

Virtual Blockchain Network for Secure Financial and Industrial Applications

Alexander Bogdanov[1], Valery Khvatov[2], Alexei Uteshev[1], and Nadezhda Shchegoleva[1](✉)

[1] St. Petersburg University, Saint Petersburg, Russia
{a.v.bogdanov,a.uteshev,n.shchegoleva}@spbu.ru
[2] DGT Technologies AG, Toronto, Canada

Abstract. This study introduces blockchain virtualization as a solution to tackle modern challenges. Evaluating the DGT network as a model, experiments probe the impact of virtualization (network-of-networks) on scaling and latency, shedding light on its potential for enhanced performance. Conclusively, the study emphasizes the significance of blockchain virtualization for enhancing blockchain performance and scalability. Future directions of research are discussed, including testing of security and privacy within virtualized environments and the potential of virtualization in shaping cloud-based blockchain-as-a-service solutions. In sum, blockchain virtualization emerges as a pivotal innovation poised to redefine the landscape of blockchain technology and its applications.

Keywords: DGT · Layer 1 digital platform · multi-party computation over blockchain · decentralization

1 Introduction

More than a decade has passed since Satoshi Nakamoto introduced the groundbreaking concept of blockchain, revolutionizing the way we perceive decentralized transactions and particularly cryptocurrencies. Despite this initial innovation, the blockchain landscape remains relatively stagnant. Initiatives like Ethereum, Algorand, Ripple, and Stellar have contributed their unique features, yet the underlying architecture largely echoes Nakamoto's original design. While blockchain has immense potential, its broader adoption has been hampered by persistent challenges that seem to demand a reevaluation of its architecture.

A closer examination of the current state of blockchain technology reveals several bottlenecks that have hindered its widespread acceptance:

– **Scalability Woes**: As participation in blockchain networks grows, the speed of transaction processing tends to decrease. This phenomenon stems from the communication-intensive nature of peer-to-peer solutions and the trade-offs presented by the "blockchain trilemma" 1 (also known as CAP theorem). It dictates that decentralized solutions can prioritize two out of three traits: decentralization, scalability, and security.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14815, pp. 142–161, 2024.
https://doi.org/10.1007/978-3-031-65154-0_9

- **Escalating Transaction Costs**: High transaction costs, often unrelated to cryptocurrencies, arise from redundancy and communication inefficiency within the blockchain network 2. This, in turn, affects the overall efficiency of the solution.
- **Confidentiality Gaps**: While public blockchains offer anonymous ownership, transaction details remain transparent. The absence of built-in private transactions prevents blockchain technology from being embraced by enterprises, including financial institutions, due to privacy concerns 3.
- **Smart Contract Insecurities**: Vulnerabilities within smart contracts, though enabling customization, expose the network to security threats 4. Simultaneously, the computational complexity of executing these contracts raises communication costs and limits efficiency.
- **Interoperability Impediments**: The blockchain ecosystem's lack of seamless integration between networks has prevented the technology from realizing its full potential. Solutions like Polkadot, Cosmos, and Avalanche have attempted to address this, yet the overall architecture has limited their effectiveness 5.

In response to these challenges, this work introduces the concept of the Virtual Blockchain Network, which amalgamates the best architectural practices from various distributed solutions 6. This paradigm envisions a revamped approach to blockchain architecture that promises to surmount the limitations inherent in traditional blockchains.

Blockchain virtualization is rethought in terms of key architectural solutions that allow participants in information exchange to interact effectively, including launching their own ecosystems. Blockchain virtualization entails abstracting the blockchain infrastructure, enabling the creation and management of multiple virtual instances within a shared physical blockchain network. This novel approach offers enhanced scalability, isolation, and resource allocation. By deploying tailored blockchain networks that cater to specific organizational requirements, the Virtual Blockchain Network overcomes the constraints imposed by a single, communal blockchain.

At its core, this virtualization leverages a hybrid architecture in which clusters mimic independent blockchain ecosystems. A two-layer consensus mechanism underpins this arrangement, ensuring consensus both at the cluster level and across the broader network. This innovative architecture effectively addresses scalability constraints while bolstering transaction processing speed and preserving decentralization.

The transformative potential of the Virtual Blockchain Network becomes evident in its capability to rectify the existing limitations of classical blockchain architectures. This advancement, characterized by an efficient and scalable consensus mechanism, integration of Directed Acyclic Graph (DAG) technology, and a hybrid cluster-segment structure, paves the way for a blockchain ecosystem that is more scalable, cost-effective, and suitable for broader adoption.

To illustrate the practical application of this concept, the DGT network is employed as a testament to the real-world viability of virtualized networks. DGT, with its hybrid approach 15, exemplifies how a Virtual Blockchain Network can transcend traditional barriers and catalyze the evolution of blockchain technology.

The versatility of the Virtual Blockchain Network concept extends to various use cases 7:

- **Financial Processing**: Virtual blockchain networks offer a platform for efficient, secure, and cost-effective financial transactions. Smart contracts executed on the network facilitate seamless cross-border payments, trade settlements, and supply chain finance while ensuring transparency and immutability.
- **Distributed Identity**: Virtualized blockchains enhance identity management by allowing users to control their digital identities securely. Utilizing self-sovereign identity solutions, individuals can manage and share personal information while maintaining privacy.
- **Secure Data Sharing**: Organizations can utilize virtual blockchain networks to securely share sensitive data across partners, customers, and stakeholders. The integration of cryptographic techniques ensures data integrity and confidentiality throughout the sharing process
- **Industrial Coo**peration: Virtualized blockchain networks pave the way for enhanced collaboration within industries. Consortiums can establish their own dedicated blockchains, enabling streamlined supply chain management, data exchange, and interoperability between diverse stakeholders
- **Virtual Data Networks**: Virtual blockchain networks can act as frameworks for the creation of decentralized data marketplaces. Such platforms allow users to share and monetize their data while maintaining control over its usage and ownership.

Each of these use cases harnesses the potential of virtualized blockchain networks to overcome traditional limitations and drive innovation across industries. By offering improved scalability, enhanced security, and tailored functionality, these networks facilitate the integration of blockchain technology into diverse applications.

2 Evolving the Blockchain Blueprint: Architectural Innovations and Concepts

The evolution of blockchain technology has been driven by the constant pursuit of addressing its inherent challenges and limitations. In this article, we delve into the fundamental aspects of blockchain solutions, explore the layered approach to blockchain architecture, and shed light on the paradigm-shifting concepts of Web 3 and tokenomics. We also delve into the emerging need for virtualized blockchains and the critical importance of striking the right balance between centralization and decentralization.

2.1 Foundations of Blockchain Architecture

At the heart of any blockchain architecture lies a distributed ledger that forms the foundation for recording transactions in a secure and transparent manner. This ledger, often referred to as the blockchain, consists of a chronological chain of blocks, with each block containing a set of transactions. The architecture encompasses various components and mechanisms that collectively ensure the integrity and immutability of the data stored within the blockchain. NISTIR 8202 8 and ITU-T 9 guidelines offer foundational insights into understanding this intricate architecture (Fig. 1).

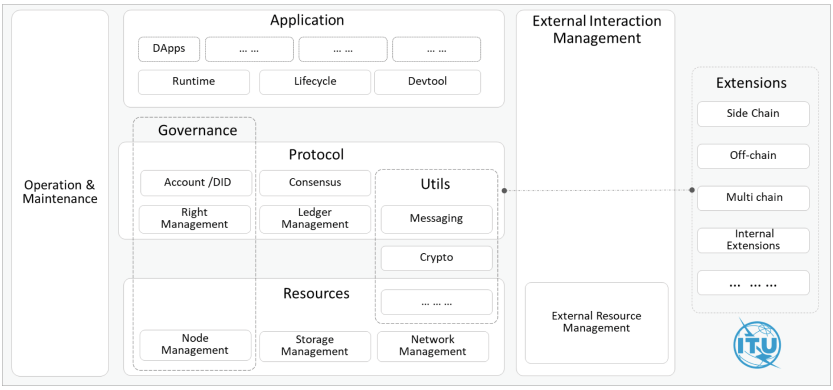

Fig. 1. TU's DLT Reference Architecture.

Main Components of Classical Blockchain Architecture:

- Transactions: Transactions are the fundamental units of data in a blockchain. They represent actions or events that alter the state of the system. Transactions can include financial transfers, smart contract executions, or any action that requires recording.
- **Blocks**: Blocks are containers that group a set of transactions together. Each block includes a reference to the previous block (creating a chain), a timestamp, and a cryptographic hash of its contents. The hash ensures the integrity of the data within the block and establishes a strong link to the previous block.
- **Decentralized Network**: A network of nodes maintains and verifies the blockchain. Each node has a copy of the entire blockchain. The decentralized nature ensures that no single entity has control over the network, enhancing security and preventing single points of failure.
- **Consensus Mechanism**: Consensus mechanisms determine how transactions are validated and added to the blockchain. Traditional mechanisms include Proof of Work (PoW), where nodes compete to solve complex puzzles to validate transactions, and Proof of Stake (PoS), where validators are chosen based on the number of tokens they hold.
- **Smart Contracts**: Smart contracts are self-executing contracts with predefined rules and conditions. They automatically execute when certain conditions are met, eliminating the need for intermediaries, and enhancing automation.
- **Cryptography**: Cryptography plays a pivotal role in blockchain security. It ensures the privacy of transactions, verifies identities, and secures communication between nodes.
- **Public and Private Keys**: Users have a pair of cryptographic keys – a public key for identification and a private key for signing transactions. The private key is kept secret and is used to prove ownership of assets.
- **Hashing**: Cryptographic hash functions generate fixed-length strings of characters (hashes) from variable-length input. Hashes are used to ensure the integrity of data and create the linkage between blocks.
- **Security and transparency** are the cornerstones of any blockchain architecture, establishing a foundation of trust in a decentralized environment. These mechanisms

work in tandem to safeguard the integrity of data, prevent tampering, and promote openness throughout the network. By combining cryptographic techniques, decentralized consensus, and immutability, blockchain architecture ensures that information remains unalterable, transactions are verified, and participants can have confidence in the validity of the recorded data. This short article delves into the essential mechanisms that underpin security and transparency within blockchain systems, shedding light on their crucial roles in shaping the future of secure, trustworthy transactions.

2.2 Permission Network Design

Blockchain networks exhibit a versatile range of designs to accommodate different use cases and requirements. These designs can be broadly categorized into three main types: public networks, private networks, and consortium networks. Each variant caters to distinct scenarios, offering tailored solutions for various entities and collaborations.

- **Public Networks**: Public blockchain networks, exemplified by pioneers like Bitcoin and Ethereum, uphold the essence of decentralization and inclusivity. These networks are open to all participants, irrespective of their identity or affiliation. Transactions are validated and recorded by a distributed network of nodes, ensuring transparency and consensus through protocols such as Proof of Work (PoW) and Proof of Stake (PoS). Public networks emphasize transparency, as all transactions are visible to anyone and can be independently verified.
- **Private Networks**: In contrast, private blockchain networks are designed for specific entities seeking a controlled and confidential environment. These networks restrict participation to pre-approved participants, ensuring a closed ecosystem. Private networks are well-suited for enterprises or organizations that require a secure platform for internal processes, supply chain management, or inter-departmental interactions. The degree of decentralization and transparency may vary, and participants typically have more control over consensus mechanisms.
- **Consortium Networks**: Consortium networks strike a balance between public and private designs, representing a collaborative effort among multiple entities. These networks are governed by a group of organizations with shared interests, making them suitable for industries or sectors where cooperation and data sharing are pivotal. Consortium networks offer more decentralization and transparency compared to private networks, while maintaining some level of controlled access.

2.3 Consensus Mechanisms and Network Hierarchies: Ensuring Agreement and Efficiency

The essence of blockchain technology rests upon consensus mechanisms, the mechanisms by which network participants achieve agreement on the state of the shared ledger 10. These mechanisms play a pivotal role in maintaining the integrity and trustworthiness of distributed ledgers. Diverse consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT) share the common objective of achieving consensus through various means, while simultaneously exhibiting their unique strengths and limitations.

PoW, the algorithm underpinning Bitcoin and several other networks, demands computational effort as a proof of commitment. While it ensures robust security by requiring miners to compete for block validation, its energy consumption and slow transaction finality are notable drawbacks. The energy-intensive nature of PoW raises environmental concerns and constrains scalability.

On the other hand, PoS assigns the block validation privilege to participants who hold a significant stake in the network's native cryptocurrency. This approach mitigates the energy inefficiency of PoW, but introduces challenges related to centralization risks and the "nothing at stake" problem, where validators might support multiple chains simultaneously.

BFT consensus mechanisms aim for fast and deterministic finality by requiring network participants to agree on each transaction's validity before appending it to the blockchain. While offering quick transactions, BFT algorithms face challenges in terms of scalability and communication cost.

Consensus mechanisms differ in their consensus determination methods: deterministic (BFT) or probabilistic (PoW and PoS). Deterministic consensus ensures finality with high certainty, while probabilistic consensus offers statistical finality. The trade-off lies between absolute certainty and faster confirmation times.

The GOSSIP protocol 11, commonly employed for node communication, employs a peer-to-peer approach where nodes spread information to their peers. While simple and decentralized, GOSSIP's efficiency diminishes as the network scales due to communication redundancy, latency, and potential data loss.

Hierarchical network 12 designs provide an innovative alternative to address these challenges. By segmenting nodes into clusters, hierarchical networks reduce the direct communication required among all nodes. This structure enhances scalability and performance, tackling the communication bottleneck of flat P2P architectures.

2.4 Layered Architectural Approach

To address the inherent limitations of blockchain technology, a common approach is to break down the architecture into separate functional layers 13. This allows for more efficient and effective management of the triple limitations of blockchain, as well as addressing key characteristics like security, scalability, and functionality. The decomposition of complex systems into layers is a widely accepted approach and can vary in emphasis. In some cases, the decomposition is used to highlight the fundamental conceptual entities of the technology, including a data layer, network layer, and application layer.

Such approaches inherit the classical network model known as the Open Systems Interconnection model (OSI model, 16). The approach describes the component structure of the system well but avoids the issues of decentralization that are essential for the blockchain.

Within the framework of this approach, the following components can be distinguished (Fig. 2):

– **Layer 0 (L0)** represents the physical layer of the blockchain, which includes hardware, Internet protocols, cloud solutions, and protocols that facilitate interaction

between different protocols at the architecture level. It also encompasses Blockchain as a Service (BaaS) solutions and Blockchain DevOps infrastructure.

- **Layer 1 (L1)** is the base protocol layer of the blockchain architecture, responsible for fundamental blockchain functionality, such as transaction validation and network consensus. Layer 1 prioritizes security, particularly the consensus mechanism. Common Layer 1 blockchain solutions include Bitcoin, Ethereum, Binance Smart Chain (BSC), and Algorand.
- **Layer 2 (L2)** solutions work in conjunction with Layer 1 to provide additional features or improvements without compromising the security and scalability of the underlying blockchain network. Examples of L2 solutions include payment channels (Lightning Network, Raiden Network, and Polygon), sidechains, Plasma, sharding, and rollups.
- **Layer 3 (L3)** focuses on enabling interoperability, supporting decentralized identity, and providing off-chain computation capabilities. This layer ensures different blockchain networks and systems can communicate and interact seamlessly. It also includes the development of decentralized data storage and exchange solutions, such as IPFS, and off-chain computation solutions like Quant and Chainlink.
- **Layer 4 (L4)**, also known as the Application and Blockchain API layer, is the topmost layer of the blockchain architecture. This layer includes applications that use the blockchain network and APIs that allow developers to build decentralized applications (DApps) on top of the blockchain. It is responsible for providing a user interface for accessing blockchain features and interacting with the blockchain network. Examples of applications in Layer 4 include decentralized exchanges, digital asset marketplaces, and voting systems. Blockchain APIs, such as Ethereum's Web3.js and Bitcoin's JSON-RPC API, also operate in Layer 4.

It is important to understand that the layered blockchain architecture model presented is a logical interpretation and that final solutions can span across multiple layers. Moreover, different layers can be utilized for data exchange, considering the workload profiles and specific characteristics such as the amount and dynamics of data transferred, and the required level of security. In the following examples, the DGT platform will be presented as an integrated system, utilizing mechanisms from different layers.

WEB 3 and Tokenomics

The evolution of the internet has brought us to the cusp of a new era known as Web 3.0 17, where blockchain technology plays a pivotal role in redefining online interactions. Web 3.0 (Web 3) envisions a decentralized digital landscape that prioritizes privacy, security, and user empowerment. At its core, Web 3 leverages blockchain's unique attributes to enhance data ownership, privacy, and interoperability. Tokenomics, a fundamental aspect of Web 3, introduces a paradigm shift in how value is generated and distributed across digital ecosystems. By seamlessly integrating tokens into various aspects of the online experience, tokenomics reshapes the dynamics of digital economies, fostering innovation, inclusivity, and sustainable growth.

Web 3 Paradigm: Web 3 introduces a user-centric internet, enabling individuals to regain control over their data and identity. It emphasizes peer-to-peer interactions, decentralization, and data ownership. The foremost contribution of the Web 3 concept to network evolution lies in introducing tokenomics and privacy-by-design. Both aspects necessitate a profound shift in blockchain architecture.

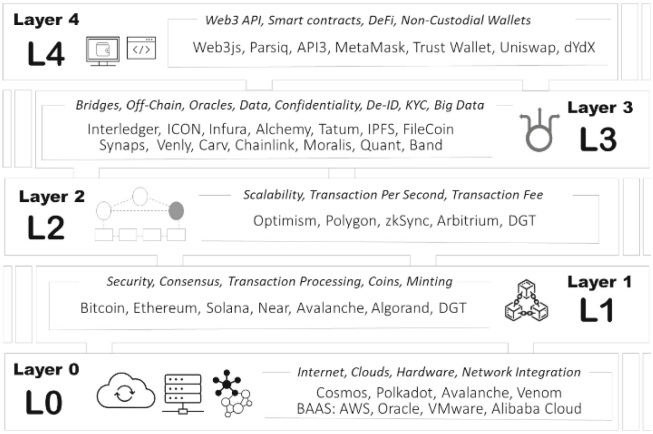

Fig. 2. TU's DLT Reference Architecture Layered Blockchain Solutions Model.

Tokenomics and Hybrid Approach: Tokens serve as the lifeblood of the blockchain ecosystem, representing value and enabling participation. They incentivize network contributors, facilitate governance, and streamline transactions. While tokens are intrinsic to public blockchains, even private blockchain systems like Hyperledger Fabric benefit from tokenization. The hybrid approach, combining public and private features, addresses redundancy and infrastructure limitations.

2.5 Requirements for a Virtualized Blockchain: Orchestrating Seamless Connectivity

In the pursuit of constructing a virtualized blockchain ecosystem, a set of critical requirements emerges to ensure its effectiveness, adaptability, and utility 18. These requirements are aimed at facilitating the creation and management of multiple interconnected blockchain instances, fostering collaboration and interoperability among diverse networks. As a network of networks, a virtualized blockchain must meet several key prerequisites:

- **Scalability and Performance Enhancement**: A virtualized blockchain should transcend the limitations of individual blockchains by enabling horizontal and vertical scaling. This ensures that the ecosystem can accommodate a multitude of interconnected networks without compromising transaction speed or network performance.
- **Isolation and Customization**: Each blockchain instance within the virtualized environment should maintain its own characteristics, allowing for tailored customization and specialization according to unique use cases, regulatory frameworks, and business requirements.
- **Interoperability**: An essential feature of virtualized blockchains is the seamless exchange of data, assets, and value across instances. The architecture should facilitate

communication and collaboration among disparate networks, fostering an ecosystem of interconnectedness.
- **Security and Privacy**: Ensuring data confidentiality, integrity, and privacy across interconnected blockchains is paramount. Strong cryptographic mechanisms, Zero-Knowledge Proofs, and advanced privacy-preserving technologies should be incorporated to safeguard sensitive information.
- **Consensus Flexibility**: The architecture should support multiple consensus mechanisms to accommodate various use cases and network requirements. This includes Proof of Work (PoW), Proof of Stake (PoS), Byzantine Fault Tolerance (BFT), and more, enabling the selection of the most suitable consensus for each instance.
- **Resource Allocation and Optimization**: Efficient resource allocation ensures that the virtualized blockchain network operates optimally, avoiding overutilization or underutilization of resources. Dynamic allocation mechanisms can ensure fairness and efficient utilization across instances.
- **Decentralized Governance**: A decentralized governance model should guide decision-making processes across the virtualized environment. Clear rules and protocols for network upgrades, maintenance, and dispute resolution should be established to maintain the integrity of the ecosystem.
- **Adaptive Protocol Framework**: The architecture should allow for seamless protocol upgrades and enhancements to accommodate evolving technological standards, security measures, and industry best practices.
- **Ease of Use and Accessibility**: User-friendly interfaces, developer-friendly APIs, and comprehensive documentation should simplify the deployment, management, and interaction with virtualized blockchain instances.
- **Economic Sustainability**: The economic model should incentivize participation and contributions across interconnected networks. Tokenomics should be designed to reward validators, developers, and participants, ensuring long-term sustainability.
- **Cross-Chain Communication**: A standardized protocol for cross-chain communication and asset exchange should be established, facilitating frictionless value transfer between different blockchain instances.
- **Compliance and Regulation**: The architecture should support compliance with regulatory frameworks in various jurisdictions, enabling businesses to operate within legal boundaries while benefiting from the advantages of a virtualized blockchain network.

By meeting these requirements, this network of networks can unlock a new era of connectivity, collaboration, and innovation in the world of distributed ledger technology. The architecture should be rooted in Layer 1 networks while incorporating essential components from Layer 0 and Layer 2, offering a comprehensive and effective solution for a dynamic virtualized blockchain ecosystem.

2.6 Decentralization Issues in Virtualized Blockchain Ecosystems: Navigating the Spectrum

Decentralization, a foundational principle of blockchain technology, remains a cornerstone in the design of virtualized blockchain ecosystems 19. However, the quest for

an optimal level of decentralization presents a multifaceted challenge that requires a nuanced approach. While a fully decentralized network offers unparalleled security and resilience, it may not always align with practical implementation and performance demands.

The conventional metric for decentralization calculates the number of independent nodes participating in a network. Yet, this metric doesn't account for broader aspects that influence the degree of decentralization and its implications for practical applications. Factors like governance, token distribution, and network influence also contribute significantly to the architecture's decentralization.

A central issue in the realm of decentralization is the concept of "51% attack," whereby a single entity or coalition acquires majority control over the network's computational power. This concern highlights the need for mechanisms that safeguard against centralization of power, both in terms of computational resources and decision-making authority.

Striking a balance between full centralization and decentralization has led to the emergence of hybrid solutions. These hybrid approaches leverage the benefits of both centralized and decentralized architectures to create flexible, modular, and adaptive systems. Such hybrid models offer a higher degree of security compared to fully centralized systems while retaining a level of efficiency and scalability often associated with centralized setups.

The advantages of decentralized hybrid solutions are manifold. They encompass enhanced security, enabling resistance against single points of failure and malicious attacks. Scalability is another benefit, as decentralization allows the network to scale horizontally by adding nodes and instances as needed. This modular design fosters adaptability, making it possible to tailor solutions to specific use cases while maintaining interoperability.

Furthermore, decentralized hybrid architectures can mitigate latency issues that arise due to geographical distribution and network propagation delays. The architecture's modular nature enables strategic placement of nodes and instances to optimize communication paths and reduce latency.

Importantly, such architectures pave the way for smoother regulatory compliance. By striking a balance between decentralization and centralization, they can navigate the intricate regulatory landscape while upholding data integrity and security.

3 DGT as a Framework for Virtualization

In the pursuit of an optimal architectural solution for virtualized blockchain ecosystems, the DGT platform 15 stands as a testament to innovation and adaptability. Built upon a hybrid architecture, DGT presents a formidable framework that not only embraces decentralization principles but also offers a set of features tailored to engage institutional players, thereby fostering widespread adoption and usability.

DGT Digital Platform

The DGT platform is a pioneering blockchain solution characterized by its innovative Hybrid-Network Architecture (H-NET). This architecture 15 leverages a combination

of clusters and segments to establish an interconnected network of networks, enabling enhanced scalability, privacy, and customized consensus mechanisms. DGT empowers various blockchain instances within a unified ecosystem, supporting decentralized applications, secure data exchange, and efficient financial transactions. DGT provides a robust and reliable framework for decentralized data exchange, embracing the Web 3.0 principles of decentralization, sovereignty, and user empowerment. It fosters a new era of internet interactions, where users have greater control over their data, participate actively in network governance, and contribute to a more inclusive and decentralized digital ecosystem:

DGT is moving forward within the D3 paradigm:

- **Data integration** based on an innovative consensus mechanism.
- **Data management** through the entire life cycle.
- **Data delivery** enabling data presentation for any user in real time.

This allows DGT to implement applied innovative products within a single paradigm and in a short time. Features of the DGT solution include:

- **H-NET Architecture**: At the heart of DGT's design lies the innovative H-NET architecture. This architecture envisions the network as an amalgamation of interconnected clusters and segments. Each cluster functions as an independent entity with its own nodes, leaders, and arbitrators, fostering modularity and scalability.
- **Two-Level Consensus**: DGT leverages a two-level consensus mechanism called the F-BFT Consensus 20. At the cluster level, a Byzantine Fault Tolerant (BFT) consensus, such as the P-BFT, Hot-Stuff, or Lagrange Construction 24, ensures agreement within clusters. At the higher level, a ring of arbitrators employs a Proof-of-Stake (PoS) or an anchor mechanism (certified arbitrators) to finalize decisions and resolve inter-cluster conflicts.
- **Transaction Families**: DGT introduces the concept of transaction families, akin to smart contracts. These transaction processors handle transactions based on predefined validation rules, offering versatility and optimized execution.
- **Hybrid Ledger:** DGT's ledger combines the conventional block structure with a Directed Acyclic Graph (DAG). This innovative approach not only maintains transaction connections but also facilitates independent network time through the Heartbeat mechanism, enhancing both structural integrity and synchronization.
- **Off-Chain Notaries**: DGT incorporates specialized nodes known as Notaries to address functions unsuited for on-chain execution. These Notaries function as oracles, accessing extensive data and supporting Zero-Knowledge Proof (ZKP) mechanisms 22, thus enabling private transactions, and enhancing data confidentiality. They also play a crucial role in decentralized identification and verification processes.
- **DEC Processing Family**: DGT features a dedicated DEC processing family that includes comprehensive tokenization functionalities, adhering to the ISO 20022 21 compliance standards. This family enables the issuance and management of internal DEC tokens, streamlining financial operations and supporting a robust token economy.

3.1 Basic Network Design

In the ever-evolving landscape of blockchain technology, the concept of virtualized blockchain networks has emerged as a promising frontier. These networks transcend the traditional notion of individual nodes to encompass entire network instances. However, achieving such a feat requires a departure from the conventional flat peer-to-peer (p2p) structure facilitated by the GOSSIP protocol.

The DGT Platform strides boldly into this realm of innovation by adopting a sophisticated topology, moving beyond the limitations of simple p2p frameworks. Central to this advancement is the H-NET network model 15, a cornerstone of DGT's architecture. H-NET introduces a revolutionary paradigm wherein networks are not just clusters of nodes but are orchestrated as a synergy of diverse fragments or segments. These segments offer the flexibility to establish unique rules for node behavior, local transaction families, and even custom consensus mechanisms. This distinctive approach serves as the bedrock for crafting hybrid network environments, accommodating diverse permission design models under a single cohesive framework.

3.2 Hierarchical Structure: Redefining Scalability

H-NET's hierarchical architecture addresses one of the blockchain ecosystem's pressing challenges: scalability. By organizing clusters into segments, which in turn form a hierarchical network, DGT achieves a scalable structure that can handle increasing transaction volumes without compromising performance.

The hierarchy ensures that individual clusters manage their transactions seamlessly, minimizing communication bottlenecks. At the same time, segments permit cross-cluster interactions, granting the flexibility to cater to diverse applications. This synergy between clusters and segments paves the way for a network that can evolve in tandem with growing demands Fig. 3.

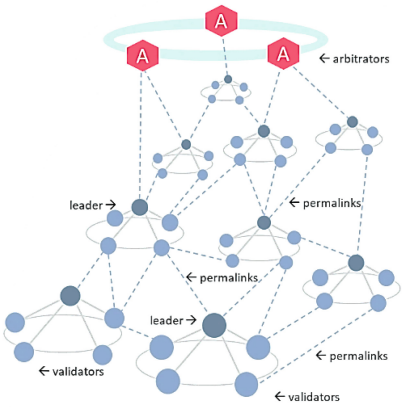

Fig. 3. H-Net Architecture.

3.3 Efficiency and Modularity: A Harmonious Balance

The H-NET architecture emphasizes modularity, enabling easy integration of new clusters and segments to accommodate evolving requirements. Each cluster operates with minimal interdependence, fostering rapid innovation and experimentation. This modularity translates into efficient upgrades, reduced maintenance downtime, and a seamless user experience.

Additionally, the H-NET architecture prioritizes resource optimization by distributing computational tasks across clusters and segments. This design promotes parallel processing, resulting in faster transaction validation and enhanced network responsiveness.

3.4 Adaptive Consensus Mechanisms: Tailored for Excellence

The DGT platform has several technical solutions that define the approach to decentralized and distributed computing:

- **Permalinks:** Unlike classical p2p networks, DGT supports communication between nodes through routes called permalinks. Each node can have several connections, one main one, and multiple reserve ones in case of loss of the main channel. Such networking allows for a reduced cost of communication through the entire network.
- **Layered Ledger**: The ledger has a block structure, on top of which a directed graph (DAG) is built. The block approach allows for the formation of the classic blockchain structure. The DAG supports additional connections between transactions, while also allowing to set characteristic network time based on the topological sorting property of the directional graph. Such network time (implemented by a special Heartbeat Mechanism) is the basis of relatively static network configurations – Network Eras.

In contrast, at the network level, a ring of arbitrators employs Proof-of-Stake (PoS) or anchor mechanisms to finalize decisions. This two-level consensus approach harmonizes efficiency and security, ensuring that both cluster-level and network-wide consensus are achieved seamlessly.

While the cluster and data transfer layer use a BFT (F-BFT) approach, arbitrators represent a critical part of the DGT infrastructure and defend against Sybil-type attacks with a second layer of a PoS consensus 15.

- **Initiation**. Transactions are initiated on a client (computer, phone) communicating with a node through a standardized service API layer.
- **Components**. Each transaction consists of a header and the main body of the transaction (payload). A header contains the digital signature of the customer who created the transaction and the input and output (address) fields for the transactions.
- **Processing**. The transaction processor provides capabilities for processing individual transaction families and validating transaction properties. The Journal component, which is separate from the business logic of transactions, provides parallel processing and advanced batching management [10].
- **Stages**. All transactions are wrapped in batches before being sent to the ledger, which allows for additional processing acceleration. Below are the main steps of transaction formation.

- **Validation**. At this stage of processing, the nodes in the cluster "vote" for transactions, forming the usual quorum for BFT. The immediate BFT consensus mechanism can use the options P-BFT ("Lazy Mode"), Pipelined Fast-HotStuff ("Fast- Run"), or Lagrange Construction ("Alpine") 24.
- **Arbitration**. Maintaining the integrity of the network combined by the ledger is carried out through the second layer of transaction processing, when the nodes included in the so-called "ring of arbitrators" consider transactions, check for integrity, and directly place them in blocks and branches of the DAG. As noted above, the PoS mechanism (or a similar "anchor" principle) is used at this level. Arbitrators are delegates who implement an increased level of security.

Cluster-Based BFT Consensus

In the pursuit of optimizing the functionality and performance of a hybrid network, this section delves into the implementation and functioning of a cluster-based consensus mechanism known as Fast-RUN. It is important to note that Fast-RUN represents just one among several consensus options that can be employed within a cluster-based environment. In this context, the Fast-HotStuff consensus algorithm will be elucidated as a notable choice, showcasing its advantages and operational intricacies.

Fast-RUN Consensus Implementation with Fast-HotStuff

Fast-RUN, operating within the realm of cluster-based consensus, is characterized by its integration of the Fast-HotStuff consensus algorithm 23. This integration is achieved through the development of a dedicated plugin within a transaction family, granting validation capabilities to the transaction body. Importantly, this plugin is accessible across all nodes within the cluster, enabling seamless consensus implementation.

The core principle of the Fast-RUN algorithm revolves around enhancing the performance of Practical Byzantine Fault Tolerance (PBFT) consensus by incorporating Quorum Certificates at the cluster level. This innovative approach significantly bolsters security and concurrently minimizes communication costs associated with leader changes, specifically the Change View process 23.

Fast-Run Algorithm Workflow

- **The Fast-HotStuff** consensus algorithm, operational within the Fast-RUN framework, orchestrates its workflow through a series of distinct steps:
- **Leader Proposes a Block**: At the onset, a designated leader node undertakes the responsibility of proposing a block, housing a collection of transactions. The leader accompanies the block proposal with a certificate, attesting to the block's validity.
- **Block Validation by Nodes**: Validators, encompassing nodes engaged in the consensus, conduct a comprehensive validation of the proposed block and its corresponding certificate. Upon consensus regarding the block's legitimacy, validators append their signatures to the certificate.
- **Certificate Broadcast by Leader**: After securing enough validator signatures, the leader disseminates the certificate across the network.
- **Block Commitment by Nodes**: Receiving validators ascertain the authenticity of the certificate, scrutinizing its endorsement by fellow validators and the inclusion of

a bona fide block proposal. Upon verification, validators incorporate the block into their localized states.
– **Pipelined Block Proposals**: During the block commitment phase, the leader initiates the proposal of the subsequent block. This overlapping of proposal and commitment phases accelerates the consensus process, augmenting overall efficiency.

3.5 Transaction Families: DEC Processing

The DEC (Digital Economic Component) transaction family constitutes a pivotal element within the DGT platform 15, essential for its functional model. Unlike conventional solutions, DGT employs a unified transaction structure emphasizing headers and payloads. This design allows the network to efficiently process diverse transactions, both token-based and token-less, concurrently. In particular, the DEC transaction family assumes prominence in the DGT ecosystem due to its multifaceted nature and pivotal role in assessing the virtualized structure's performance.

Key Functions of the DEC Transaction Family

– **Token Issuance and Management**: The DEC transaction family facilitates the creation and management of DEC tokens. This encompasses mechanisms for minting new tokens and dynamically adjusting the token supply to align with network demands and token circulation.
– **Transfers**: It enables secure and seamless transfers of DEC tokens between accounts, forming the core of the DGT economic model. Participants within the network can engage in transactions, leveraging DEC tokens as the medium of exchange.
– **Banking Operations**: The DEC family extends its capabilities to support banking operations, encompassing tasks such as generating and overseeing invoices and virtual cards. This expansion broadens the utility of DEC tokens, enabling their use in various applications across the DGT platform.
– **Secondary Token Support**: Beyond the native DEC tokens, this transaction family accommodates the issuance and management of secondary tokens. This functionality fosters a diversified token landscape within the DGT ecosystem, enabling the creation of custom tokens tailored to specific use cases.
– **Security and Compliance**: The DEC transaction family prioritizes security and compliance (ISO 20022). It incorporates robust cryptographic techniques to safeguard transactions while integrating mechanisms to ensure adherence to pertinent regulatory frameworks.

4 Experiments and Comparisons

4.1 Empirical Evaluation of Blockchain Virtualization: Performance Analysis and Insights

Virtualization serves as a pivotal tool in addressing diverse challenges within the blockchain domain. Among these challenges, one significant task involves examining the hypothesis of heightened network performance within segmented networks, where communication complexity is constrained. To investigate this, a series of experiments

were conducted on the DGT platform, targeting latency measurement as the number of nodes increased under virtualization (cluster and segment allocation). Additionally, a comparison was made with non-virtualized conditions using the conventional GOSSIP protocol.

Experimental Design
The study utilized the H-NET architecture of DGT to configure the network. Seven physical machines, each running Ubuntu 20.04, were employed, varying in RAM from 2 GB to 64 GB. These physical machines collectively hosted 15 virtual machines, organized into three clusters based on the initial configuration. An extra network segment was introduced, containing virtual nodes ranging from 15 to 30. This segment mimicked a scalable virtual blockchain network.

Methodology
Transaction Generation: An API-based transaction generator emulated authentic blockchain activity. Transactions of varying complexity, including basic transfers, digital object registrations, and DEC processing family-based account attribute alterations, were executed. Each transaction was tagged with size and type, simultaneously integrated into both the DAG structure and the 1 MB limited block.

Network Configuration: The DGT network was orchestrated with the stipulated physical and virtual machines, clusters, and segments. This ensured seamless synchronization and interaction between the nodes. The node count spanned from 10 to 60 across different consensus mechanisms (configured via an independent microservice). In the virtualized context, up to 25% of nodes formed the arbitrator ring, significantly influencing overall performance.

Consensus Mechanisms: Five consensus scenarios were tailored for each cluster:

- PBFT (universally across all nodes)
- SBFT (Extended Consensus, No Blockchain Virtualization)
- HotStuff for virtualized blockchain (segments and clusters)
- F-BFT (Lazy Path), an enhanced PBFT for virtualized blockchain
- F-BFT (FAST-RUN), Fast-HotStuff pipeline atop the virtualized blockchain system.

Data Collection Transactions were generated through APIs, and latency was gauged from transaction submission to consensus confirmation. Multiple iterations were executed for each scenario to ensure statistical robustness.

Performance Metrics: Latency, quantified in milliseconds, served as the primary performance metric. Additionally, CPU and memory usage were closely monitored for comprehensive resource consumption insights.

Outcomes: The results, graphically illustrated below, affirm the constructive impact of virtualization on performance enhancement. Latency was markedly curtailed compared to the use of non-virtualized P-BFT, with the best-case scenario demonstrating latency reduction by 5–6 times.

4.2 Comparative Analysis of Blockchain Virtualization Approaches

Blockchain virtualization, involving the creation of a "network of networks," has led to the emergence of various approaches aimed at improving scalability and interoperability. In addition to DGT's hierarchical network structure, other notable initiatives in this space include the Polkadot's parachains-based model 25 and Avalanche's multi-chain architecture 26. This section provides a comparative overview of these approaches, highlighting their distinctive features and potential implications (Table 1).

Discussion
While DGT introduces a novel approach by using clusters and segments for virtualized blockchain instances, Polkadot's parachains and Avalanche's multi-chain architecture also offer innovative solutions. Each approach has its own strengths and limitations, which need to be carefully considered based on the specific use case requirements. DGT's use of arbitrators to form segments represents an interesting departure from the conventional models, promising efficient resource utilization and tailored solutions for various applications. On the other hand, Polkadot's parachain model ensures strong interoperability, while Avalanche's multi-chain architecture capitalizes on the Avalanche protocol's strengths to enhance throughput and latency. The choice between these approaches ultimately depends on factors such as scalability needs, interoperability goals, and the nature of the applications to be supported.

Table 1. Comparative Overview.

Aspect	DGT	Polkadot	Avalanche
Network Topology	Hierarchical structure with clusters and segments forming independent blockchain instances	Central relay chain (parachains) communicating with heterogeneous and independent sharded chains	Multi-chain architecture comprising Exchange Chain (X-Chain), Contract Chain (C-Chain), and Platform Chain (P-Chain)
Consensus Mechanism	Two-level consensus with BFT clusters and PoS-based arbitrators	Relay chain using nominated Proof-of-Stake (NPoS) consensus	Avalanche protocol with multiple sub-protocols
Node Connection	Clusters and segments based on arbitration	Parachains connected to relay chain	Chains connected via the Avalanche protocol
Strengths	Efficient resource utilization due to arbitration-based segment formation	Strong interoperability between parachains	High throughput and low latency through Avalanche protocol

(*continued*)

Table 1. (*continued*)

Aspect	DGT	Polkadot	Avalanche
Limitations	Complexity in managing arbitrator rings	Dependency on the relay chain's availability	Sub-protocols can increase communication complexity
Prospects	Potential for diverse application scenarios with clusters and segments	Enhanced scalability through parallel processing	Continued protocol enhancements for improved performance

5 Conclusions and Future Directions: Unleashing the Potential of Blockchain Virtualization

In the journey to redefine the landscape of blockchain technology, this article has extensively explored the realm of blockchain virtualization with the Distributed Governance Technology (DGT) platform as a pivotal example. The innovative concept of blockchain virtualization, particularly in the context of hybrid networks, presents a transformative solution to the critical challenges facing traditional blockchain architectures. By abstracting the blockchain infrastructure, DGT introduces a paradigm shift that enables the creation and management of multiple virtual instances of blockchains on a shared physical blockchain network. This unique approach facilitates improved scalability, isolation, and resource allocation, addressing the limitations of conventional single-blockchain networks.

Experiment and Implications
The experiment conducted within the DGT environment provided illuminating insights into the tangible benefits of blockchain virtualization. The demonstration of reduced latency through virtualization, especially when implementing the Fast-RUN consensus option, showcased the potential to significantly enhance blockchain performance. This empirical evidence substantiates the promise of virtualization in ameliorating latency issues and thus cultivating a more efficient blockchain ecosystem.

Future Works
Moving forward, this exploration gives rise to new research objectives:

- **Security and Privacy Testing**: Future research should encompass rigorous testing of security and privacy aspects within a virtualized blockchain environment. As virtualization introduces novel dynamics, evaluating these dimensions becomes paramount to ensure the robustness and confidentiality of the system.
- **Impact on Deployment and Cloud Solutions**: The influence of blockchain virtualization on deployment methodologies and the evolution of cloud-based Blockchain-as-a-Service (BaaS) solutions presents a promising avenue. Virtualization enables more versatile and customized blockchain networks, propelling the evolution of cloud-based services and their alignment with diverse enterprise needs.

- **Interoperability and Network Compatibility**: Exploring the interplay of virtualized networks within a broader ecosystem remains an area of interest. How virtualized instances interact with other blockchain networks and legacy systems, and how standards are upheld, warrant comprehensive study.
- **Evolving Ecosystem**: As blockchain virtualization fosters scalability, reduces entry barriers for institutions, and introduces private transaction capabilities, it has the potential to revolutionize the blockchain landscape. Its adoption paves the way for more widespread institutional participation and real-world enterprise use cases.

References

1. Carrara, G.R., Burle, L.M., Medeiros, D.S.V., et al.: Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. Ann. Telecommun. **75**, 163–174 (2020). https://doi.org/10.1007/s12243-020-00751-w
2. Fang, M., Liu, J.: Toward low-cost and stable blockchain networks. In: ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1–6 (2020). https://doi.org/10.1109/ICC40277.2020.9148615
3. Zhang, R., Xue, R., Liu, L.: Security and Privacy on Blockchain. ACM Comput. Surv. **52**(3), 1−34 (2019). https://doi.org/10.1145/3316481
4. Khan, S.N., Loukil, F., Ghedira-Guegan, C., et al.: Blockchain smart contracts: applications, challenges, and future trends. Peer-to-Peer Netw. Appl. **14**, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0
5. Wang, G., Wang, Q., Chen, S.: Exploring blockchains interoperability: a systematic survey. ACM Comput. Surv. **55**(13s), 1−38 (2023). https://doi.org/10.1145/3582882
6. Taskou, S.K., Rasti, M., Nardelli, P.H.J.: Blockchain function virtualization: a new approach for mobile networks beyond 5G. IEEE Netw. **36**(6), 134–141 (2022). https://doi.org/10.1109/MNET.009.2100473
7. Sharma, A.: Beyond Cryptocurrency - More To Blockchain (2020). https://doi.org/10.13140/RG.2.2.24976.23049
8. Yaga, D., Mell, P., Roby, N., Scarfone, K.: Blockchain Technology Overview, NISTIR 8202 (2019). https://doi.org/10.6028/NIST.IR.8202
9. ITU-T Focus Group on Application of Distributed Ledger Technology, Technical Specification FG DLT D3.1, Distributed ledger technology reference architecture (2019)
10. Khobragade, P., Turuk, A.K.: Blockchain consensus algorithms: a survey. In: Prieto, J., Benítez Martínez, F.L., Ferretti, S., Arroyo Guardeño, D., Tomás Nevado-Batalla, P. (eds.) Blockchain and Applications, 4th International Congress. BLOCKCHAIN 2022. Lecture Notes in Networks and Systems, vol. 595. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-21229-1_19
11. Attamah, M., van Ditmarsch, H., Grossi, D., van der Hoek, W.: A framework for epistemic gossip protocols. In: Bulling, N. (eds.) Multi-Agent Systems. EUMAS 2014. LNCS, vol. 8953. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-17130-2_13
12. Sahoo, S., Fajge, A.M., Halder, R., Cortesi, A.: A hierarchical and abstraction-based blockchain model. Appl. Sci. **9**(11), 2343 (2019). https://doi.org/10.3390/app9112343
13. Newell, J., Mamun, Q., Rehman, S., Islam, Md.: A Generalised Logical Layered Architecture for Blockchain Technology (2021)
14. Deloitte 2021 Global Blockchain Survey: Global Financial Services Industry Undergoing Seismic Shift; Banks Must Embrace Inevitable Digital Future
15. DGT Technical Documentation, Revision 21, (2023). https://dgtnetwork.gitbook.io/dgt-docs

16. Hammoudi, A., Khanfar, K.: OSI Model (2022)
17. Wang, Q., Li, R., Wang, Q., Chen, S., Ryan, M., Hardjono, T.: Exploring Web3 From the View of Blockchain (2022)
18. Uddin, M., Khalique, A., Jumani, A., Ullah, S.S.: Next-generation blockchain-enabled virtualized cloud security solutions: review and open challenges. Electron. **10**, 1–23 (2021). https://doi.org/10.3390/electronics10202493
19. Di Bona, G., Bracci, A., Perra, N., Latora, V., Baronchelli, A.: The decentralized evolution of decentralization across fields: from Governance to Blockchain (2022). https://doi.org/10.48550/arXiv.2207.14260
20. Bogdanov, A., et al.: Testing and comparative analysis of the F-BFT-based DLT solution. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2021. ICCSA 2021. LNCS, vol.12952. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-86973-1_3
21. ISO 20022, Universal financial industry message scheme. https://www.iso20022.org/
22. Buchanan, W.: Zero-knowledge Proof (ZKP) and Privacy Preserving (2022). https://doi.org/10.1201/9781003337751-12
23. Jalalzai, M.M., Niu, J., Feng, C.: Fast-HotStuff: A Fast and Resilient HotStuff Protocol (2020)
24. Bogdanov A., Uteshev A., Khvatov V.: Error Detection in the Decentralized Voting Protocol, Computational Science and Its Applications – ICCSA 2019, https://doi.org/10.1007/978-3-030-24296-1_38
25. Abbas, H., Caprolu, M., Pietro, R.: Analysis of Polkadot: Architecture, Internals, and Contradictions (2022). https://doi.org/10.48550/arXiv.2207.14128
26. Tanana, D.: Avalanche blockchain protocol for distributed computing security. In: 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), pp.1–3. (2019) https://doi.org/10.1109/BlackSeaCom.2019.8812863