Review

Privacy-Preserving Blockchain Technologies

Dalton Cézane Gomes Valadares *, Angelo Perkusich, Aldenor Martins Falcão, Chris Seline

Posted Date: 26 May 2023

doi: 10.20944/preprints202305.1874.v1

Keywords: Security; Trusted Execution Environments; Technical Analysis; Privacy Preservation

Article

Privacy-Preserving Blockchain Technologies

Dalton Cézane Gomes Valadares [1,2,*], Angelo Perkusich [1], Aldenor Falcao Martins [3] and Chris Seline [4]

[1] Federal University of Campina Grande, Campina Grande, Paraíba, Brazil;
[2] Federal Institute of Pernambuco, Caruaru, Pernambuco, Brazil;
[3] Signove Tecnologia S/A, Campina Grande, Paraíba, Brazil;
[4] Darkblock, Washington, District of Columbia, United States.
* Correspondence: dalton.valadares@embedded.ufcg.edu.br

Abstract: The main characteristics of blockchains, such as security and traceability, have enabled their use in many distinct scenarios, such as the rise of new cryptocurrencies and decentralized applications (dApps). However, part of the information exchanged with the typical blockchains is public, which can lead to privacy issues. To avoid or mitigate these issues, some blockchains are applying mechanisms to deal with data privacy. Trusted Execution Environments, the basis of confidential computing, and secure Multi-party Computation are two technologies that can be applied in that sense. In this paper, we analyzed seven blockchain technologies that apply mechanisms to improve data privacy. We defined seven technical questions related to common requirements for decentralized applications and, to answer each question, we reviewed the available documentation and gathered information from chat channels. We briefly present each blockchain technology and the answers to each technical question. Finally, we present a table summarizing the information and showing which technologies are more prominent.

Keywords: Security; Trusted Execution Environments; Technical Analysis; Privacy Preservation

1. Introduction

A blockchain is a decentralized chain of blocks that register lists of transactions organizing them hierarchically [1]. Every block added to a blockchain must be mathematically validated by its nodes. This characteristic provides security for the transactions, allowing their auditability. There are three categories of blockchains [2,3]: public, in which anyone can read, send or receive transactions, and any node can participate in the consensus protocol, making decisions regarding the transactions to be accepted; consortium, in which only a set of participants have influence on the consensus process, although anyone can read in the network; and private, in which a unique participant has to write permissions and can control the consensus process, although read permissions can be open to anyone or a set of participants.

Although blockchain technology has gained attention with the Bitcoin arising [4], many application ideas have emerged since then [5], mainly because of technological advances, such as the adoption of smart contracts, which allow code execution in the blockchain nodes. This evolution goes from Blockchain 1.0 with digital currencies, passing by Blockchain 2.0 with smart contracts, and reaching what we have now as Blockchain 3.0 with a high level of trust, security, and accountability [2,6–10]. Due to the distributed nature of blockchains, many of these new applications receive the name of DApps (decentralized applications). This market is growing fast, with much financial and academic (research) investment.

Generally, a blockchain should ensure the following security characteristics: tamper-resistant, pseudonymity, consistency, and resistance to DDoS (Distributed Denial-of-Service) and double-spending attacks [2]. Although these characteristics provide a good level of security, many applications may demand additional properties. For instance, even with pseudonymity achieved, an adversary can perform de-anonymization inference attacks, gathering user transactions and background knowledge to infer the user's true identity. Even considering a user can have various

 doi:10.20944/preprints202305.1874.v1

pseudonymous addresses, all transactions on the ledger are publicly traceable using the sender and receiver addresses. This way, simple analyses can relate the transactions to the used addresses, which can lead to discovering the total amount and number of bitcoins moved to a specific account, for instance. Besides, it is possible to link multiple accounts that use a unique IP address to send and receive transactions.

Another common characteristic that can be a problem for some blockchains is the lack of confidentiality once addresses and transactions' content are available publicly. When considering smart contracts, a requirement is that data and code should be publicly available, which can also be a target for adversaries exploring these data to infer information from the users.

As we can see, despite the security properties provided by the blockchains, we still have privacy issues once privacy leakage can occur by using publicly available transactions' information. Because of this, new blockchains are adopting mechanisms to enhance security, and privacy [11]. Besides using specific protocols that require encrypting the sensitive data, some require that part of the blockchain nodes, at least the validators, run on a Trusted Execution Environment (TEE), which executes code in a protected and isolated region of memory. This way, only a TEE application should process the sensitive information. Other blockchains have adopted cryptographic protocols such as Secure Multi-Party Computation (SMPC), which distributes the computation of a secret among multiple parties with no party knowing about other parties' data.

In this sense, we decided to investigate blockchain technologies that deal with data security and privacy concerns and what they propose as solutions. For this, after researching, we found out and analyzed the following blockchain technologies: Oasis Network[1], Secret Network[2], Phala Network[3], Integritee[4], Ternoa[5], NuCypher[6] [12], and Lit Protocol[7]. Then, to analyze each of these technologies, we defined a few technical questions and explored the available documentation (e.g., white papers and websites), chat channels, and news. This paper summarizes the investigated technologies and presents a rank considering the answers to the technical questions.

Our main contributions are listed below, considering the seven specified blockchain technologies:

- a brief review on each technology that provides means to improve data security and privacy;
- a brief analysis regarding each technology based on the specified technical questions;
- a ranking for the technologies considering their technical analyses.

The remainder of this paper is organized as follows: Section 2 presents the basics of blockchains and trusted execution environments; Section 3 briefly explains the methodology used for the study, including the definition of the technical questions; Section 4 presents each of the seven blockchain technologies investigated; Section 5 brings our technical analysis considering the answers to the technical questions; and Section 6 concludes this work, summarizing the study.

2. Background

2.1. Blockchain principles

A blockchain can be viewed as a distributed ordered data structure with a time stamp where data are only appended. Blockchains' additional properties include immutability, transparency, censorship resistance, and decentralization, enabling a distributed peer-to-peer network. For such a network, non-trusting members can verifiably interact without needing a trusted [11,13]. Application fields are

1 https://oasisprotocol.org/
2 https://scrt.network/
3 https://phala.network
4 https://integritee.network/
5 https://www.ternoa.com/
6 https://www.nucypher.com/
7 https://litprotocol.com/

 doi:10.20944/preprints202305.1874.v1

Internet of Things [14], Vehicular Networks [15], energy [16], supply chains, transport and logistics [17], Healthcare [18] among many others [5,19]. It was introduced in the whitepaper by S. Nakamoto [4] on Bitcoin. It is a distributed ledger that uses independent computers (nodes) to record, share and synchronize transactions in their respective electronic ledgers, connected in a peer-to-peer network. Transactions are the fundamental units in a blockchain. A definite number of transactions are stored in a block, and blocks are continuously and sequentially appended, resulting in a chain. It highlights the significance of decentralization, where most entities participating in the blockchain are authentic and make the decision collectively based on a consensus mechanism.

Different Consensus mechanisms exist[20–22], and the most used is *Proof-of-work (PoW)*. PoW requires solving a complicated computational process, such as finding hashes with specific patterns for authentication and verification. Proof-of-Stake (PoS) protocols split stake blocks proportionally to the current wealth of miners [23] instead of splitting blocks across proportionally to the relative hash rates of miners, providing a more fair selection mechanism and avoiding the domination of stronger participants. Many blockchains, such as Ethereum in 2022, are gradually shifting to PoS, motivated by the lower power consumption and improved scalability. Byzantine Fault Tolerance [24] and its variants [5,22,25] are examples of other possible consensus mechanisms.

Blockchain networks can be classified in different ways [5,23,25,26] considering network's management and permissions as public, private, and federated or hybrid. New users or node miners can join anytime in public blockchains, also known as *permissionless*. Besides, participants can perform operations such as transactions or contracts. On the other hand, in private blockchains, with the federated belonging to the permissioned blockchain category, a whitelist of allowed users is usually defined with particular characteristics and permissions over the network operations. A critical security aspect is that Sybil attacks are almost impossible there [27,28] private blockchain networks can avoid expensive PoW mechanisms. Instead, a more comprehensive range of consensus protocols based on disincentives could be adopted. A federated blockchain is a hybrid combination of public and private blockchains [25]. Although it shares similar scalability and privacy protection level with a private blockchain, their main difference is that a set of nodes, named leader nodes, is selected instead of a single entity to verify the transaction processes. This enables a partially decentralized design where leader nodes can grant permissions to other users. In this article, we provide a more fine-grained blockchain network classification than the current state-of-the-art [13,25,26] because, in addition to classical features such as the ownership and management of the information shared in the blockchain, we consider features such as transaction approval time or security aspects such as the anonymity.

More details related to blockchain technology are beyond the scope of this paper. The interested reader may refer to the work of Habid et al. [29] for scalability issues, Hassan et al. [30] for anomaly detection, Ryan et al. [31] and Taylor et al. [3] for security and privacy issues, and Christidis et al. [13] for smart contracts.

2.2. Trusted Execution Environments

Trusted Execution Environments (TEEs) are the basis for confidential computing, which protects data during processing [32]. The TEEs provide means to create a protected and isolated environment to process data securely, i.e., a TEE creates a tamper-resistant region of memory running with a separated kernel and considering the separation into two execution environments: the "trusted world" and the "normal world" [33]. The isolated and protected environment is the trusted world, which guarantees states integrity for memory and CPU, code authenticity, and confidentiality for data and code.

A TEE application aims to reduce the attack surface, which stays limited to the CPU boundary and prevents direct attacks on the sensitive data or code in memory. The idea is that the data enter the trusted world encrypted, are decrypted, and processed securely inside the trusted world, and the results return to the normal world encrypted [34]. The TEE applications maintain data and code confidentiality even if an adversary gets control of the physical machine.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

The two more adopted TEE technologies commercially available are the ARM TrustZone[8] and the Intel Software Guard Extensions (SGX)[9]. TrustZone requires a trusted operating system to run the trusted world, and SGX works differently, with its trusted environments being called enclaves, which run on the same operating system.

3. Review Methodology

To carry out this study, we first searched for blockchains that propose security and privacy improvements, applying mechanisms to enhance data confidentiality and privacy. We found these seven prominent technologies: Integritee, Lit Protocol, NuCypher, Oasis Network, Phala Network, Secret Network, and Ternoa. To guide us in this work, we decided to establish technical questions based on basic security requirements for decentralized applications that demand sensitive data protection. Thus, we defined the following seven technical questions (TQs):

- TQ1 - How is the communication with the blockchain nodes? Does it support HTTPS or another secure communication method?
- TQ2 - Is it secure? Does it allow/require confidential computing (i.e., trusted processing and storage)? What are the limitations of the programs running in the confidential environment?
- TQ3 - Does it have access control mechanisms? How are they?
- TQ4 - Does it scale? What is the approximate throughput (requests per day)?
- TQ5 - What is the cost? How are payments made? (It is relevant knowing how is the payment for the resources consumed.)
- TQ6 - Does it support communication with other blockchain technologies? How difficult is the communication?
- TQ7 - Is the platform well supported, well funded, and appears successful?

To analyze each technology, answering each of the seven technical questions, we collected information from the official web pages, white papers, news, and chat groups (e.g., Discord[10] groups).

4. Privacy-based Blockchains

4.1. Secret Network

Secret Network is a blockchain based on Cosmos[11] and built with the Cosmos SDK[12], which aims at providing privacy, smart contracts, scalability, and interoperability. It employs proof of stake using Tendermint's[13] Byzantine fault-tolerant consensus algorithms and uses CosmWasm[14] for integration with Cosmos SDK and ecosystem. The CosmWasm provides secure architecture, tools for developing and testing smart contracts, and Cosmos Inter-Blockchain Communication protocol (IBC)[15] integration. The IBC allows interoperability with other blockchain networks. The native token of the Secret Network is the SCRT and its smart contracts are called secret contracts[16].

The SNIP-20 (Secret Network Improvement Proposal)[17] specifies the interactions among tokens and contracts. It is based on Ethereum's ERC-20[18] and ERC-777[19] standards and is a superset of

---

8 https://developer.arm.com/ip-products/security-ip/trustzone
9 https://software.intel.com/pt-br/sgx
10 https://discord.com
11 https://cosmos.network/
12 https://v1.cosmos.network/sdk
13 https://docs.tendermint.com/master/introduction/what-is-tendermint.html
14 https://cosmwasm.com/
15 https://ibcprotocol.org/
16 https://docs.scrt.network/dev/secret-contracts.html
17 https://github.com/SecretFoundation/SNIPs/blob/master/SNIP-20.md
18 https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
19 https://ethereum.org/pt/developers/docs/standards/tokens/erc-777/

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

CosmWasm's CW-20[20]. SecretSCRT (sSCRT) is the first implementation of the SNIP-20 specification and has the following guarantees: all balances and transaction arguments in a transfer are encrypted. Viewing keys can be created to allow third parties or other contracts to access private information (e.g., balance). The token wSCRT is a wrapped SCRT on Ethereum used to provide liquidity and can be redeemed for sSCRT/SCRT (1:1) using the Ethereum-Secret Network bridge[21]. The secret contracts are Rust-based smart contracts that compile to WebAssembly (wasm). Every six seconds, a block is created and appended to the network, with a limit of twenty-two transactions per second (but the theoretical limit is ten thousand transactions per second with the current architecture and protocol) [35].

The network applies encryption protocols, key management, and confidential computing to achieve data privacy. Thus, Trusted Execution Environments (TEE) are required to protect data processing in all the network's validator nodes. Inputs, outputs, and states can be encrypted and securely processed inside a TEE. The consensus seed (256 bits) is the most critical part of the Secret Network encryption schema, being sealed and stored at `\$HOME/.sgx\_secrets/consensus\_seed.sealed` in the validator nodes. The protocol uses the consensus seed and HKDF-SHA256[22] to derivate keys. The public keys are published to the Secret Network `genesis.json`. Curve25519[23] is used to generate asymmetric encryption keys, and ECDH (Elliptic-curve Diffie-Hellman) is used to derive symmetric encryption keys. These symmetric keys are used to encrypt data with AES-128-SIV.

Secret NFTs, defined by the SNIP-721[24] (based on ERC721[25]), allow the NFT owner to decide what data are public and what are private. These NFTs have a name, a value, and a privacy level. The privacy level can be public, protected, or private. For the public level, all the data are publicly available. For the protected, only some property names are public. And, for the private level, only the owner can see the name and the value. When an NFT is sold, Stash[26] charges a fee of 2.75% of the NFT price or 0.05 sSCRT, which is automatically deducted by the platform. A small SCRT amount is also required to pay operation fees to the Secret Network. The NFT is encrypted, uploaded to IPFS[27], and pinned via Pinata[28]. Its public preview is available at Azure. A creator can specify a royalty to be deducted automatically by the platform whenever a collector sells the NFT. Although the royalty addresses are private, their percentages and number of payments are public.

4.2. Oasis Network

The Oasis blockchain [36] is a smart contract platform that provides scalability and privacy. Its smart contracts can be efficiently verified and confidentially executed. Oasis was designed to be:

- flexible - easy to modify system parameters;
- extensible - easy to add new components like confidential computing techniques;
- scalable - throughput should increase with the number of nodes;
- secure - the system should enforce security policies and provide confidential computing;
- and fault-isolated - the system should be fault-tolerant in terms of security and performance.

Oasis' native token is named ROSE (although the native token of the testnet is TEST). The average time to generate a new block is 6s.

The platform has a modular design containing two main layers: the consensus layer and the paratimes layer [37]. The name paratimes comes from parallel runtimes, which means multiple

---

[20] https://docs.cosmwasm.com/cw-plus/0.9.0/cw20/spec/
[21] https://bridge.scrt.network/
[22] https://www.devglan.com/online-tools/hmac-sha256-online
[23] https://cr.yp.to/ecdh.html
[24] https://github.com/SecretFoundation/SNIPs/blob/master/SNIP-721.md
[25] https://eips.ethereum.org/EIPS/eip-721
[26] https://stashh.io/faq
[27] https://ipfs.io/
[28] https://www.pinata.cloud/

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

runtimes can run simultaneously in the network. A verifiable computing implementation (discrepancy detection) provides an optimized consensus execution, more efficient than traditional BFT (Byzantine Fault Tolerance) techniques, improving the smart contracts' scalability. The consensus layer is based on the Tendermint BFT consensus protocol, uses proof of stake as the block proposer protocol, and can be replaced by another consensus mechanism, i.e., allows easy changing of the consensus mechanism. The consensus layer receives a Merkle hash of the encrypted paratime state, keeps the information confidential, and simultaneously supports different smart contract runtimes.

Anyone can implement, register, and operate a paratime. A reference paratime implementation (Oasis Eth/WASI Runtime[29]) enables confidential smart contract execution using TEEs and verifiable computing using discrepancy detection. It supports smart contracts developed in Rust and Solidity. Emerald is the official EVM compatible paratime [38], allowing full EVM compatibility, scalability, 99% lower fees than Ethereum, a cross-chain bridge for interoperability, and easy integration with EVM-based DApps.

The Oasis modular architecture presents a separation between the consensus and paratime smart contract execution layers [39]. It allows enterprises to execute their private paratimes on a specific set of server nodes. If a paratime fails for whatever reason, the others are not affected, and there will be no updates to the blockchain (encapsulation and fault isolation).

The paratimes must pay fees for each consensus layer transaction. A paratime can implement its own token independent of the consensus layer token. The confidential execution of smart contracts occurs within paratimes. For the TEE-based paratimes, the contract executes in a TEE application, and its state is encrypted before being stored. Besides, such paratimes have a key manager component, responsible for managing the cryptographic keys used by the confidential smart contracts.

Oasis SDK[30] provides a modular framework to help developers implement paratimes and wasm-based smart contracts using Rust language. Parcel[31] is another available paratime, which enables the creation of a secure and privacy-preserving layer for the users' data. Parcel SDK allows developers to implement access policies, data ownership, governance, and data storage and analyses, in a privacy-preserving environment [40]. It has APIs to upload datasets, set policies, provide data consent, register applications for data sharing, and schedule off-chain jobs. Parcel SDK also brings means to turn any data file into an NFT. The Wormhole[32] bridge allows transferring of Ethereum, Solana, Avalanche, BSC, Terra, or Polygon tokens for the Oasis Network.

4.3. Phala

Phala Network (PHA) focuses on secure and private distributed computing [41]. The project started in 2018. Phala is a Web 3.0 computing cloud that supports data privacy while remaining trustless. It offers a service to access distributed computing TEE Secure Enclave through a blockchain [42]. Any participant wishing to purchase secure computer resources and services can do so by acquiring the Phala Network token (PHA) to access it through Polkadot[33]. The users can access the same services through Polkadot's Canary Network, Kusama[34], using PHA or its specific token, K-PHA. The vision is to become the world's largest P2P computing network, a decentralized cloud based on Web3.

Phala is a Polkadot parachain developed based on the Substrate framework[35]. Thus, it gains access to all Polkadot's features, mainly the relay chain service providing bridge services to other

[29] https://github.com/oasislabs/oasis-ethwasi-runtime
[30] https://docs.oasis.dev/oasis-sdk/
[31] https://docs.oasislabs.com/parcel/latest/
[32] https://wormholenetwork.com/
[33] https://polkadot.network/
[34] https://kusama.network/
[35] https://substrate.io/

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

blockchains. Phala achieves scalability by implementing two software design patterns: Event Sourcing and CQRS (Command Query Responsibility Segregation)[36] [42]. Event Sourcing is construed when the events causing state transitions are recorded in an append-only log instead of storing the latest state of the data. The events receive timestamps and can be re-accessed to rebuild the state at any time. The second software pattern is the CQRS, which handles read/write operations separately. Such engineering decisions are based on the claim that these patterns make the system scale and avoid conflicts.

The interoperability is kept through secure messaging in contract invocation and token transferring. Phala provides the ability to execute Smart Contracts offering [41,42]:

- Confidentiality, only authorized queries to the contract are answered;
- Code Integrity, verification on the blockchain of an output produced by a specific smart contract;
- State Consistency, verification of execution at specific chain state;
- Availability, no single point of failure (gatekeepers and miners);
- Interoperability, contracts can interoperate with other contracts and blockchains.

The Phala protocol provides the following roles: Users, Worker Nodes, Remote Attestation Service, and Blockchain [42]. Users can invoke, query, and deploy smart contracts. Worker nodes run confidential contracts in compatible TEE hardware and are off-chain. Each worker node runs a program called pRuntime, deployed to an enclave, providing a VM to run contracts. There are three types of Worker Nodes [41]:

- Genesis Node, which bootstraps the network and is destroyed after launch;
- Gatekeepers, which manage the secrets and ensure availability and security of the network;
- Miners, which execute the confidential contracts.

The Remote Attestation Service (RAS) is a public service to validate if a Worker Node deployed a pRuntime correctly inside a TEE. Phala is using the IAS (Intel Attestation Service) for RAS. The last role is the Blockchain, the backbone of the Phala network.

The pRuntime provides, through RAS, the security necessary to execute confidential contracts and implements the Phala protocol. This isolation guarantees that no Byzantine fault can happen unless the pRuntime and TEE are compromised. The executors, miners, are stateless. They get the latest state from a confidential contract by sequentially executing all the input events on the blockchain or from cached contracts and events after that. The blockchain is the only canonical source of contract inputs. Contract states are encrypted and verified on the blockchain with a symmetric key. Each pRuntime registers its identity and establishes secure connections to users with an asymmetric key pair. Since pRuntime registers on the blockchain, any user can validate its identity. The complete process ensures that all Worker Nodes need to register on the blockchain before participating in mining or Gatekeeper election.

The process to deploy the secure execution of code on a distributed structure goes on like this:

- the user/developer publishes the contract to the blockchain;
- gatekeepers generate a symmetric contract key;
- gatekeepers save the encrypted key to the blockchain;
- the user/developer finds an available Miner to load the contract;
- the Miner pRuntime connects to a Gatekeeper through a secure connection and asks for the contract key;
- the Miner uses the received key to encrypt the contract state and saves it to the blockchain.

[36] https://www.eventstore.com/cqrs-pattern

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

4.4. Integritee

Integritee is the new name for a Parachain from a W3 foundation grant called Substratee, having the objective to provide a Trusted Off-Chain Compute Framework for substrate blockchains (SubstraTEE GitHub)[37].

It is now under a company called Integritee AG[38], responsible for driving the development and community efforts for Integritee. The network launched its token TEER to cover payment and governance [43]. Until recently, it has operated its mainnet as an independent project. On February/2022, the community successfully secured a Parachain slot in KUSAMA through a crowd loan process, where they provided rewards for those earlier investors. Their book (Integritee Book) [44] defined Integritee as a framework for Parity Substrate, allowing to call a custom state transition function (STF) inside a TEE, namely an Intel SGX enclave, thereby providing confidentiality and integrity. The enclaves operate on an encrypted state which can be read and written only by a set of provisioned and remote-attested enclaves.

The Integritee website states that the community aims to be the blockchain choice for a secure operating environment that will be scalable, decentralized, and trusted. The company behind Integritee declares that they can scale up to 1 M transactions per second (TPS) due to the decentralized choice of using Polkadot and Kusama infrastructure. The Tokenomics of Integritee will provide a cap on the token availability of 10 M TEER for the project [45].

According to developers, Integritee would be able to provide:

- confidential decentralized state transition functions for private transactions, private smart contracts, off-chain confidential personal data records (GDPR), decentralized identity with selective disclosure, and subscription-based content delivery networks;
- scalability by providing a second layer to substrate-based blockchains for off-chain smart contracts and payment hubs;
- trusted chain bridges;
- trusted oracles.

According to Integritee GitHub [46], the project is structured as:

- The Substratee node (archived);
- Integritee Node (Substratee node with TEE registry validating remote attestation);
- Integritee Worker (Integritee off-chain worker and sidechain "validateer").

An example of an appropriate use case would be a Content Delivery Network (CDN) [47]:

1. subscriptions managed on-chain, and Integritee worker holds the content-encryption key (CEK – RSA-AES) to IPFS and registers the content on-chain;
2. the consumers request content from the Integritee worker over a TLS channel (e.g., HTTPS or WSS), the worker authenticates the consumers and looks at subscription status on-chain;
3. fetches the trusted content from IPFS;
4. decrypts the content;
5. sends the content to the consumer over the previous TLS channel.

The Integritee project completed the M6 and M7 milestones, providing modularity in RUST and the possibility to create shards distributed under multiple processors (Intel SGX). A new feature (not yet funded) for the subsequent releases is the possibility to support Ink![39] (Substrate's smart contracts language). This feature is a crucial functionality to enable easiness in implementing the support for NFTs handling inside the platform.

---

[37] https://github.com/integritee-network/substraTEE
[38] https://integritee.network/company
[39] https://ink.substrate.io/

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

4.5. Ternoa

Ternoa's founder created this blockchain to share his memories with his children in the future. The NFTs work as the vehicle for data transmission and data handling. Ternoa provides the means to store data permanently in any format with the user controlling access and availability [48]. CAPS is the token of the Ternoa blockchain, being used for transactions' payment and governance.

Ternoa allows secure data storage and transmission, providing an SDK to help develop and integrate applications [48]. It is based on the Substrate[40] framework and the Polkadot blockchain, and is designed to be a parachain of Polkadot. Thus, Ternoa enables the connection to other Polkadot-based blockchains. For decentralized storage, it uses other blockchains such as Storj[41], Sia[42], or Arweave[43]. The Rust language is used to develop the smart contracts, and the NFTs are based on the ERC721 standard.

As Ternoa is a Polkadot-based blockchain, the community claims it consumes approximately 0.001% of the Bitcoin blockchain's energy consumption. This reduced consumption is possible because the Ternoa blockchain uses proof of stake (NPOS - nominated proof of stake) as the block proposer protocol instead of proof of work (PoW) [49]. The PoW consumption is estimated at 48.14 kWh per transaction, while the NPoS consumption is estimated in 0.8 GWh per year (800,000 kWh) [50].

Regarding security, data are encrypted and sent to decentralized servers. The scheme uses a Merkle tree for each stored file. Ternoa has a social recovery module named Trusted Friend [48], which allows users to recover accounts in case of losing the authentication key. The user needs to choose M of N "trusted friends" to enable the process of account recovery. To benefit from the social module, a user must hold encrypted keys from other users.

The Ternoa chain has the concept of capsules [51], which encapsulate the encrypted data and are associated with NFTs. Each capsule contains a unique share. This share can be encrypted and stored on different cloud services and decrypted by the NFT owner. The encrypted share can be exported in text format (txt). Ternoa uses Shamir's Secret Sharing[44] (SSS) to secure the capsules, splitting the sensitive data into multiple "shares" used to reconstruct the original data [52]. A threshold defines the minimum number of shares needed to rebuild the data. The capsules keep data protected by using asymmetric GPG encryption[45].

The basic communication flow follows these steps:

1. Create a capsule with an NFT;
2. Encrypt the capsule content with a GPG key;
3. Generate shares from the GPG key using the Shamir Secret Sharing method;
4. Send the shares to master nodes with Intel SGX;
5. Define the time protocol for the capsule and send it to the Ternoa chain.

The time protocol specifies when a capsule should be delivered. Once the time protocol is triggered, the recipients can retrieve the capsule and claim the shares to get the GPG key and decrypt the capsule's content. A transfer protocol allows sending the capsule's keys to a new owner based on a specific date. The blockchain has specific protocols to pass a capsule's access to other users according to conditions like the owner's death or a specified date/countdown. Currently, there is no exact price for the capsules, but the costs will depend on the capsule's design, the transmission date, and the weight of the transmitted files.

---

40 https://substrate.io/
41 https://www.storj.io/
42 https://sia.tech/
43 https://www.arweave.org/
44 https://medium.com/@keylesstech/a-beginners-guide-to-shamir-s-secret-sharing-e864efbf3648
45 https://www.redhat.com/sysadmin/encryption-decryption-gpg

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

The mainnet was planned for Q1 2022 [53]. The testnet has over 200,000 minted NFTs, 150 nodes installed worldwide, and more than 35 marketplaces [54]. According to DotMarketCap[46], Ternoa is the 31st among the most active Polkadot-based blockchains in terms of capitalization, with a market cap of almost US$ 30M. There is a bridge for exchanging Ethereum (ERC20) and Binance (BEP20) tokens [55].

4.6. NuCypher

NuCypher [56] is a data encryption and protection layer for Ethereum (and eventually other public networks) and decentralized applications (dApps) without relying on a central service provider. The protocol, which the team calls a decentralized key management system (KMS), allows developers to store, share, and manage private data on public blockchains. Developers receive this encryption service via a network of NuCypher nodes in exchange for a fee (paid for in ETH). Participants can only spin up a node by staking NuCypher's token, NU, on the network as collateral.

NuCypher is a blockchain-based cryptographic infrastructure for privacy-preserving applications, dynamic control access, secrets management, and secure computation [56,57]. Besides, NuCypher enables users to manage a range of computational secrets, such as identity and access management (IAM) tokens and database and secure shell (SSH) credentials to access servers remotely.

NuCypher uses a decentralized network to remove the dependency on central service providers, proxy re-encryption for cryptographic access control, and a token incentive mechanism to ensure reliability, availability, and correctness [58,59]. Because of proxy re-encryption, an unencrypted symmetric key that can decrypt private data is never exposed server-side. There is no single point of security failure. Even if compromised, hackers would only get re-encryption keys, but access to the file is still protected.

The technology provides a decentralized key management system based on blockchain technology and claims it can be used in DDRM, Decentralized Digital Rights Management, for secret key transformation [59]. In Nucypher's network, the content key is encrypted by the owner's public key, and only the owner's private key can decrypt it. With authorization from the owner, the encrypted key will be fragmented and re-encrypted by several proxy nodes. Nodes are unaware of each other and cannot collude with the receiver. After re-encryption, the receiver collects the re-encrypted fragments and decrypts them.

The NuCypher network focuses on providing extensible runtimes and interfaces for data, named secrets, management, and dynamic access control. It provides shared access to data based on a proxy re-encryption schema (PRE). Access permissions are baked into the underlying encryption, and the data owner is the only one who can explicitly grant access via sharing policies [59]. Consequently, the data owner has ultimate control over access to their data. The NuCypher network cannot decrypt the data nor determine the underlying private keys. NuCypher KMS is a decentralized key management service and cryptographic access control layer for the blockchain and decentralized applications. Developers and enterprises can leverage it to create highly-secure applications in healthcare, financial services, and more. By bringing private data sharing and computation to the public blockchain, NuCypher KMS enables everything from encrypted content marketplaces to secret credentials management and patient-controlled electronic health records.

4.7. Lit Protocol

The LIT (Lockable Interactive Token) Protocol is a decentralized access control protocol running on top of Ethereum and other Ethereum Virtual Machine (EVM) chains (Full list EVM chains)[47]. Based on LIT on-chain access control conditions allows [60]:

---

[46] https://www.dotmarketcap.com/
[47] https://github.com/LIT-Protocol/lit-js-sdk/blob/main/src/lib/constants.js#L14

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

- Encrypt and lock static content, among images, videos, and music, behind an on-chain condition such as ownership of an NFT;
- Decrypt static content that was locked behind an on-chain condition;
- Authorize network signatures that provide access to dynamic content (for example, a server or network resource) behind an on-chain condition
- Request a network signed JWT (JSON Web Token Authentication) that provisions access and authorization to dynamic content behind an on-chain condition.

With this functionality, the LIT protocol enables the creation of locked NFTs that only their owners can unlock [61]. It also allows access to a given server or network resource only to NFT owners. Rather than a simple JPEG, LIT NFTs can be HTML/JS/CSS web pages that can be interactive and dynamic.

The network acts as a decentralized access control list (ACL) which leverages on-chain data to grant users access to content, software, and other decentralized networks [62]. LIT supports many standard contracts and plans to support any RPC call soon. The LIT Protocol is in an alpha state (the "AlphaNet"), and the creators are running all the nodes. During the writing of this paper, the LIT network is unaudited, and the nodes still need to be distributed. Various security improvements must be made, and crypto-economic guarantees resulting from staking are not in place yet. Data are persistent and planned to perpetuate the network. Data can be stored, for example, in IPFS and Google Drives. Developers can use the Lit Protocol SDK [63], currently integrated with EVM chains and storage providers like Ceramic Network[48].

For static content, the SDK encrypts the user's content and uploads the conditions for decryption to each Lit Protocol node. When someone wants to access the content, the SDK requests a message signature from the user's wallet that proves the user owns the NFT associated with the content to each Lit Protocol node. The Lit Protocol nodes will then send down the decryption shares, and the SDK will combine them and decrypt the content.

The SDK can create the authorization conditions for a given resource and store them with the Lit Protocol nodes for dynamic content. For this type of content, the flow is similar: when an entity requests a network signature to access a resource, typically a server that serves some dynamic content, the SDK also requests a message signature from the wallet and verifies if the entity owns the NFT associated with the resource to each Lit Protocol node. Each node will verify what entity owns the NFT, sign the JWT to create a signature share, then send down that share. The SDK will combine the signature shares to obtain a signed JWT, which can be presented to the resource to authenticate and authorize the user.

Nodes can provide the user a key to access specific content, whether to decrypt something or access some service. That is a gateway that many can use. For instance, Shopify[49] merchants could use it to enable NFTs to act as coupon discounts. The nodes can also provide conditions for unlocking, such as someone who owns more than three CryptoPunks[50] can access a given file. A user sends signed messages to each blockchain node to unlock something, creating a decryption share. The network uses BLS (Boneh–Lynn–Shacham) threshold encryption[51]. And then, like a torrent, those decryption shares are sent to the user in the client.

Encrypted messages can be used where only the user address can decrypt a message. The net result is that the user data are sovereign. Users can allow various individuals, applications, or agents to access those data. That means one can own the data and decide what to do with them on the decentralized web without relying on centralized authorities to hold the data. The protocol enables on-chain conditions, such as NFTs, to act as keys to Web 2 and Web 3 experiences. There is no limit to the amount of data a token can be used to control access because it is up to the user to decide

---

48 https://developers.ceramic.network/learn/welcome/
49 https://www.shopify.com/
50 https://www.larvalabs.com/cryptopunks
51 https://alinush.github.io/2020/03/12/scalable-bls-threshold-signatures.html

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

where they want data stored. Lit Protocol provides the access control layer in the stack. Also, the user might not constantly be unlocking data and could be opening a perk, reward, content, or metaverse experience.

There are multiple parties in the network. Some nodes provide the service, with different parties doing encryption and decryption. Whether this is legal or not in a particular country varies with each nation's encryption laws and policies. It depends on the rules in a stakeholder's role and their location.

Also, there is a portal for connecting blockchain wallets to the rest of the Internet, powered by Lit Protocol named Lit Gateway [64]. Apps let a user create resources exclusive to a crypto community, for example, Google drive files that are only accessible to members of the user's DAO (Decentralized Autonomous Organization) or a given NFT's owners. It can offer rewards, discounts, NFTs, and airdrops that can only be accessed if the wallet meets specific criteria, such as owning a given token. Once a wallet is connected, offers that are available can be seen.

5. Technical Analysis

In this Section, we answer each of the seven technical questions described in Section 3 for each of the technologies described in the previous Section.

5.1. How is the communication with the blockchain nodes? Does it support HTTPS or another secure communication method?

5.1.1. Secret Network

In general, developers use SecretJS[52] to connect to a Secret Network node. SecretJS is a javascript/typescript library based on the CosmWasmJS[53] library, and this library allows the creation of a client that connects to a node. The available examples use an HTTPS address for communication with the network nodes, but it is unclear if the communication is performed only with HTTPS. Independently, the communication channel is only one of the concerns regarding data transmission, which can be mitigated by encrypting the sensitive data before transmission. This way, a protected communication channel (HTTPS, for instance) is a plus, not necessarily a requirement.

5.1.2. Oasis Network

Yes. The blockchain supports secure communication with the nodes. By looking at a few code examples, we can see the communication can be established with HTTPS or WSS.

5.1.3. Phala Network

All the worker nodes are non-byzantine nodes, and all contract communications are encrypted off-chain. All communication was designed to be secure, using asymmetric, symmetric keys, keys rotation, node registration, state recovery, and monitoring of responsiveness, in which case the non-compliant nodes will be slashed, where the gatekeepers are under severer scrutiny. Looking at some code examples, we can see that the communications are established with HTTPS or WSS.

5.1.4. Integritee

Integritee will work on top of Polkadot and Kusama. Depending on the application, the project allows specifying what will be executed securely on TEE and what parts will be processed on and off-chain. All Polkadot/Kusama relay/parachains can interface with Integritee workers or sidechains

---

[52] https://www.npmjs.com/package/secretjs
[53] https://github.com/CosmWasm/CosmWasmJS

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

through the XCMP (Polkadot cross-chain messaging protocol). The communication of off-chain workers can happen over any TLS channel.

5.1.5. Ternoa

In general, developers use the SDKs provided by the community. In Ternoa's GitHub, we can find SDKs for the testnet operations, SecretNFTs[54], and marketplace. The documentation is not very good/clear, bringing only the API endpoints. We deduce that Rust language is used for the smart contracts' development while NodeJS is used for the dApps development. In the code examples, we can see URLs with HTTP and HTTPS. We are unsure if they require HTTPS in the testnet, but we believe the mainnet will require it. Independently, the communication channel is only one of the concerns regarding data transmission, which can be mitigated by encrypting the sensitive data before transmission, as mentioned before.

5.1.6. NuCypher

According to the NuCypher Blog, the underlying threshold PRE scheme used in NuCypher, named Umbral, has been rewritten in Rust (rust-umbral), which then can be compiled into JavaScript. Besides, NuCypher itself is being rewritten in TypeScript (nucypher-ts[55]). It is still ongoing work and will allow developers to build apps with full PRE functionality (grant, receive, revoke, among other operations). Nucypher also provides REST-like HTTP endpoints for working with characters (HTTP Character Control).

5.1.7. Lit Protocol

The SDK requires an active connection to the LIT nodes to perform most functions (notably, a connection to the LIT nodes is optional if you are verifying a JWT). The connection is typically done on the first page load in web apps and can be shared between all its pages. In NodeJS apps, this is done when the server starts. Also, a web-ready package is provided with all dependencies included at build/index.web.js, which can be imported to a webpage using a script tag:

$< scriptonload =' litJsSdkLoaded()' src = "https : //jscdn.litgateway.com/index.web.js" >< /script >$

5.2. Is it secure? Does it allow/require confidential computing? What are the limitations to run in the confidential environment?

5.2.1. Secret Network

Yes, it requires that the validator nodes run on TEEs, which run code securely even if an attacker has privileged permissions on the node host. Although TEE is not a "bullet-proof" security solution, it is the most secure employed currently. Thus, the validator nodes run secret contracts preserving data privacy during processing. The TEEs in the validator nodes, together with the encryption mechanisms and the Secret Network standards (SNIP-20 and SNIP-721), provide privacy by design to the network. Intel SGX is the TEE in use for the current validator nodes. Thus, the limitations are the memory size limit for running code and the programming difficulty, which is considered challenging by the community. The memory size should be fine for the secret contracts unless they run complex operations demanding a high amount of memory. Regarding the programming difficulty, code libraries may arise to help the development of secret contracts.

---

[54] https://www.secret-nft.com/
[55] https://github.com/nucypher/nucypher-ts

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

5.2.2. Oasis Network

Yes. The confidential paratime, named Oasis Eth/WASI Runtime[56] (also called Cipher), allows running smart contracts that preserve data privacy since the paratime's nodes employ TEE. This way, the smart contracts receive encrypted data, decrypt and process them inside a protected memory region (e.g., enclave), and encrypt the results before transmission. As the employed TEE is Intel SGX, the limitations are the same for the Secret Network. Regarding the programming difficulty, the Oasis community provides SDKs to ease the development of DApps and smart contracts using Rust and Typescript languages.

Another paratime, named Parcel, employs GCP (Google Cloud Platform) Confidential VMs, which provide VMs that run on AMD SEV processors. The Oasis documentation suggests the development of other confidential paratimes using other security mechanisms, such as homomorphic encryption, zero-knowledge proof, and secure multi-party computation.

5.2.3. Phala Network

All the operations are under a confidential contract and, by definition, end-to-end encrypted between TEE, blockchain, and the user. The communication between TEE and the user is end-to-end encrypted with the Diffie-Hellman algorithm. Developers can implement "fat contracts" using Rust language.

5.2.4. Integritee

Yes. Integritee allows secure data processing by requiring/providing Intel SGX (TEE) in their nodes. The overall security depends on the application design that will use Integritee. For example, a project can be designed to run a CDN where the keys to decrypt the content are the only data processed under the TEE. Once the process is confirmed, the keys to decrypt will be provided to the client and pointed to the URL holding the content. To attest that a specific node runs on an Intel SGX enclave, the requestor node checks the remote enclave's information with the IAS (Intel Attestation Service).

By design, Integritee can adapt to many use cases. The developer decides which part should work under the TEE.

5.2.5. Ternoa

Although there is no good documentation, we deduce that the blockchain requires that the validator nodes, called masternodes, run on Trusted Execution Environments (TEEs). The TEEs in the masternodes and the encryption mechanisms provide privacy by design to the network. Intel SGX is the TEE in use for the current masternodes, although someone said in the Discord's channel that they were changing: "Hi, at the beginning we were planning to use SGX from Intel, but we had to change the technology. Some node types use the TEE to encrypt the information and make sure. There will be few types of nodes, and not all of them will have the TEE features."

We did not get the answers when asked for more information regarding these TEE nodes and their operations. Thus, the limitations are the memory size limit for running code in the SGX enclaves (if the nodes are still using Intel SGX). We believe the Ternoa chain is using the Rust library to develop SGX applications regarding the programming difficulty.

5.2.6. NuCypher

It is secure from the application point of view through the use of PRE. There is no need for confidential computing specific hardware support such as TEE.

---

[56] https://github.com/oasislabs/oasis-ethwasi-runtime

 doi:10.20944/preprints202305.1874.v1

5.2.7. Lit Protocol

Yes, it uses BLS threshold encryption. However, it does not protect data processing, i.e., there is no need for confidential computing-specific hardware support such as TEE.

5.3. Does it have access control mechanisms? What are they?

5.3.1. Secret Network

Yes, but it is not fine-grained. The private information is only available for its owner or those who receive the viewing keys. Thus, the access control relies on the viewing keys, controlling who can see the private information. Regarding the network nodes, the protocol requires that the validator node candidates run on Intel SGX (TEE) and follow some specific rules.

5.3.2. Oasis Network

Yes, at least for the Parcel paratime. According to its documentation, an entity can establish grants (policies) that allow other entities to access data. The Parcel SDK provides APIs to set policies and manage permissions.

5.3.3. Phala Network

The Phala Network provides three kinds of entities: client (user), which operates on normal devices, no need for special hardware; worker, which operates on the TEE and computes confidential contracts; gatekeeper, which operates on the TEE and serves as the authority and key manager. There is no information regarding fine-grained access control mechanisms for DApps. Thus, the DApps should implement their permissions protocol.

5.3.4. Integritee

Integritee blockchain does not have native and fine-grained access control mechanisms. Thus, the applications must implement access control. As mentioned earlier, the client will provide the TEE worker with what should be processed under the Integritee chain and what should be processed off-chain. The communication channels can be encrypted over TLS. The TEE environment has the security guarantees provided by Intel SGX and can be attested with the Intel Attestation Service (IAS). The public attestation part of the task's action would be registered over the Integritee blockchain, providing a public audit.

5.3.5. Ternoa

Yes, but it is not fine-grained. The private information is only available to its owner or those who receive permission to access the capsules' content through the available protocols. Thus, the access control relies on the NFT owners controlling who can see the private information. The protocol requires that the masternodes run on TEE and follow some specific rules regarding the network nodes.

5.3.6. NuCypher

Nucypher Implements dynamic access control that conditionally grants and revokes access to sensitive data. Conditional access specifies conditions for sharing data, such as time-based and behavior-based access. Access revocation revokes access on-demand or automatically under customizable, pre-specified conditions.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

5.3.7. Lit Protocol

Yes. Access control conditions are based on standard contract types like ERC20, ERC721, and ERC1155. Additional conditions are wallet address ownership, proof of humanity, and possession of POAP (Proof of Attendance Protocol). Conditions can be set and define how to grant access.

5.4. Does it scale? What is the approximate throughput?

5.4.1. Secret Network

Yes. The community claims the network is scalable, but it is unclear how much scalable. The gray paper mentions that the theoretical cap is 10,000 transactions per second, which results in 864,000,000 transactions per day.

5.4.2. Oasis Network

Yes. The community claims the network is scalable and versatile. The Emerald parachain allows a throughput of 1,000 TPS, which gives 86,400,000 transactions per day.

5.4.3. Phala Network

Due to protocol decisions, they were able to minimize duplication of execution for validation and decoupling the execution from consensus tasks, as the most intensive tasks inside the TEE are executed off-chain. They have already achieved a trustless cloud of 20,000 registered computing nodes (workers), with 15,000 running on Khala. These servers provide around 120000 vCPUs. The project states that Phala can manage as many as 1 million CPU cores from over 100,000 nodes.

We did not find any information regarding the Phala throughput, but, as Phala is a parachain of Polkadot, we believe its scalability is similar to the one of Polkadot, which is 1,000 TPS (86,400,000 transactions per day). However, the community claims it can reach a greater number when the network evolves to its full operation.

5.4.4. Integritee

The project states that the Integritee blockchain will hold up to 1M TPS, the claimed maximum throughput for Polkadot-based blockchains (parachains). There is a limitation regarding Polkadot/Kusama's capacity to handle over 100 parachains. Securing a parachain is through a bid process where different projects compete for a slot, which can become pricey competition.

5.4.5. Ternoa

Since the documentation does not mention information regarding the blockchain's scalability, we asked in the Discord channel. However, we did not get the information: "Currently, we have no fully updated doc as many things have evolved since the beginning of the blockchain building. However, the team knows that it's necessary and is working on creating the documentation and then updating the white paper with the new core product/feature".

As Ternoa was developed to be a parachain of Polkadot, we believe its scalability is similar to Polkadot's scalability. Besides, the Polkadot community claims the parachains can improve throughput and scalability. For now, we can read that Polkadot is offering 1,000 TPS (86,400,000 transactions per day), but this number can reach 166,000 (or even 1,000,000 when the network evolves to its full operation).

5.4.6. NuCypher

NuCypher's decentralized access control system offers developers and their users a departure from this opaque and trust-dependent paradigm. It enables end-to-end encrypted data-sharing workflows within applications without sacrificing scalability, redundancy, or performance. Applicable

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

to data payloads of any form, size, structure, sensitivity, or production cadence. Users share privileges they currently take for granted but are not obliged to trust the application developers or third-party access control services, such as centralized servers or key management systems, with their data.

5.4.7. Lit Protocol

It is not available in the documentation. We asked on Discord about details but did not receive an answer. Nevertheless, as the Lit Protocol runs on top of Ethereum and this blockchain is still moving the block proposer protocol from proof of work (PoW) to proof of stake (PoS), we can associate the scalability of Lit Protocol to that of Ethereum: 12-15 transactions per second (TPS). This scalability gives more than 1 million transactions per day. When Ethereum 2 starts, the community claims its scalability can reach 100,000 TPS.

5.5. What is the cost? How are payments made?

5.5.1. Secret Network

The payments are made in SCRT, the native token, but depend on the performed operations. The launched Supernova mainnet has promised fees up to 10 times cheaper. In general, it seems the minimum gas fee is 0.25 SCRT. According to a contract's sample code, here are some suggested fees for the main operations: "upload" - 5 SCRTs, "init" and "exec" - 0.5 SCRT, "send" - 0.08 SCRT.

5.5.2. Oasis Network

The payments are made in ROSE, the platform's native token, but depend on the performed operations. The community claims Oasis has 99% reduced fees compared to Ethereum. In the Oasis' Discord channel, we receive the information that the transactions "usually land at about 0.000001 Rose or roughly 2.6 * 10^-7 USD for a regular transfer".

5.5.3. Phala Network

There are already 272,000,000 PHA in circulation with a maximum supply of 1,000,000,000 and already traded in Binance, OKX, DigiFinex, Mandala Exc. and CoinTige, the current value of the token (Feb 2nd, 2023) is 0.1824 USD.

Although we did not find information regarding the cost of operations, we believe the payments should be similar to Polkadot, which adopts a weight-based fee model instead of a gas-metering model. The fees are calculated based on these three parameters: weight fee (base + calls weight), length fee, and an optional tip. The weight fee is based on the time spent to execute the transaction, and the length fee is a multiplier applied to the transaction's size (in bytes).

5.5.4. Integritee

Integritee has a Governance Council that will decide the price to operate in the blockchain. All the work will be rewarded as a TEER token. The token has a dual function of utility and governance. The TEER used as a utility will reward those tasks inside the chain. The TEER used in the governance works as a stake to operate the Integritee blockchain, promote development and council, and decide the price that will operate in the TEE oracle to USD. The Integritee project plans to have companies participating as providers for those services (fiat, TEE), although Integritee AG is the only one operating in the ecosystem.

We believe the payments should be similar to Polkadot, so the same explained for the Phala Network applies to the Integritee (i.e., the fees consider the mentioned parameters).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

5.5.5. Ternoa

We did not find information regarding the costs in Ternoa's documentation, even when we asked on Discord's channel. We could do an estimation as we did for the scalability, based on the Polkadot, but we read that the parachains do not depend on the Polkadot fees. They are independent to require their specific taxes in their specific tokens. As we believe the payments should be similar to Polkadot, they also follow what we explained for the Phala Network.

5.5.6. NuCypher

The minimum and default fee rates are 350 GWEI, while the maximum fee rate is 3500 GWEI per period, per policy, per Ursula. An Ursula is a node that receives information about a user policy to access encrypted data and is rewarded for re-encrypting that data through proxy re-encryption. Ursulas are to NuCypher what validators are to other proof-of-stake networks.

The minimum and maximum fee rates are lower and upper bound to constrain the fee rate a "staker" may offer. The default fee rate is the rate that will be displayed and provided for Alices if the staker chooses not to configure this parameter themselves or chooses a rate outside the boundaries of the global fee range. The default rate will also be used if the range's boundaries are updated, a staker's specified rate now falls outside the range, and they fail to change it.

5.5.7. Lit Protocol

It is not available anywhere in the documentation. We asked on Discord about details, but we did not get an answer so far. Gas or transaction fees are network-dependent, and LIT can interact with any EVM-based chain. It should follow the basics of any EVM-based network.

5.6. Does it support communication with other blockchain, web technologies? How difficult is the communication?

5.6.1. Secret Network

Yes. There are already some bridges between distinct blockchains (e.g., Ethereum, Binance, and Monero) and Secret Network, and they are implementing solutions based on the IBC (Inter-Blockchain Communication). The Secret Network already participates in the "IBC Gang", together with other blockchains.

5.6.2. Oasis Network

Yes. There is a bridge between distinct blockchains (e.g., Ethereum, Solana, Avalanche, BSC, Terra, and Polygon) and Oasis Network. Moreover, the Oasis Network paper mentions that the IBC protocol can be applied for communications between paratimes.

5.6.3. Phala Network

Yes, Phala is built as a Polkadot parachain and can benefit from the Polkadot's shared security, transaction settlements, and consensus. A registered user in the Polkadot Ecosystem requests a quote through a gatekeeper to execute a smart contract following the Phala protocol. By definition, any blockchain in Polkadot can access a TEE through Phala Blockchain.

5.6.4. Integritee

Most of the project is written using Substrate in RUST, a framework with the main goal of providing chains of chains. The system supports Polkadot and Kusama, and, by design, Polkadot can interface with different chains. In the light paper [65], the authors described the intent to support the Ethereum blockchain.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 May 2023 doi:10.20944/preprints202305.1874.v1

5.6.5. Ternoa

Yes. Currently, there are bridges for Ethereum and Binance blockchains. Besides, communication with Polkadot and any of its parachains is considered simple.

5.6.6. NuCypher

Yes, it is a decentralized threshold cryptography service implemented as a layer 2 network on top of Ethereum.

5.6.7. Lit Protocol

Yes, the LIT Protocol is a decentralized access control protocol running on top of Ethereum and other Ethereum Virtual Machine (EVM) chains (Full list EVM chains): Ethereum; Polygon; Fantom; Xdai; Bsc; Arbitrum; Avalanche; Harmony; Kovan; Mumbai; Goerli; Ropsten; Rinkeby.

5.7. Is the platform well supported and well funded? Does it appear successful?

5.7.1. Secret Network

Yes. The community is growing, attracting investments. In 2022, they announced an investment of $400 million to be applied in the Shockwave, their new initiative to solidify the network as the Web3 privacy hub.

5.7.2. Oasis Network

Yes. The community has attracted investments. In 2022, the platform received financial support from Binance, reaching US$ 200 million for expanding the Oasis ecosystem. Besides, companies such as Meta AI are becoming Oasis' partners.

An interesting application built on Oasis is The Music Fund[57], which gives funds to artists in advance for a percentage of royalties during two years.

5.7.3. Phala Network

Yes, the platform was well-funded by IOSG Ventures in September 2020. The company was founded in 2018, with 1 round, not publicly disclosed, and is at the seed stage. Phala raised USD 1.68M in token sales in 2 rounds. In 2022, it joined the Blender Developer Fund to accelerate Metaverse 3D Modeling and Rendering. The company received 3 Web3 Foundation grants. Khala Network is the Phala activity inside the Kusama blockchain, where they secured a slot on July/2021. The company secured a Kusama slot raising 132,281 KSM (USD 15,258,584). Phala Network is the activity of Phala inside Polkadot. They raised 343,024 DOT (USD 5,460,949) in 2021.

5.7.4. Integritee

The platform is funded with grants from Web3 and a total investment of up to USD 6.5 M. In 2022, the community secured a Parachain in Kusama through Crowdloan[58], a proof of confidence from the crypto market in the proposal. The project secured a slot in Kusama in February-2022, raising a total of 20 000 KSM ($2 298 200).

---

[57] https://themusic.fund/
[58] https://polkadot.network/features/crowdloans/

 doi:10.20944/preprints202305.1874.v1

5.7.5. Ternoa

Not so much. The documentation could be improved a lot. Although the mainnet was launched in the first semester of 2022, we could not find detailed information regarding the blockchain or its dApps (e.g., SecretNFT).

5.7.6. NuCypher

Most information on the use is from the academic side.

5.7.7. Lit Protocol

Documentation is quite limited [63]. LIT Protocol has few followers. Discussion on the Discord channel is superficial and not quite technical. However, the community raised $2.2M to use NFTs for decentralized access passes.

5.8. Summary

Table 1 summarizes the investigated technologies considering each technical question. For each question, we evaluated the technology with a number in the range of 1-5, with one meaning not available and five meaning excellent. We added an extra column regarding the SDKs and tutorials available for each investigated technology.

Table 1. Summary

Technology	Secure Channel	TEE on Nodes	Access Control	Scalability	Costwise	Communication with blockchains	Support and maturity	SDKs and Tutorials	Total
Secret	5	5	4	5	4	5	5	4	**37**
Oasis	5	5	4.5	5	4	5	5	4	**37.5**
Phala	5	5	4	5	1	5	3	4	**32**
Integritee	5	5	5	5	1	5	2	3	**31**
Ternoa	5	3	4	5	2.5	5	2.5	2	**29**
NuCypher	4	1	4	3	2	2	2	4	**22**
Lit Protocol	3	1	5	3	2	2	1	4	**21**

6. Conclusion

Although the general blockchains grant some security properties, they lack mechanisms to protect the privacy and confidentiality of sensitive data. To solve this issue, new blockchain technologies are applying techniques, tools, and protocols, such as TEE and MPC. In this context, we have searched the available technologies and analyzed how prominent they are, considering what they propose to enhance data confidentiality and privacy. For this analysis, we defined seven technical questions based on basic security requirements. We then analyzed seven blockchain technologies, summarizing their strengths and weaknesses, and classified them considering the answers to the technical questions.

For future work, we suggest running basic experiments with the seven investigated technologies, producing a benchmark and a testbed. Besides, information on other new technologies can enrich our study.

Author Contributions: Conceptualization, D.C.G.V.; methodology and protocol, D.C.G.V.; technologies selection, D.C.G.V., A.P., A.F.M., C.S.; writing–original draft preparation, D.C.G.V.; writing and editing, D.C.G.V., A.P., A.F.M.; review, D.C.G.V., A.P., A.F.M., C.S.; supervision and project administration, D.C.G.V.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Aste, T.; Tasca, P.; Di Matteo, T. Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer* **2017**, *50*, 18–28. doi:10.1109/MC.2017.3571064.

2. Zhang, R.; Xue, R.; Liu, L. Security and Privacy on Blockchain. *ACM Comput. Surv.* **2019**. doi:10.1145/3316481.
3. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security. *Digital Communications and Networks* **2020**, *6*, 147–156. doi:10.1016/j.dcan.2019.01.005.
4. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* **2008**, p. 21260.
5. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics* **2019**, *36*, 55–81. doi:10.1016/j.tele.2018.11.006.
6. Fatima, N.; Agarwal, P.; Sohail, S.S. Security and Privacy Issues of Blockchain Technology in Health Care—A Review. ICT Analysis and Applications; Fong, S.; Dey, N.; Joshi, A., Eds.; Springer Nature Singapore: Singapore, 2022; pp. 193–201.
7. Chander, B., Deep Dive Into Blockchain Technology: Characteristics, Security and Privacy Issues, Challenges, and Future Research Directions. In *Smart City Infrastructure*; John Wiley & Sons, Ltd, 2022; chapter 1, pp. 1–32. doi:10.1002/9781119785569.ch1.
8. Alzoubi, Y.I.; Al-Ahmad, A.; Kahtan, H. Blockchain technology as a Fog computing security and privacy solution: An overview. *Computer Communications* **2022**, *182*, 129–152. doi:10.1016/j.comcom.2021.11.005.
9. Qahtan, S.; Sharif, K.Y.; Zaidan, A.A.; Alsattar, H.A.; Albahri, O.S.; Zaidan, B.B.; Zulzalil, H.; Osman, M.H.; Alamoodi, A.H.; Mohammed, R.T. Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems. *IEEE Transactions on Industrial Informatics* **2022**, *18*, 6415–6423. doi:10.1109/TII.2022.3143619.
10. Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and Distributed Computing* **2022**, *164*, 152–167. doi:10.1016/j.jpdc.2022.03.009.
11. Gimenez-Aguilar, M.; de Fuentes, J.M.; Gonzalez-Manzano, L.; Arroyo, D. Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems* **2021**, *124*, 91–118. doi:10.1016/j.future.2021.05.007.
12. Cao, Z.; Zhao, L. A Design of Key Distribution Mechanism in Decentralized Digital Rights Management Based on Blockchain and Zero-Knowledge Proof. 2021 The 3rd International Conference on Blockchain Technology; Association for Computing Machinery: New York, NY, USA, 2021; ICBCT '21, p. 53–59. doi:10.1145/3460537.3460556.
13. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. doi:10.1109/ACCESS.2016.2566339.
14. Issa, W.; Moustafa, N.; Turnbull, B.; Sohrabi, N.; Tari, Z. Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey. *ACM Comput. Surv.* **2022**. Just Accepted, doi:10.1145/3560816.
15. Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. *Vehicular Communications* **2022**, *34*, 100458. doi:10.1016/j.vehcom.2022.100458.
16. Gawusu, S.; Zhang, X.; Ahmed, A.; Jamatutu, S.A.; Miensah, E.D.; Amadu, A.A.; Osei, F.A.J. Renewable energy sources from the perspective of blockchain integration: From theory to application. *Sustainable Energy Technologies and Assessments* **2022**, *52*, 102108. doi:10.1016/j.seta.2022.102108.
17. Pournader, M.; Shi, Y.; Seuring, S.; Koh, S.L. Blockchain applications in supply chains, transport and logistics: a systematic review of the literature. *International Journal of Production Research* **2020**, *58*, 2063–2081. doi:10.1080/00207543.2019.1650976.
18. Saeed, H.; Malik, H.; Bashir, U.; Ahmad, A.; Riaz, S.; Ilyas, M.; Bukhari, W.A.; Khan, M.I.A. Blockchain technology in healthcare: A systematic review. *"PLoS ONE* **2022**, *17*, 1–31. doi:10.1371/journal.pone.0266462.
19. Abou Jaoude, J.; George Saade, R. Blockchain Applications – Usage in Different Domains. *IEEE Access* **2019**, *7*, 45360–45381. doi:10.1109/ACCESS.2019.2902501.
20. Lashkari, B.; Musilek, P. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. doi:10.1109/ACCESS.2021.3065880.
21. Mingxiao, D.; Xiaofeng, M.; Zhe, Z.; Xiangwei, W.; Qijun, C. A review on consensus algorithm of blockchain. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2017, pp. 2567–2572. doi:10.1109/SMC.2017.8123011.
22. Nijsse, J.; Litchfield, A. A Taxonomy of Blockchain Consensus Methods. *Cryptography* **2020**, *4*. doi:10.3390/cryptography4040032.

23. Pilkington, M. Blockchain technology: principles and applications. In *Research handbook on digital transformations*; Edward Elgar Publishing, 2016.
24. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Trans. Comput. Syst.* **2002**, *20*, 398–461. doi:10.1145/571637.571640.
25. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *International journal of web and grid services* **2018**, *14*, 352–375.
26. Zhang, J.; Zhong, S.; Wang, T.; Chao, H.C.; Wang, J. Blockchain-based systems and applications: a survey. *Journal of Internet Technology* **2020**, *21*, 1–14.
27. Platt, M.; McBurney, P. Sybil attacks on identity-augmented Proof-of-Stake. *Computer Networks* **2021**, *199*, 108424. doi:10.1016/j.comnet.2021.108424.
28. Hafid, A.; Hafid, A.S.; Samih, M. A Tractable Probabilistic Approach to Analyze Sybil Attacks in Sharding-Based Blockchain Protocols. *IEEE Transactions on Emerging Topics in Computing* **2022**, pp. 1–1. doi:10.1109/TETC.2022.3179638.
29. Hassan, M.U.; Rehmani, M.H.; Chen, J. Anomaly Detection in Blockchain Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials* **2022**, pp. 1–1. doi:10.1109/COMST.2022.3205643.
30. Hafid, A.; Hafid, A.S.; Samih, M. Scaling Blockchains: A Comprehensive Survey. *IEEE Access* **2020**, *8*, 125244–125262. doi:10.1109/ACCESS.2020.3007251.
31. Henry, R.; Herzberg, A.; Kate, A. Blockchain Access Privacy: Challenges and Directions. *IEEE Security & Privacy* **2018**, *16*, 38–45. doi:10.1109/MSP.2018.3111245.
32. Valadares, D.C.G.; Will, N.C.; Spohn, M.A.; de Souza Santos, D.F.; Perkusich, A.; Gorgônio, K.C. Confidential computing in cloud/fog-based Internet of Things scenarios. *Internet of Things* **2022**, *19*, 100543. doi:10.1016/j.iot.2022.100543.
33. Valadares, D.C.G.; Will, N.C.; Caminha, J.; Perkusich, M.B.; Perkusich, A.; Gorgônio, K.C. Systematic Literature Review on the Use of Trusted Execution Environments to Protect Cloud/Fog-Based Internet of Things Applications. *IEEE Access* **2021**, *9*, 80953–80969. doi:10.1109/ACCESS.2021.3085524.
34. Valadares, D.C.G.; Will, N.C.; Caminha, J.; Perkusich, M.B.; Perkusich, A.; Gorgônio, K.C. Systematic Literature Review on the Use of Trusted Execution Environments to Protect Cloud/Fog-Based Internet of Things Applications. *IEEE Access* **2021**, *9*, 80953–80969. doi:10.1109/ACCESS.2021.3085524.
35. Secret Network: A Privacy-Preserving Secret Contract & Decentralized Application Platform. https://bit.ly/3XU64LB. Accessed: 2022-07-10.
36. The Oasis Blockchain Platform. https://bit.ly/41kzwgo. Accessed: 2022-07-10.
37. Oasis Network Primer. https://bit.ly/3xK8RMw. Accessed: 2022-07-10.
38. Oasis Emerald — EVM ParaTime is live on Mainnet. https://bit.ly/3lNrLPS. Accessed: 2022-07-10.
39. A Beginner's Guide to Oasis. https://bit.ly/3lOhwe6. Accessed: 2022-07-10.
40. Introducing Parcel Beta. https://bit.ly/3RSsgU3. Accessed: 2022-07-10.
41. What is Phala Network (PHA)? https://bit.ly/3krDYt8. Accessed: 2022-07-10.
42. Phala Network: A Secure Decentralized Cloud Computing Network Based on Polkadot. https://bit.ly/3lM7fz5. Accessed: 2022-07-10.
43. All Systems Go for Integritee in the Coming Weeks. https://bit.ly/3DypWND. Accessed: 2022-07-10.
44. Integritee Book. https://bit.ly/3Iuus0G. Accessed: 2022-07-10.
45. Integritee Token Economics. https://bit.ly/3f15J8P. Accessed: 2022-07-10.
46. Integritee Network. https://bit.ly/3YOFDrM. Accessed: 2022-07-10.
47. Integritee Use Cases - CDN Subscriptions. https://bit.ly/3IhfVFk. Accessed: 2022-07-10.
48. TERNOA - White Paper. https://bit.ly/3LnJSok. Accessed: 2022-07-10.
49. The Ternoa blockchain. https://bit.ly/3SgaJ7R. Accessed: 2022-07-10.
50. Duchemin, N. Ternoa, Creating Environmentally-Friendly Augmented NFTs. https://bit.ly/3LpGoBz. Accessed: 2022-07-10.
51. Ternoa capsules. https://www.ternoa.com/capsules. Accessed: 2022-07-10.
52. Schreyer, D. How is Ternoa using TEE technology to maximize security? https://bit.ly/3Ueqmih. Accessed: 2022-07-10.
53. Eshwarla, P. Ternoa Phase 1 Roadmap: Alphanet and Mainnet . https://bit.ly/3LuXuOD. Accessed: 2022-07-10.
54. Gabriel, G. Introducing Ternoa. https://bit.ly/3UmcUIU. Accessed: 2022-07-10.

 doi:10.20944/preprints202305.1874.v1

55. Gabriel, G. Ternoa Bridge. https://bit.ly/3UuR5XY. Accessed: 2022-07-10.
56. NuCypher Documentation. https://bit.ly/3khF0YT. Accessed: 2022-12-10.
57. A Deep Dive Into NuCypher. https://bit.ly/3IKDjfI. Accessed: 2022-12-10.
58. Egorov, M.; Wilkison, M.; Nuñez, D. NuCypher KMS: Decentralized key management system. Blockchain Protocol Analysis and Security Engineering 2018, 2018.
59. Egorov, M.; Nuñez, D.; Wilkison, M. NuCypher : A proxy re-encryption network to empower privacy in decentralized systems. 2018.
60. What is the Lit Protocol? https://bit.ly/41tJFaW. Accessed: 2022-12-10.
61. Lit Protocol Use Cases. https://bit.ly/3Ze8NR6. Accessed: 2022-12-10.
62. Introduction to Decentralized Access Control. https://bit.ly/3YUrKIB. Accessed: 2022-12-10.
63. Lit Protocol SDK. https://bit.ly/3klQfzs. Accessed: 2022-12-10.
64. Lit Gateway. https://bit.ly/3Zf1OXN. Accessed: 2022-12-10.
65. Integritee Lightpaper. https://uploads-ssl.webflow.com/60c21bdfde439ba700ea5c56/612892db018a36f054100b4d_IntegriteeAGLightpaper.pdf. Accessed: 2023-02-20.