PoCW Vision Document

Proof of Causal Work (PoCW) is a consensus mechanism designed to incorporate causal ordering and mutations within a decentralized knowledge graph. Unlike traditional Proof of Work (PoW), where computational effort is spent on solving arbitrary cryptographic puzzles, PoCW focuses on validating and ordering transactions based on their causal relationships within a knowledge graph. This ensures that the system not only achieves consensus but also maintains a logically consistent and verifiable history of data mutations.

PoCW addresses several critical limitations inherent in traditional consensus mechanisms like PoW and Proof of Stake (PoS). In PoW, the reliance on computational power to solve arbitrary puzzles leads to significant energy consumption and environmental concerns, while also creating a barrier to entry due to the need for specialized hardware. PoS, on the other hand, mitigates energy usage but introduces risks of centralization, as wealthier participants with larger stakes gain disproportionate influence over the network. Both mechanisms often prioritize transaction ordering based on temporal or economic factors, which can overlook the logical dependencies and causal relationships between transactions.

PoCW, by contrast, emphasizes the validation and ordering of transactions based on their causal relationships within a Decentralized Knowledge Graph (DKG), which serves as the foundational structure for the system. This approach not only reduces energy consumption by focusing on meaningful computational effort but also ensures a more robust and logically consistent history of data mutations. By aligning consensus with the inherent structure of the data, PoCW enhances the integrity, scalability, and usability of decentralized systems, making it particularly suited for applications requiring verifiable and context-aware transaction histories, such as supply chain tracking, collaborative knowledge bases, and decentralized AI training.

At the core DKG represents entities, relationships, and their evolution over time, with nodes symbolizing data points or entities and edges capturing the relationships or communication between them, altogether it also serves as a framework for attribution based on the different actions by the entities. Unlike traditional centralized systems, the knowledge graph in PoCW is decentralized, meaning no single entity has control over its structure or updates. This decentralization ensures transparency, resilience, and trustlessness, making it ideal for applications requiring collaborative and verifiable data management.

DKGs powered by PoCW are particularly valuable in collaborative research and knowledge sharing, particularly in fields like scientific discovery and decentralized AI training. In the case of scientific discoveries, researchers often rely on vast amounts of interconnected communication data, where the provenance and causal relationships between data points are crucial. A DKG can represent hypotheses, experiments, results, and citations as nodes and edges, ensuring that contributions are accurately attributed and that the evolution of knowledge is logically consistent. If a new scientific discovery builds upon prior research or a collaboration then the

DKG can trace the causal chain of ideas, ensuring proper credit and reducing the risk of misinformation.

In the case of a decentralized AI training network where researchers, organizations, and individuals contribute datasets or model updates to improve a shared AI model. Each dataset, model version, or update can be represented as a node in the DKG, while edges capture the causal relationships between them—such as how one model iteration builds upon another or how a specific dataset influenced a particular improvement. This structure ensures that every contribution is traceable and verifiable, addressing key challenges like data provenance and attribution. If a model update introduces a bias or error, the DKG allows participants to trace back through the causal chain to identify the source of the issue, enabling corrective actions while maintaining trust in the system.

1. Decentralized Knowledge Graph

The decentralized knowledge graph serves as the backbone of the PoCW system, providing a distributed, tamper-resistant data structure that represents entities, relationships, and their evolution over time. The graph is cryptographically secured using verifiable logical clocks, ensuring that all changes are causally ordered and immutable, which is critical for maintaining logical consistency and traceability in decentralized systems. Unlike traditional centralized databases, the DKG is maintained collectively by network participants, ensuring transparency, resilience, and trustlessness. This structure enables precise causal ordering, where dependencies between actions—such as model updates in decentralized AI training, intellectual property, and royalty management, scientific research—are explicitly recorded, ensuring a verifiable and logically consistent history. Additionally, the DKG facilitates contribution tracking, allowing stakeholders to attribute actions and contributions accurately, which is essential for fairness, accountability, and incentivization in decentralized networks in use cases such as DeSi, governance protocols, user reputation management, etc. The following are the key components that are foundational to a distributed knowledge graph:

a. **Nodes:** Represent entities or identity-based data points. For example, in a DeSi agent use case, nodes could represent AI-powered agents catered to serve users with science-related ML inferences along with p2p communication features.
b. **Edges:** Represent relationships or communication between nodes. In the same DeSi example, an edge could represent the collaboration among scientific collaborators.
c. **Attributes:** Both nodes and edges can have attributes that store additional metadata. For instance, a DeSi agent entity might have attributes like "agent ID" or "stake," while an edge might have attributes like "timestamp" or "transaction ID."

The DKG is stored on the same device as the base chain, enabling seamless cross-referencing of actions. In the initial version, agentic frameworks are equipped with connectivity endpoints to ensure that their p2p actions are recorded within the DKG. This integration allows the DKG to serve as a comprehensive ledger of interactions, contributions, and causal relationships.

2. Causal Ordering and Verifiable Logical Clock (VLC)

Causal ordering is a critical component of PoCW, ensuring that communications are correctly attributed and adhere to their logical dependencies. Using the causal ordering of p2p knowledge, further processing of such graph data can be done correctly and eventually structured as a block transaction. This is achieved using VLCs which assign logical timestamps to events based on the sequence of interactions between nodes. Each node maintains a counter (Lamport ID) that increments with every event it generates or receives. When a node sends a message, it includes its current Lamport timestamp, and the receiving node updates its own timestamp to be greater than the received timestamp, ensuring causality is preserved. For example, if Event A causally precedes Event B, the logical timestamp of A will be less than that of B. This mechanism ensures that the DKG captures the true sequence of events, even in a distributed system where physical clocks may not be synchronized.

PoCW leverages the Decaying Onion Bloom Clock (DOBC), a novel logical clock construct to achieve scalability and fault tolerance. DOBC uses layers of Bloom filters to record state transition history, with recent transitions stored in the top layer and older transitions compressed into lower layers. This allows DOBC to probabilistically determine causality between objects with a depth difference of at most *k*, ensuring accurate causality inference for recent histories while gracefully degrading accuracy for distant past events. DOBC also supports merging clocks from different objects, enabling the DKG to maintain a consistent and verifiable history of data mutations. By combining VLCs and DOBC, PoCW provides a robust framework for maintaining causal ordering and ensuring the integrity of decentralized systems, where the proof generated by VLCs validates the relation between a subgraph.

3. Mutations on the Graph

Mutations are the fundamental operations that drive the evolution of the DKG. They represent changes to the graph's structure, such as adding new nodes, updating relationships, or deleting obsolete data. The DKG's data structure is intentionally minimal and loosely structured, providing significant flexibility for agents to communicate and interact as they see fit, while adhering to a very basic framework. This flexibility allows applications to establish Turing-complete logic on top of the DKG, enabling complex behaviors and interactions. Within a block, the DKG graph data, mutations, and transactions coexist, and semantically, the data within DKG nodes and transactions must be valid to ensure consistency between the graph's state and the transactions that reference it. This is particularly critical during block validation, where nodes programmatically verify that the semantics of DKG mutations are accurately reflected in the transactions, ensuring both structural and logical integrity.

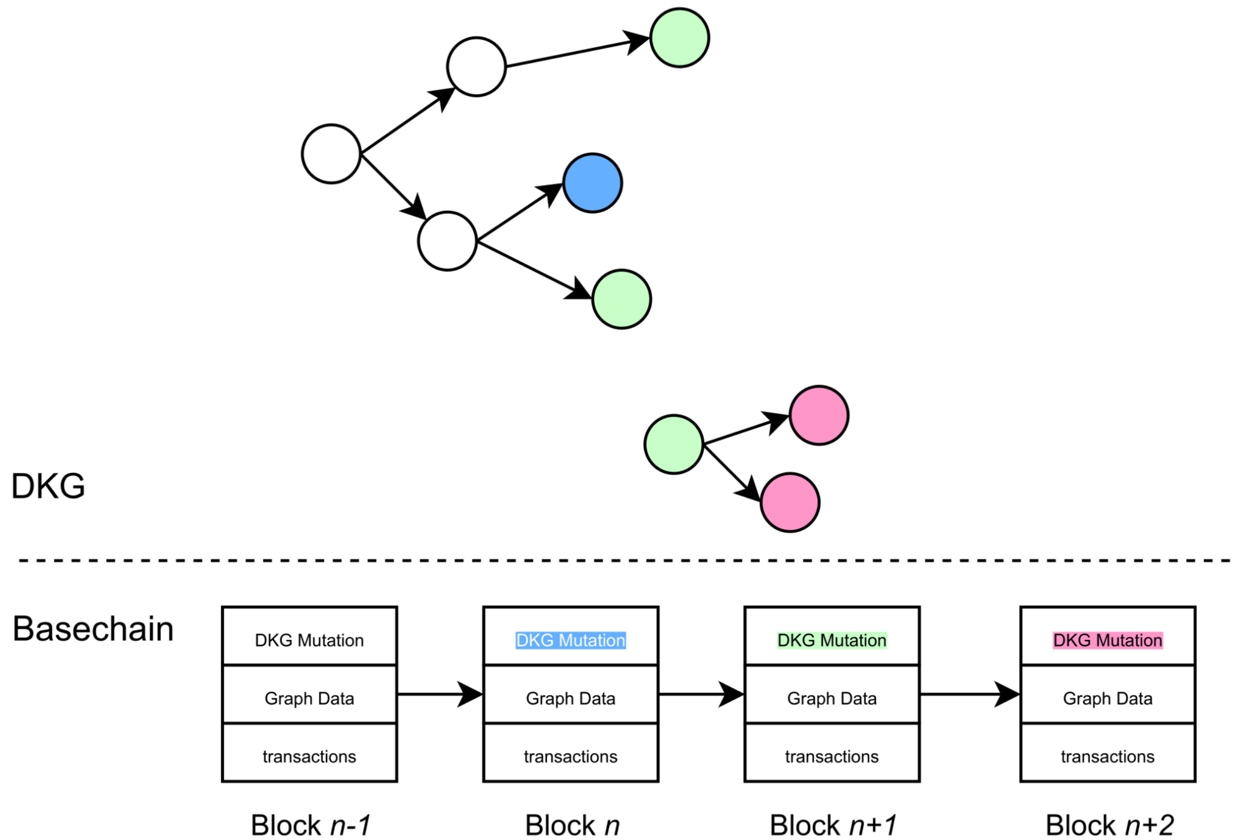
To achieve this, smart contracts can be employed as a solution. Smart contracts can encode the rules and logic for validating DKG mutations and their corresponding transactions, ensuring that only semantically correct and consistent changes are accepted. When a new block is proposed, the smart contract automatically verifies that the mutations adhere to predefined semantic rules and that the transactions align with the graph's state. This approach not only enforces integrity but also maintains the DKG's flexibility, allowing agents to communicate and interact freely within the loosely structured framework. Additionally, smart contracts can facilitate the merging of forks by defining rules for resolving conflicts, further enhancing the system's resilience. By leveraging smart contracts, the PoCW system strikes a balance between flexibility and rigor, enabling decentralized agents to operate dynamically while ensuring the system's overall coherence and verifiability.

4. Proof of Causal Work (PoCW)

The Proof of Causal Work is the consensus mechanism that ties everything together. It ensures that the computational work performed by validators is tied to the logical structure of the knowledge graph, rather than arbitrary cryptographic puzzles. The workflow of PoCW is as follows:

a. **Sub-Graph Selection:** In this step, the block producer picks a sub-graph that it considers causally ordered. It can either be based on the just previous block or any block in the past (it will be a fork in this case).
b. **Causal Validation:** The validator verifies the causal ordering of the DKG using the VLC mechanism. The output of this is a DKG state mutation along with the subgraph nodes.
c. **Block Packing:** PoCW along with transactions provides a cohesion between p2p communication done over DKG and making processed decisions on such graph mutation.

As illustrated in the figure below, decentralized knowledge subgraphs undergo progressive mutations, with new graph nodes and their corresponding VLC proofs being packed into blocks. These blocks also include transactions that are logically consistent with the causal graph data. Notably, two independent subgraphs can be causally ordered, and it is possible to merge them after a conflict check, ensuring coherence and integrity across the decentralized knowledge graph.



5. Block Structure

The block structure in PoCW is designed to encapsulate all the components discussed above, ensuring that each block is secure, consistent, and verifiable. Block structure comprises of the following key components:

a. **Header:** Contains metadata such as the block hash, previous block hash, and timestamp.
b. **VLC Proof:** A combination of graph mutation along with a subset of graph nodes that are newly causaled.
c. **Transactions:** A set of transactions that are results of the processing based on the causal relationship of the communication.

6. Base Chain

The base chain is an immutable ledger on which blocks containing mutations, proofs of causal ordering, and processed transactions based on the DKG mutation are recorded. It provides the foundational layer for the PoCW system, ensuring that all changes to the DKG are securely stored and verifiable. Agents use the chain to track past actions and the current state, enabling a transparent and auditable history of data mutations.

A key characteristic of the PoCW system is the absence of an objective function to determine which DKG to extend, making forks common. The decision on which DKG to extend depends on the subjective valuation of validators, reflecting their individual preferences or incentives. Over time, certain DKGs gain popularity, leading to intersubjective consensus as validators converge on a preferred state. Additionally, the DKG supports the merging of multiple forks, allowing divergent paths to reconcile and ensuring that the system can recover from temporary divergences while maintaining a coherent and consistent history. This flexibility, combined with the immutability of the base chain, makes PoCW highly resilient and adaptable to dynamic, decentralized environments. The Hetu chain, a DAG-based high-throughput chain, is particularly well-suited for this purpose due to its scalability and efficiency in handling concurrent transactions.