Hela Whitepaper

*Institute of High Performance Computing, A*STAR, Singapore*
Hela Labs

Abstract

This whitepaper introduces Hela, a next-generation Layer 1 blockchain system designed to address the limitations of existing public blockchain technologies in supporting a broader range of applications across a broad range of industries and sectors. We identify four key problems with existing public blockchain technologies: data fragmentation and poor interoperability, inadequate confidentiality mechanisms, lack of identity management, and unstable transaction fees due to token price volatility.

Hela proposes a modular architecture with an integration layer for enhanced interoperability and to mitigate data fragmentation. It offers flexible, auditable confidentiality via the trusted execution environment (TEE) and encryption mechanisms, combined with a community-driven regulatory mechanism. Hela also introduces a multi-level decentralized identity (DID) management protocol and proposes the use of stable coins for transaction fee settlement to address price volatility.

These design features enable Hela to potentially expand the application of blockchain technology to more varied, real-world scenarios, while addressing issues of data fragmentation, privacy, identity management, and transaction fee stability. In doing so, Hela seeks to bring blockchain technology closer to the everyday user, bridging the gap between the current state of public blockchain and a more universally applicable blockchain technology.

1 Introduction

Blockchain technology, emerging in the wake of financial uncertainties in 2008, fundamentally transforms the way we perceive trust and transaction validation in digital networks. At the heart of this revolution is its ability to facilitate trustless, peer-to-peer transactions, eliminating the necessity for intermediaries. This is achieved through a combination of cryptography and game theory, enabling distant, untrusting parties to reliably transfer value. The innovation does not stop at mere transactions; the underlying blockchain—a distributed, public transaction ledger—provides an open platform for any participant to verify and settle transactions in a transparent manner. Furthermore, this system is underpinned by rules that incentivize legitimate transaction propagation, reconcile conflicting information, and foster consensus about the ledger's true state in a decentralized environment. From an economic standpoint, blockchains offer many benefits of centralized platforms, such as network effects, without the pitfalls of increased market power, data control, or single points of failure.

Blockchain, in essence, is a decentralized distributed ledger maintained by a plethora of P2P nodes. First introduced by Satoshi Nakamoto in 2008 with Bitcoin, it showcased a groundbreaking approach to value transfer, emphasizing cryptographic proof over trust [67]. It has since matured with projects like Ethereum [21]. While blockchain technology has advanced over the past decade, its application in public domains remains restricted. Predominantly, public blockchains serve financial domains, including cryptocurrencies [38, 54, 69, 82, 94], decentralized finance (DeFi) [75, 84, 90], non-fungible tokens (NFT) [14, 68, 88], GameFi [32, 50, 70], etc. [22, 30, 41, 60, 65, 66]. As the scope broadens to diverse sectors like governance, services, and agriculture, many existing public blockchain projects struggle to offer comprehensive support.

What prevents public blockchain technology from leading the way to more pervasive applications? We summarize the reasons as follows. These are also the core problems faced by many public blockchain projects at present.

Insufficient Data Integration and Interoperability. Although the scalability and customizability of blockchains has been enhanced with the introduction of various modular blockchain systems [21, 53, 89] and Layer 2 protocols [35,45,46], these enhancements have been accompanied by increasing data fragmentation and poor interoperability. Specifically, some DApps (decentralized application) are now deployed in multiple *domains* (e.g., Layer 1, Layer 2, subchain, runtime) [36, 59, 63]. For example, just one decentralized exchange (DEX), Uniswap [9], is now deployed in three Layer 2 networks (i.e., Optimism [7], Arbitrum [45], Polygon [46] and on Ethereum's Layer 1 network. This has created a serious liquidity segmentation problem for Uniswap [55]. More importantly, users' assets are also dispersed across domains in order to use the corresponding services. Users as well as smart contracts often have to rely on insufficiently reliable cross-domain protocols (e.g., bridges) [17, 61, 76] to interact across different domains. These above factors bring up issues such as usability, security, and efficiency, which hinder the popularity of DApps.

Inadequate Confidentiality Mechanisms. Many existing blockchain protocols lack confidentiality [21, 62, 67, 72, 92]. All transactions can be inspected by anyone with access to the respective blockchain explorer. This is clearly an invasion of user privacy [4]. Other blockchain protocols enforce a consistent level of confidentiality for all transactions [40, 80, 83]. However, this one-size-fits-all approach to privacy protection deprives users of control over their data on the one hand, and is not conducive to data auditing and monitoring by relevant authorities on the other. This makes these platforms easy to turn into a breeding ground for criminals [28, 47, 81].

Lack of Identity Management. In many existing blockchains, users are usually anonymous [13, 39, 96]. This anonymity makes it difficult for many existing blockchain protocols to control the identity of users and poses security issues such as Sybil attacks [95]. In addition, the lack of identity management for users also makes it difficult for blockchain technology to become adoptable in numerous scenarios requiring KYC (Know Your Customer) (e.g., online ticketing, credit lending, etc.) [37] and poses a challenge for regulators to oversee.

Volatile Transaction Fees. In the current blockchain protocols, users need to purchase protocol-specific tokens to pay transaction fees and use the corresponding features. However, the fluctuation of token prices is often very dramatic [10, 11, 18]. This leads to a huge variance in the price of transaction fees for users over time. For example, due to the volatility of Ethereum's ETH price, its transaction fee prices vary by more than 1,000 times at different times [1]. This makes platforms by users planning to settle millions of transactions unadoptable [2].

To address these issues and enable the adoption of blockchain technology across a broader range of industries, we propose Hela, a next-generation Layer 1 blockchain system. Specifically, Hela offers the following:

Modular Architecture with Integration Layer. Hela adopts a modular architecture to provide better customizability and scalability. In addition to the basic consensus layer, execution layer, and storage layer, Hela innovatively proposes an integration layer to solve the problem of data segmentation and poor interoperability. Specifically, the primary purpose of the integration layer is to integrate users assets across domains and to assist the users in performing cross-domain operations (e.g., cross-runtime asset exchange). Through the integration layer, users will not need to physically transfer assets when

operating across runtimes. A secondary feature of the integration layer is that it allows for integration of execution logic across multiple domains to enable more generalized cross-domain interoperability protocols. Based on this functionality, Hela's integration layer enables atomic cross-domain smart contract execution (e.g., addressing cross-chain train-hotel problems [8] efficiently), thus extending interoperability protocols to a wider range of applications. The integration layer also acts as a cross-domain service provider, offering Hela's unique features (e.g., DID management, privacy protection) to other chains. Through the designs of the integration layer, Hela can mitigate data fragmentation and optimize interoperability. As a result, it makes managing and using assets simpler and more efficient, leading to a better user experience and opening up more ways to use the technology.

Flexible and Auditable Confidentiality. To provide flexible confidentiality, Hela applies a design combining the trusted execution environment (TEE) [29,42,73] and the encryption mechanism [43,51]. Users send their transactions encrypted, the transactions are decrypted within the TEE (the secret key is jointly managed by the TEE and the user) and executed. Then the executed data is then encrypted and published on the blockchain by the TEE. Due to this design, users have the flexibility to choose whether to encrypt transactions or not (thus protecting privacy) and they can also set constraints on who is authorized to use their data, what data to used, how to use the data, etc. The TEE will process the transactions under the set rules. More importantly, to provide data auditability, Hela also proposes a community-driven regulatory mechanism. When relevant authorities need to audit data on the blockchain, Hela will decide whether to authorize this action through community governance (via Hela DAO, see Section 4 for more details). After authorization, the relevant departments can then regulate and audit the corresponding data through TEE according to the authorized rules.

Multi-Level DID Management. Hela provides multi-level decentralized identity (DID) management for users. Hela's DID management protocol follows the W3C standard [3]. Users can generate their own digital identifiers (a soul-bound token, SBT [87] on or off-chain. Multiple identifiers verified by relevant organizations (e.g. DAO [74], universities, etc.) together form a user's digital identity. The user enjoys fine-grained control over her digital identity through the Hela wallet. Correspondingly, DApp developers can also customize their digital identity requirements in their applications to control the identity of users of their services. For example, a DApp for online ticketing may require verification of the user's name, cell phone number, passport number, and other digital identifiers. Of course, due to the design of Hela's confidentiality mechanism, the user's corresponding digital identifiers will also be verified and used by the DApp in a privacy-protected manner.

Stable Transaction Fees. To address the volatility of transaction fee pricing, Hela proposes to use stablecoins for transaction fee settlement. The HELA token, on the other hand, is designed a native token on the platform and will be used in the context of securing the network through staking, enabling community governance through voting, and incentivizing good behavior through rewards and slashing. To facilitate public supervision of the minting and burning process for stablecoins, Hela designs a voting-based on-chain governance mechanism. Hela also designs a taxation mechanism that deposits a certain percentage of collected transaction fees as taxes into an insurance fund. This insurance fund is managed by the community and is used to compensate compromised users to avoid a major black swan event [77,78,93]. Moreover, Hela proposes a community-driven (via Hela DAO) transaction fee adjustment strategy in response to the devaluation of stablecoins due to inflationary issues. The transaction fee is adjusted periodically to balance the user's transaction fee expenses and the node's transaction fee rewards. In the future, Hela will allow users to pay transaction fees with a wide selection of stablecoins, further enhancing usability.

With the presentation of the above designs, Hela is officially unveiled to the public. Hela, as a modular blockchain, alleviates existing data fragmentation and improves interoperability via its integration layer design. Hela's flexible and auditable privacy protection mechanism and multi-level DID management protocol together provide users with complete personal sovereignty and provide enhanced auditability and compliance for data. Hela addresses the volatility of existing transaction fee pricing by proposing to use stablecoins to pay for transaction fees. Hela also ensures the transparency and decentralization of stablecoin management through on-chain community governance. By combining these features, Hela is able to expand the adoption of blockchain technology to a wide variety of industries and actors, truly bringing it to our everyday life.

2 Background and Motivation

2.1 Blockchain and Its Applications

As an innovative technological paradigm, blockchain technology has attracted extensive attention worldwide. The public blockchain, stands as the foundation and core of peer2peer transaction settlement. A public blockchain is an open, transparent, and decentralized blockchain network. The birth of the public blockchain originates from Bitcoin [67]. In 2008, anor multiple individuals known by the pseudonym Satoshi Nakamoto published the Bitcoin white paper, proposing a decentralized electronic cash system. This marked the inception of public blockchain technology.

The advent of Ethereum [21] further propelled the innovation of public blockchain technology. Ethereum introduced

	Hela	Ethereum 2.0	Oasis	Cosmos	Sui	Aptos
Consensus	Tendermint Core	Proof of Stake (POS)	Tendermint Core	Tendermint Core	Narwhal and Bullshark	AptosBFT
EVM Compatibility	✓	✓	✓	⊖	⊖	⊖
Modularity	✓	✓	✓	✓	⊖	✓
Integration Layer	✓	⊖	⊖	⊖	⊖	⊖
Built-in Confidentiality	✓ (Flexibility, Auditability)	⊖	✓	⊖	⊖	⊖
Native DID	✓ (Multi-Level Management)	⊖	⊖	⊖	⊖	⊖
Transaction Fee Stability	Very Stable (Stablecoin Gas Fees)	Fluctuate	Fluctuate	Fluctuate	Fluctuate	Fluctuate
Stablecoin Governance	✓	⊖	⊖	⊖	⊖	⊖

Figure 1: Comparison between Hela and several mainstream blockchain protocols.

the concept of smart contracts, transforming blockchain from a mere transaction platform to a globally distributed computer, capable of running complex logic applications. Subsequently, many public blockchain projects such as Cosmos [53], Solana [92], and Avalanche [72] have emerged. They aim to address different issues like scalability, security, and usability, in search of broad adoptability.

In the financial sector, blockchain technology has the potential to make profound impacts. One example is Decentralized Finance (DeFi) [27, 75, 84, 85, 90], which has the potential to overturn the operational model of traditional finance. For instance, Uniswap [9], a decentralized exchange operating on Ethereum, executes transactions automatically via smart contracts, eliminating the need for intermediaries. Other applications in the financial field, such as Decentralized Autonomous Organizations (DAOs) [15, 60, 65, 66, 71], Non-Fungible Tokens (NFTs) [14, 25, 68, 86, 88], and Game Finance (GameFi) [32, 48–50, 70], also show great potential.

However, while public blockchain technology has achieved significant early traction in the field of decentralized finance, its application in other sectors faces several limitations. First, some existing blockchain systems have limited processing capabilities and scalability [21, 56–58, 67]. For large-scale data processing demands, such as in AI or cloud computing, current public blockchain technology may not meet user's future needs. Second, the transparency of blockchain, while beneficial in many cases by enhancing trust and traceability in transactions, can be a challenge in scenarios requiring privacy protection. For example, in healthcare or personal data management, users may not want their sensitive information exposed on a public blockchain network visible to everyone. Last, regulatory issues also serve as a significant barrier to blockchain adoption in across industries [44, 91, 97]. Given that blockchain is an open, anonymized system, the lack of proper identity management can provoke several complex auditing and regulatory challenges.

2.2 Data Fragmentation

To address the scalability issue inherent to many blockchain systems, several solutions have emerged, such as modular design and Layer 2 networks. Modular design [21, 53, 89] allows different runtimes (or blockchains) to work together within a single network, thus improving scalability and providing customizability. On the other hand, Layer 2 networks [35, 45, 46] operate on top of existing Layer 1 blockchains to enhance scalability. These solutions process transactions off-chain,

thereby alleviating the burden on the main chain.

While these methods can enhance scalability and offer customizability, they are not without drawbacks. A significant issue is the fragmentation of data. As the network expands and processes more transactions, data is dispersed across different domains (i.e., runtimes, layers, chains). For instance, in the Cosmos ecosystem, each subchain has its independent transaction history, which cannot be directly accessed from other chains. Similarly, transactions conducted on Ethereum's Layer 2 networks may not be directly visible on the main chain. Furthermore, operating across Layer 1 (L1) and Layer 2 (L2) chains introduces "bridge risk", which pertains to the potential vulnerabilities or failures when assets move between layers. There is also the question of "finality", a crucial concept in finance and other sectors, which deals with the assurance that once a transaction is completed, it cannot be reversed or altered, a challenge that becomes pronounced when navigating between different domains.

This fragmentation of data can have several adverse effects. First, it may challenge users and developers in terms of data accessibility and interoperability. Users might have to interact with multiple domains to access all necessary data, which can be tedious and inefficient. For developers, writing applications that need data from different domains, access might also be complicated. Second, data fragmentation can bring about regulatory and compliance issues. For example, auditing transactions distributed across multiple domains is more challenging, potentially making illicit activities easier to overlook. Adhering to data protection laws is also more complex when data is fragmented across different blockchain protocols.

2.3 Privacy Protection

In the current ecosystem of public blockchains, privacy protection remains an essential and unresolved issue. Bitcoin and Ethereum, two of the most well-known public blockchain projects, incorporate certain anonymity in their design, such as pseudonymous addresses. However, the records between addresses are public, allowing anyone to trace the sender and receiver, as well as the economics of the transaction. This level of openness most certainly will lead to a problems, including the tracking of user transaction behaviors, the leakage of personal details to adverse actors, how could use them for illicit activities.

Some public blockchain projects have attempted to incorporate privacy protection mechanisms into their designs. For instance, Zcash [40] and Monero [83] are blockchain projects that have made privacy protection their core feature. Zcash utilizes a technology known as Zero-Knowledge Proofs (zk-SNARKs [64]) to achieve transaction privacy protection, making details inaccessible to anyone except those holding a specific viewing key. Monero, on the other hand, uses ring signatures and stealth addresses to conceal the information of transaction senders and receivers.

Nonetheless, the above designs featuring strong privacy protection also introduce some issues. First, privacy protection is mandatory, users cannot flexibly control the privacy protection level of their data. More importantly, these design choices for privacy protection could be exploited to conduct illicit activities, such as money laundering and tax evasion. Such activities that are deemed illegal in many jurisdictions have already drawn the attention of regulatory agencies and present challenges for data auditing.

2.4 Decentralized Identity Management

In the current public blockchain systems, anonymity is a prevalent feature. Take Ethereum as an example: users transact through digital addresses, which somewhat enhances users' anonymity. However, such anonymity comes with missing identity management, which brings about several issues. First, anonymity could potentially encourage illicit activities as criminals may exploit this characteristic for illegal transactions, such as money laundering and terrorist financing. Secondly, excessive anonymity may pose challenges for regulatory auditing as it might be difficult to trace the real origins of transactions. Lastly, the lack of identity management limits the application scenarios of existing public blockchains, because in many real-world use cases, it is necessary to acquire user identity information.

There are some blockchain projects that attempt to introduce identity management mechanisms. For instance, Ontology [6] is a blockchain that focuses on identity verification as a core feature, offering a decentralized identity verification solution. Such a design can enhance the traceability of transactions and is conducive to compliance requirements. However, this design also brings about some challenges. First, it could lead to the leakage of user details. For example, if the system's identity management is hacked, users' personal information would be compromised. Moreover, decentralized identity verification systems may also face fraud-related issues, as there is no centralized institution to verify users' identity information when they are first submitted to the system. This could allow malicious actors to forge identities, that would in turn allow them to engage in fraudulent activities without being identifyable.

2.5 Transaction Fees

In the current public blockchain systems, users are required to purchase specific tokens to use the platform's services. Again, Ethereum and Bitcoin are two prominent examples. On the Ethereum network, users must first purchase ETH to pay for Gas fees, to execute transactions and smart contracts. Similarly, on the Bitcoin network, users also need to pay with the native BTC coin to get transactions settled.

However, this design has given rise to several issues. First, due to the high price volatility of cryptocurrencies, transaction fees may fluctuate significantly, posing an additional risk to users [10, 11, 18]. Second, public blockchain systems often use their unique tokens to cover transaction fees. With each system having its own distinct token, users might find themselves frequently exchanging between various tokens to interact with different systems. This constant switching not only introduces added transaction costs and complexity but can also deter newcomers due to the increased complexity. Additionally, having numerous tokens can dilute the market, making some tokens less liquid or harder to trade, which can be an impediment for users.

2.6 Motivation

After observing the various issues existing across the current blockchain ecosystems, we are motivated to propose Hela, a next-generation Layer 1 public blockchain network. Hela's objective is to solve the issues described earlier which will make it a very adoptable Layer 1 blockchain compared to what is currently available in the market. To address the aforementioned issues and achieve our objectives, Hela has made the following key design proposals. First, we propose a modular architecture with an integration layer to address the problem of data fragmentation and poor interoperability. By using our novel integration layer, users and Dapps can interact securely and efficiently with each runtime and other chains at this layer. Second, we propose flexible and auditable confidentiality and multi-level decentralized identity management to balance privacy protection, personal sovereignty, and the compliance and auditability of data. Finally, we propose the use of stablecoins for transaction fee settlements to reduce the impact of price fluctuations on users and enhance usability. Our community-driven token governance model also adds transparency and decentralization to the process of managing tokens in Hela, benefiting its long-term operation. Figure 1 compares Hela with some mainstream public blockchain projects.

3 Modular Architecture

In this section, we introduce Hela's overall modular system architecture, which consists of four main layers: consensus layer (Section 3.1), execution layer (Section 3.2), integration layer (Section 3.3), and storage layer (Section 3.4). An illustration of the Hela modular architecture is shown in Figure 2.

3.1 Consensus Layer

The role of the consensus layer is to reach consensus on the network-wide state and to finalize transactions. In addition, the consensus layer is also responsible for performing tasks such as issuing HELA tokens, managing node identities, and staking.

The consensus layer of Hela currently utilizes a Byzantine Fault Tolerant consensus protocol known as Tendermint [20]. Byzantine Fault Tolerance refers to the property in the field of distributed computing where a system can still reach agreement even when a portion of its components may be faulty (including malicious behavior) [23]. Through the Tendermint protocol, nodes within the network can reach consensus on transaction records without the need for centralized control. Similar to BFT-type consensus protocols, Tendermint can ensure network security and liveness in the presence of <1/3 malicious voting weight. More importantly, since Tendermint is a BFT-type consensus protocol, it can provide deterministic and instantaneous transaction finality (unlike Nakamoto-type consensus), enhancing the user experience. For a detailed description of the Tendermint protocol, please refer to [20].

Within Hela's consensus layer, nodes are categorized as validators and delegators. Validators are responsible for proposing new blocks and voting on blocks proposed by other validators, thereby achieving network consensus. Delegators can delegate their HELA tokens to validators, thereby participating in the consensus process and receiving a portion of the staking rewards. In Hela, validators become candidate validators by staking HELA tokens, and a portion of validators are then selected based on their staked amount and the amount delegated to them by delegators. These selected validators are responsible for the consensus process and the network's security. Hela implements a strict Proof of Stake (PoS) mechanism for nodes participating in the consensus process. During the consensus process, each validator's voting weight is associated with its stake (and delegated amount).

It is noteworthy that Hela's consensus layer and execution layer are separated. This separation allows for high flexibility and scalability. The separation of the consensus and execution layers means in practice that each layer can be upgraded and improved independently without affecting other layers. This design allows Hela to better adapt to future technological changes and market demands and to support a variety of applications and services. Additionally, a comparatively lightweight consensus layer allows Hela to process a large number of transactions and reach consensus quickly while maintaining network security.

Hela's consensus mechanism is designed with robust solutions to overcome challenges commonly encountered by Layer 1 platforms. A primary concern in such systems is ensuring the honesty of validators and preventing large-scale colluding attacks. To address this, Hela has implemented measures that guarantee the integrity of validators and safeguard against extensive collusive activities. Through staking and penalty mechanisms, validators are held accountable for their actions. Any misconduct can result in their staked funds being slashed. Additionally, the Hela community rigorously audits the identity of each candidate validator, permitting only vet-

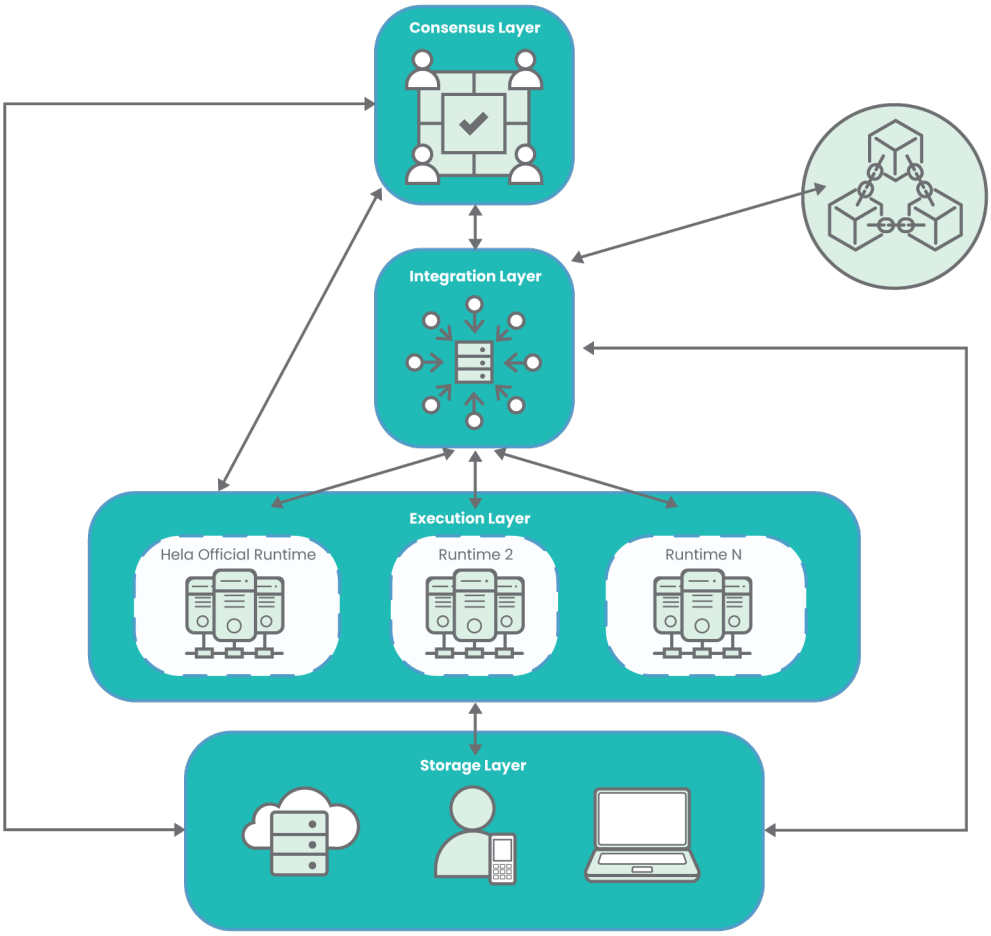


Figure 2: Overview of Hela modular architecture.

ted entities to partake in the consensus process. Moreover, by incorporating delegators, Hela amplifies participation in the consensus, preventing excessive power consolidation among validators and, in turn, bolstering network security.

Hela will continue to conduct exploratory, theoretical and empirical research of consensus mechanisms, to further improve its blockchain consensus efficiency and security, and to ensure best in class incentivives for validators and delegators while keeping our core design features to make the platform adoptable widely.

3.2 Execution Layer

The main responsibility of the execution layer is to handle specific transactions. To make Hela available to the public as soon as possible, we take Oasis [5] as our implementation reference. In addition, since users need to interact with this layer, it provides confidentiality and features identity management functionality.

As depicted in Figure 2, the execution layer of Hela is situated above the consensus layer. Within the execution layer, multiple runtimes can operate. Each runtime can have its own state machine and rules, and can run various types of applications and services, including but not limited to smart contracts and confidential computing.

The design philosophy of the runtime originates from the pursuit of network flexibility and scalability. Each runtime can customize the characteristics of its environment, such as programmability, privacy protection, and security. This design

allows different applications to select or create a runtime that meets their specific needs. For instance, Hela provides flexible and auditable confidentiality in its official runtime (which will be explained in detail in section 4), along with DID management (see section 5), and stable transaction fees (see section 6). Whereas developers might chose a different runtime with other characteristics, depending on their use case.

Each runtime is maintained and operated by a set of compute nodes, which are responsible for processing and executing transactions and smart contracts. When a new transaction is submitted to a runtime, the compute nodes in charge receive it. The compute nodes then execute the transaction according to the rules and state machine of the runtime. This could involve reading or modifying the state of the runtime, executing smart contracts, or triggering other transactions, etc. After the transaction is executed, the compute nodes generate a new state and execution results.

Once the compute nodes have processed a transaction, they need to submit the results to the consensus layer for validation and recording. Specifically, the compute nodes package the new state, execution results, and proof information into a block, and then submit it to the network through the consensus layer. The nodes on the consensus layer (also known as validators) verify this block to ensure that the compute nodes have correctly executed the transaction. The verification process may involve validating proof information, comparing the new state and execution results, and so on. Only when the majority of validators confirm that the block is valid will it be added to the blockchain and become part of the network. This design ensures that all transactions are executed and recorded under the supervision of the majority of validators, thereby enhancing the security and credibility of the network.

Compute nodes are required to stake a certain amount of HELA tokens to participate in the operation of a runtime. If the compute nodes are found to have errors or malicious behavior, their staked tokens will be forfeited. This staking and penalty mechanism encourages compute nodes to execute transactions honestly.

Although the design of the runtime enhances the flexibility and scalability of Hela, it also brings about some challenges and issues. For instance, how to solve the data segmentation issue among different runtimes? To address this issue, Hela proposes the integration layer, as will be introduced below.

3.3 Integration Layer

The integration layer is responsible for state integration across runtimes and chains. This layer allows users to interact with individual runtimes and other chains.

The first objective of Hela's Integration Layer is the integration of assets (e.g., users' tokens) across each runtime. This addresses the problem of data fragmentation. In other cross-domain interoperability protocols, it is often necessary for each domain to maintain a cross-domain pool of assets, or to facilitate the transfer of assets via mint and burn or the use of bridges. Numerous hacking attacks have shown that such cross-domain protocols are insecure. In Hela, however, the user's assets will be managed by the secure integration layer. When a cross-runtime interaction occurs (e.g., a user in runtime A wants to invoke a contract in runtime B), there is no actual cross-runtime transfer of the user's assets. Instead, the integration layer defines a series of cross-runtime communication protocols. These operations are coordinated by the integration layer by passing different messages to the relevant runtimes (e.g., sending the asset information of the user of runtime A that it needs to the contract of runtime B in the form of a virtual asset).

In the next step, Hela's integration layer will focus on the integration of the execution logic in each chain. This is mainly to solve the application limitations of existing interoperability protocols and expand the application scope. Most of the existing interoperability protocols can only support simple atomic cross-chain asset transfers, but cannot realize more general atomic cross-chain smart contract operations (e.g., atomic cross-chain train-hotel problem, atomic cross-chain arbitrage, atomic cross-chain flash loan, etc.). In Hela, we will provide atomic cross-chain smart contract operations by designing an integrated execution logic and a common cross-chain interoperability protocol, thus expanding the cross-chain application scenarios to a wider range of use cases.

In the future, Hela's integration layer will also play the role of a cross-chain service provider. For example, Hela will provide DID verification, management and other services for other chains that do not have DID features through the integration layer. Similarly, Hela can also provide confidentiality services through the integration layer for other chains that do not have privacy-preserving features. Applications on these chains only need to interact with Hela when they need the corresponding services, and Hela can provide them with the desired services accordingly. It is worth mentioning that the robustness of Hela's interoperability protocol is intrinsically linked to the security of its consensus layer. In essence, when the consensus layer operates securely, it ensures the safety and reliability of Hela's cross-chain interactions.

3.4 Storage Layer

The storage layer stores Hela's entire ledger and provides data availability for Hela. The data in this layer also requires confidentiality guarantees.

The storage layer is a critical component in our blockchain infrastructure, designed to enhance the availability, reliability, and security of data across all nodes in the system. One of its primary roles is to combat 'data withholding attacks', where malicious nodes refrain from sharing or publishing certain data to disrupt the system. Such attacks can hinder the transparency and trustworthiness of decentralized networks. By

addressing this concern, the storage layer significantly improves overall transparency and trust within the blockchain.

The core functionality of the storage layer hinges on two fundamental techniques: data availability sampling and data availability verification, supported by the integration of essential technologies such as erasure coding [16] and Merkle Trees [79].

Data availability sampling is predicated on the assumption that by checking a random subset of a large data set, we can accurately infer the availability of the complete data set. This process, also known as probabilistic data checking, hinges on the robustness of erasure coding – a sophisticated method of data protection.

Erasure coding involves the division of data into fragments which are then expanded and encoded into additional redundant data pieces. These pieces are subsequently dispersed across multiple locations. The unique feature of erasure coding lies in its redundancy which allows any part of the data to be reconstructed from a subset of fragments, even if some are missing or inaccessible. In the context of our blockchain, each data block is fragmented and encoded using erasure coding before being dispersed across the nodes. This significantly enhances data redundancy (and hence robustness) and allows for efficient and reliable data sampling without the necessity of downloading and storing entire data blocks.

Data availability verification is a process that certifies the correctness and consistency of the sampled data. This verification is achieved using Merkle Trees, a type of binary tree used extensively in blockchain systems for efficient data verification.

In a Merkle Tree, each leaf node corresponds to a block of data, and each non-leaf node is the hash of its child nodes. This design enables an efficient and secure method for verifying the content of large data sets, even when the entire data set is not available. When a node samples a fragment of a data block, it can use the corresponding Merkle proof (a path in the Merkle Tree from the leaf node associated with the data fragment to the root) to verify the data fragment's authenticity against the block's Merkle root, which is stored in the blockchain's header.

The amalgamation of erasure coding in the data sampling process and Merkle Trees in the data verification process allows for robustness of the storage layer. The distributed storage scheme ensures a high degree of data redundancy and facilitates efficient data availability checks. Concurrently, the application of Merkle Trees provides a secure and efficient mechanism for validating data authenticity without the necessity of maintaining the entire data set.

4 Confidentiality

In this section, we describe how Hela enables privacy protection and provides flexibility and auditability.

Hela leverages a Trusted Execution Environment (TEE) and cryptography (e.g., asymmetric and symmetric encryption, key exchange algorithm, secret sharing) to provide confidentiality. A TEE is a hardware component providing a secure area of a main processor that guarantees code and data loaded into the TEE is protected with respect to confidentiality and integrity. It provides a shielded execution space, separate from the rest of the device, where applications can run securely even if the wider system is compromised. This is achieved by ensuring that the code and data residing inside the TEE are inaccessible to other software running on the same device, including the operating system. Additionally, the TEE remains isolated from the 'hypervisor'—a software layer that allows multiple operating systems to run on a single physical machine by virtualizing the hardware resources.

For privacy protection, TEE has certain advantages over zero-knowledge proofs (ZKP). ZKPs are cryptographic methods which allow one party to prove to another that a given statement is true, without conveying any additional information. While ZKPs are potent tools for privacy protection, they can be computationally expensive and complex to implement, often requiring significant resources and time. On the other hand, TEEs, by their design, offer a more streamlined and efficient solution. TEEs can process large amounts of data quickly and securely, providing real-time data protection. They do not require heavy computational resources, and are thus more cost-effective and scalable. In addition, TEEs offer a versatile solution, as they can handle various types of data and different forms of computations, while ZKPs may require specific constructions for different types of computations.

In Hela, we adopt Intel's Software Guard Extensions (SGX) as our implementation of TEE. Intel SGX introduces the concept of an 'enclave', which is a protected area within the application's memory that ensures private regions of code and data are kept secure. The code outside the enclave (referred to as the untrusted part of the application) is disallowed from accessing the enclave's memory. Meanwhile, the data inside the enclave is encrypted and authenticated, providing robust security guarantees. This unique feature allows Hela to create protected spaces for sensitive data processing, preserving the data's confidentiality and ensuring its integrity.

Moreover, we acknowledge that different TEEs can offer different advantages and compatibility with various systems. Therefore, we aim to extend support for more types of TEEs in the future. These may include ARM TrustZone, a system-wide approach to security for a wide array of client devices, and AMD Secure Encrypted Virtualization (SEV), which is designed to protect virtual machines from malicious administrators or hypervisors. By embracing the variety and versatility of these technologies, we will ensure that our system can be deployed flexibly and securely across various platforms, extending the advantages of secure and private computation to a wider range of users and use cases across industries. Figure blah illustrates an overview of Hela's flexible and auditable

confidentiality scheme.

Flexible Confidentiality. Flexible confidentiality allows Hela to protect users' privacy while safeguarding their personal sovereignty and data autonomy. Since Hela's privacy protection is guaranteed by TEE and multiple encryption algorithms, users of Hela can make informed decisions about their data: whether to disclose it, when, which parts, and to whom. An essential tool in this process is the 'ephemeral key', a temporary encryption key used for a single session or transaction, ensuring data security and privacy. For instance, if user A wants to disclose a transaction to user B, user A can submit its ephemeral key associated with the transaction to the nodes equipped with TEE. The TEE then uses these ephemeral keys to decrypt the transaction from user A and re-encrypt it for user B. The transaction, now encrypted with user B's ephemeral key, is sent to user B, ensuring that only user B can view the transaction.

Auditable Confidentiality. Auditable confidentiality allows Hela to maintain transaction privacy while ensuring the blockchain is in line with regulatory standards. Unlike some existing blockchains that employ zero-knowledge proofs for privacy, making their data hard to scrutinize, Hela's TEE-based protocols are designed for blockchain compliance, ensuring transparency, accountability, and auditability. We emphasize that truly successful blockchains cannot function entirely outside of regulatory oversight. We believe that decentralized applications will only gain widespread acceptance if they operate within a framework that allows governments to deter and address illicit activities.

In Hela, we balance the roles of traditional authorities (e.g. government) and blockchain through community-driven regulation (via Hela DAO). When the relevant authorities need to regulate and audit the data in Hela, they can initiate a proposal in the Hela community. After the proposal is approved by the community, the relevant authorities can interact with TEE using the ephemeral key associated with the required data, and TEE will encrypt the data to be audited using their ephemeral key and return it to ensure that only the authorities has access to the data. The entire community governance process is realized through smart contracts to ensure transparency and traceability.

5 Decentralized Identity

The concept of a decentralized Identity (DID) is crucial as it empowers individuals with ownership, control, and portability of their digital identities, enabling enhanced privacy, security, and interoperability in the digital realm. In the current DID landscape, there is a pressing need for (i) credential service providers to facilitate the issuance and verification of verifiable credentials (VCs), (ii) a reliable DID service provider offering confidential authentication mechanisms to enhance privacy and security, and (iii) the development of user-friendly

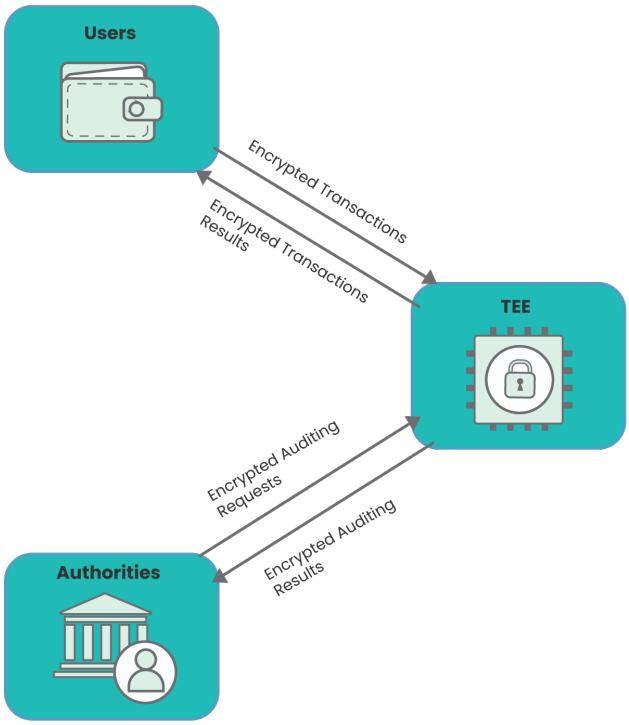


Figure 3: Overview of Hela's flexible and auditable confidentiality.

DID wallets to improve accessibility and ease of use for individuals, corporates and, other entities managing their DIDs and VCs.

Hence, we build a new DID ecosystem called *Held*. Fig. 4 illustrates Held's system architecture. Each component will be further described in the following sections.

5.1 DID Service Provider

We propose a new W3C-compatible DID method, `held`, as follows:

`did:held:0xABC...`

The DID Method-Specific Identifier, the last part of the DID format, involves a user's HELA address, offering a seamless identification user experience for credential holders.

To resolve and register our DIDs, we are actively building a robust and scalable DID resolver and a DID registry as smart contracts deployed on our execution layer, conforming to ERC-1056[1]. The DID resolver serves as a critical component in resolving and retrieving identities. By leveraging Hela's execution layer, we ensure the integrity, immutability, and decentralized nature of the resolution process. Our resolver enables efficient and reliable retrieval of DID data,

[1] https://github.com/ethereum/EIPs/issues/1056

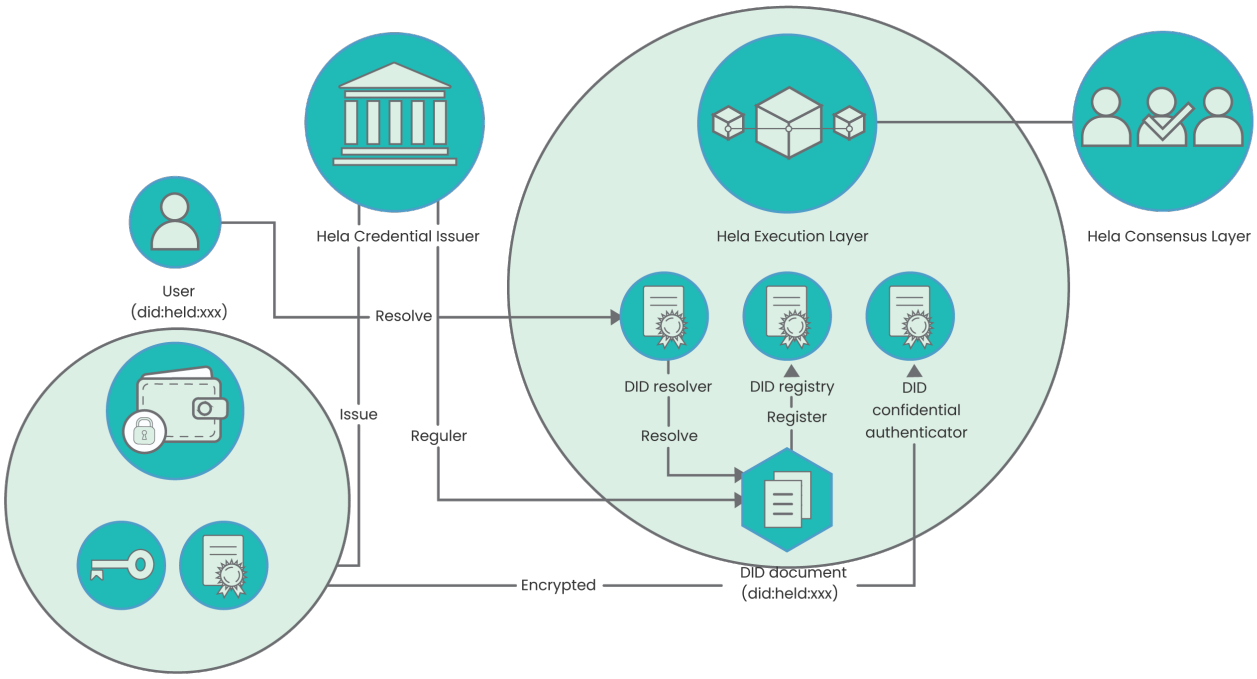


Figure 4: Overview of Held ecosystem.

facilitating seamless interactions between users, verifiers, and service providers within the decentralized identity ecosystem. Additionally, our DID registry acts as a trusted source for registering and managing DIDs, providing a secure and tamper-proof record of decentralized identities. This allows individuals and organizations to securely claim and manage their identities, establishing a foundation for self-sovereign identities and enhancing interoperability across various platforms and services.

The last component, a DID confidential authenticator, will enable users and other DApps to confidentially verify encrypted VCs. The respective smart contract will be rolled out once our confidential execution layer is enabled.

5.2 Credential Issuer

One of the challenges in the current landscape of Decentralized Identity (DID) is the lack of credential issuers. In traditional identity systems, institutions such as governments, universities, and financial organizations play a crucial role when issuing credentials like passports, driver's licenses, academic degrees, and financial certifications. However, there is a need for these institutions to adapt and participate in the decentralized ecosystem by becoming verifiable credential issuers.

Currently, the transition from centralized credential issuance to decentralized models is in its early stages. Many organizations are only exploring the possibilities and implications of issuing verifiable credentials using decentralized technologies. This lack of high-quality issuers poses a challenge for individuals seeking to obtain official and recognized credentials in the decentralized digital realm.

Hence, we will operate a scalable, industry-grade verifiable credential issuing service that leverages users' Know Your Customer (KYC) information. KYC procedures are commonly used by financial institutions and other entities to verify the identities of their customers. By harnessing the power of decentralized identity technology, we aim to provide a secure and privacy-enhancing solution for individuals to store and manage their KYC data themselves. Our VC issuer will enable users to obtain digitally signed and tamper-proof verifiable credentials based on their verified KYC information. These credentials can then be selectively shared with trusted entities, such as financial service providers or online marketplaces, to streamline onboarding processes, enhance

security, and foster trust. By giving individuals control over their KYC data through verifiable credentials, we empower them through enhanced privacy, reduced data redundancy, and a more efficient and user-centric digital identity ecosystem.

5.3 A User-Friendly DID Wallet

Another obstacle in the adoption and usability of DID is the limited availability of user-friendly DID wallets [52]. DID wallets are digital wallets that allow individuals to securely manage their decentralized identities, store their verifiable credentials, and control the sharing of their personal data with trusted entities.

Currently, many existing DID wallet applications are targetting developers and technical users, requiring a certain level of technical expertise to navigate and operate effectively. The lack of user-friendliness and intuitive user experience poses a barrier to widespread adoption among non-technical individuals.

Furthermore, many individuals are unaware of the need to manage and secure their verifiable credentials, which will become increasingly important in the decentralized identity landscape. As a result, there is a pressing need to provide a user-friendly and intuitive way to back up and manage their verifiable credentials in their wallets.

To address these challenges, we will release a wallet application that prioritizes simplicity, ease of use, and seamless integration with existing digital experiences. By designing a seamless and user-centric backup mechanism, we aim to ensure that individuals have a convenient means to safeguard their valuable credentials. This approach will help users by enabling them to confidently navigate the decentralized identity space and protect their digital identity assets from loss or unauthorized access. By emphasizing the need for backup functionality and providing a user-friendly solution, we strive to enhance user adoption and promote responsible self-sovereign identity management.

We can pave the way for broader adoption and acceptance of Decentralized Identity, empowering individuals with enhanced control over their identities and personal data while promoting trust and interoperability in the digital realm.

6 Stable Transaction Fees

In this section we expand on how Hela achieves stable transaction fee prices (Section 6.1) and how on-chain and community governance takes place (Section 6.2).

6.1 Stablecoin as Transaction Fees

To ensure transaction fee pricing does not fluctuate based on the volatility of the native token, Hela proposes to use stablecoins for transaction fee settlement. Since the actual processing of users' transactions occurs at the execution layer, the settlement of transactions via stablecoin also occurs at the execution layer (by default within the official runtime). Hela uses a gas fee model similar to that of Ethereum, where the gas fee consumed per transaction is related to the complexity of the transaction. The gas fee is in turn converted equivalently to stablecoin for settlement. Therefore, Hela implements stablecoin support at the lowest level of the execution layer, making them a native token of the official runtime.

By default, the stablecoin used by Hela is HLUSD (Hela USD), a fiat-collateralized stablecoin anchored to the U.S. dollar. HLUSD is backed by "off-chain" reserves of FIAT currency - the "collateral". A regulated company is responsible for controlling the FIAT funds and minting or burning the HLUSD tokens in the runtime accordingly.

Hela uses HLUSD as the native token in its official runtime, while the native token in Hela's consensus layer is HELA. This leads to the question of how to manage both HELA and HLUSD tokens in the official runtime. We design a dual token mechanism in the official runtime. Specifically, HLUSD exists as a native token in the official runtime, while HELA will be stored in the form of ERC20 tokens in a system-level smart contract. To enable HELA token interaction between the consensus layer and the execution layer, we implement a secure cross-layer communication protocol. This protocol will allow users to easily transfer HELA tokens from the consensus layer to the official runtime for to use or spend or alternatively transfer HELA tokens in the other direction, from the official runtime to the consensus layer, for example for staking.

To support with adoption, Hela will also offer a variety of regional stablecoins (e.g., HLSGD, HLEUR, etc.) in addition to HLUSD for payment of transaction fees. Instead of going through the tedious process of converting currencies, users will be able to pay transaction fees directly in their national currency's corresponding stablecoin.

Remarks. It is worth noting that only the official runtime uses our stablecoin, HLUSD, by default to settle transaction fees. For other customized runtimes, developers can set different native tokens according to their requirements and use those to settle transaction fees. In addition, in Hela, HELA tokens are produced on the consensus layer, while HLUSD is minted in the execution layer (the official runtime).

6.2 Stablecoin Governance

The governance of stablecoins is critical for ensuring transparency, decentralization, and accountability in their operation. While blockchain technology itself is decentralized, many decentralized applications (DApps), including stablecoins, are often controlled by a single entity or owner of the smart contracts, which introduces a level of centralization. This centralization raises concerns regarding the control and management of stablecoins, as demonstrated by various con-

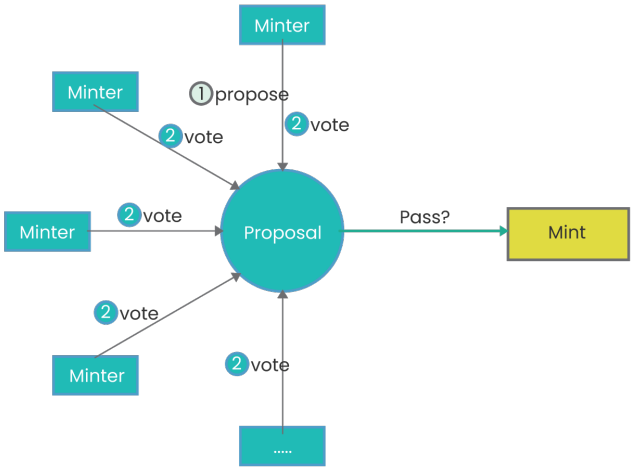


Figure 5: Mint action of stable coin governance.

troversies and incidents in recent history. One example is the lack of transparency in asset-backed stablecoins. For instance, USDT (Tether), a widely used stablecoin, has faced regulatory scrutiny for failing to provide audits that adequately document the backing of its tokens with sufficient reserves [24]. Similarly, the recent exit scam of Merlin DEX highlighted the vulnerabilities, as rogue developers abused their private key privileges, resulting in a loss of approximately $2 million USD in user funds [26].

To address these issues and enhance transparency and decentralization in stablecoin governance, Hela proposes a set of on-chain and community-driven governance mechanisms.

On-Chain Voting. Hela introduces an on-chain voting mechanism to regulate critical processes like minting, burning, whitelisting, blacklisting, and other significant actions related to stablecoin operations. The proposed governance model involves a committee consisting of reputable companies who will be responsible for managing the portfolio of FIAT-based assets and their custody, regular auditing.

The governance model consists of five roles and six actions in our system: role *Admin* with actions *set_role* and *set_quorum*, role *Minter* with action *mint*, *Burner* with *burn*, *Whitelister* with *whitelist* and *Blacklister* with *blacklist*. Each role is exclusively permitted to raise proposals within their designated purview. For instance, an *Admin* role can propose actions related to role modifications by *set_role* or quorum adjustments by *set_quorum*. A *Minter* role can propose new minting action by *mint* etc. The proposal process involves a voting mechanism wherein roles, other than the proposer, cast their votes as **yes, no** or **abstain**. For a proposal to be accepted, a predefined quorum must be met. The specific quorum requirement for each action can be set and modified by the *Admin*s via the *set_quorum* action.

Consider the case of the *mint* action as depicted in Figure 5. Prior to initiating a minting proposal, the relevant *Minter* committee should already be established by the *Admin*s. The proposal process unfolds as follows:

- A *Minter* submits a proposal (step ①).
- The *Minter* committee undertakes an off-chain verification process to validate the existence of corresponding collateral, thereby enhancing transparency and trust in the proposed action.
- Upon successful off-chain verification, *Minter* roles cast their votes on the proposal (step ②).
- If the required quorum (set at 80%) is met, the proposed minting action is executed on-chain.

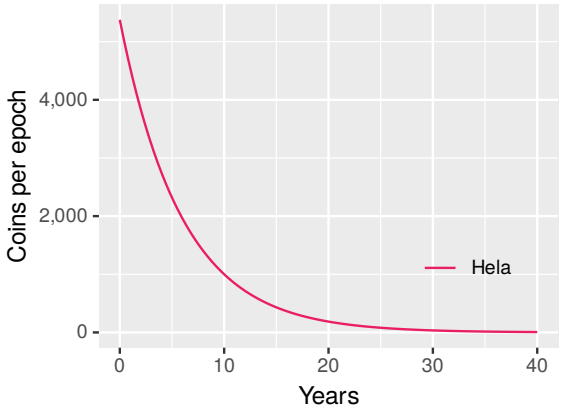
The quorum, vital to the success of any proposal, can be subject to future adjustments by the *Admin*s.

Our on-chain voting mechanism ensures that decisions related to stablecoin operations are collectively made by reputable entities, enhancing decentralization and reducing the reliance on a single controlling authority. By implementing this governance system, Hela aims to foster a more transparent, decentralized, and accountable framework for stablecoins. These mechanisms promote community participation, minimize the risks associated with centralization, and improve the overall integrity of stablecoin operations.

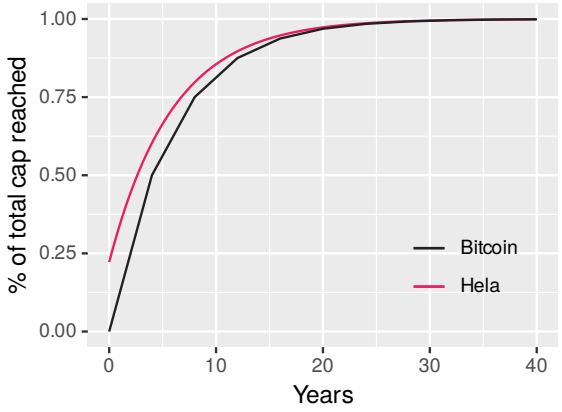
Insurance Fund. Hela is implementing an insurance fund mainly to reduce the impact of unforeseeable events affecting the Hela ecosystem. Moreover, the fund is also responsible for controlling the inflation of the HELA token (see Section 7.5). In Hela, a portion of the transaction fees collected (e.g., 90%) is used to reward compute nodes, while the remaining portion (e.g. 10%) is deposited as a tax into an insurance fund account. The management of the insurance fund account is the joint responsibility of the Hela community (through the community members in Hela DAO).

When an adverse event (e.g., hacking or other non-foreseable incidents) occurs, the community can propose and vote on whether to use the funds in the insurance fund account to compensate for related losses, thus limiting the impact of the event.

Countermeasure to Stablecoin Devaluation. Hela uses stablecoin to settle transaction fees, and FIAT currencies exhibit inflation. Inflation leads to a diminishing purchasing power vis-avis other currencies or a basket of goods. On the Hela blockchain the effect would be that transaction fees charged, do not adequately reward compute nodes anymore. Furthermore, it also would devalue the insurance fund. To address this issue, the Hela community can periodically vote on the adjustment of transaction fees to better balance user expenses against node rewards (i.e., HLUSD).



(a) Coins per epoch.



(b) % of total cap reached.

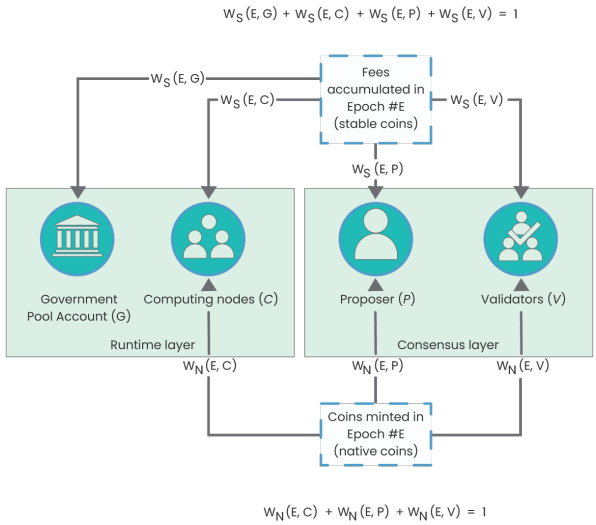


Figure 7: Overview of Hela's tokenomics.

7 Tokenomics

The issuance and distribution of new native tokens play a pivotal role in the operation and sustainability of a blockchain network. This section outlines the key objectives and importance of issuing new tokens, reward functions, and design of other mechanisms, highlighting roles in compensating for the costs of blockchain operation and contributing to the overall security of Hela.

The detailed design and analysis of our tokenomics will be separately released as scientific papers.

7.1 Native Coin Minting

Figs. 6a and 6b show HELA tokens to be minted over time and their cumulative curve. The issuance of HELA tokens is capped at 360 million. 80 million of the issuance is pre-minted and preserved in our initial nodes. The rest will be disbursed to committee members (i.e., computing nodes, proposers, and validators) for their contribution to the governance and security of the network.

Hela has three phases for token issuance. The purpose of the first phase, a year-long, is to stabilize the network economy. Specifically, it is closed and internal, where our team of developers manages all actors/roles that maintain the network. The second phase, also one year long, is for soft adoption. It is semi-closed, where stakeholders can join the Hela network to manage nodes. The third phase is for mass adoption; it is open, and anyone can participate given their stake is large enough.

We use an exponential distribution with its curvature parameter, λ, $\lambda = 0.0000192$ to gradually release our native tokens.

$$R_e = \lambda \exp(-\lambda e). \tag{1}$$

The percentage of the total cap reached is expressed as follows.

$$P(R_e) = 1 - \exp(-\lambda e). \tag{2}$$

where $P(\cdot)$ is the cumulative distribution function.

7.2 Reward-Sharing Functions

A reward-sharing function determines how we split the fees collected in the execution layer and native tokens into nodes. A reward-sharing function has to be designed to achieve the following objectives.

1. **Security.** The reward-sharing function is designed with strong security measures to prevent potential attacks, such as Sybil attacks or double-spending attempts, ensuring the integrity of the rewarding process and maintaining trust within the network. By extending the idea

of [19], It is designed to achieve the committee size of k_c validators on the consensus layer and k_r on the runtime layer, each having the same amount of stakes.

2. **Fairness and Equality.** A good reward-sharing function ensures fairness by treating all participants equally [31].

3. **Incentivization.** The reward-sharing function provides meaningful incentives to participants, motivating them to actively engage and contribute to the network's growth and success.

4. **Flexibility.** A good reward-sharing function is flexible and adaptable to changing circumstances. It should allow for adjustments in reward distribution based on evolving network needs, performance metrics, or changes in Hela's roadmap and global macro developments affecting the platform.

Fig. 7 is a graphical representation of Hela's tokenomics design. The idea is to dynamically set each weight of rewards according to various factors. For example, the cost of each operation [33]. Two types of tokens are distributed as rewards, which are (i) total fees collected on the runtime layer in epoch E, in HLUSD, and (ii) native HELA tokens minted on the consensus layer. Fees in epoch E, $F(E)$, are distributed to four types of nodes, namely (i) the tax collection account, (ii) a proposer, (iii) computing nodes, and (iv) validators.

$$w_S(E,G) + w_S(E,C) + w_S(E,P) + w_S(E,V) = 1 \quad (3)$$

The first term is considered a tax and will be used for buying back Hela tokens to control their values. In Phase 1, we distribute stable coin fees equally among computing nodes.

Similarly, newly minted HELA tokens are distributed among the committee members with weights.

$$w_N(E,C) + w_N(E,P) + w_N(E,V) = 1 \quad (4)$$

As we run nodes internally only in the first year, we distribute tokens equally among the contributing committee members.

7.2.1 Punishment

Each committee type (i.e., proposers, validators, and computing nodes) operates under its own set of punishment rules. Proposers face penalties including loss of ability to propose a block or temporary suspension if they propose invalid or conflicting blocks. Validators are subject to punishment if they engage in malicious behavior, such as abstaining from voting. Punishments for validators can include slashing. Computing nodes have their privileges restricted or temporarily suspended if they report wrong smart contract execution results to the consensus layer.

7.3 Committee Selection

The committee selection process determines who will be a proposer, validators, and computing nodes in each epoch. The selection process aims to ensure a fair and decentralized committee composition. In Phase 1, we randomly select proposers, validators, and computing nodes. Later, we will introduce a committee selection algorithm based on stakes and age. Nodes with a larger stake have a higher probability of being selected to join the committee. This design encourages token holders to actively participate in the network by staking their tokens, increasing their chances of being chosen as committee members.

7.4 Delegation

Staking delegation is a mechanism that allows participants to delegate their staking rights to other validators on the network. On Hela, staking involves holding and "staking" a certain amount of HELA tokens as collateral to secure the network and participate in block validation. However, not everyone may possess the technical expertise, resources, or competitive edge to run their validator nodes or effectively cover the costs associated with node operation. Staking delegation addresses this challenge by enabling individuals to delegate their staking rights to trusted and competent validators who can carry out the validation process on their behalf. By delegating their stake, participants can still earn staking rewards.

Under a delegation mechanism, participants have three choices, namely (i) operating a node to run for validators, (ii) becoming a delegator, and (iii) abstaining. Researchers have studied participants' strategic behavior using game theory (e.g., [19,34]). This research provides insights as to how much commission fees validators should earn to maximize their revenues. As only the internal nodes organize the committee in Phase 1, the delegation mechanism will be rolled out in Phase 2.

7.5 Taxation and Buyback Mechanism

Taxation and buyback mechanisms play significant roles in Hela, contributing to stability, sustainability, and value creation. The taxation mechanism collects 10% of the stable coin fees on the execution layer and uses them to purchase and burn Hela native tokens.

$$w_S(E,G) = 0.1. \quad (5)$$

The buyback mechanism will support token value and show the credibility of operation [12]. A buyback is periodically executed considering the market situation with the approval of committees.

8 Conclusions

In conclusion, this whitepaper provides an in-depth introduction of Hela, a next-generation Layer 1 public blockchain system designed to address the prevailing challenges in the current public blockchain landscape. These challenges, namely data fragmentation, interoperability, inadequate confidentiality mechanisms, absence of effective identity management, and unstable transaction fees, have hindered the broader and more comprehensive adoption of blockchain technology across industries.

We believe Hela's innovative solutions - a modular architecture with an integration layer, flexible and auditable confidentiality, multi-level decentralized identity management, and stable transaction fees - will resolve these issues. By offering these features, Hela fosters an environment conducive to expanded blockchain adoption, thus allowing this groundbreaking technology to penetrate deeper into various sectors of industry and everyday life.

References

[1] CoinMarketCap. https://coinmarketcap.com, 2023.

[2] Crypto's growing pains: Why assessing sustainability characteristics is crucial. https://realise.asia/cryptos-growing-pains-why-assessing-sustainability-characteristics-is-crucial/, 2023.

[3] DID W3C standard. https://www.w3.org/TR/did-core/, 2023.

[4] Give me some privacy: How blockchains can achieve mass adoption. https://realise.asia/give-me-some-privacy-how-blockchains-can-achieve-mass-adoption/, 2023.

[5] Oasis. https://oasisprotocol.org, 2023.

[6] Ontology. https://ont.io, 2023.

[7] Optimism. https://www.optimism.io, 2023.

[8] Train-And-Hotel Problem. https://ethresear.ch/t/solving-train-and-hotel-problem-with-asynchronous-message-and-await-async/5836, 2023.

[9] ADAMS, H., ZINSMEISTER, N., SALEM, M., KEEFER, R., AND ROBINSON, D. Uniswap v3 core. *Tech. rep., Uniswap, Tech. Rep.* (2021).

[10] AKYILDIRIM, E., CORBET, S., LUCEY, B., SENSOY, A., AND YAROVAYA, L. The relationship between implied volatility and cryptocurrency returns. *Finance Research Letters 33* (2020), 101212.

[11] AL GUINDY, M. Cryptocurrency price volatility and investor attention. *International Review of Economics & Finance 76* (2021), 556–570.

[12] ALLEN, D. W., BERG, C., AND DAVIDSON, S. Buyback and burn mechanisms: Price manipulation or value signalling? *Available at SSRN 4231845* (2022).

[13] ANDOLA, N., YADAV, V. K., VENKATESAN, S., VERMA, S., ET AL. Anonymity on blockchain based e-cash protocols—a survey. *Computer Science Review 40* (2021), 100394.

[14] ANTE, L. Non-fungible token (nft) markets on the ethereum blockchain: Temporal development, cointegration and interrelations. *Economics of Innovation and New Technology* (2022), 1–19.

[15] ARROYO, J., DAVÓ, D., MARTÍNEZ-VICENTE, E., FAQIR-RHAZOUI, Y., AND HASSAN, S. Dao-analyzer: Exploring activity and participation in blockchain organizations. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing* (2022), pp. 193–196.

[16] BALAJI, S., KRISHNAN, M. N., VAJHA, M., RAMKUMAR, V., SASIDHARAN, B., AND KUMAR, P. V. Erasure coding for distributed storage: An overview. *Science China Information Sciences 61* (2018), 1–45.

[17] BELCHIOR, R., VASCONCELOS, A., GUERREIRO, S., AND CORREIA, M. A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR) 54*, 8 (2021), 1–41.

[18] BOURI, E., LAU, C. K. M., LUCEY, B., AND ROUBAUD, D. Trading volume and the predictability of return and volatility in the cryptocurrency market. *Finance Research Letters 29* (2019), 340–346.

[19] BRÜNJES, L., KIAYIAS, A., KOUTSOUPIAS, E., AND STOUKA, A.-P. Reward sharing schemes for stake pools. In *Proc. of IEEE European Symposium on Security and Privacy (EuroS&P)* (Sept. 2020), pp. 256–275.

[20] BUCHMAN, E. *Tendermint: Byzantine fault tolerance in the age of blockchains*. PhD thesis, University of Guelph, 2016.

[21] BUTERIN, V., ET AL. A next-generation smart contract and decentralized application platform. *white paper 3*, 37 (2014), 2–1.

[22] CAO, L. Decentralized ai: Edge intelligence and smart blockchain, metaverse, web3, and desci. *IEEE Intelligent Systems 37*, 3 (2022), 6–19.

[23] CASTRO, M., LISKOV, B., ET AL. Practical byzantine fault tolerance. In *OsDI* (1999), vol. 99, pp. 173–186.

[24] COMMISSION, C. F. T. Order instituting proceedings pursuant to section 6(c) and (d) of the commodity exchange act, making findings, and imposing remedial sanctions, 2021.

[25] DAS, D., BOSE, P., RUARO, N., KRUEGEL, C., AND VIGNA, G. Understanding security issues in the nft ecosystem. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (2022), pp. 667–681.

[26] DECRYPT. 'rogue developers' drain merlin dex of $1.82 million, 2023.

[27] DOS SANTOS, S., SINGH, J., THULASIRAM, R. K., KAMALI, S., SIRICO, L., AND LOUD, L. A new era of blockchain-powered decentralized finance (defi)-a review. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (2022), IEEE, pp. 1286–1292.

[28] DYSON, S., BUCHANAN, W. J., AND BELL, L. The challenges of investigating cryptocurrencies and blockchain related crime. *arXiv preprint arXiv:1907.12221* (2019).

[29] EKBERG, J.-E., KOSTIAINEN, K., AND ASOKAN, N. Trusted execution environments on mobile devices. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (2013), pp. 1497–1498.

[30] EL FAQIR, Y., ARROYO, J., AND HASSAN, S. An overview of decentralized autonomous organizations on the blockchain. In *Proceedings of the 16th international symposium on open collaboration* (2020), pp. 1–8.

[31] FANTI, G., KOGAN, L., OH, S., RUAN, K., VISWANATH, P., AND WANG, G. Compounding of Wealth in Proof-of-Stake Cryptocurrencies. In *Financial Cryptography and Data Security* (2019), Springer International Publishing, pp. 42–61.

[32] FAR, S. B., RAD, A. I., AND ASSAR, M. R. Blockchain and its derived technologies shape the future generation of digital businesses: A focus on decentralized finance and the metaverse. *Data Science and Management* (2023).

[33] FOOLADGAR, M., MANSHAEI, M. H., JADLIWALA, M., AND RAHMAN, M. A. On incentive compatible role-based reward distribution in algorand.

[34] GERSBACH, H., MAMAGEISHVILI, A., AND SCHNEIDER, M. Staking Pools on Blockchains. *arXiv [cs.GT]* (Mar. 2022).

[35] GUDGEON, L., MORENO-SANCHEZ, P., ROOS, S., MCCORRY, P., AND GERVAIS, A. Sok: Layer-two blockchain protocols. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24* (2020), Springer, pp. 201–226.

[36] HAN, P., YAN, Z., DING, W., FEI, S., AND WAN, Z. A survey on cross-chain technologies. *Distributed Ledger Technologies: Research and Practice 2*, 2 (2023), 1–30.

[37] HANNAN, M. A., SHAHRIAR, M. A., FERDOUS, M. S., CHOWDHURY, M. J. M., AND RAHMAN, M. S. A systematic literature review of blockchain-based e-kyc systems. *Computing* (2023), 1–30.

[38] HASHEMI JOO, M., NISHIKAWA, Y., AND DANDAPANI, K. Cryptocurrency, a successful application of blockchain technology. *Managerial Finance 46*, 6 (2020), 715–733.

[39] HEILMAN, E., BALDIMTSI, F., AND GOLDBERG, S. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In *International conference on financial cryptography and data security* (2016), Springer, pp. 43–60.

[40] HOPWOOD, D., BOWE, S., HORNBY, T., WILCOX, N., ET AL. Zcash protocol specification. *GitHub: San Francisco, CA, USA 4*, 220 (2016), 32.

[41] HUYNH-THE, T., GADEKALLU, T. R., WANG, W., YENDURI, G., RANAWEERA, P., PHAM, Q.-V., DA COSTA, D. B., AND LIYANAGE, M. Blockchain for the metaverse: A review. *Future Generation Computer Systems* (2023).

[42] JAUERNIG, P., SADEGHI, A.-R., AND STAPF, E. Trusted execution environments: properties, applications, and challenges. *IEEE Security & Privacy 18*, 2 (2020), 56–60.

[43] JEAN, J., NIKOLIC, I., PEYRIN, T., AND SEURIN, Y. Deoxys v1. 41. *Submitted to CAESAR 124* (2016).

[44] KAKAVAND, H., KOST DE SEVRES, N., AND CHILTON, B. The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. *Available at SSRN 2849251* (2017).

[45] KALODNER, H., GOLDFEDER, S., CHEN, X., WEINBERG, S. M., AND FELTEN, E. W. Arbitrum: Scalable, private smart contracts. In *27th USENIX Security Symposium (USENIX Security 18)* (2018), pp. 1353–1370.

[46] KANANI, J., ARJUN, A., NAILWAL, S., AND BJELIC, M. Polygon whitepaper. *Bengaluru, India: Polygon, Apr* (2021).

[47] KETHINENI, S., AND CAO, Y. The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review 30*, 3 (2020), 325–344.

[48] KIONG, L. V. *DeFi, NFT and GameFi Made Easy: A Beginner's Guide to Understanding and Investing in DeFi, NFT and GameFi Projects*. Liew Voon Kiong, 2021.

[49] KIONG, L. V. *Metaverse Made Easy: A Beginner's Guide to the Metaverse: Everything you need to know about Metaverse, NFT and GameFi*. Liew Voon Kiong, 2022.

[50] KIONG, L. V. *Web3 Made Easy: A Comprehensive Guide to Web3: Everything you need to know about Web3, Blockchain, DeFi, Metaverse, NFT and GameFi*. Liew Voon Kiong, 2022.

[51] KLEPPMANN, M. Implementing curve25519/x25519: A tutorial on elliptic curve cryptography.

[52] KORIR, M., PARKIN, S., AND DUNPHY, P. An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control. In *Proc. of Symposium on Usable Privacy and Security (SOUPS)* (2022), pp. 195–211.

[53] KWON, J., AND BUCHMAN, E. Cosmos whitepaper. *A Netw. Distrib. Ledgers 27* (2019).

[54] LEE, J. Y. A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Business Horizons 62*, 6 (2019), 773–784.

[55] LEHAR, A., PARLOUR, C. A., AND ZOICAN, M. Liquidity fragmentation on decentralized exchanges. *Available at SSRN 4267429* (2022).

[56] LI, M., LIN, Y., ZHANG, J., AND WANG, W. Cochain: High concurrency blockchain sharding via consensus on consensus.

[57] LI, M., LIN, Y., ZHANG, J., AND WANG, W. Jenga: Orchestrating smart contracts in sharding-based blockchain for efficient processing. In *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)* (2022), IEEE, pp. 133–143.

[58] LI, M., WANG, W., AND ZHANG, J. Lb-chain: Load-balanced and low-latency blockchain sharding via account migration. *IEEE Transactions on Parallel and Distributed Systems* (2023).

[59] LI, Y., LIU, H., AND TAN, Y. Polybridge: A crosschain bridge for heterogeneous blockchains. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2022), IEEE, pp. 1–2.

[60] LIU, L., ZHOU, S., HUANG, H., AND ZHENG, Z. From technology to society: An overview of blockchain-based dao. *IEEE Open Journal of the Computer Society 2* (2021), 204–215.

[61] LIU, Z., XIANG, Y., SHI, J., GAO, P., WANG, H., XIAO, X., WEN, B., AND HU, Y.-C. Hyperservice: Interoperability and programmability across heterogeneous blockchains. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (2019), pp. 549–566.

[62] LOKHAVA, M., LOSA, G., MAZIÈRES, D., HOARE, G., BARRY, N., GAFNI, E., JOVE, J., MALINOWSKY, R., AND MCCALEB, J. Fast and secure global payments with stellar. In *Proceedings of the 27th ACM Symposium on Operating Systems Principles* (2019), pp. 80–96.

[63] MADINE, M., SALAH, K., JAYARAMAN, R., AL-HAMMADI, Y., ARSHAD, J., AND YAQOOB, I. appxchain: Application-level interoperability for blockchain networks. *IEEE Access 9* (2021), 87777–87791.

[64] MAYER, H. zk-snark explained: Basic principles. *URL https://blog. coinfabrik. com/wp-content/uploads/2017/03/zkSNARK-explained_basic_principles. pdf* (2016).

[65] MEHAR, M. I., SHIER, C. L., GIAMBATTISTA, A., GONG, E., FLETCHER, G., SANAYHIE, R., KIM, H. M., AND LASKOWSKI, M. Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack. *Journal of Cases on Information Technology (JCIT) 21*, 1 (2019), 19–32.

[66] MOZUMDER, M. A. I., SHEERAZ, M. M., ATHAR, A., AICH, S., AND KIM, H.-C. Overview: Technology roadmap of the future trend of metaverse based on iot, blockchain, ai technique, and medical domain metaverse activity. In *2022 24th International Conference on Advanced Communication Technology (ICACT)* (2022), IEEE, pp. 256–261.

[67] NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review* (2008).

[68] PIYADIGAMA, D., AND PORAVI, G. An analysis of the features considerable for nft recommendations. In *2022 15th International Conference on Human System Interaction (HSI)* (2022), IEEE, pp. 1–7.

[69] POONGODI, M., SHARMA, A., VIJAYAKUMAR, V., BHARDWAJ, V., SHARMA, A. P., IQBAL, R., AND KUMAR, R. Prediction of the price of ethereum blockchain cryptocurrency in an industrial finance system. *Computers & Electrical Engineering 81* (2020), 106527.

[70] PROELSS, J., SEVIGNY, S., AND SCHWEIZER, D. Gamefi-the perfect symbiosis of blockchain, tokens, defi, and nfts? *Tokens, DeFi, and NFTs* (2023).

[71] QIN, R., DING, W., LI, J., GUAN, S., WANG, G., REN, Y., AND QU, Z. Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems 53*, 4 (2022), 2073–2082.

[72] ROCKET, T. Snowflake to avalanche: A novel metastable consensus protocol family for cryptocurrencies. *Available [online].[Accessed: 4-12-2018]* (2018).

[73] SABT, M., ACHEMLAL, M., AND BOUABDALLAH, A. Trusted execution environment: what it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/Ispa* (2015), vol. 1, IEEE, pp. 57–64.

[74] SANTOS, F., AND KOSTAKIS, V. The dao: a million dollar lesson in blockchain governance. *School of Business and Governance, Ragnar Nurkse Department of Innovation and Governance* (2018).

[75] SCHÄR, F. Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB of St. Louis Review* (2021).

[76] SCHULTE, S., SIGWART, M., FRAUENTHALER, P., AND BORKOWSKI, M. Towards blockchain interoperability. In *Business Process Management: Blockchain and Central and Eastern Europe Forum: BPM 2019 Blockchain and CEE Forum, Vienna, Austria, September 1–6, 2019, Proceedings 17* (2019), Springer, pp. 3–10.

[77] SHI, H., WANG, S., HU, Q., AND CHENG, X. Black swan in blockchain: Micro analysis of natural forking. *IEEE Transactions on Dependable and Secure Computing* (2022).

[78] SWAN, M., ET AL. Blockchain theory of programmable risk: Black swan smart contracts. *Blockchain Economics: Implications of Distributed Ledgers, World Scientific* (2019), 171–194.

[79] SZYDLO, M. Merkle tree traversal in log space and time. In *Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23* (2004), Springer, pp. 541–554.

[80] THIBAULT, L. T., SARRY, T., AND HAFID, A. S. Blockchain scaling using rollups: A comprehensive survey. *IEEE Access* (2022).

[81] TROZZE, A., KAMPS, J., AKARTUNA, E. A., HETZEL, F. J., KLEINBERG, B., DAVIES, T., AND JOHNSON, S. D. Cryptocurrencies and future financial crime. *Crime Science 11* (2022), 1–35.

[82] VALDEOLMILLOS, D., MEZQUITA, Y., GONZÁLEZ-BRIONES, A., PRIETO, J., AND CORCHADO, J. M. Blockchain technology: a review of the current challenges of cryptocurrency. In *Blockchain and Applications: International Congress* (2020), Springer, pp. 153–160.

[83] VAN SABERHAGEN, N. Cryptonode v 2.0, monero white paper. 2016.

[84] WANG, B., LIU, H., LIU, C., YANG, Z., REN, Q., ZHENG, H., AND LEI, H. Blockeye: Hunting for defi attacks on blockchain. In *2021 IEEE/ACM 43rd International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)* (2021), IEEE, pp. 17–20.

[85] WANG, B., YUAN, X., DUAN, L., MA, H., SU, C., AND WANG, W. Defiscanner: Spotting defi attacks exploiting logic vulnerabilities on blockchain. *IEEE Transactions on Computational Social Systems* (2022).

[86] WANG, Q., LI, R., WANG, Q., AND CHEN, S. Non-fungible token (nft): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447* (2021).

[87] WEYL, E. G., OHLHAVER, P., AND BUTERIN, V. Decentralized society: Finding web3's soul. *Available at SSRN 4105763* (2022).

[88] WHITE, B., MAHANTI, A., AND PASSI, K. Characterizing the opensea nft marketplace. In *Companion Proceedings of the Web Conference 2022* (2022), pp. 488–496.

[89] WOOD, G. Polkadot: Vision for a heterogeneous multi-chain framework. *White paper 21*, 2327 (2016), 4662.

[90] XU, J., AND FENG, Y. Reap the harvest on blockchain: A survey of yield farming protocols. *IEEE Transactions on Network and Service Management 20*, 1 (2022), 858–869.

[91] YADAV, S. P., AGRAWAL, K. K., BHATI, B. S., AL-TURJMAN, F., AND MOSTARDA, L. Blockchain-based cryptocurrency regulation: An overview. *Computational Economics 59*, 4 (2022), 1659–1675.

[92] YAKOVENKO, A. Solana: A new architecture for a high performance blockchain v0. 8.13. *Whitepaper* (2018).

[93] YAROVAYA, L., MATKOVSKYY, R., AND JALAN, A. The effects of a "black swan" event (covid-19) on herding behavior in cryptocurrency markets. *Journal of International Financial Markets, Institutions and Money 75* (2021), 101321.

[94] YUAN, Y., AND WANG, F.-Y. Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems 48*, 9 (2018), 1421–1428.

[95] ZHANG, S., AND LEE, J.-H. Double-spending with a sybil attack in the bitcoin decentralized network. *IEEE transactions on Industrial Informatics 15*, 10 (2019), 5715–5722.

[96] ZHENG, Z., XIE, S., DAI, H.-N., CHEN, X., AND WANG, H. Blockchain challenges and opportunities: A survey. *International journal of web and grid services 14*, 4 (2018), 352–375.

[97] ZWITTER, A., AND HAZENBERG, J. Decentralized network governance: blockchain technology and the future of regulation. *Frontiers in Blockchain 3* (2020), 12.