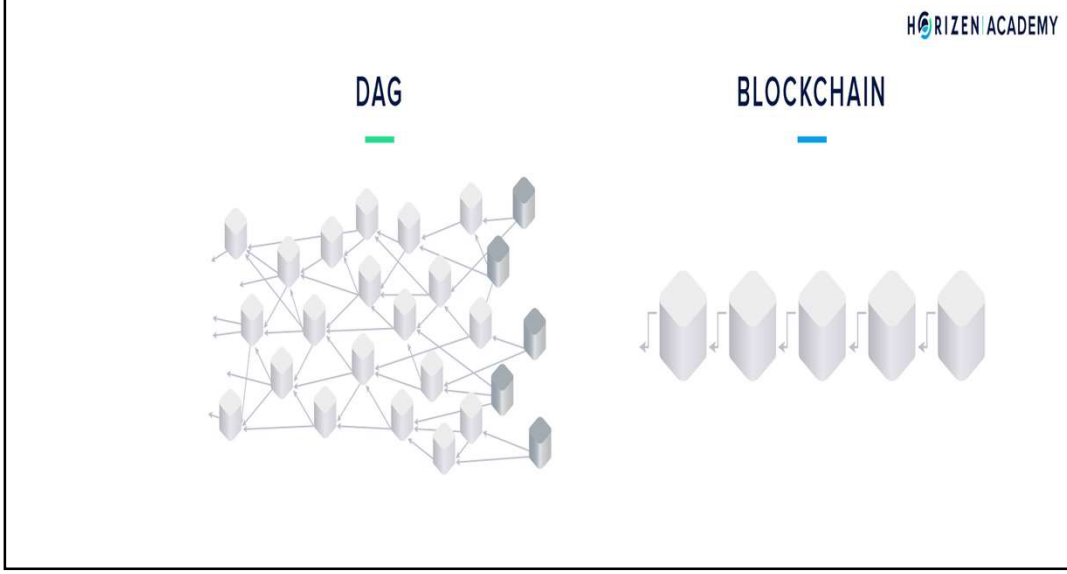
- RCPA imitates a relaxed DLS protocol with an artificial BFT bound of 1/5.
- It further requires no more than 1/5 of nodes are faulty in every UNL clique in order to ensure overall network consensus.
- Compared to PBFT that achieves 1/3 Byzantine fault tolerance with $O(N^2)$ message complexity in a fully connected network,
- RPCA's 1/5 fault tolerance bound trades for a lower connectivity requirement and thus lower message complexity per block cycle, which is $O(MK^2) = O(NK)$ where K is the clique size and M = N/K is the number of cliques.
- Therefore Ripple demonstrates the possibility of trading fault tolerance for better performance when a certain level of trust is assumed.
- down side, of RCPA's multi-round broadcast scheme among a UNL clique and the quick convergence of votes require high synchrony among clique members.
- This impairs Ripple's decentralization capability in practical settings
- Ripple's current customers are primarily established corporations and financial institutions.
  - Possible reasons include the above-mentioned synchrony requirement and that the 1/5 fault tolerance can be too restrictive for low-trust environment

- One of the major challenges in making blockchain technology ready for mass adoption is scalability.
- most blockchains can only handle a handful of transactions per second, while payment networks like VISA support several thousand transactions per second.
- There are many different methods to scale blockchains, and Horizen is evaluating two of these possible solutions.
  - One of them is building a Block-DAG protocol, the other is enabling sidechains

- DAG stands for Directed Acyclic Graph.
- a simple graph, made up of nodes and edges connecting the nodes.
- In a directed graph, each connection has a direction, indicated by arrows.
- A directed acyclic graph (DAG) does not allow circular relationships of nodes like the one you can see in the bottom part of the directed graph



- A block in the Block-DAG is similar to a block in a blockchain.
- A Block in a DAG also has a block header and contains a number of transactions, just as a block in the blockchain does.
- Miners mine the block, ie. they attempt to solve an intensive computational task based on choosing an initial random number.
- The miner that solves the task first gets to create the next block in the chain, therefore deciding the order of transactions.
- This method of the network coming to a consensus on the order of transactions is the same that is used by most blockchains,suhc as PoW
- difference is that each block in the blockchain always references the previous block, while a block in the Block-DAG can reference multiple preceding blocks. Another adjustment is needed to establish a final order within the blocks of a DAG.



BlockDAG-based Consensus Protocols

- increasing interests in non-linear ledger structures for the aim of better performance,
  - among which directed acyclic graph (DAG) has received the most attention.
- Block-DAG uses the **same consensus mechanism as a blockchain to agree on the order of events**, but uses a different structure to connect the individual blocks.
- Consensus schemes with DAG ledger structure mark a significant divergence from Nakamoto's blockchain design.
- Their key insight is that transaction throughput should not be limited by a restrictive consensus object, such as a linearly growing chain of blocks with fixed time intervals.
- Instead, the inflow of transactions should drive the ledger expansion.
- two types of DAG ledgers:
  - block-based DAG (blockDAG) and transaction-based DAG (txDAG).

- In a blockDAG, every vertex contains a collection of transactions which is similar to the block concept in blockchain.
- What sets blockDAG apart from blockchain is that every block can be hash-pointed to multiple parent blocks.
- This leads to a situation that every new block can be appended to the DAG with considerable flexibility on how many and which parents to point to.
- This parent-selecting difficulty problem is commonly regarded as the major challenge for DAG-based consensus schemes and
- pertains to the system's transaction processing capability
- and security against Sybil and doublespending attacks.
- Two blockDAG schemes,
  - SPECTRE and PHANTOM, with a focus on parent-selection mechanism.

SPECTRE

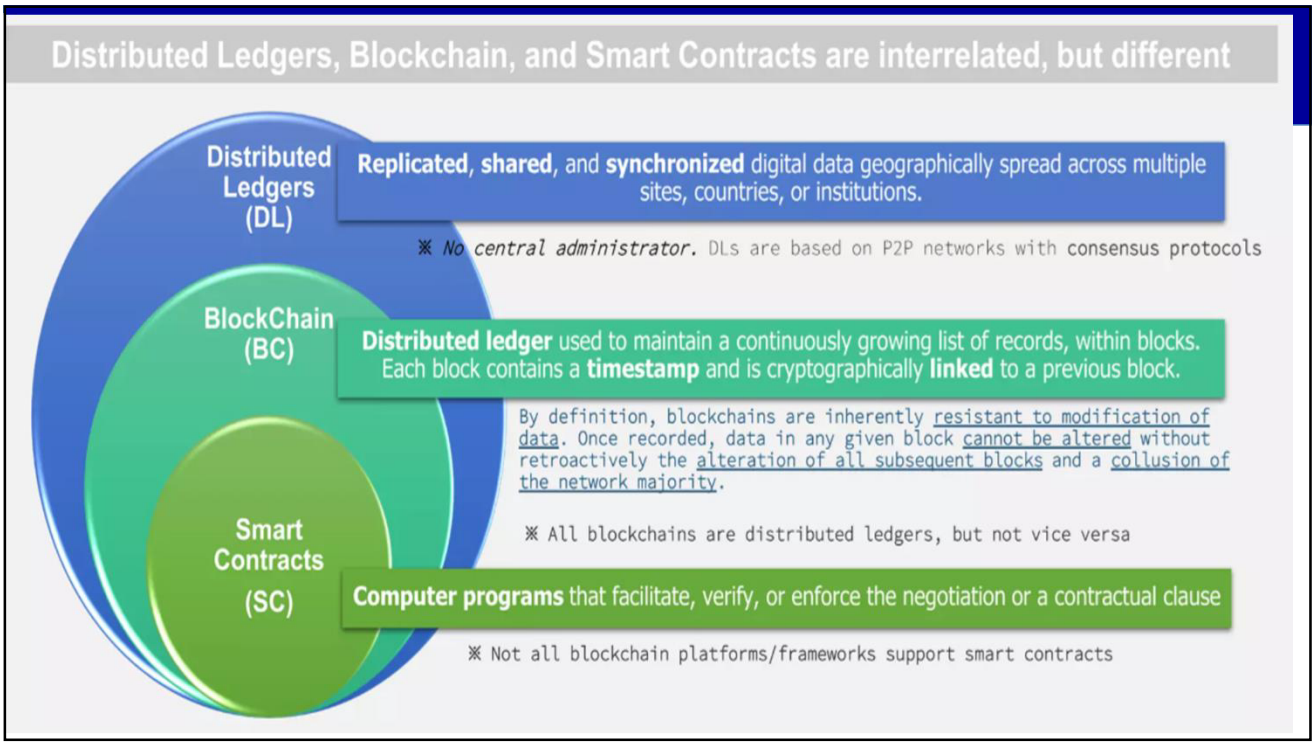
- Proposed in 2016
- SPECTRE is one of the first well-documented blockDAG proposals.
- SPECTRE requires any node who wants to mine a new block to find
  - all blocks of zero in-degree (i.e. “tips”) in the DAG and
  - hash-point the new block header to these tips before starting the PoW mining for the new block.
- The node broadcasts the newly mined block to the network.
- Every node initiates a recursive voting procedure to determine the order of any two blocks in the current DAG.
- This recursive procedure eventually results in a pairwise ordering over the blockDAG.
- Every new block should be incremental to the past pairwise ordering effort.
- This pairwise ordering scheme essentially allows SPECTRE to decide between two conflicting blocks (i.e. containing transactions that spend the same UXTO).

PHANTOM

- a concurrent blockDAG proposal of SPECTRE by the same authors.
- One notable weakness of SPECTRE is that
  - the pairwise ordering of blocks may not extend to a fully linear ordering.
  - Which leads to SPECTRE’s weak liveness (i.e. only supports naturally chronological transactions)
  - an increased risk of balancing attacks in that conflicts may not be solved.
- In contrast, PHANTOM realizes fully linear ordering of transactions and blocks in the DAG via the following algorithm.
- Every node searches the blockDAG for the largest k-cluster of blocks.
- k denotes the node degree in the cluster, and is a predefined security parameter that rarely k or more honest blocks are created simultaneously.
- The k-cluster is regarded as honest and all blocks within are linearly ordered.
- The transactions covered by the cluster are then validated in the new order.
- Notably, the largest 0-cluster case is equivalent to the longest-chain rule of Nakamoto consensus.
- PHANTOM can be utilized alongside SPECTRE for more flexible consensus performance, as the two ordering schemes are complimentary to each other.

Security analysis

- SPECTRE and PHANTOM inherit other protocol components from Nakamoto's, including PoW-based block proposal, gossip-based information propagation, validity check on PoW and transactions.
- Therefore, the two blockDAG based schemes can tolerate up to 50% of maliciously controlled computing power.
- On the performance side, blockDAG-based schemes can theoretically support arbitrary throughput capacity, only to be capped by network bandwidth and nodes' processing speed.
- On the downside, the increased parent-selection flexibility may expose more attack surfaces to adaptive attackers (such as the balancing attack against SPECTRE), which is still an ongoing research topic.
- Alternatively, BlockDAG can be designed to incorporate a specific blockchain as a main chain, reflecting a similar idea as the GHOST rule.
- Conflux, a recent blockDAG scheme proposed by Li et , resorts to the GHOST rule for the finalization of a pivot chain, which is used as the reference for partitioning the blockDAG into chronological order.
- This scheme yields high transaction throughput but also higher confirmation latency



Hyperledger

- Hyperledger is an open-source blockchain platform, hosted by the Linux Foundation, focused on creating enterprise-grade blockchain solutions.
- A distributed ledger technology that provides an efficient and secure infrastructure for the issuance and exchange of digital assets

Hyperledger Project

Hyperledger is an open source and collaborative effort created in 2015 to advance cross-industry blockchain technologies

THE LINUX FOUNDATION

HYPERLEDGER PROJECT

□ A global collaboration that includes (global) leaders in various areas :