CSIT Conference 2023, Yerevan, Armenia, September 25 - 30

Virtual Blockchain Network: Why and How

Alexander Bogdanov
St. Petersburg University
St. Petersburg, Russia
e-mail:
a.v.bogdanov@spbu.ru

Valery Khvatov
DGT Technologies AG.,
Canada
e-mail:
valery.khvatov@gmail.com

Alexei Uteshev
St. Petersburg University
St. Petersburg, Russia
e-mail:
a.uteshev@spbu.ru

Nadezhda Shchegoleva
St. Petersburg University
St. Petersburg, Russia
e-mail:
n.shchegoleva@spbu.ru

***Abstract*—This research paper explores methods for balancing privacy and performance in distributed systems, specifically within multilayered architectures. We propose a potential solution for secure data exchange on a hybrid blockchain platform, leveraging cryptographic tools to protect sensitive data while maintaining system functionality. The paper emphasizes the importance of considering both privacy and performance in distributed system design and implementation.**

***Keywords*—Layer 1 digital platform, multi-party computation over blockchain, decentralization.**

I. INTRODUCTION

The challenges of the modern world, including the growth of state influence and increasing transparency, the issue of trust in technology companies, and the acceleration of digitalization, are impacting businesses in unprecedented ways. Furthermore, the distributed nature of modern business and the prevalence of big data calls for a response to these challenges.

As state influence continues to grow, businesses must find ways to navigate complex regulatory environments while maintaining transparency and ethical standards. The issue of trust in technology companies is also becoming increasingly acute, as data leaks and other security incidents erode consumer confidence in digital services. The balance between privacy and performance is a crucial issue in the design and implementation of distributed systems, particularly within multilayered architectures. In recent years, blockchain technology has emerged as a promising solution for achieving this balance [1]. However, it should be noted that blockchain-based systems in their classic form do not provide complete confidentiality. As a result, the balance between performance and security inevitably leads to the division of the blockchain network into layers, including an explicit off-chain computing component for information that cannot be placed inside a distributed ledger.

Possible use cases for blockchain-based systems with multi-layered architectures and specialized cryptographic tools include:

– Distributed identification: blockchain technology can be leveraged to create secure and tamper-proof digital identities that enable efficient and transparent authentication and verification processes.

– Secure data sharing: blockchain technology can facilitate secure and efficient data sharing, enabling better risk assessment, fraud detection, and compliance management.

– Intersection of private sets: by leveraging advanced cryptographic techniques, blockchain-based systems can enable the secure intersection of private sets between different entities, such as state institutions and private information providers.

These are just a few examples of the potential applications of blockchain technology in achieving the balance between privacy and performance in distributed systems. As the technology continues to evolve, new use cases will likely emerge, making this a promising area for further research and Innovation [2].

II. ONCE AGAIN ABOUT STRUCTURE AND MAIN TRENDS

In fact, the market can be divided into several segments that are closely intertwined [3]:

– actual infrastructure platforms (networks, L1 platforms). This layer can also include L3/2 - cross chains, bridges and side chains.

Sometimes referred to as L2.

– Financial services (DeFi) - also belong to L2, include payments, wallet services (Custodians), Lending and Crediting, token issuing platforms (including RWA and Commodities), investment management, exchanges (DEX), derivatives trading

– WEB3 - this includes DAO (sometimes also referred to as DeFi), NFT, Metaverse and specific services, decentralized IDs, intellectual property, etc.

– Services - blockchain development and consulting.

A. Estimating the L1 market is difficult for the following reasons

There are several different metrics that allow you to rank L1 networks: Market Cap (total market volume), TVL (Total Value Locked, funds reserved in tokens) and investment level (by the number of transactions and by their volume). Each of these characteristics shows a different view of the market.

L1s are, by definition, infrastructure solutions. It is often difficult to estimate how much is invested directly in them, and how much is invested in applications or the L2 layer, as in add-ons to them.

There are several types of infrastructure solutions that are close in meaning but have different architectures: independent

networks themselves (for example, BTC, Ethereum), side-chains (networks that can be interpreted as relatively independent), Bridges (or cross-chains, networks that emphasize specifically on the integration of other networks), Smart Contracts (such networks can be positioned as a synonym for L1, however, this is an optional condition. Among them, there are also EVM - compatible, as well as WASM and other virtual machines).

B. 2.2 Tokenization

All platforms of the L1 class are launched on their own native token, have passed the ICO or IDO stage, and are traded on the stock exchange, the crypto-currency makes up a significant part of their capitalization.

– Token Supply - Some native tokens have a limited supply. The absence of restrictions makes it possible to flexibly change the inflation of tokens and distribute payments in the long term, but makes them weaker;

– Governance - different platforms use explicit and implicit governance procedures, at the technical and organizational level, as well as through social networks.

– Transaction fees - native tokens are usually the only form of payment, but in some cases (e.g., Polkadot parachains) native tokens can be used there.

The commission can be sent to validators, created (part of), or reworked. In Ethereum EIP-1559, burn the amount in general, as a means of combating high fees.

The technical design is different both in terms of networking and the minimum system requirements for each node.

The network topology can vary: – One Validator Set - One Chain. For the entire network - one set of validators (Algorand, Binance Smart Chain, Ethereum and Solana)

– One Validator Set, Multiple Chains. For this configuration, the nodes support multiple networks - Ethereum 2.0 and Polkadot

– Multiple Validator Sets, Multiple Chains. Different validators and many networks combined together - this is the design of Cosmos and Avalanche.

Most systems build a dual defense system: Consensus and Sybil Resistance. Most L1s use some variation of PoS whereby security is achieved by having distributed bases of token holders stake their native tokens. In the case of networks with limited sets of validators, they have different parameters for how validators are elected to the active set. Through delegation, token holders who do not use computer hardware can participate in consensus by assigning their tokens to active validator nodes [4].

Another problem is finality (expectation by the user, Finality). If these networks cannot reach a consensus, they stop creating new blocks until 2/3 of the network reaches an agreement on the last block. In the Avalanche consensus, transactions are grouped into vertices. If a node contains conflicting transactions, all transactions in it are rejected and reissued for execution. ETH 2 and Polkadot prioritize liveness vs. safety. If these live networks fail to reach an agreement on a block, they will continue to propagate new blocks and execute transactions, but will not reach finality.

Reorganization or rollback of previously executed transactions is not possible for security networks. Any violation of the finality of a single block would require more than 1/3 of the set of validators to be slashed (if the network supports slashing). In the Algorand Pure Proof of Stake consensus, a committee and leader are randomly selected from a global set of validators using a verifiable random function (VRF), and the consensus is reached within these committees, which changes each block.

In Avalanche's Avalanche consensus for its Directed Acyclic Graphs ("DAG"), the nodes repeatedly perform their own random selections of the network and update their states periodically until most of the network comes to an agreement.

Binance Smart Chain, Cosmos, and Polkadot currently limit their validator sets to 21, 125, and 300, respectively. Unlike other networks that use sampling strategies, these networks are designed to reduce communication overhead.

Ethereum's flagship smart contract language, Solidity, and its execution environment, the Ethereum virtual machine, are far from the only platforms available for deploying decentralized applications. Many platforms support different smart contract languages with unique attributes. For example, Algorand smart contracts can be coded in Python and compiled into lower-level smart contract languages such as Teal.

In addition, languages like Clarity are "resolvable" and provide guarantees of how smart contracts will function before they are permanently deployed in real production environments, thus reducing the attack surface of applications. Although consensus algorithms are a critical component of how networks operate, they also affect one of their most important attributes: performance. Performance is best measured by two metrics: throughput levels and maturity levels

Throughput determines how many transactions a network can process in a given amount of time and is usually measured in transactions per second (TPS). Finality determines how long a user typically has to wait until there is reasonable certainty that their transactions will not be rolled back.

Avalanche: 4500 TPS in a 2000-node testnet environment. The main Avalanche network currently consists of three separate chains with different consensus algorithms that provide different levels of throughput. Accordingly, these estimates of 4500 TPS likely refer to its light X chain, which is structured as a Directed Acyclic Graph (DAG) and facilitates the creation and exchange of assets. The throughput levels achievable on its Ethereum-compatible C-chain, which facilitates smart contract transactions, are likely substantially lower than these testnet levels.

Cosmos Hub - Tendermint Consensus. When simulating a testnet with 64 nodes, Tendermint regularly processed around 4000 TPS. The Cosmos Hub validator set currently consists of 125 nodes. Therefore, communication overhead in a production environment is likely to be higher, and testnet levels may be slightly inflated.

Solana reached approximately 50,000 TPS in a testnet environment. However, the execution engine does not distinguish between messages such as consensus voting (which nevertheless requires payment of a transaction fee) and more typical peer-to-peer value transfers and smart contract transactions. Therefore, testnet levels are likely inflated compared to other platforms due to how transactions are defined. In addition, this throughput was achieved with approximately 200 nodes, which is about 1/3 of the nodes currently on its main network, and communication overhead in a production environment is likely higher.

Daily traffic depends not only on bandwidth, but also on the actual load, and on the cost of the commission. To date, asset transfers between chains via bridges such as RSK's Pow-Peg have been the most tangible examples of what interoperability looks like. They allowed users to transfer assets between chains and use them in different environments.

III. Main Advantages Of L-1 Platforms

1. **Security**: Tier 1 platforms are responsible for establishing the rules and consensus mechanisms that ensure the security and integrity of the blockchain network. This includes things like preventing double-spend attacks, keeping the registry accurate and immutable, and protecting the network from intruders.
2. **Scalability**: Tier 1 platforms must be able to scale to support a large number of transactions and users. This requires efficient consensus algorithms, high throughput, and low latency to enable real-time transactions.
3. **Decentralization**: Tier 1 platforms are designed to be decentralized, which means they are not controlled by any one entity. This is important because it ensures that the network is resistant to attacks, censorship, and other forms of centralization.
4. **Flexibility**: Tier 1 platforms must be flexible enough to support a wide range of use cases and applications. This includes things like smart contracts, decentralized finance (DeFi), non-fungible tokens (NFTs), and more.
5. **The modular design** of the platform allows you to quickly implement in-demand digital products

A. DGT digital platform

The DGT digital platform is a universal product (LAYER 1) that allows you to use it to collect, analyze and visualize data for a variety of purposes: quality analysis, event integration and building complex networks with differential privacy.

DGT is moving forward within the D3 paradigm:
– Data integration based on an innovative consensus mechanism;
– Data management along the entire life cycle;
– Presentation of data for any users in real time
This allows DGT to implement applied innovative products in a single paradigm and in a short time.

B. Basic network design

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 you to reduce the cost of communication through the entire network.
– Ledger. The ledger has a block structure, on top of which a directed graph (DAG) is built. The block approach allows you to form the classic blockchain structure. DAG supports additional connections between transactions, while also allowing you to set the 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.
While the cluster and data transfer layer uses 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.
– 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.
– Stages. All transactions are wrapped in batches before being sent to the ledger, which allows for additional acceleration in processing. Below are the main steps of the transaction formation.

The basis of processing consists of transactions: messages that go from client to ledger storage (commit to block), and then the ledger copy is distributed throughout the network.

Each transaction has a specific structure (header and body - payload). The client signs the transaction; it is then checked on the server/validator, which "votes" for the transaction, offering it to be committed into a new block.

All clients communicate through a universal mechanism – API. The preparation of API requests for inserting a new transaction requires cryptography and serialization of transactions and is performed using SDKs available in several languages (Python, Java, C++).

Transactions can be of several types [5], which allows you to use the ledger for applications with different business logic. Inside the validator, the transaction is processed by a special mechanism - the Journal Engine, which is responsible for parallelizing the processing of transactions and their publication.

The initial consideration of a transaction is done inside the cluster, which includes the node supporting the client, then the transaction spreads in the network based on special nodes - validators. This kind of consensus is based on the F-BFT approach.
– In private networks, where access is strictly controlled, an approach based on consensus mechanisms such as CFT (Crash Fault Tolerance) can be used (ex. RAFT).
– Public networks such as Bitcoin use the PoW approach, which has proven to be effective in terms of security but does not scale well and is extremely costly from an energy point of view. For small networks with regular participants, it is possible to use consensuses such as PBFT, which allows you to reach a consensus through a special communication scheme.
– However, PBFT has great communication complexity, making it inapplicable for networks larger than 50 nodes (communication complexity is O(n2), where n –the total number of nodes). Under the DGT, F-BFT consensus is applied based on the following assumptions:
– The communication complexity of the network is reduced by the division of the network into clusters, within which a limited number of nodes uses the P-BFT approach to achieve consensus (with variable leaders who organize interaction);

– Arbitrator nodes form the second level of consensus; their signature is required to insert transactions into the registry;
– Arbitrators are protected by a PoS mechanism that provides Sybil Resistance;
– For the functioning of arbitrators in the public segment, the use of a threshold signature scheme is required

C. Fast-run way

The fast-RUN algorithm speeds up the action of PBFT by applying Quorum Certificates at the cluster level. This creates greater security and lower communication costs for changing the leader - Change View, since it does not require the end and confirmation of blocks in the network before the change [6]. The main steps are:
1. Leader proposes a block: In Fast-HotStuff, a leader node is responsible for proposing a block, which contains a set of transactions. The leader includes a certificate with the block proposal that attests to the validity of the block.
2. Nodes validate the block: Validators (nodes participating in the consensus) check the validity of the block and the certificate. If they agree that the block is valid, they sign the certificate.
3. Leader broadcasts the certificate: Once the leader collects a sufficient number of signatures from validators, it broadcasts the certificate to the network.
4. Nodes commit the block: Validators that receive the certificate check that it is signed by a sufficient number of other validators and contains a valid block proposal. If so, they commit the block to their local state.
5. Pipelined block proposals: While validators are committing a block, the leader can begin proposing the next block. This allows the consensus process to operate quicker by overlapping different stages of the consensus process.
Fast-Run aims to reduce the number of message rounds required to reach consensus, reduce the time it takes to reach consensus and increase network throughput.

GARANASKA PROCESSING DGT is a comprehensive system that can handle various types of transactions [7]. With the introduction of the MATAGAMI version, the platform is now separated into two distinct parts: CORE, which is responsible for the system's main functionality and is licensed under the Apache 2.0 license, and GARANASKA, which handles the financial aspect of the system and is licensed under the AGPL v. 3.0 license.

GARANASKA on top of the base layer develops those parts that are responsible for tokenization and circulation of tokens.

GARANASKA supports the functions of decentralized identification and operation with digital objects at the level of the native protocol Dec native currency represents the economy of the platform, allowing you to swap secondary tokens, support smart contracts and give rewards to nodes. Seamless operations with notaries (special nodes such as oracles) allow you to implement the integration of off-chain and on-chain operations Plans include Garanaska Expansion through tight integration with L3/L4 applications such as wallets and Lending Apps

DEC: Unprecedented Native Coin
– Reliable governance Minting based on SLA, no POW / POS
– Based on real economic theory Robust tokenization model
– F-BFT Consensus Infinitely scalable and utmost secure
– Absolutely transparent Trustworthy distribution and rules
– Supports multiple economies Each new use case raises value
– Neural Network enabled Security, distribution, learning
Versatile white-label tokenization DGT Network [8] enables the creation of any white-label token with no limits on its properties. These tokens are ideal for rapid enterprise development and deployment:
– Any value -Variable transactions; any digital asset
– Atomic swap - Internal zero-fee exchange mechanism
– Mirroring - Anchor possibilities in other blockchains
– White-label tools - Including mobile wallet apps, APIs, dashboards
– Security - Absolute security against attack vectors
– Volatility-free - Independent value from core native coin.

IV. Tokenization Nature

In a decentralized economy, solution owners can earn income through a variety of sources [9]:
– **Token rewards.** Solution owners may receive tokens as a reward for contributing to the network. These tokens may have value and can be traded for other assets or used within the network itself
– **Transaction fees.** Solution owners can earn income by processing transactions within the network. This is similar to how miners earn income in blockchain networks like Bitcoin.
– **Staking rewards.** Some decentralized networks allow users to "stake" their tokens, which means they hold them in a special wallet and use them to participate in network governance. Solution owners can earn rewards for staking their tokens and participating in governance.
– **Service fees.** Solution owners can provide services to other users within the network and charge fees for those services. For example, they may offer data storage or computing power.
A token, in the context of cryptocurrency [10], is a digital asset that represents a unit of value or utility within a blockchain network. Tokens can be used to represent various assets, such as a currency, a commodity, a company's shares, or even a unique asset like a piece of artwork.

A. Modeling approach

Using the Stochastic approach for DGT, the platform economy is modeled as a complex system of parameters based on random Markov processes. Native tokens gain value as more users join, reflecting the platform's intrinsic value. The model excludes speculative influences [11].

The main focus of the model is on the dynamic balance between the platform owners and users, represented in a Markov equilibrium with state variables At and Lt. Achieving this equilibrium involves solving the Hamilton–Jacobi–Bellman equation (HJB) [12]. The initial version of the HJB model has some limitations, including:
– A vast number of endogenous model parameters resulting in significant variability of model outcomes.
– The assumption of infinite price growth is not reasonable for the platform economy.
– The model's assumption of an endogenous token price does not account for significant factors such as the technology's popularity, political events, and other economic factors that could impact the platform economy [13].
– To address the above limitations of the endogenous model, a hybrid dynamic model for the crypto-platform economy has been proposed. The model parameters are evaluated based on

competitive solutions' known characteristics, with a maximum limit set for the token price and the maximum number of platform users. The model operates within a nine-year working interval.

B. Supply and demand

The token distribution in this framework is based on these proposals:

– Tokens enter the ecosystem through the Foundation's distribution mechanisms (20% of emission amount, including team distribution, Airdrop, and 10% sale) and minting mechanism where tokens are given to nodes in exchange for SLA (80% of the value).

– Tokens are needed for the system's development and operation, including paying commissions, staking as an arbitrator, and paying for network services.

– To balance token supply and demand, the network uses the Fisher equation of exchange, which calculates the market capitalization based on token circulation speed (users investing by holding tokens).

– The node economy comprises two components: distribution of minting and commission. In the initial stage with a low number of transactions, minting contributes significantly more to the node's revenue. However, as the number of transactions increases, minting slows down, and the node's income is primarily determined by transaction commissions.

V. CONCLUSIONS

Our DGT platform is still under development, but the presented consensus mechanism shows promise for industrial use, particularly in a hybrid architecture and hierarchical network [14]. This architecture can be used to address problems of vertical and horizontal integration and can facilitate the building of ecosystems. For example, it could be used in supply chain management to connect various entities, or in the Internet of Things to integrate smart devices and sensors with a central network [15]. It also has potential in the financial sector for cross-border transactions, and in the energy sector for coordinating power generation and distribution.

Overall, the DGT platform shows potential for use in a variety of industries and applications. The current DGT token model is designed to address the need for a balanced token supply and demand within the network. The token distribution is based on a combination of foundation distribution mechanisms and a minting mechanism that rewards nodes for maintaining a high level of service [16].

– In terms of the node economy, there are two primary sources of revenue:

minting and transaction fees. At the initial stage of the network, minting plays a more significant role in node revenue. However, as the number of transactions increases, transaction fees become the primary source of revenue.

– To ensure a balance between token supply and demand, the Fisher equation of exchange is used to calculate the market capitalization of the network based on the velocity of token circulation. This encourages users to hold and transact with the token, which can increase the network's value and growth potential over time.

– Overall, the DGT token model appears to be designed to incentivize users to actively engage with the network, while also ensuring a balanced token supply and demand for the long-term success and sustainability of the platform [17].

ACKNOWLEDGMENT

Paper is supported by Center of AI, St-Petersburg State University, Grant id: 94062114.

REFERENCES

[1] A. Litan. Hype Cycle for Blockchain 2021; More Action than Hype. https://blogs.gartner.com/avivah-litan/2021/07/14/hype-cycle-for-blockchain-2021-more-action-than-hype/

[2] Deloitte's 2021 Global Blockchain Survey. https://www2.deloitte.com/za/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html

[3] Consortium Blockchain Explained / https://www.mycryptopedia.com/consortium-blockchain-explained/

[4] H. Pervez, M. Muneeb, M. U. Irfan and I. U. Haq, "A Comparative Analysis of DAG-Based Blockchain Architectures," *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*, Lahore, Pakistan, 2018, pp. 27-34, doi: 10.1109/ICOSST.2018.8632193.

[5] D. Mazi `Eres The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus/ https://www.stellar.org/papers/stellar-consensus-protocol.pdf

[6] DGT. For Developers. https://dgt.world/for-developers.html

[7] DGT ENTERPRISE GATEWAY TO WEB3. https://dgt.world/docs/DGT_About.pdf

[8] DGT. The Blockchain Handbook. https://dgt.world/docs/DGT_BLOCKCHAIN_ABC.pdf

[9] What Are Crypto Tokens and How Do They Work? https://b2binpay.com/ru/what-are-crypto-tokens-and-how-do-they-work/

[10] DGT and blockchain definitions https://dgt.world/glossary.html

[11] Technical Report FG DLT D1.2/ Distributed ledger technology overview, concepts, ecosystem. / https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf

[12] J. Howell Top use cases of distributed ledger technology (DLT). https://101blockchains.com/distributed-ledger-technology-use-cases/

[13] ISO 23257 Blockchain and distributed ledger technologies — Reference architecture/ https://www.iso.org/standard/75093.html

[14] DGT. Technical Deep Dive. https://dgt.world/docs/DGT_TECHNOLOGY.pdf

[15] DGT.GARANASKA https://dgt.world/docs/DGT_GARANASKA_TOKENIZATION.pdf

[16] DGT. Capturing Non-Core Value. Cross-Enterprise Ecosystem/ https://dgt.world/docs/DGT_HORIZONTAL_INTEGRATION.pdf

[17] DGT. Achieving Data-Rich Value Chains. Cross-Enterprise Integration. https://dgt.world/docs/DGT_VERTICAL_CASE.pdf