*Interdisciplinary Description of Complex Systems* 22(6), 738-762, 2024

# SUITABILITY OF BLOCKCHAIN FOR STORING PRIVATE DATA FROM IOT DEVICES

**Marija Cekuš[1,*] and János Simon[2]**

[1]Subotica Tech-College of Applied Sciences
Subotica, Serbia

[2]University of Szeged, Faculty of Engineering, Department of Mechatronics and Automation
Szeged, Hungary

DOI: 10.7906/indecs.22.6.8
Regular article

*Received:* 14 September 2024.
*Accepted:* 28 November 2024.

## ABSTRACT

The explosive growth of Internet of Things devices over the past two decades has created pressing challenges for storing the vast amounts of data generated by connected devices. Concurrently, blockchain technology has rapidly evolved, providing new avenues for storing data securely, efficiently, and in near real-time. This article investigates the suitability of various blockchain platforms for Internet of Things data storage, selecting seven platforms – namely, IOTA, Signum, Ethereum, Solana, Polygon, Stellar, and Hyperledger Sawtooth. A comprehensive set of criteria and scoring methodology were developed to assess each platform's strengths and limitations for this use case.

Our findings identify IOTA as the most suitable platform due to its feeless transactions, high transaction throughput, and extensive data storage. Signum and Ethereum also showed potential, though with noted limitations in community support, transaction fees, and speed. Platforms like Solana, Polygon, and Stellar demonstrated effective storage capabilities on Layer 2, which introduces additional complexity and costs. The methodology developed here provides a framework for future research, suggesting that additional platforms be evaluated, the scoring criteria refined with weighted parameters, and practical validation conducted through a prototype Internet of Things system to further validate and optimize blockchain selection for Internet of Things data storage.

## KEY WORDS

internet of things, blockchain, data protection

## CLASSIFICATION

JEL: E59

*Corresponding author, $\eta$: 28122005@vts.su.ac.rs; +381 60 6669904;
Marka Oreškovića 16, 24 000 Subotica, Serbia

## INTRODUCTION

The Internet of Things (IoT) has experienced substantial growth over the past two decades. In the early 2000s, IoT technology was in its early stages of development with limited application in specific industries. Since then, the global use of IoT devices has increased substantially, reaching billions of connected devices. In 2003, with a global population of approximately 6,3 billion, around 500 million devices were connected to the internet, equating to roughly 0,08 connected devices per person. The rapid growth of handheld devices dramatically increased the number of connected devices to around 12,5 billion by 2010, while the population rose to 6,8 billion, resulting in more than one connected device per person, specifically 1,84 devices per individual, Figure 1.

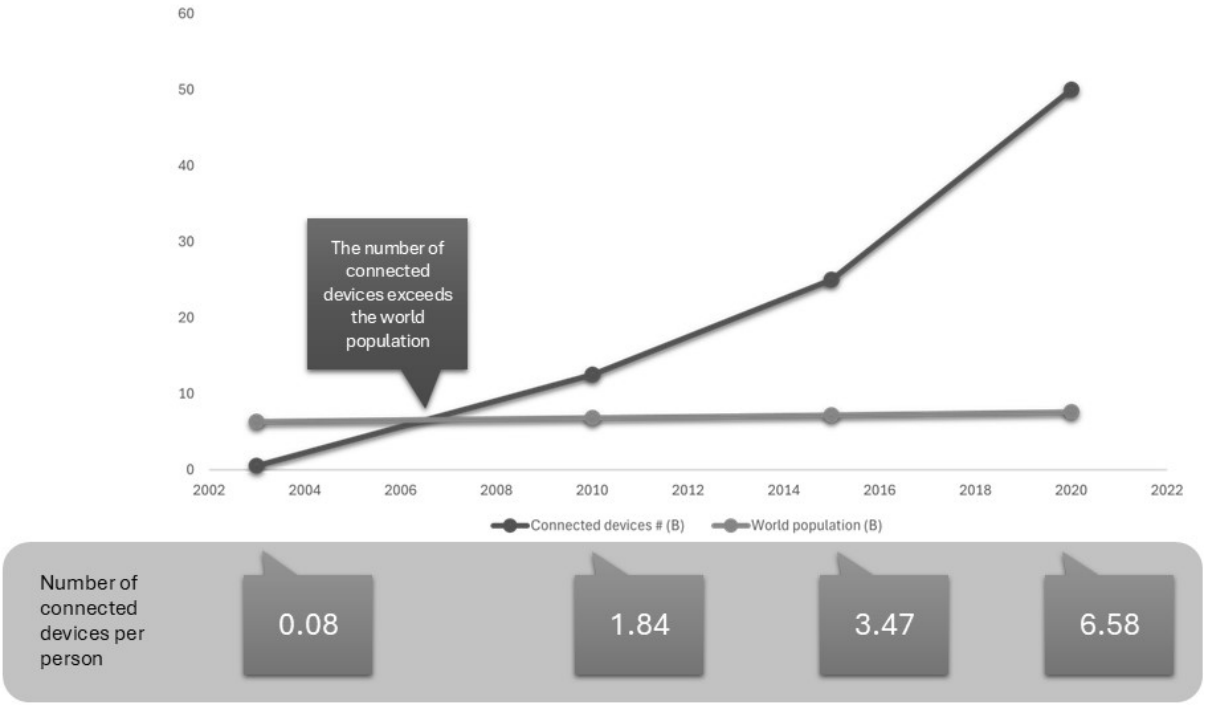


**Figure 1.** The growth of the world population and the number of connected devices.

Cisco's forecasts from over 10 years ago [1] predicted that the number of connected devices would reach 50 billion by 2020. Further predictions suggest that the number of connected devices will surpass 100 billion by 2050 [2].

With this pace of development, one of the challenges that will inevitably need to be addressed in the near future is the storage and protection of data generated by connected devices. Due to their design, IoT devices are not suitable for data storage in the general case, and most IoT devices lack the capacity to encrypt data on the device itself.

Blockchain technology, which is somewhat newer than IoT and has gained popularity after the emergence of Bitcoin in 2008, is also rapidly evolving. Although the original idea of Bitcoin's creator, the famous Satoshi Nakamoto, was to use blockchain for implementing a cryptographically secure peer-to-peer payment system [3], further development of this technology has introduced additional applications of blockchain in various industries such as finance, healthcare, logistics, and others [4]. It is expected that blockchain technology will continue to grow rapidly in the coming years. In addition to the need for fast, secure, and transparent transactions, the development of distributed applications (dApps) will expand the ways blockchain can be used. Some blockchain solutions already allow data storage.

## RESEARCH AIM

This article investigates the suitability of currently available blockchain solutions for storing data generated by IoT devices. To achieve this, we propose a scoring methodology that evaluates key features of selected blockchains, enabling a clear assessment of each platform's appropriateness for IoT data storage. Our research is based on a comprehensive review of documentary sources, including academic papers, websites, code repositories, community documentation, and other relevant materials.

## RELATED WORK

The convergence of IoT and blockchain technology has been explored from various perspectives, with researchers proposing numerous solutions for their integration across diverse use cases. Hashemi et al. [5] introduced a three-component architecture in "World of Empowered IoT Users", leveraging blockchain to securely store IoT data and provide users with direct control over data access. This decentralized framework supports applications in healthcare, smart cities, and autonomous vehicles, facilitating transparent management across multiple domains [5].

In "Survey on Blockchain for Internet of Things", Wang et al. provide an in-depth evaluation of blockchain technologies tailored to the specific needs of IoT applications. Their comparative analysis of ten blockchain platforms examines both strengths and limitations, offering insights into how factors like scalability, security, and efficiency align with IoT requirements [6].

Dai, Zheng, and Zhang [7] introduced the "Blockchain of Things" (BCoT) concept in their survey, "Blockchain for Internet of Things: A Survey". The BCoT framework merges blockchain and IoT to tackle challenges related to scalability, security, and interoperability, positioning blockchain as a key enabler of IoT network integrity and data transparency [7].

Kotel et al. [8] investigated the application of Hyperledger Fabric to enhance security in IoT-enabled smart homes. Their study, "A Blockchain-Based Approach for Secure IoT", emphasizes blockchain's decentralized architecture as a means to strengthen data integrity and user privacy, making Hyperledger Fabric a promising platform for secure IoT environments [8].

Bouras et al. propose a "Lightweight Blockchain-Based IoT Identity Management Approach" that uses a permissioned blockchain for efficient IoT identity management. Their framework emphasizes lightweight operation and high security, addressing the constraints of resource-limited IoT devices [9].

Kumar and Sharma [10] conducted a comprehensive review of trust management approaches in IoT, comparing conventional and blockchain-based techniques. Their findings, published in "Leveraging Blockchain for Ensuring Trust in IoT: A Survey", highlight blockchain's advantages in transparency and resilience over traditional methods [10].

Tseng et al. [11] examined blockchain-based databases for IoT, focusing on the Bitcoin Backbone Protocol (BBP) as a foundation. Their study, "Blockchain-Based Database in an IoT Environment: Challenges, Opportunities, and Analysis", identifies challenges and proposes a consistency mechanism that addresses scalability and reliability in IoT data management [11].

Athavale and Bansal [12] explored a framework using Hyperledger Fabric to securely manage and store IoT data. Their work emphasizes blockchain's capacity to decentralize IoT data management, addressing key issues in secure data handling [12].

Lastly, Zhao et al. [13] propose a secure storage solution for agricultural IoT data in their study. By combining RC5 encryption with blockchain, their framework enhances data confidentiality and integrity, providing a tamper-proof system for managing sensitive agricultural information [13].

### ARTICLE OUTLINE

1) Introduction: This section provides the context and objectives of our research and presents a brief overview of relevant related work by other authors.
2) The Internet of Things and the Data it Generates: This section introduces the concept of IoT, reviews common applications of IoT devices, and addresses key challenges related to data privacy and security.
3) Blockchain Technology: This section explains blockchain fundamentals and highlights significant aspects of blockchain operations relevant to this study.
4) Analysis of Blockchain Suitability for Storing IoT Data: Here, we present our scoring methodology, detailing the blockchain parameters evaluated and the evaluation criteria applied.
5) Analysis of Blockchain Solutions for Storing IoT Data: This section offers a summary of seven selected blockchain platforms based on documentary research and applies our scoring methodology to assess each platform.
6) Conclusions: In the final section, we summarize the scoring results, discuss the findings, and suggest directions for future research.

## THE INTERNET OF THINGS AND THE DATA IT GENERATES

IoT is a term used to denote a large group of heterogenous physical devices, embedded with sensors, software and other technologies that allow them to connect to the internet and exchange various types of data with other systems and devices over the internet. The data generated by these devices is diverse, extensive, and often requires real-time processing and storage. For certain types of IoT data, preserving privacy and confidentiality is also necessary, both at the point of generation, during transfer, and in storage. Due to the limited hardware capabilities of IoT devices, as well as the constraints of available storage space on the devices themselves, encryption and data storage on the devices is often not possible. Additionally, some IoT devices are in inaccessible areas where broadband internet or stable, uninterrupted connection cannot be guaranteed, making the secure and safe transfer of data from the device to the storage location a complex challenge.

IoT devices generate various types and formats of data, often depending on the device's purpose. Some applications of IoT devices lead to the creation of high volumes of data. The type and format of data sent by IoT devices over the network largely depend on the task performed by the IoT device, as well as its position, mode, and operation method.

For this article, the data generated by IoT devices will be grouped according to the application of the devices.

### APPLICATIONS OF IOT DEVICES

IoT data is crucial for the development of smart cities, enabling efficient management of resources, traffic, and services. In smart cities, IoT devices are used to form smart grids – various measurement devices and sensors are used to measure energy consumption, availability of services, or resources. They are also used for traffic monitoring, particularly in so-called "connected vehicles", in traffic cameras, GPS devices, which track traffic flow, vehicle locations, public transportation, road conditions, and more. Part of the smart city concept is environmental monitoring, done through air quality sensors, weather stations, noise sensors, which generate data on air pollution, temperature, humidity, and noise levels. In public safety monitoring in smart cities, surveillance cameras, emergency response sensors, and gunshot detectors are used to generate data on crime rates, incidents, as well as real-time video footage.

IoT devices are used in smart buildings, where they monitor and control heating, cooling, lighting, and track human presence in certain rooms or parts of the building. In such applications, IoT devices generate data on energy usage and indoor air quality, among other things. IoT devices also play a role in waste management, where they monitor waste levels, generating data on the amounts of collected waste, waste collection regimes, and the level of recycling. With the help of IoT devices, water systems in smart cities are also monitored, including water flow rates, water consumption, detection of pipeline damage and supply interruptions, as well as water quality [14].

IoT devices have found special applications in medicine and healthcare, where they are used to monitor patients' vital parameters. IoT devices for monitoring body parameters have found widespread use – from smartwatches and fitness trackers, wearable glucose monitors, blood pressure monitors, to smart inhalers, infusion pumps, and connected implants, and sensors that monitor patient conditions in hospital beds [15].

Industrial IoT refers to the use of IoT devices in industrial environments to improve efficiency, safety, and maintenance. IoT devices in industrial environments are used for predictive maintenance – i.e., monitoring the parameters of industrial systems, such as vibrations, temperature, oil levels, wear of parts, process optimization, monitoring material flow and consumption, production speed and quality, as well as monitoring compliance with safety standards [16].

Agriculture is another field where IoT devices are used. They are tasked with monitoring soil conditions – especially parameters such as moisture, pH value, temperature, monitoring weather conditions – temperature, air humidity, precipitation, wind speed, as well as crop health and condition – growth, presence of diseases and pests, nutrient levels. IoT devices are used to control and monitor irrigation on agricultural land [17].

This, of course, is not an exhaustive and comprehensive overview of all possible applications, but merely a limited list. However, this brief overview shows that IoT devices are diverse and used in various environments for a wide range of tasks. Consequently, the data generated by IoT devices is also highly varied – from short textual data sent, through more complex structures, to photos and video materials.

## SECURITY AND PRIVACY OF DATA GENERATED BY IOT DEVICES

As IoT devices become increasingly present in everyday life, from smart homes to industrial systems, the issue of privacy and security of the data these devices generate is becoming more significant. Additionally, the storage of large amounts of data generated by these devices is becoming a growing challenge.

Some of the challenges in managing data security and privacy include:

- hardware limitations of the devices themselves – IoT devices often have limited resources, such a processing power and memory, making the implementation of security protocols a challenge [18],
- heterogeneity – IoT devices use different standards and protocols, depending on device manufacturers, which introduces challenges in interoperability and security gaps [19],
- large data volume – timely analysis and detection of generated data is hampered by the large volume of data [20],
- device maintenance – IoT devices often have a long lifespan, but updating and upgrading security features is not guaranteed or regular.

To address these challenges, various measures can be implemented to protect data privacy and security, such as:

- data encryption applied during transmission and storage, to protect data integrity and prevent unauthorized access,
- authentication and authorization: if implemented using modern, secure methods, such as two-factor authentication (2FA), it allows control of access, ensuring that access to the device and data is granted only to authorized users,
- regular security updates and maintenance: by maintaining the software and firmware of IoT devices, known vulnerabilities of devices and systems on them are removed,
- security protocols such as TLS/SSL, ensure secure data transmission,
- applying machine learning techniques on generated data helps detect unusual patterns in the data that may indicate security threats [21].

## BLOCKCHAIN TECHNOLOGY

Blockchain is a decentralized, cryptographically secured database shared across network participants. Although the concept dates back to 1982 [22], the first fully decentralized blockchain was implemented in 2008 with the advent of Bitcoin. Bitcoin solved the problem of double-spending and initiated the development of technology that today counts tens of thousands of blockchains with over 100 000 cryptocurrencies.

A blockchain represents a decentralized ledger of transactions. Nodes on the Bitcoin network, also referred to as miners, add validated transactions to the ledger, Figure 2. By applying mutually agreed rules of transaction validation, Bitcoin nodes build the authoritative ledger of transactions that establishes who owns what.

A blockchain can function perfectly well without cryptocurrency.

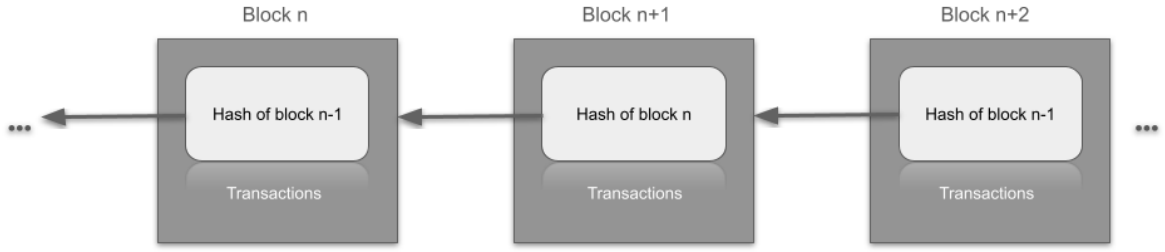


**Figure 2.** A schematic representation of blocks and their connections in a blockchain.

Transactions or records on the blockchain are grouped into timestamped blocks. Each block is identified by its cryptographic hash and references the hash of the previous block. This establishes a connection between blocks, creating a chain of blocks, or blockchain. Any node with access to this ordered list of linked blocks can read it and determine the state of the data exchanged on the network.

We will examine the operation of a blockchain network, in order to understand how the blockchain gets extended by new blocks. The network of a blockchain consists of nodes (clients) that each hold a copy of the database and exchange information with the blockchain. Multiple blockchain users can use a single node as an entry point, but we will assume, for simplicity, that each user issues transactions using their own node. The nodes are connected into a peer-to-peer network, where:

1) Each participant in the blockchain network holds a set of private and public keys, which they use in interactions with the blockchain. The private key signs transactions. The public key is the user's address on the network. Once a node issues a transaction and signs it, the transaction is broadcast to the network.

2) Neighboring nodes validate incoming transactions. Valid transactions are propagated further to the network, invalid transactions are discarded. This is how correct, validated transactions reach all nodes on the network.
3) Validated transactions are collected into a new block, which is proposed at regular intervals. Transactions in the proposed block are time-consumed and ordered by time. The new block is mined by a node, which propagates the block to the network. (The way the mining node is chosen, and the block content depends on the consensus mechanism the network uses.)
4) Before appending the new block to the blockchain, nodes verify transactions validity, and ensure the correct hash is referenced from the previous block. In case the block fails verification, it is discarded. If the new block is verified, the nodes apply the transactions contained in it and update the state of the blockchain. This process is repeated at regular intervals.

The blockchain network is made up of untrusted nodes, that share a database without a trusted intermediary and write data to this database. To help the network achieve a common global view (i.e. reach consensus), all blockchain networks implement a set of specific rules that every participant in the validation process must follow.

The rules applied to determine if an incoming transaction is valid, and whether it should be propagated to the network or not, are uniform for all participants in the validation process. This ensures consensus is reached without the need for trusted intermediaries.

When all nodes follow the steps described above, a blockchain becomes an authenticated and timestamped record of the activity of nodes that participate in the network. As a result, trust emerges within the blockchain from the interactions between participants in the network.

This is a fairly simplified and generalized description of how blockchain operates. Blockchain can also be used for the transfer and tracking of digital assets or for executing code [23].

## TYPES OF CONSENSUSES AND HOW THEY ARE ACHIEVED

Blockchain nodes must reach consensus on the transactions and their sequence in newly generated blocks. If this consensus is not achieved, the blockchain will differ at different nodes, causing a fork in the blockchain. When nodes hold different versions of the network's global state, the unified authoritative chronology of the blockchain is disrupted, unless forks are resolved.

To address this, every blockchain network employs a distributed consensus mechanism. The specific consensus mechanism, through which the nodes continuously validate the network's state, is determined by the blockchain's architecture and design.

If all validating nodes would vote on the transaction order, and transactions receiving the majority vote would be added to the next block, a blockchain that operates in an open, public network, could be exposed to "Sybil" attacks [26], where a single participant manipulates the network by creating multiple identities to vote, potentially seizing control of the blockchain in their favor.

To handle potentially malicious participants on the network, distributed consensus mechanisms that blockchains implement require a form of "investment" – referred to as "proof" that increases the cost of the manipulation of the blockchain.

## PROOF OF WORK

Bitcoin addresses the consensus issue by making block mining computationally intensive, so having multiple identities on the network does not increase the probability of mining a block. Any node on the network can propose the next block, if it computes the random number (nonce) in the block header leading to the block header's hash to have the required number of leading zeros.

The node that solves this computational puzzle produces the Proof of Work (PoW) and earns the right to create and publish the next block in the chain.

Other nodes can easily verify the provided solution and extend their copy of the blockchain with the new block, as the block header is created using a cryptographic hash function. Forks in the blockchain network can occur in rare cases when two nodes publish a new block at the same time. These forks are resolved automatically by the next block, as the PoW mechanism extends the branch with the most accumulated work. The longest chain will be accepted by the nodes, and the consensus will be restored on the correct order of transactions.

Different cryptographic hash functions, such as SHA-256, Blake-256, and scrypt are used for PoW. Some systems combine several algorithms together, like Myriad [25].

## PROOF OF STAKE

Proof of Stake (PoS) is an alternative consensus mechanism, offering far lower computational demand than PoW. In blockchains that implement PoS, a node's chance of mining the next block is directly proportional to the amount of cryptocurrency staked in a wallet. Implementations of PoS can be quite intricate and come with their own set of advantages and drawbacks.

Some variations of PoS are:

- Chain-Based PoS: The validator holding the largest stake on the network creates the next block. Examples include Nxt and Peercoin,
- Byzantine Fault Tolerance (BFT) PoS: Uses delegates chosen to validate blocks, allowing faster consensus with security. Examples include Tendermint and Cosmos,
- Delegated Proof of Stake (DPoS): Users (nodes) vote for delegates who will validate transactions, achieving faster and more efficient validation. Implemented on the EOS and Tron blockchains,
- Bonded PoS: Validators "bond" or stake tokens as the right to validate blocks. If validators act dishonestly, the staked tokens can be forfeited. Examples include Cosmos and Polkadot,
- Hybrid PoS/PoW: Hybrid consensus mechanisms introduce greater security and decentralization by combining PoW and PoS, as implemented on the Decred blockchain [26].

## PROOF OF SPACE OR PROOF OF CAPACITY

Proof of Space, referred to sometimes as PoC, is a consensus algorithm that leverages unused hard drive space instead of computational power or staked cryptocurrency tokens. This reduces the energy consumption required for block mining, addressing one of the common criticisms of PoW, and it is less prone to centralization compared to PoS.

PoS operates by having network participants (miners) allocate a portion of their hard drive space to store plot files, which are precomputed hashes of cryptographic functions. The larger the miner's plot file, the greater the likelihood that they will create the next block.

One of the main advantages of PoS is its energy efficiency compared to PoW, as well as the accessibility of resources – users typically already have hard drives and do not need to acquire specialized equipment as they would with PoW. However, like other consensus algorithms, PoS is not immune to centralization risks, where users with disproportionately large amounts of storage can dominate the mining process. A potential attack vector in this system is the "grinding attack" where malicious actors falsely inflate their allocated space to gain an advantage [27].

Burstcoin was one of the first blockchains to implement Proof of Space. Chia is another well-known blockchain that uses a modified version of this consensus "Proof of Space and Time" a combination that further enhances network security.

## IMPLEMENTATION METHODS

The previous sections described the main concepts of consensus algorithms used in blockchain networks. It is important to note that each type of proof requires participants on the network to

possess a certain type of resource – work, stake, or space – which grants them a varying degree of likelihood to create a new block and thereby extend the blockchain.

Although blockchain technology is still in its infancy, with less than 20 years of history, some of the early weaknesses in consensus algorithms have been identified, and newer solutions often implement hybrid consensus mechanisms by combining two or more types of proofs. This is the case with Decred, for example, or the new version of Burstcoin, which has been renamed Signum, and implements a consensus algorithm that combines Proof of Space and PoS.

## ANALYSIS OF BLOCKCHAIN SUITABILITY FOR STORING IOT DATA

To assess the suitability of blockchain for storing data generated by IoT devices, we will examine, compare, and evaluate the parameters of various operational blockchain solutions. It is estimated that there are currently at least 1000 different operational blockchain networks. Among them are large public blockchain networks such as Bitcoin and Ethereum, as well as specialized blockchain networks designed for specific industries or applications. Some active blockchain networks have very active communities that contribute to the promotion, development, and operation of the network.

### PARAMETERS FOR EVALUATING BLOCKCHAIN SUITABILITY FOR STORING IOT DATA

In principle, many aspects of blockchain technology could be evaluated in the context of blockchain suitability for storing data from IoT devices. However, for the purposes of this article, the parameters considered are limited to:

1) Access to blockchain: private, public, limited
2) Layer on which data is stored: Layer 1, Layer 2, or higher layers,
3) Cost per transaction on the blockchain: costs will be converted to USD/tx (U.S. dollar per transaction),
4) Transaction speed on the blockchain: measured by the speed of generating new blocks and/or the speed of confirming transactions. Transaction speed will be converted to transactions per second (TPS),
5) Data storage capacity: measured by the maximum size (or length) of data that can be sent in a single transaction,
6) Existing security and data protection features,
7) Existence of a community that promotes, maintains, and develops the blockchain,
8) Complexity of implementation measured by the availability of tools, libraries, source code and documentation.

As mentioned earlier, there are dozens of parameters that can be used for comparison and evaluation in addition to the ones listed above.

### EVALUATION METHODOLOGY

To store data generated by IoT devices, the optimal blockchain should possess the following characteristics:

- public access – not requiring permissions, registration, or payment to access the blockchain,
- blockchain architecture that allows storing data on Layer 1,
- low transaction cost – measured by the amount of money paid to add a transaction to the blockchain,
- fast transaction confirmations and block generation on Layer 1 – short block time and high number of TPS,

- high data storage capacity – the amount or arbitrary data that can be stored with a single transaction,
- existing security and data protection measures – libraries or built-in features that secure arbitrary data,
- active community that maintains the blockchain and its ecosystem of distributed applications, measured by the existence, availability, and activity of communication channels (social networks, platforms, repositories),
- available tools and libraries that facilitate easy integration of middleware and applications written in popular programming languages.

In Table 1 we are presenting how we evaluate the selected blockchain parameters and how we assign scores:

**Table 1.** Evaluation methodology.

| Parameter | Score: 10 | Score: 5 | Score: 0 |
|---|---|---|---|
| **Access** | Public access, with no payment or authentication | Limited access (e.g. approval-based) | Authenticated access or required payment, private blockchain |
| **Layer for data storage** | Layer 1 | Layer 2 | Layer 3 or higher |
| **Price of a single transaction, USD/tx** | 0 | < 0.01 | ≥ 0.01 |
| **Transaction Speed, TPS** | ≥ 999 (L1) | < 999 (L1); Any (L2) or configurable | N/A |
| **Data storage capacity, Byte** | > 1000 | ≤ 1000, unclear or configurable | N/A |
| **Existing data security and protection features** | Data security and protection features available | N/A | Data security and protection features not available |
| **Community** | > 1 million followers on social media | ≤ 1 million followers on social media | N/A |
| **Implementation complexity** | Libraries available in TIOBE Top 10 programming languages [28] | Libraries available in programming languages outside TIOBE Top 10 | N/A |

We use scores of 10, 5 and 0 to achieve sufficient differentiation among the platforms we are analyzing. Entries in Table 1 marked as "N/A" are not used.

- Access: blockchains with free, public access that require no authentication are scored with a 10, blockchains where the access is limited by, for example invitation or approval will be scored 5. Private blockchains are scored with 0.
- Layer for data storage: if it is possible to store IoT data on Layer 1, we will assign score 10. If it is possible to store data on Layer 2 (Smart contracts) we will assign a score of 5, if data storage is possible only on Layer 3, we will assign 0. Note that we assign score based on lowest layer where data storage is possible (e.g. if it is possible to store data on Layer 1 and Layer 2, we will assign a 10).
- Price of a single transaction (USD/tx): If transactions are free (no fee), we will score the blockchain with 10, if the fee payable for execution of one transaction is less than 0.01 USD (less than 1 USD cent), we will assign a score 5, and for transaction fees equal to or above 0,01 USD, we assign a score of 0.

- Transaction speed: as stated above, we favor Layer 1 data storage possibility, and prefer high transaction speed on Layer 1. Therefore, we assign a score 10 to blockchains where the Layer 1 transaction speed is equal to or above 999 TPS, and a score 5 for blockchains with transaction speed less than 999 TPS on Layer 1. All blockchains where data storage is possible on Layer 2 or higher layers are scored with 5 for transaction speed.
- Data storage capacity (Byte): Blockchains that allow more than 1000 Byte of data to be stored with one transaction are scored 10. Blockchains where the amount of data that can be stored with one transaction is equal to or less than 1000 Byte, or where the amount of data that can be stored with one transaction is not clear (e.g. Ethereum) are scored with 5.
- Existing data security and protection features: blockchains wich allow additional data security and protection – such as encryption of arbitrary data – are assigned a score of 10. Blockchaisn that have no such features, are assigned a score 0.
- Community: if the blockchain communities on X (formerly Twitter) and Reddit have more than 1 million followers (combined) we assigned a score of 10. If the sum of two social media following is less than 1 million, we assigned a score of 5.
- Implementation complexity: as the optimal blockchain described at the beginning of this chapter will have tools and libraries that allow for easy implementation of additional tools, distributed applications and middlewares, we score the implementation complexity by the available tools and libraries that facilitate integration of other tools and interfaces. If libraries and tools are available and are written in programming languages that are in the top 10 of the TIOBE index, we assign a score of 10. If libraries, tools and SDKs are available in programming languages that are not in TIOBE top 10, we assigned a score of 5, due to the potential difficulty of finding developers who are familiar with such programming languages.

The parameter scores for each blockchain will be summed up to obtain a total score, which can have a maximum value of 80.

This way, we will rank the selected blockchains, and the one with the highest total score will be considered the most suitable for storing IoT data.

### LIST OF BLOCKCHAIN SOLUTIONS FOR ANALYSIS

After preliminary research of existing blockchain solutions, we have compiled a list of 7 blockchain solutions that will be analyzed in detail. During the preliminary research, we eliminated solutions from further analysis that would certainly not meet the criteria outlined in the previous section.

The detailed analysis, following the methodology from the previous section, will be conducted on the following blockchain solutions: IOTA, Signum, Ethereum, Solana, Polygon, Stellar, and Hyperledger Sawtooth.

## ANALYSIS OF BLOCKCHAIN SOLUTIONS FOR STORING IOT DATA

### IOTA

**History and Creators:** IOTA was founded in 2015 by Sergey Ivancheglo, Serguei Popov, David Sønstebø, and Dominik Schiener. The project originated from the Jinn project, which focused on developing ternary hardware for the IoT ecosystem. After rebranding Jinn to IOTA, the first token sale was held in October 2015. IOTA was developed by the IOTA Foundation, a non-profit organization based in Berlin, Germany. The organization oversees the development and maintenance of the network and protocol.

**Purpose:** IOTA is designed to enable secure and efficient data exchange and payments between devices in the IoT ecosystem. Its mission is to become standard for transactions between connected devices, ensuring interoperability and security without the need for intermediaries.

**Architecture:** The core of the IOTA network is the Tangle, a structure based on a Directed Acyclic Graph (DAG), Figure 3. Unlike traditional blockchain systems where transactions are grouped into blocks, Tangle allows the addition of individual transactions that mutually confirm previous transactions. This enables parallel transaction confirmation without a centralized authority, eliminating miners and transaction fees, making the network more scalable and efficient.

**Consensus Algorithm:** IOTA uses a unique consensus approach through the Tangle. When a user initiates a new transaction, they must confirm two previous transactions on the network, ensuring validation without centralized mining. Each transaction requires minimal computational resources to solve cryptographic puzzles via PoW algorithms, preventing spam. This approach allows for fast and fee-free transaction processing.

In the latest versions, such as IOTA 2.0, additional mechanisms like Fast Probabilistic Consensus (FPC) have been introduced to enhance decentralization and security. The removal of the central Coordinator is planned through a project called Coordicide, which will allow for complete decentralization of the network [29-32].

**Additional Information:** WOTS (Winternitz One-Time Signatures) are quantum-resistant, ensuring the security of transactions even in a future where quantum computers are more prevalent [33], Table 2. This feature adds an additional layer of protection to IOTA's network, making it resilient against emerging technological threats, which is particularly important for long-term data security in the IoT ecosystem.

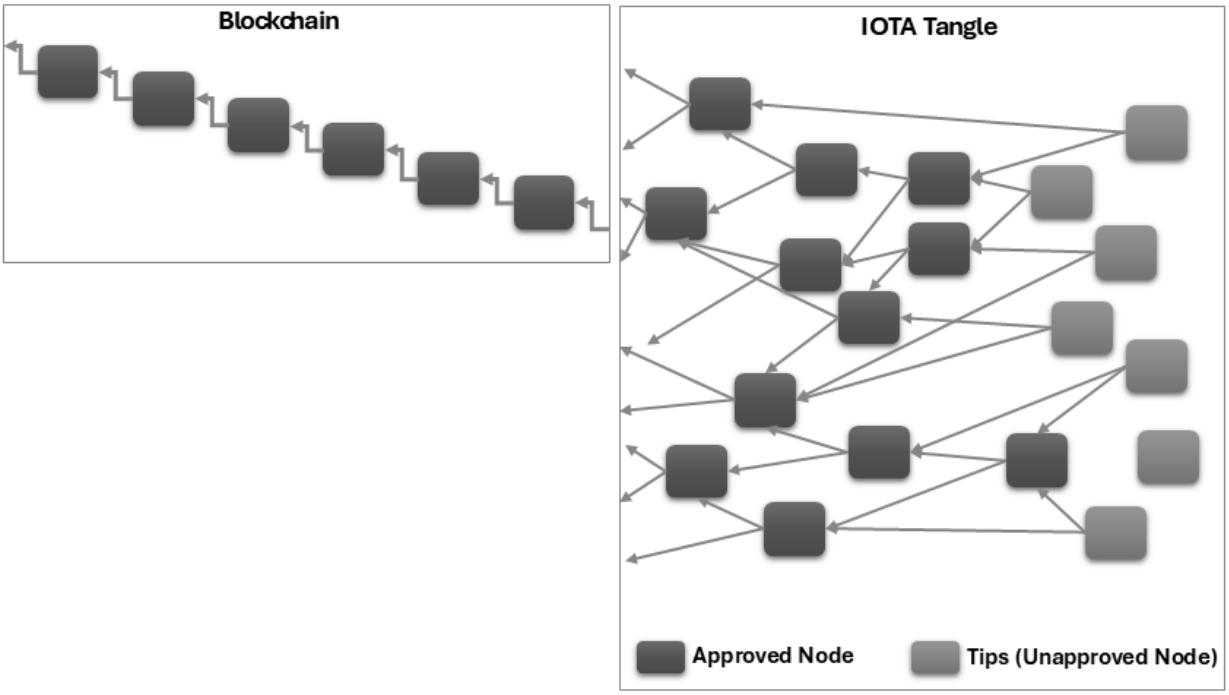


**Figure 3.** Comparison of the structure of a blockchain and the IOTA Tangle (DAG).

**Table 2.** Score for IOTA.

| IOTA | Value/Description | Score |
|---|---|---|
| **Access** | Public | 10 |
| **Layer for data storage** | L1, possible on higher levels | 10 |
| **Price of a single transaction, USD/tx** | 0 | 10 |
| **Transaction Speed, TPS** | Up to 1000 | 10 |
| **Data storage capacity, Byte** | 8192 | 10 |
| **Existing data security and protection features** | WOTS signatures<br>DAG architecture<br>MAM<br>Coordicide<br>Kerl (SHA-3) algorithm | 10 |
| **Community** | Reddit: 144 000 followers (top 2%)<br>X: 270 000 followers | 5 |
| **Implementation complexity** | Libraries: JavaScript/Node.js, Python, Java, C | 10 |
| **Total score:** | | 75 |

## SIGNUM

**History and Creators:** The Signum blockchain evolved from Burstcoin, the first blockhain to implement the Proof of Capacity (PoC) consensus. Burstcoin was initially launched in 2014. The original creator of Burstcoin is an anonymous individual whose identity remains undisclosed. Burstcoin was later renamed to Signum and is supported by a community of developers and enthusiasts, with development now overseen by the Signum Foundation, making it an open and collaborative project.

**Purpose:** Signum was developed to be a sustainable and environmentally friendly blockchain platform, Figure 4. Its primary purpose is to provide solutions for smart contracts, decentralized applications, and various financial transactions without the need for costly and energy-intensive mining.

**Architecture:** Signum uses PoC+ (Proof of Commitment Plus), an advanced algorithm that combines PoC with PoS. Blocks are added to the existing chain every 4 minutes. This algorithm ensures the security of the network through mining that utilizes the existing hard drive space of users, with additional staking included for enhanced security and sustainability.

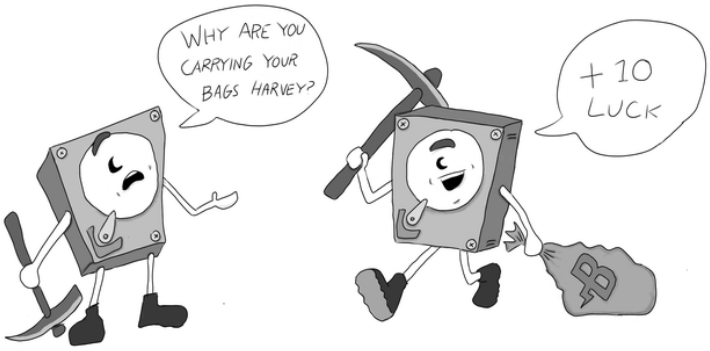


**Figure 4.** Harvey the hard drive – one of the mascots of Signum and PoC+ mining.

**Consensus Algorithm:** The PoC+ algorithm enables mining on the Signum network by utilizing the free space on a user's hard drive. Any user can "commit" disk space and participate in transaction validation. Transactions are added to blocks after being validated through the PoC+ algorithm, which is more energy-efficient compared to the PoW algorithm [34, 35]. This approach makes Signum a more sustainable and accessible blockchain solution, combining the benefits of both PoC and PoS, Table 3.

**Table 3.** Score for Signum.

| Signum | Value/Description | Score |
|---|---|---|
| **Access** | Public | 10 |
| **Layer for data storage** | L1, possible on higher levels | 10 |
| **Price of a single transaction, USD/tx** | 0,00001-0,00003 | 5 |
| **Transaction Speed, TPS** | Up to 5 000 | 10 |
| **Data storage capacity, Byte** | 1000 | 5 |
| **Existing data security and protection features** | Possible message encryption | 10 |
| **Community** | Reddit: 883 followers (top 21%) X: 2 580 followers | 5 |
| **Implementation complexity** | Signum Network SDK, JavaScript library | 10 |
| **Total score:** | | 65 |

## ETHEREUM

**History and Creators:** Ethereum was first described in late 2013 in a white paper by Vitalik Buterin. Buterin was one of the co-founders of Bitcoin Magazine and a programmer at the time. Formal development of the Ethereum software began in 2014 through the Swiss company Ethereum Switzerland GmbH (EthSuisse). The public was first able to purchase Ethereum tokens (ether) during a public sale in July and August 2014. Ethereum was launched in 2015, with Buterin, along with Gavin Wood, Charles Hoskinson, and others, becoming one of the founders of Ethereum.

**Purpose:** Ethereum was designed as a decentralized platform that allows the creation of smart contracts and decentralized applications (dApps). Its purpose is to enable developers to create and deploy applications that operate without intermediaries, increasing efficiency and reducing transaction costs, Figure 5.

**Architecture:** Ethereum's unique architecture solution is based on a global virtual machine known as the Ethereum Virtual Machine (EVM). The EVM allows the execution of smart contracts in a decentralized manner, where each network participant holds a copy of the machine's state and can request the execution of any code. The architecture is designed so that all nodes on the network can agree on the current state and all executed transactions.

**Consensus Algorithm:** After using PoW initially, Ethereum transitioned to PoS in September 2022. In the PoS system, validators (who must stake a certain amount of ether as collateral) are randomly selected to propose blocks, which are then verified and added to the blockchain by other validators. This transition significantly reduced the energy consumption of the Ethereum network [36-38].

**Additional Information:** Transaction fees on Ethereum significantly fluctuate. Depending on the type of transaction, fees can be up to 100 times higher than those listed in Table 4. The fees in Table 4 refer to standard transactions between two Ethereum accounts. The website https://etherscan.io/gastracker provides real-time transaction fees on Ethereum.

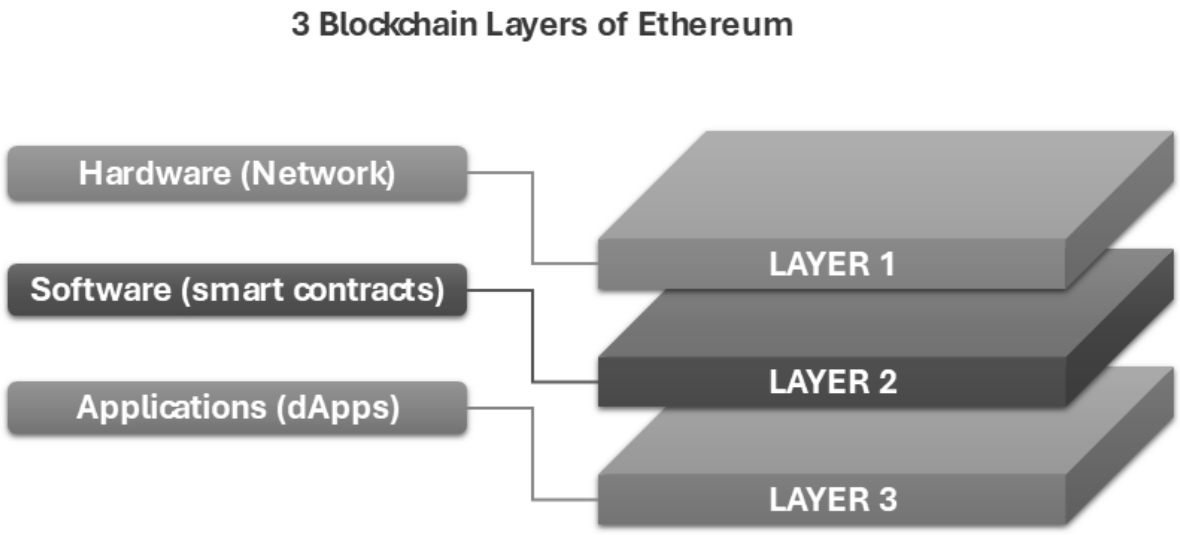


**Figure 5.** Ethereum layers.

**Table 4.** Score for Ethereum.

| | Value/Description | Score |
|---|---|---|
| **Access** | Public | 10 |
| **Layer for data storage** | L1, possible on higher levels | 10 |
| **Price of a single transaction [USD/tx]** | 0.06-0.09 | 0 |
| **Transaction Speed [TPS]** | 15-30 on L1<br>Up to 65 000 on L2 | 5 |
| **Data storage capacity [Byte]** | Up to 220.588 | 5 |
| **Existing data security and protection features** | Possible encryption, zK-SNARKs | 10 |
| **Community** | Reddit: 3 200 000 followers (top 1%)<br>X: 3 400 000 followers | 10 |
| **Implementation complexity** | Libraries: Web3.js, Ether.js, Web3.py, Web3j, go-ethereum, ether-rs, web3swift | 10 |
| **Total score:** | | 65 |

The size of data that can be stored on Ethereum within a Layer 1 transaction is limited by the so-called "gas limit", which is 15 000 000. Theoretically, this allows for 220 588 bytes of data, but it is not possible to use the entire gas limit for data storage – some of the gas must be reserved for other operations necessary for executing the transaction. Additionally, using the

maximum gas for data storage would raise the cost of a single transaction to a level of complete unprofitability. Hence, the data storage capacity has been given a score of 5.

## SOLANA

**History and Creators:** Solana was founded in 2017 by Anatoly Yakovenko. To overcome the limitations of scalability and transaction speed in existing blockchain networks, Yakovenko designed Proof of History (PoH) as a key innovation that enables faster and more scalable transactions, making Solana one of the fastest growing blockchain platforms.

**Purpose:** Solana is designed as a high-performance blockchain platform intended for decentralized applications (dApps) and financial systems, Figure 6. Its purpose is to provide infrastructure that can scale and support many users and transactions with minimal costs and delays, which is particularly beneficial for applications requiring fast transactions, such as gaming, payments, and NFTs.

**Architecture:** Solana utilizes a unique architecture that combines PoH with the Tower BFT consensus algorithm. PoH serves as a timestamp for all events on the network, allowing nodes to agree on the order of transactions without the need for direct communication. This enables the network to be extremely fast and efficient in processing transactions.

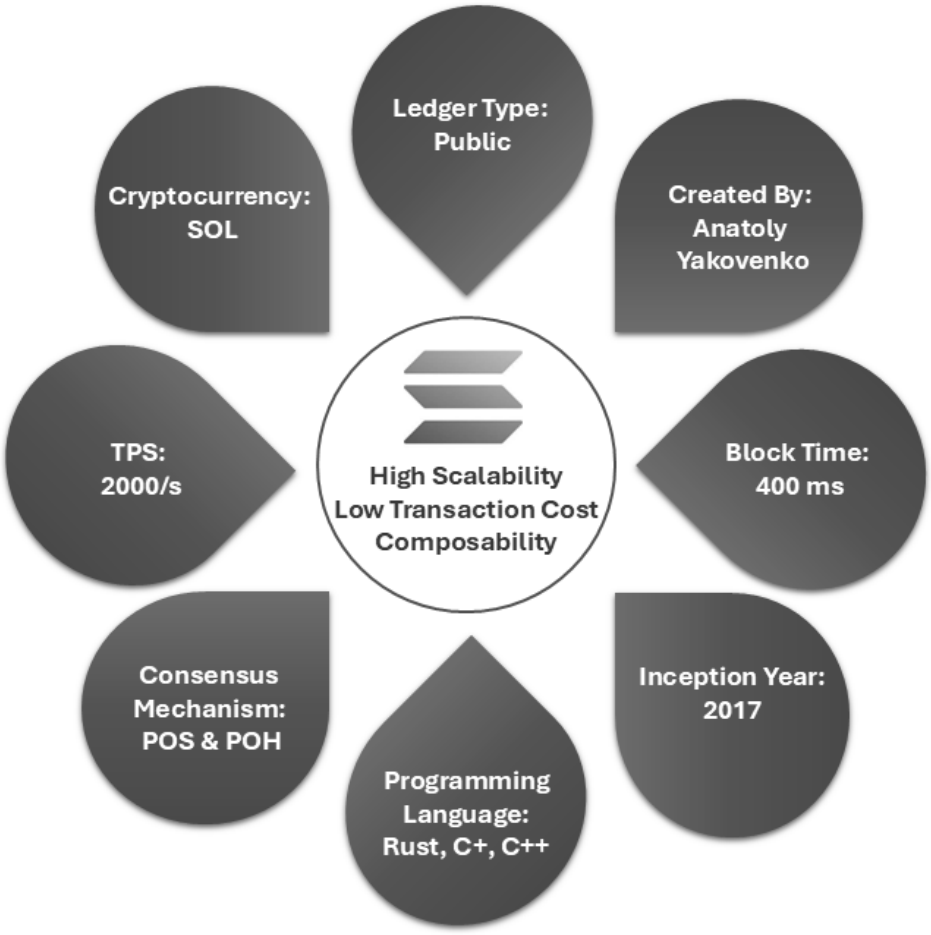


**Figure 6.** Solana features overview.

**Consensus Algorithm:** Solana employs a combination of PoS and PoH algorithms. PoH creates a cryptographic timestamp that allows transactions to be organized and processed more quickly, while PoS enables the validation of these transactions by validators who stake and lock their SOL tokens [39-41], Table 5.

**Table 5.** Score for Solana.

| Solana | Value/Description | Score |
|---|---|---|
| **Access** | Public | 10 |
| **Layer for data storage** | L2, possible on higher levels | 5 |
| **Price of a single transaction, USD/tx** | 0,00025 | 5 |
| **Transaction Speed, TPS** | Up to 50 000 | 5 |
| **Data storage capacity, Byte** | 1 232, up to 10 MB per address | 10 |
| **Existing data security and protection features** | Possible encryption | 10 |
| **Community** | Reddit: 260 000 followers (top 1 %)<br>X: 2 700 000 followers | 10 |
| **Implementation complexity** | Libraries: Solana Program Library (SPL), Anchor framework (all Rust) | 5 |
| **Total score:** | | 60 |

## POLYGON

**History and Creators:** Polygon, formerly known as Matic Network, was launched in 2017 by four software engineers: Jaynti Kanani, Sandeep Nailwal, Anurag Arjun, and Mihailo Bjelic. The project was rebranded to Polygon Technology in 2021, Figure 7, with the aim of solving scalability and high transaction cost issues on the Ethereum network. Since then, Polygon has become one of the most popular Layer 2 solutions for Ethereum.

**Purpose:** Polygon was designed as a Layer 2 solution to enhance scalability and reduce transaction costs on the Ethereum network. Its primary purpose is to enable faster and cheaper transactions while maintaining the security and decentralization provided by Ethereum.

**Architecture:** Polygon uses a layered architecture with a PoS chain as its foundation, known as the Polygon PoS Chain. This architecture allows for fast transaction processing and supports various Layer 2 solutions such as Plasma and zk-rollups. The Polygon PoS chain connects with the Ethereum network via smart contracts, ensuring security and interoperability.

**Consensus Algorithm:** Polygon uses the PoS consensus algorithm, which requires validators to lock a certain amount of MATIC tokens as collateral to participate in transaction validation, for which they receive a commission. Validators are randomly selected based on their stake, and their reward is paid in MATIC tokens. This model significantly reduces energy consumption compared to the PoW algorithm [42, 43], Table 6.

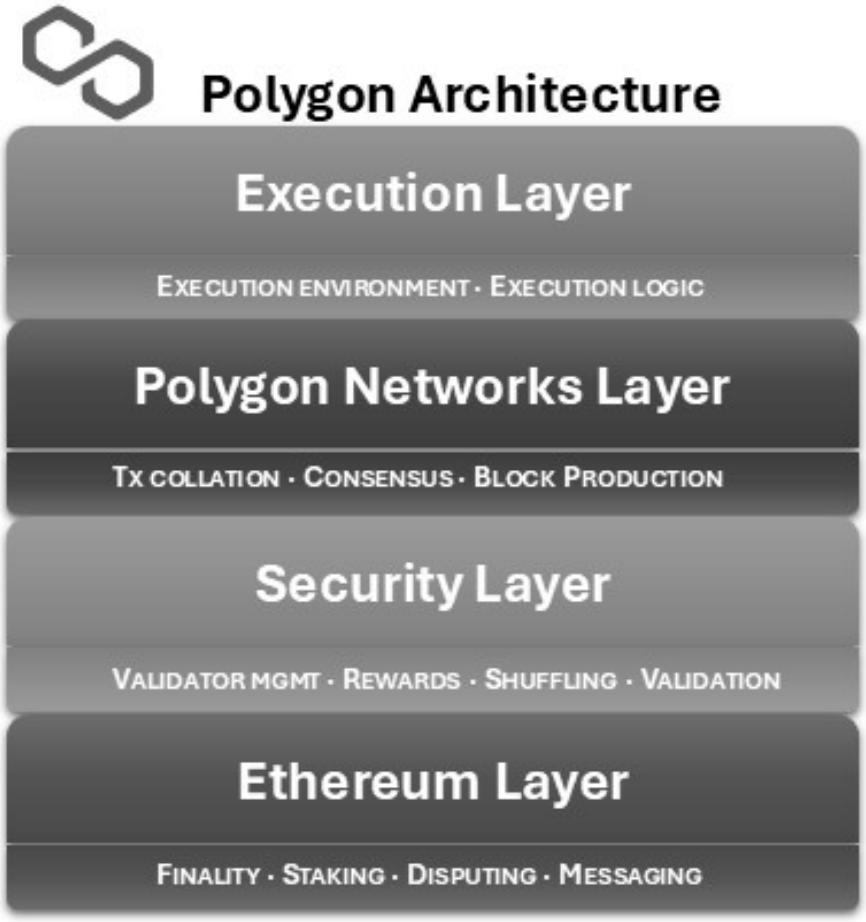


**Figure 7.** Polygon architecture overview.

**Table 6.** Score for Polygon.

| Polygon | Value/Description | Score |
|---|---|---|
| **Access** | Public | 10 |
| **Layer for data storage** | L2, possible on higher levels | 5 |
| **Price of a single transaction [USD/tx]** | 0,01 | 0 |
| **Transaction Speed [TPS]** | Up to 65 000 | 5 |
| **Data storage capacity [Byte]** | Up to several hundred Byte (more data requires paying additional fees) | 5 |
| **Existing data security and protection features** | Possible encryption, zk-SNARKs | 10 |
| **Community** | Reddit: 61 000 followers (top 2%)<br>X: 2 000 000 followers | 10 |
| **Implementation complexity** | Libraries in Rust, CLI tools | 10 |
| **Total score:** | | 55 |

## STELLAR

**History and Creators:** The Stellar blockchain was launched in 2014 by Jed McCaleb, who previously founded Mt. Gox and co-founded Ripple. McCaleb, together with Joyce Kim, launched Stellar as a fork of Ripple, with the goal of creating a network that enables fast and low-cost international transactions. Since then, Stellar has become recognized as a platform connecting financial institutions, payments, and users in a decentralized environment.

**Purpose:** Stellar was designed as a global marketplace to facilitate cheap and fast international transactions using various currencies. Its primary goal is to provide access to financial services, especially for people in underdeveloped regions, while reducing the cost of money transfers.

**Architecture:** Stellar operates a decentralized network that relies on a distributed ledger, Figure 8. This architecture allows all nodes in the network to synchronize information every

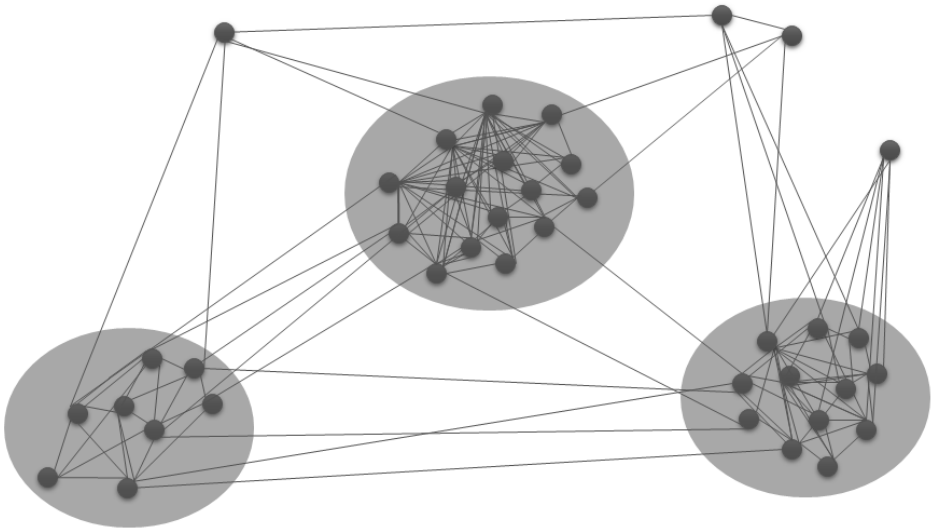

**Figure 8.** Simplified visualization of nodes and quorum slices on the Stellar network.

**Table 7.** Score for Stellar.

| Stellar | Value/Description | Score |
|---|---|---|
| **Access** | Public | 10 |
| **Layer for data storage** | L2, possible on higher levels | 5 |
| **Price of a single transaction, USD/tx** | 0,00025 | 5 |
| **Transaction Speed, TPS** | Up to 50 000 | 5 |
| **Data storage capacity, Byte** | 28 | 5 |
| **Existing data security and protection features** | Possible encryption | 10 |
| **Community** | Reddit: 259 000 followers (top 1%)<br>X: 2 700 000 followers | 10 |
| **Implementation complexity** | Libraries: Wallet SDK, JS SDK, dev tools | 10 |
| **Total score:** | | 60 |

few seconds, enabling fast transactions, Table 7. The system is also open, allowing anyone to set up a Stellar node and participate in the network.

**Consensus Algorithm:** Stellar uses the Stellar Consensus Protocol, based on the Federated Byzantine Agreement model. This protocol enables rapid consensus between nodes through quorum slices, significantly speeding up transactions compared to traditional blockchain models [44-46].

## HYPERLEDGER SAWTOOTH

**History and Creators:** Hyperledger Sawtooth is one of the projects under the Hyperledger umbrella, launched by the Linux Foundation in 2016. Sawtooth was primarily developed by Intel with the goal of providing a flexible and modular solution for building and deploying distributed applications. As part of the Hyperledger family, Sawtooth is open-source and designed for a wide range of industrial applications.

**Purpose:** Hyperledger Sawtooth is designed to enable easy programming and development of blockchain applications, focusing on security, scalability, and modularity. Its purpose is to provide infrastructure that supports various industrial uses, including financial services, IoT, and supply chain management, enabling customized blockchain networks that meet the specific needs of organizations.

**Architecture:** The modular Sawtooth architecture separates the core system from the application domain. The modularity allows defining and implementing business rules without having to understand the system's internal design. Sawtooth's architecture enables parallel transaction execution, increasing network efficiency and scalability, and can run as a permissioned or permissionless network, making it adaptable to various use scenarios.

**Consensus Algorithm:** Sawtooth supports multiple consensus algorithms, including Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance, and Raft. PoET is particularly notable for using Intel SGX security features to generate random time intervals, allowing for energy-efficient consensus without requiring high computational resources [47-49], Table 8.

**Table 8.** Score for Hyperledger Sawtooth.

| Hyperledger Sawtooth | Value/Description | Score |
|---|---|---|
| **Access** | Private | 0 |
| **Layer for data storage** | L1, possible on higher levels | 10 |
| **Price of a single transaction [USD/tx]** | 0, configurable | 10 |
| **Transaction Speed [TPS]** | Depending on the configuration | 5 |
| **Data storage capacity [Byte]** | Depending on the configuration | 5 |
| **Existing data security and protection features** | Possible encryption, DDoS protection | 10 |
| **Community** | Reddit: 3 800 followers (top 11 %)<br>X: 78 100 followers | 5 |
| **Implementation complexity** | Open-source code | 10 |
| **Total score:** | | 55 |

**Additional Information:** Hyperledger Sawtooth differs from other blockchain platforms considered in this article in that it does not have a public platform maintained by miners and validators with open access – hence, the access parameter is scored 0. Although the code is open-source and can be executed on personal infrastructure and configured according to specific needs, this significantly increases the costs of creating a solution for storing IoT data. While it's possible to configure blockchain parameters to make transactions free, one must use their own infrastructure and establish a network of validators and miners.

## CONCLUSION

After applying the methodology described in previous chapters and scoring each of the selected blockchain solutions, we present consolidated scores in Table 9.

**Table 9.** Consolidated scores.

| | IOTA | Signum | Ethereum | Solana | Polygon | Stellar | Hyper-ledger Sawtooth |
|---|---|---|---|---|---|---|---|
| Access | 10 | 10 | 10 | 10 | 10 | 10 | 0 |
| Layer for data storage | 10 | 10 | 10 | 5 | 5 | 5 | 10 |
| Transaction price, USD/tx | 10 | 5 | 0 | 5 | 0 | 5 | 10 |
| Transaction Speed, TPS | 10 | 10 | 5 | 5 | 5 | 5 | 5 |
| Data storage capacity, Byte | 10 | 5 | 5 | 10 | 5 | 5 | 5 |
| Existing data security and protection features | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| Community | 5 | 5 | 10 | 10 | 10 | 10 | 5 |
| Implementa-tion complexity | 10 | 10 | 10 | 5 | 10 | 10 | 10 |
| **Total score:** | **75** | **65** | **65** | **60** | **55** | **60** | **55** |

Among the selected blockchain platforms, IOTA achieved the highest overall score, totaling 75 out of 80. IOTA received top scores in every parameter except "Community," supporting data storage of over 8 kB per transaction on Layer 1. The platform enables feeless transactions and can reach up to 1000 transactions per second on Layer 1. Developed by the IOTA Foundation, the platform benefits from a strong foundation of libraries and documentation, which offsets its relatively small social media community. These attributes make IOTA the most suitable platform among the seven evaluated for storing IoT data.

Ethereum scored 65 out of 80, bolstered by its popularity and a large, active community. However, its suitability for IoT data storage is hindered by volatile transaction fees, lower transaction speeds on Layer 1, and limited clarity regarding data storage capacity per transaction. Signum also achieved a score of 65, offering Layer 1 messaging capabilities and allowing up to 1000 bytes of encrypted data per transaction. While promising, its limitations include transaction costs and a relatively small community supporting the network.

Solana, Polygon, and Stellar provide data storage capabilities on Layer 2, which introduces additional costs and complexities for implementing IoT data storage solutions. Hyperledger Sawtooth, along with Polygon, scored 55 out of 80. Unlike the other platforms, Hyperledger Sawtooth does not have a public network available for general use. Its comparatively lower score reflects the configurable nature of transaction speed and data storage capacity, as we made no specific assumptions about the configuration of private instances.

## FURTHER RESEARCH

Future research on blockchain's suitability for storing IoT data can be advanced in several directions:

- Expanding platform analysis – more blockchain platforms can be assessed using the methodology presented in this article to enhance the comparative insights provided by the scoring system,
- Methodology refinement – additional parameters and weighted scoring could be introduced to emphasize features most critical for IoT data storage, such as Layer 1 transaction speed versus community size,
- Practical validation – building a prototype IoT device that generates sensory data, coupled with a middleware to interface selected blockchain platforms, would enable real-world testing of relevant metrics like latency, storage capacity, efficiency, and cost. Such data can validate and refine the proposed methodology and offer practical benchmarks for future implementations.

# REFERENCES


[1] Evans, D.: *The Internet of Things: How the Next Evolution of the Internet is Changing Everything.*
https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf,

[2] Karunarathne, G.; Kulawansa, K. and Firdhous, M.: *Wireless Communication Technologies in Internet of Things: A Critical Evaluation.*
In: *International Conference on Innovations in Computing (IcoNiC)*.IEEE, 2018,

[3] Nakamoto, S.: *Bitcoin: A Peer-to-Peer Electronic Cash System*.
https://bitcoin.org/bitcoin.pdf,

[4] Tapscott, D. and Tapscott, A.: Blockchain Revolution: *How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World.*
Penguin Random House, New York, 2016,

[5] Hashemi, N.; Dorri, A. and Jurdak, R.: *World of Empowered IoT Users.*
IEEE Internet of Things Journal **3**(6), 1218-1233, 2016,
http://dx.doi.org/10.1109/IoTDI.2015.39,

[6] Wang, X., et al: *Survey on Blockchain for Internet of Things.*
Computer Communications **136**, 10-29, 2019,
http://dx.doi.org/10.1016/j.comcom.2019.01.006,

[7] Dai, H.-N.; Zheng, Z. and Zhang, Y.: *Blockchain for Internet of Things: A Survey.*
IEEE Internet of Things Journal **6**(5), 8076-8094, 2019,
http://dx.doi.org/10.1109/JIOT.2019.2920987,

[8] Kotel, S.; Sbiaa, F.; Kamoun, R.M. and Hamel, L.: *A Blockchain-based Approach for Secure IoT.*
Procedia Computer Science **225**, 3876-3886, 2023,
http://dx.doi.org/10.1016/j.procs.2023.10.383,

[9] Bouras, M.A.; Lu, Q.; Dhelim, S. and Ning, H.: *A Lightweight Blockchain-Based IoT Identity Management Approach.*
Future Internet **13**(2), No. 24, 2021,
http://dx.doi.org/10.3390/fi13020024,

[10] Kumar, R. and Sharma, R.: *Leveraging Blockchain for Ensuring Trust in IoT: A Survey.* Journal of King Saud University - Computer and Information Sciences **34**(10), 8599-8622, 2022, http://dx.doi.org/10.1016/j.jksuci.2021.09.004,

[11] Tseng, L., et al: *Blockchain-Based Database in an IoT Environment: Challenges, Opportunities, and Analysis.* Cluster Computing **23**(3), 2109-2123, 2020, http://dx.doi.org/10.1007/s10586-020-03138-7,

[12] Athavale, V.; Bansal, A. and Nalajala, S.*: Integration of Blockchain and IoT for Data Storage and Management.* Materials Today: Proceedings **45**, 3421-3429, 2020, https://www.researchgate.net/publication/346508057,

[13] Zhao, Y.; Li, Q.; Yi, W. and Xiong, H.: *Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain.* Agriculture **13**(2), No. 274, 2023, http://dx.doi.org/10.3390/agriculture13020274,

[14] Townsend, A.M.: *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*. W.W. Norton & Company, New York, 2013,

[15] Chakraborty, C.; Singh, P.K. and Miraz, M.H.: *Internet of Things for Healthcare Technologies*. Springer, New York, 2020,

[16] Jeschke, S.; Brecher, C.; Song, H. and Rawat, D.B.: *Industrial Internet of Things: Cybermanufacturing Systems.* Springer, New York, 2017,

[17] Singh, R. and Gehlot, A.: *Internet of Things in Agriculture: Technology and Tools.* CRC Press, Boca Raton, 2022,

[18] Sharma, A.; Hiran, K.K. and Kaiwartya, O.: *Internet of Things Security: Challenges, Advances, and Analytics.* CRC Press, Boca Raton, 2020,

[19] Bessis, N. and Dobre, C.: *Big Data and Internet of Things: A Roadmap for Smart Environments.* Springer, New York, 2014,

[20] Barlow, M.: *Real-Time Big Data Analytics: Emerging Architecture.* O'Reilly Media, Sebastopol, 2013,

[21] Hu, F.: *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations.* CRC Press, Boca Raton, 2016,

[22] Chaum, D.: *Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups.* https://nakamotoinstitute.org/library/computer-systems-by-mutually-suspicious-groups,

[23] Christidis, K. and Devetsikiotis, M.: *Blockchains and Smart Contracts for the Internet of Things.* IEEE Access **4**, 2292-2303, 2016, http://dx.doi.org/10.1109/ACCESS.2016.2566339,

[24] Yu, H.; Gibbons, P.B.; Kaminsky, M. and Xiao, F.: *SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks.* In: *2008 IEEE Symposium on Security and Privacy*. IEEE, Piscataway, 2008, http://dx.doi.org/10.1109/SP.2008.13,

[25] Mostefa, K., et al: *A Novel Delegated Proof of Work Consensus Protocol.* In: *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP).* IEEE, Piscataway, 2021, http://dx.doi.org/10.1109/AI-CSP52968.2021.9671096,

[26] Nguyen, C.T., et al: *Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities.* IEEE Access **7**, 85727-85745, 2019, http://dx.doi.org/10.1109/ACCESS.2019.2925010,

[27] Gauld, S.; von Ancoina, F. and Stadler, R.: *The Burst Dymaxion.* https://www.allcryptowhitepapers.com/burst-whitepaper,
[28] TIOBE Software: *TIOBE Index.* https://www.tiobe.com/tiobe-index,
[29] Shabandri, B. and Maheshwari, P.: *Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle.* In: 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE, Piscataway, 2019, http://dx.doi.org/10.1109/SPIN.2019.8711591,
[30] Popov, S.; Saa, O. and Finardi, P.: *Equilibria in the tangle.* Computers & Industrial Engineering **136**, 160-172, 2019, http://dx.doi.org/10.1016/j.cie.2019.07.025,
[31] Coingecko: *A Beginner's Guide to IOTA.* https://www.coingecko.com/learn/beginners-guide-to-iota,
[32] The Investopedia Team: *What Is IOTA (MIOTA)? Definition, How It Works, and Concerns.* https://www.investopedia.com/terms/i/iota.asp,
[33] Baek, B. and Lin, J.: IOTA: *A cryptographic perspective.* Harvard University, Cambridge, 2019, http://104.131.144.199/papers/IOTA.pdf,
[34] *Signum Community Website & Documentation Project.* https://wiki.signum.network,
[35] Keskin, M.: *Comparative Assessment of Eco-Friendly and Highest Trading Cryptocurrencies.* American International Journal of Business and Management Studies **5**(7), 120-129, 2022,
[36] Vujičić, D.; Jagodic, D. and Ranđić, S.: *Blockchain technology, bitcoin, and Ethereum: A brief overview.* In: 17th International Symposium INFOTEH-JAHORINA (INFOTEH). IEEE, Piscataway, 2018, http://dx.doi.org/10.1109/INFOTEH.2018.8345547,
[37] Ethereum.org: *History and Forks of Ethereum.* https://ethereum.org/en/history,
[38] Kelley, K.: *What is Ethereum? Explained With Features and Applications.* https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-ethereum,
[39] Solana: *Solana Documentation.* https://solana.com/docs,
[40] Duffy, F.; Bendechache, M. and Tal, I.: *Can Solana's high throughput be an enabler for IoT?* In: 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, Piscataway, pp.615-621, 2022, http://dx.doi.org/10.1109/QRS-C55045.2021.00094,
[41] Yakovenko, A.: Solana: *A new architecture for a high performance blockchain v0.8.13.* https://solana.com/solana-whitepaper.pdf,
[42] Chaurasia, V. and Kamber, M.: *Unleashing Blockchain Magic: A Comparative Journey Through Developer Ecosystems and Tools in Ethereum, Polygon, and Others*. Dogo Rangsang Research Journal **13**(6), 34-39, 2023,
[43] Weston, G.: *Polygon Architecture Explained.* https://101blockchains.com/polygon-architecture,
[44] Zhuo, X.; Irresberger, F. and Bostandzic, D.: *Blockchain for Cross-border Payments and Financial Inclusion: The Case of Stellar Network*. SSRN Electronic Journal, 2023, http://dx.doi.org/10.2139/ssrn.4550837,
[45] –: *Stellar (payment network).* https://en.wikipedia.org/wiki/Stellar_(payment_network),
[46] Takyar, A.: *What is Stellar Blockchain? A Complete Guide for Beginners*. https://www.leewayhertz.com/what-is-stellar-blockchain,

[47] Sharma, T.K.: *Hyperledger Sawtooth: A Complete Guide*. https://www.blockchain-council.org/blockchain/hyperledger-sawtooth-a-complete-guide,
[48] Weinberg, B.: *Hyperledger Sawtooth Overview: Looking at Permissioned Networks from a Different Perspective*. https://openledger.info/insights/hyperledger-sawtooth-overview,
[49] Anderson, D.: *Hyperledger Sawtooth Blockchain Security (Part One)*. https://www.hyperledger.org/blog/2018/11/09/hyperledger-sawtooth-blockchain-security-part-one.