SERA's Project

The Revolutionary Blockchain-Enabled ERP

Bringing Blockchain into Business

seraproject.org

Abstract

This whitepaper introduces **SERA**'s latest project: a new enterprise resource planning solution (ERP) running on public blockchain.

According to a survey carried out in 2019 by FORRESTER, under the title Public Blockchain is on the Horizon, 75% * of companies are considering leveraging public blockchains in the next couple of years.

Contents

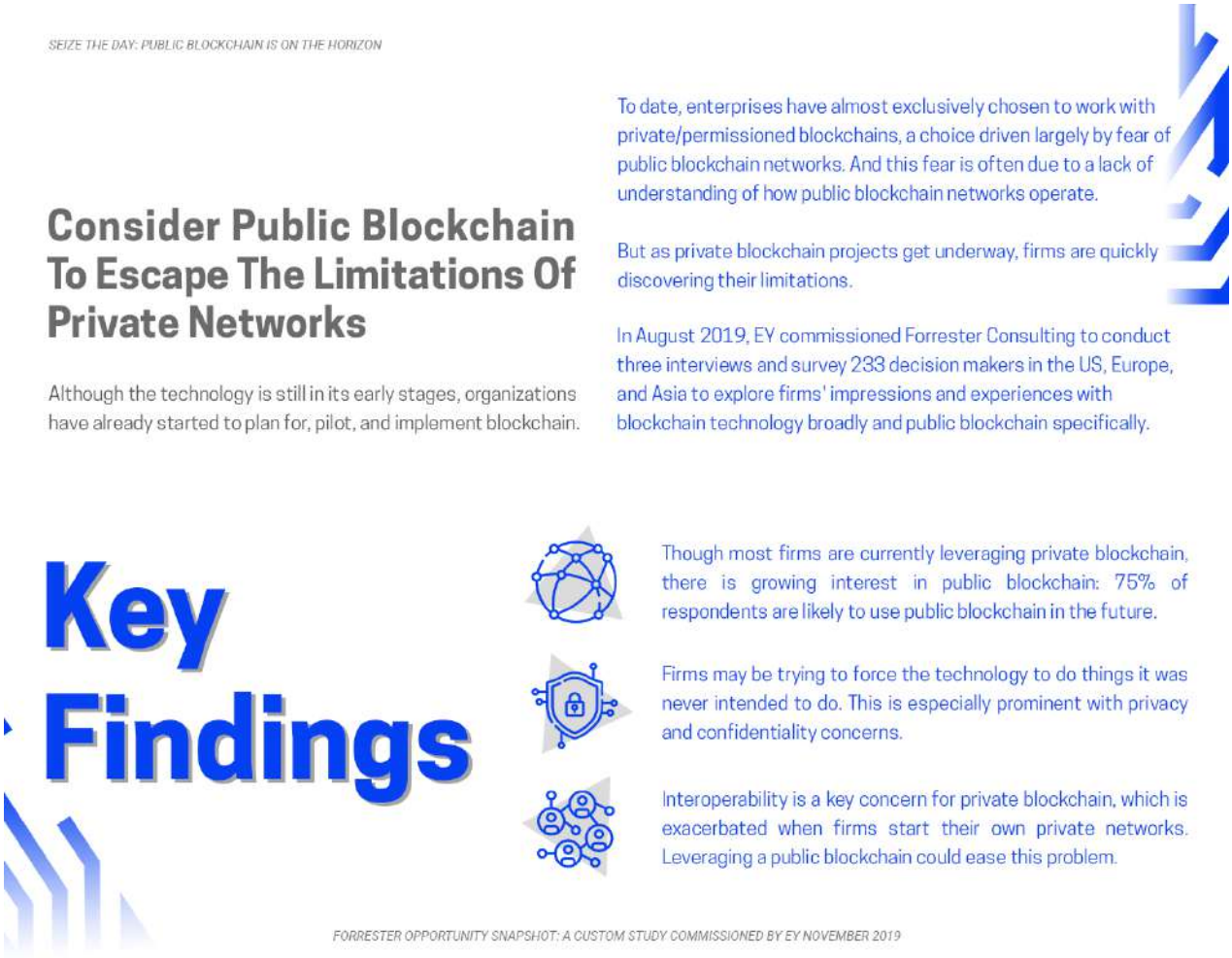


Fig 1: an illustration of the research conducted by Forrester

SERA's project tackles a number of challenges faced by businesses today, the main one being the integration of public blockchain in the business sector, thus eliminating all security and privacy concerns.

Blockchain-enable ERPs are the latest breakthrough in enterprise business application, bringing benefits to companies comparable to the ones brought by cloud computing and even to the internet.

But when it comes to public-blockchain integration, the main concern expressed by them is connected to the security and privacy of their data. By using layer-2 rollups, such as zero-knowledge proof (also known as ZK

rollup), **SERA**'s blockchain-enabled ERP brings the solution to this, combining both on and off-chain data, maximizing the use of blockchain technology.

The problem

Most companies these days understand the need to leverage blockchain, given its ability to preserve data, as well as integrity. And since it can also boost operations while keeping them at a low cost, it presents itself as the perfect solution.

In the past, private blockchains were the only option available in the market, usually found with larger ERP providers. Although efficient in what they offered, they still lacked as far as interoperability goes. Because each company could come up with their own private networks, this became a major issue.

The solutions

As mentioned above, public blockchain is a rational alternative that eliminates any concerns related to security and privacy. And since it can also boost operations while keeping them at a low cost, it presents itself as the perfect solution.

Blockchain technology is something that evolves daily and works as a great remedy to problems faced by companies today, especially when it comes to security and privacy.

And part of this is due to a technology called Layer-2, which brings us to what is known as rollups.

Rollup is a layer-2 scaling technology. Contract-state hashes, as well as transaction calls, and arguments reported as calldata, are saved on-chain in a rollup system. But the transaction itself occurs off-chain. Several off-chain transactions are then merged into a separate on-chain state transition to achieve rollup performance. It is the capacity of the on-chain contract to check the validity of state transitions that ensures rollup security. It is worth pointing out here that Optimistic Rollup and ZK-Rollup are two of the major rollup methods.

The problem

The coronavirus pandemic has put global supply chains to the test. Unprecedented disruptions have exposed the fragility and inherent risks of single-source supplier dependency. As a result, the topic of supply chain resilience has come into sharp focus.

Businesses rely heavily on banking services

If the current banking system collapses, the world supply chain will collapse as well, there is no alternative for banking sectors in case of military conflicts or a new pandemic.

Traditional B2B bank transactions are slow and expensive

Traditional B2B bank transactions typically take between 1 and 5 business days; during the pandemic, some transactions took weeks. The average transaction cost is $35.Every day, some business conduct hundreds of transactions.

The solutions

Smart Contracts

Smart contracts require certain indelible conditions to be met before payment can be issued. scanning a QR code will trigger a smart contract that confirms the transaction and transfers the payment in minutes.

Cryptocurrencies

Cryptocurrencies is the best banks alternative, a crypto transaction can take less than a minute, saving time and cost on traditional bank transactions.

Tokenization

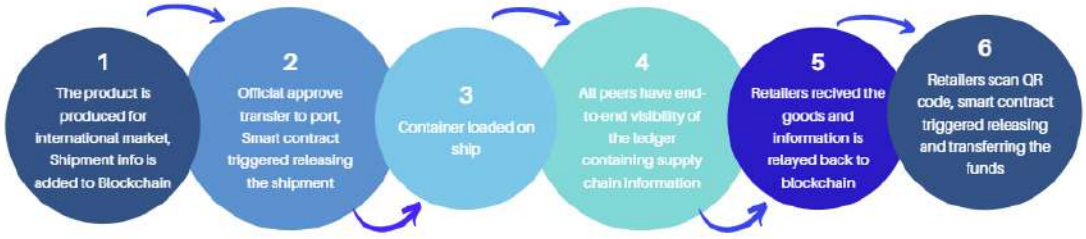
Tokenize physical assets by assigning unique identifiers allowing for better tracking, quality control and inventory management In addition to eliminating the need for third-party financial institutions such as banks.

DeFi and NFT

DeFi and NFT are game changers in business; there's no need for a traditional letter of credit anymore. DeFi reduces the hassle and lengthy formalities for SME's, which saves a lot of time.

How **SERA** works

SERA is a complete digital/blockchain transformation platform, offering 35+ extensive business modules suitable for a number of different industries. It helps companies achieve their goals through public blockchain, using a layer-2 rollup system (with both on and off-chain data) that focuses on privacy and maximum security.



SERA can be accessed through any web-enabled device, as well as through its mobile app. For technical specs and screenshots, make sure to visit our website.

Vision

As reported by the PWC, the majority of CEOs of major corporations are actively analyzing how blockchain technology can help improve their businesses, with 60% calling it the biggest tech development to take place after the internet.

At **SERA**, we believe that blockchain is going to lead the modern corporate change, which is something that has already begun.

SERA provides the foundation for a collaborative supply chain, in which enterprises are uniquely able to work together to unlock gains while also expanding their control across the supply chain. It also provides the basis

for automated reconciliation of supply chain transactions, creating accurate and strategic sourcing and collaborative planning obtaining full visibility for all SERA ecosystem partners adding traceability and transparency, cryptocurrencies and smart contracts play a major role to provide banks alternative, smart contracts require certain indelible conditions to be met before payment can be issued.

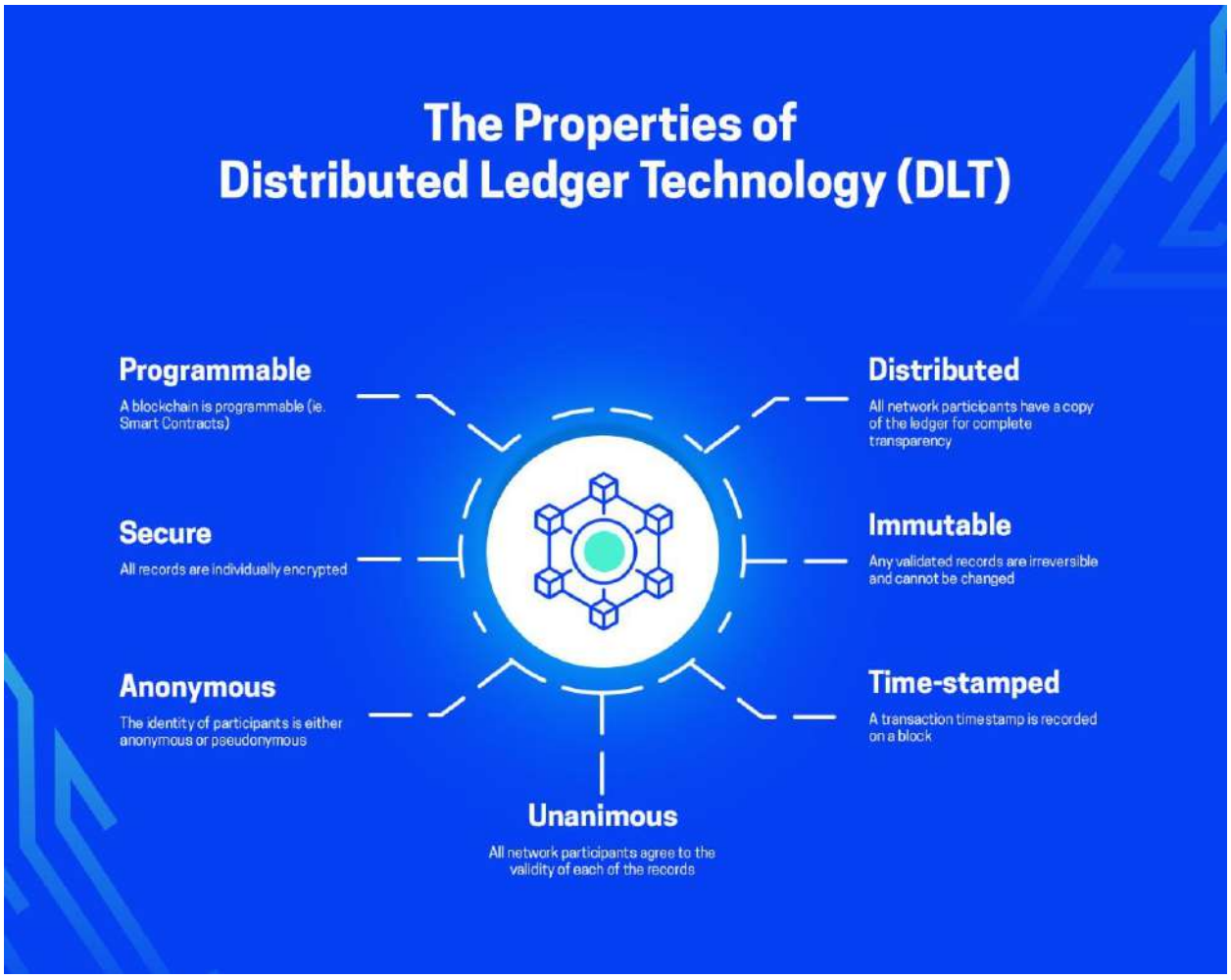
Enterprise Resource Planning (ERP)

ERP stands for enterprise resource planning—a kind of software that businesses use to handle day-to-day operations, like procurement, project management, risk management and compliance, all the way to accounting and supply chain. More premium ERPs can also help with planning, budgeting, and predicting, and even provide financial reports.

How Blockchain and Distributed Ledgers can DRASTICALLY Improve a Business's Day-to-Day Operations?

Distributed ledger

A distributed ledger is a database of transactions that is shared and synced across several devices and locations without the use of a centralized control system. Each one of them possesses an identical copy of the record, which is updated immediately whenever changes are made. Blockchains belong to this group, and are one of the types of distributed ledgers.



Blockchain in the supply chain

In almost every industry, companies are adopting software to monitor and trace products back to their source, establish authenticity and origin, avoid recalls, and speed up the flow of commodities. And thanks to blockchain

technology, accountability, and transparency and on the increase all over the supply chain.

Blockchain is being used to monitor perishables from farm to table, which is one area where it has really taken off. Food suppliers may invite anybody they choose to join the network, such as food aggregators, sustainable farmers, or even individual growers, using a permissioned blockchain. When food is harvested, it is then given a QR code that provides information about its origins, the grower's identity, and whether it is organic or from a fair-trade company. As the data flows through the supply chain, it is encoded into the blockchain and rigorously updated.

Because of that, if a product recall does occur, companies may utilize the blockchain to pinpoint which batches were harmed, lowering the waste and cost of a larger recall. On the same token, retailers and consumers may also use the QR code to examine crucial information about items after they have been delivered—even if they want to check every single fruit used in a smoothie, for example.

Blockchain for utilities

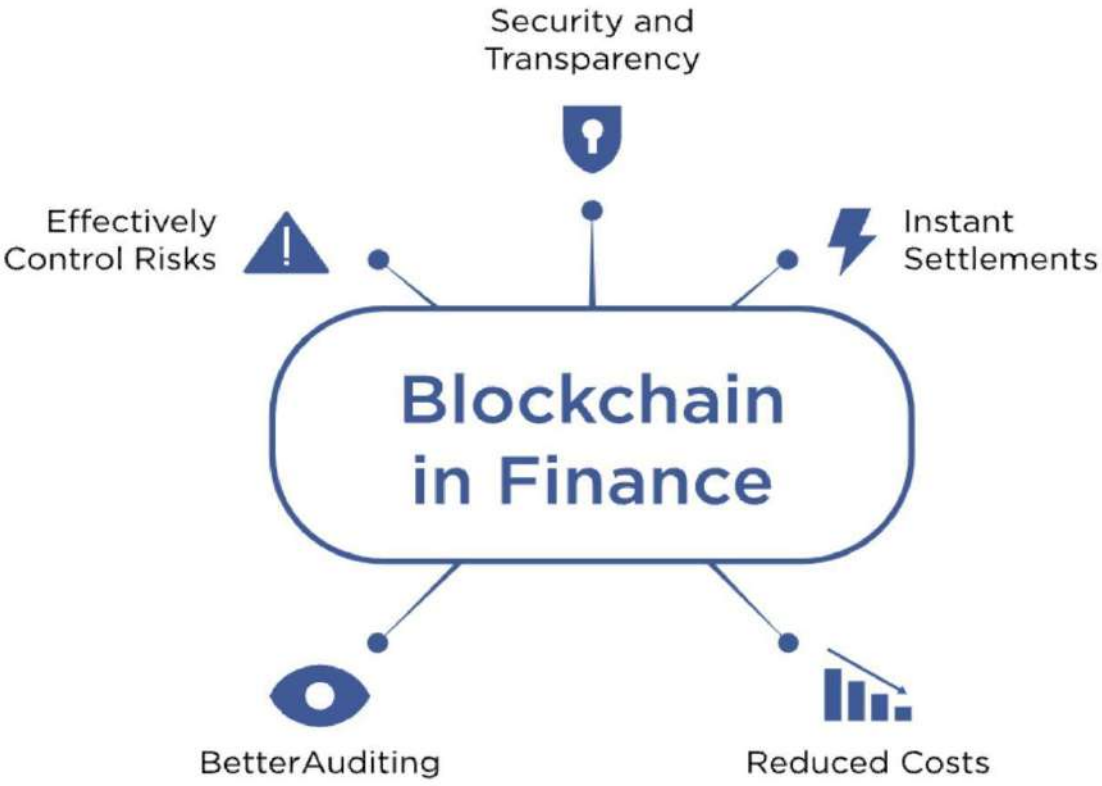
In the utilities sector, blockchain is being tested for a variety of applications, including neighbor-to-neighbor solar energy sales, energy trading across utility conglomerates, automated invoicing for autonomous electric car charging stations, and more.

Blockchain in HR

Checking a person's qualifications and expertise these days can be a long, dreadful task, considering that candidates are increasingly likely to work for several companies at a time, navigating through different fields a lot more regularly than before. With that said, HR professionals may be able to check career credentials more easily if there is a blockchain documenting education levels, certifications earned, work history, and other qualifications.

Blockchain in finance

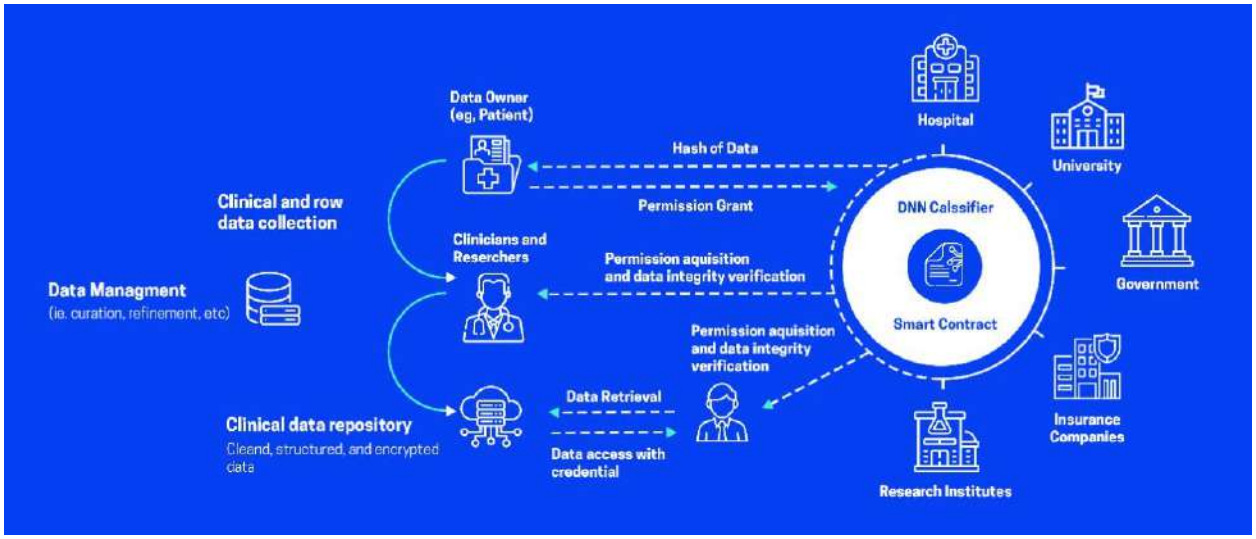
In the world of finance, blockchains can be used to simplify and accelerate services and transactions. With them, the AP department at your company, for example, would be able to make payments directly to your partners, eliminating the need for a bank. In this scenario, the payer's identity is encoded using private keys and baked into the chain before being confirmed by other computers in the network. Because the blockchain in question is updated by the recipient, the AP will no longer have to update their records. This technology is also being used with royalty payments, offering a far more efficient and automated system.



Blockchain in healthcare

Blockchain can be applied in healthcare as well, particularly when it comes to medical records and medicine supply. It streamlines drug traceability, generating data that is extremely hard to temper with, which enables

statewide interoperability and simplifies the verification of medical claims with the help of smart contracts.



Blockchain in retail

With smart contracts, companies can simplify the way inventory is managed and tracked, and also automate customer payments.

Permissioned vs Permissionless

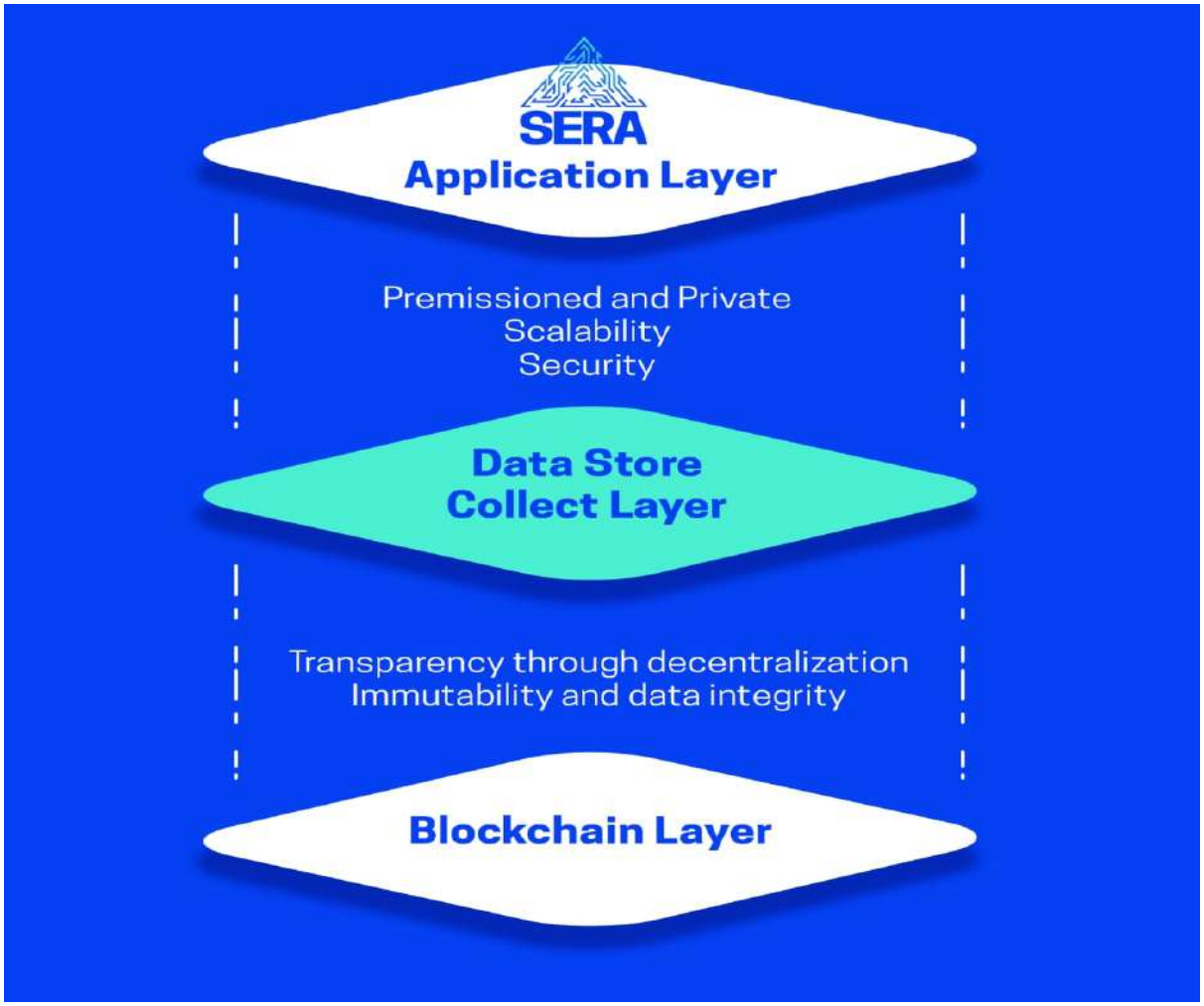
Private blockchains are often made up of many corporations, or a consortium, and they are built in such a way that prospects can only join their networks when allowed by an administrator or current members.

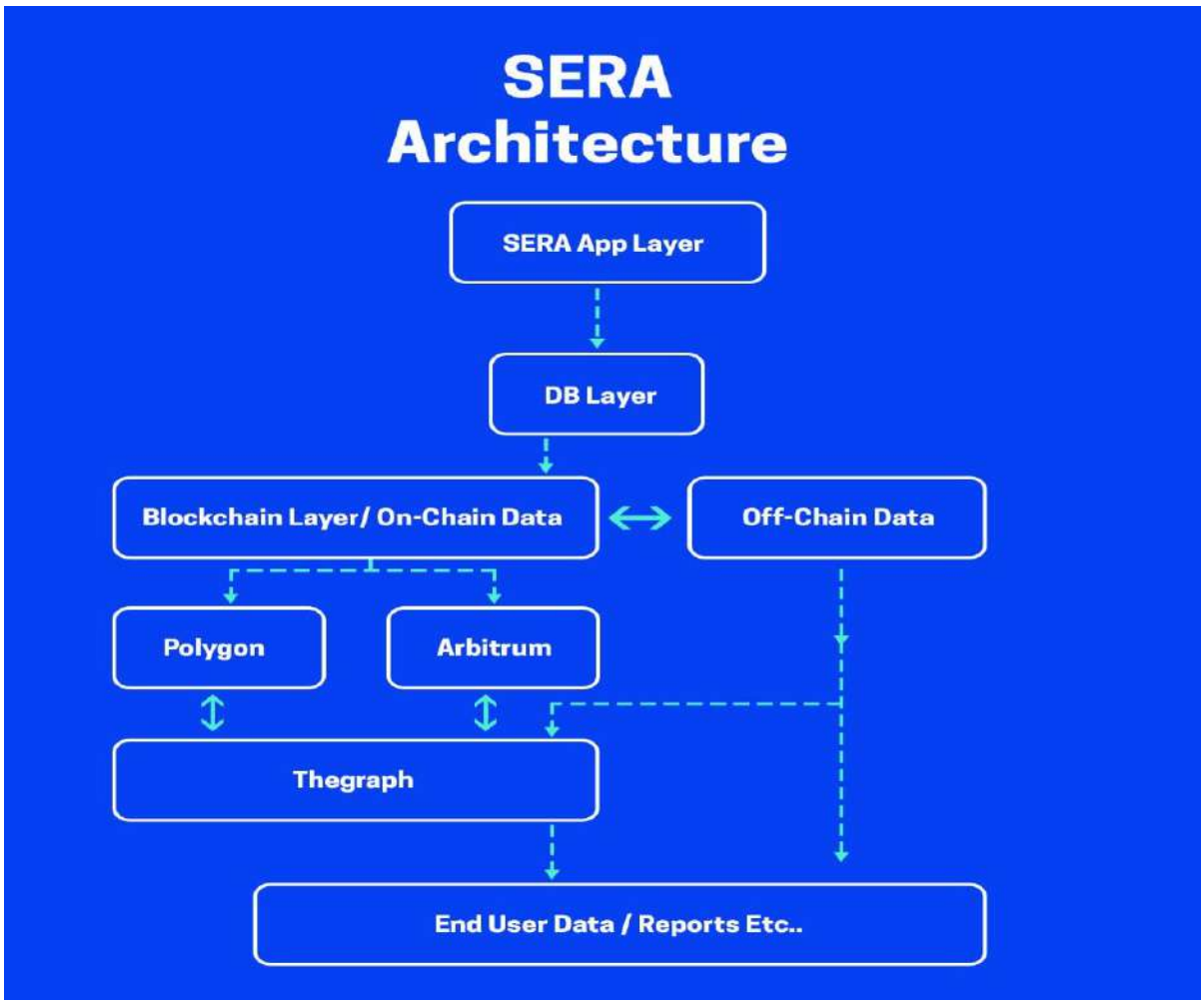
This poses a number of concerns: on those networks, acceptance and respect may not be equal for new members, especially when suggesting protocol modifications. Furthermore, there is always a possibility that members may fall into dispute, which could lead them to "roll back" the chain or alter transaction information.

Public blockchains, on the other hand, are community-driven, open-source initiatives. New members can join the network without permission or the need to prove themselves as valuable stakeholders. In other words, this enables them to develop a variety of apps using public blockchain as a

basis, erasing the need for the necessary API from a company or consortia. They can also secure the network by staking or contributing as validators.

Our Solution’s Architecture





Blockchain layer - On-Chain and Off-Chain Data

Blockchain database design

While blockchains can store transactional data, they have relatively limited querying capabilities. Another issue is the amount of effort necessary to prove that a block is legitimate since they must be approved by the majority of nodes beforehand. The longer this takes, the more nodes there are in the system. As a result, using blockchain as a database in the classic sense is difficult.

Rather, it is easier to take an existing database and add a blockchain capability to it. Two database layers would be employed in this situation. The first one using a lightweight distributed consensus protocol that assures some amount of integrity while delivering decent query speed. The second stores evidence of the previous layer's database activities on a blockchain based on proof of work (PoW).

A blockchain anchoring mechanism links the two layers together. Through this process, parts of the first layer are linked to blocks in the second one. This provides a chain of evidence that verifies the first layer's data.

Using a Hash to Protect the Reliability of an Arbitrarily Large Dataset that Might not Immediately Fit into the Blockchain

Context

The integrity of a large datum (a large collection of data, or dynamic data) that may not fit into a blockchain transaction must be safeguarded.

Problem

The blockchain has limited storage capacity, which is attributed to its complete replication throughout the network. Because of that, storing huge amounts of data within a transaction can be rather impractical. For example, Ethereum has a block gas limit to determine the number, computational complexity, and data size of the transactions included in the block. Additionally, the throughput may be restricted. Without being stored on the blockchain, data cannot benefit from the immutability and integrity guarantees. So how can reliability be protected when dealing with a large amount of data, or dynamic data?

Forces:

- Integrity: The integrity of the data must be maintained. If modifications are permitted, the integrity of the updates should be safeguarded as well.
- Scalability: The throughput and capacity of a blockchain are regulated by a number of parameters, including transaction, block, and inter-block sizes. When using blockchain to record every data update, the transaction pool may get clogged with transactions.
- Cost: Transaction fees must be paid on a permissionless blockchain network. As a result, storing data often and building huge datasets on

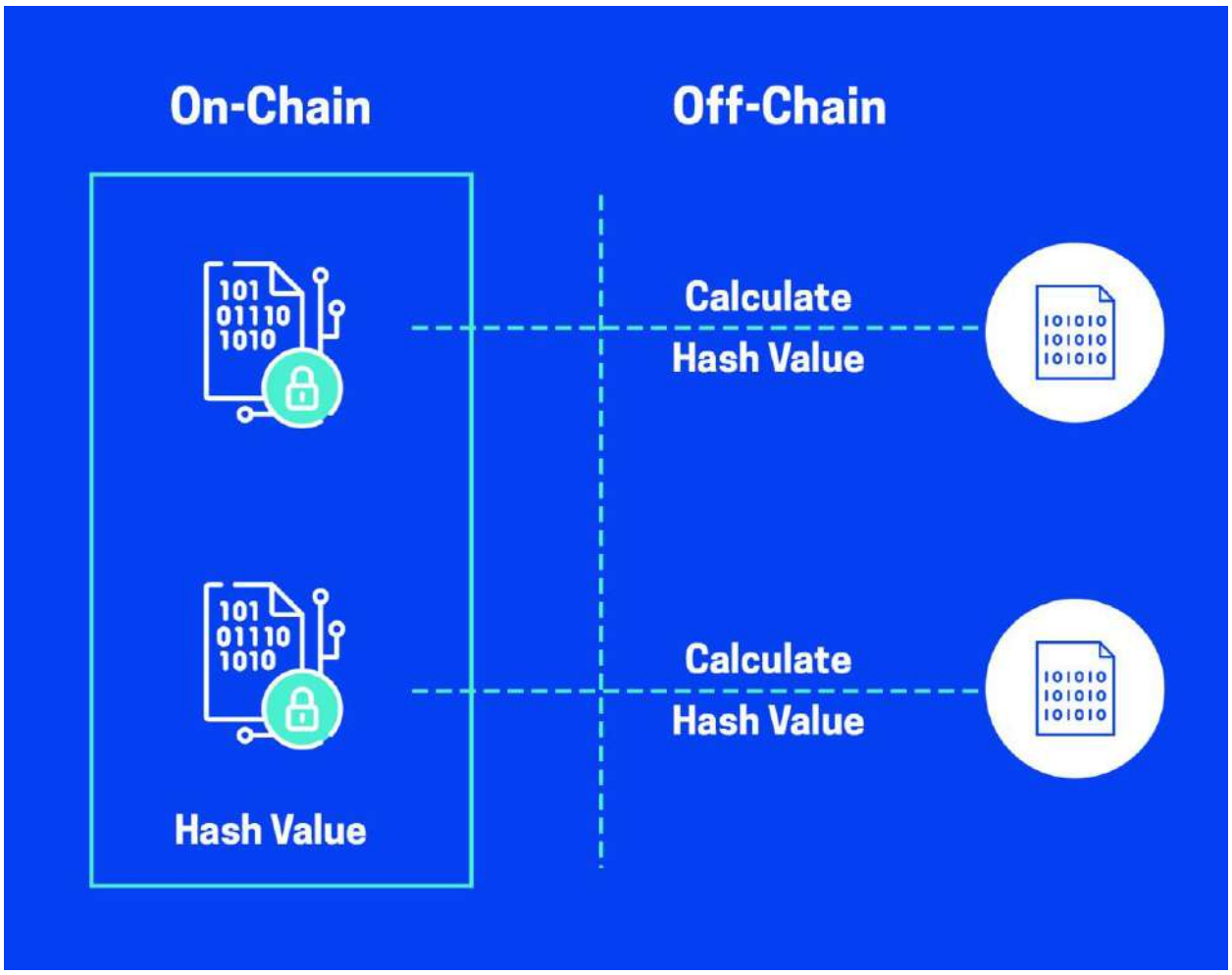
a blockchain can cost you a little too much. Even when a blockchain is permissioned, each full node keeps a copy of all previous transactions, which drives up the cost of physical storage. So, while storing data in a contract is more efficient for manipulation, it might be less versatile, given the smart contract languages' possible limits on value types and length.

- Size: The size of blocks and transactions is limited. A standard Bitcoin client, for instance, once relayed OP_RETURN transactions up to 80 bytes only on the Bitcoin blockchain, which was lowered to 40 bytes in February 2014. The amount of gas all transactions in a block are permitted to utilize is limited by Ethereum's block gas limit.

Solution

To boost integrity, rather than storing data, we can store its compact representation on-chain. We may hash the data item in question, for example, to obtain a one-of-a-kind digest/fingerprint through a consistent hashing function like SHA256. A hash function is a one-way function that is simple to compute but difficult to reverse. Even a tiny change in the input data (e.g., a single bit) can cause a large transformation in the emerging hash in consistent hash functions. Afterwards, a transaction can be used to register the hash value on the blockchain.

Because the hash value is substantially less compared to the data (e.g., 1KB data versus 256-bit hash value), this itself causes a significant reduction of data stored on the blockchain. When a user is supplied with raw data for future validation (e.g., during auditing), he or she can use it to generate a hash that can be compared to the one available on the blockchain. As a result, integrity validation can be ensured.



Off-chain data storage pattern

Decentralized Applications (Dapps) are meant to conduct business logic through smart contracts and to store data in a key-value database utilizing a blockchain as a back-end server. The transaction (TX) and block sizes of the selected blockchain platform, however, limit the amount of data that may be stored via a transaction. In the same fashion, the computational complexity of a smart contract on systems like Ethereum is limited by transaction and block size. As a result, the application of on-chain patterns is determined either by the magnitude of the data to be stored or computational complexity.

All data can be stored on the blockchain if the application data is moderate in size and non-sensitive. In these circumstances, the raw data on-chain pattern might be used to store all application data on the blockchain in an

immutable and transparent manner. On a blockchain, data may be stored in a variety of ways, including embedded in a transaction, as a smart contract variable, or as smart contract log events. These solutions come with a range of trade-offs, such as cost and flexibility. Furthermore, not only can it be slow and costly to write arbitrary data to a blockchain, but also less versatile. The transaction size, which is smaller than the block's, is the pattern's limitation.

On and off-chain data access

SERA employs zero-knowledge proof to retain data privacy, given that data stored on a blockchain network is available to all users on it. Another option to safeguard privacy is to maintain sensitive data off-chain while enabling access to them through off-chain access control logic. Traditional architectural patterns might be used by off-chain components inside a blockchain-based application to meet the needs of the specific use case. In this whitepaper, we look at a collection of traditional data access control methods that are used in the context of Self-Sovereign Identity (SSI) to limit access to off-chain credentials. The decision model is depicted in the image below.

Encrypting on-chain data (which adds to raw data on-chain) might be used to encrypt data before storing it on the blockchain, if it is designed to be available only to participants in a transaction.

To preserve privacy for on-chain data, **SERA** employs powerful encryption known as zero-knowledge proof.

We could calculate the Merkel tree hash for the full dataset if we wanted to track the integrity of a collection of data. The Merkel root could then be added to the blockchain. If a piece of data is modified often, requiring the integrity of each update to be tracked over time, each value might be treated as a single data point. Then, the Merkel tree hash could be calculated in a way that is similar to a dataset with numerous data items. In this situation, the hash of off-chain data might be recorded on the blockchain on a regular basis. In either example, the Merkel tree root produced is significantly smaller than the data. In addition to this, given that only the Merkel tree root is retained for a large number of data points, the amount of transactions necessary to record the hash on-chain is greatly

decreased. This technique is known as anchoring off-chain data to the blockchain.

Benefits

- Integrity: Because the data is stored on the blockchain as a hash, the hash value may be compared to the off-chain data to ensure its integrity.
- Cost: Because not as many transactions are submitted to the blockchain, anchoring lowers the cost of using it with regards to transaction fees (in public blockchains) and physical storage.
- Scalability: Anchoring keeps complicated and time-consuming business activities off-chain, where the hash value is seldomly recorded. As a result, blockchain-based apps can function within a blockchain platform's scaling boundaries.
- Privacy: Transactions on the blockchain are unchangeable and visible to all parties. As a result, maintaining hash values rather than genuine data helps to protect privacy.

Data privacy and Zk-rollups

Zero-knowledge rollups (ZK-rollups) bundle (or 'roll up') transactions into batches that are executed off-chain. Off-chain computation reduces the amount of data that has to be posted to the blockchain. ZK-rollup operators submit a summary of the changes required to represent all the transactions in a batch rather than sending each transaction individually. They also produce validity proofs to prove the correctness of their changes. The validity proof demonstrates with cryptographic certainty that the proposed changes to Ethereum's state are truly the end-result of executing all the transactions in the batch.

Zk-rollups and confidentiality

The second major benefit is confidentiality: by removing one of the limitations of public enterprise blockchains, i.e. the lack of privacy of transactions, enterprises enjoy the comfort of privacy without compromising collaboration, while hiding their business from competitors and untrusted sources. Thanks to the newest advancements of ZK technology, the sender, beneficiary, and transaction value of any deposit, withdrawal, and

transfer are hidden from third parties while stored and secured on chain. With the help of Zk-rollups technology, enterprises can benefit from complete anonymity of

Why Zk-rollups are important for SERA

Enterprises have high concerns about the privacy of data, and since public blockchains are accessible to everyone, the question here is: how can we maintain a high level of data privacy? The answer is ZK-rollups.

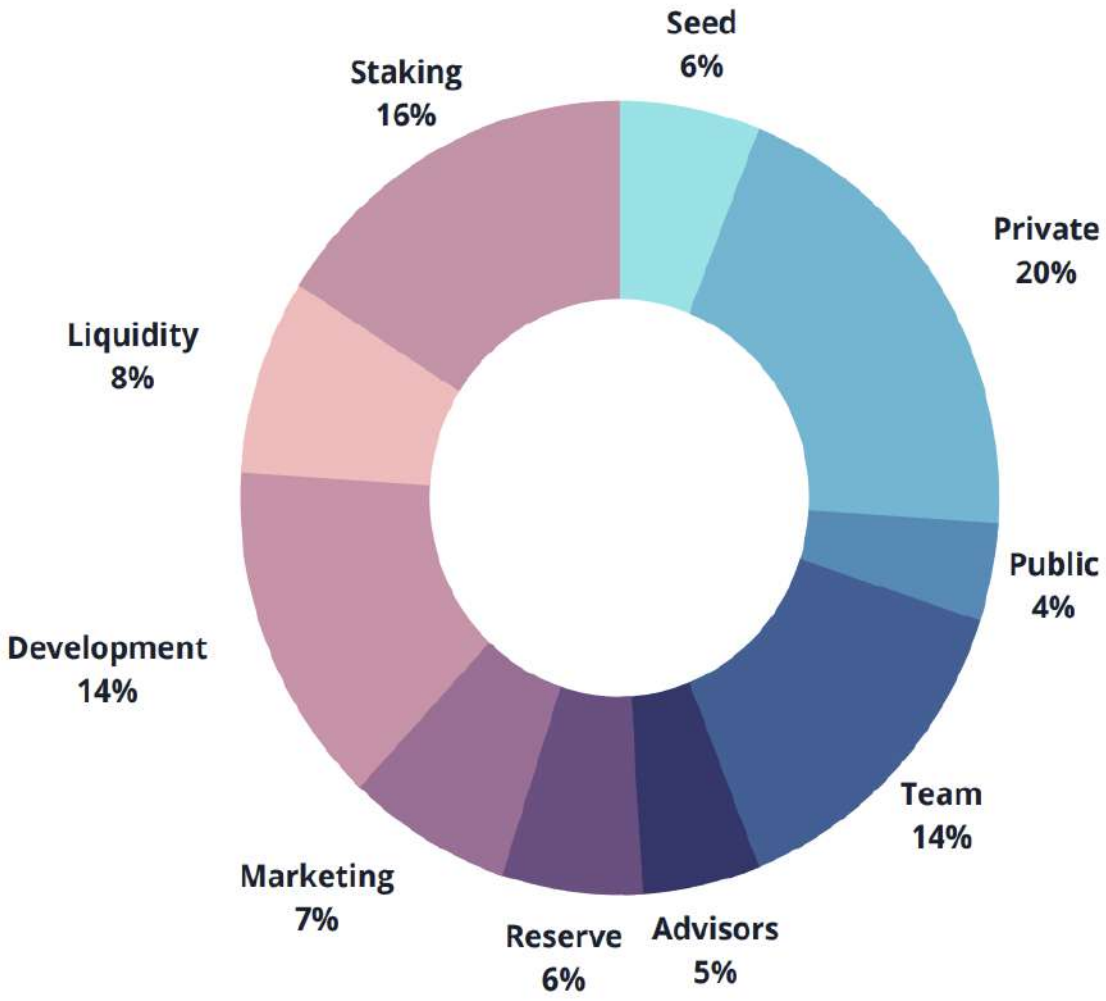
With the help of Zk-rollups technology, enterprises can benefit from complete anonymity of their transactions while participating in a public network.

SERA's Project

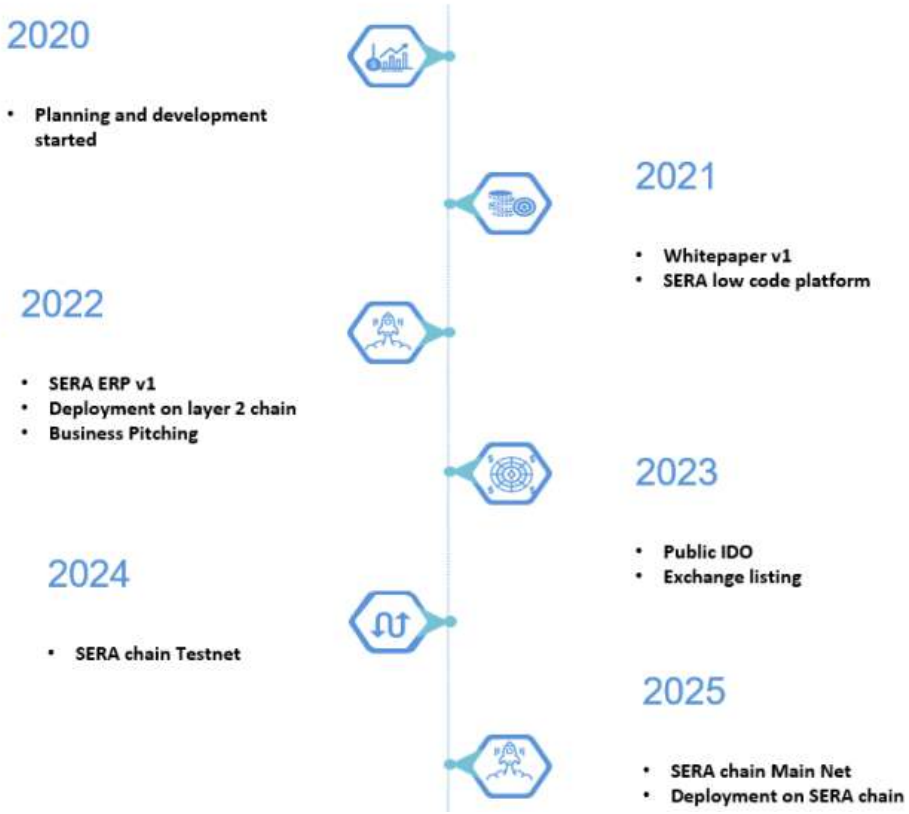
We believe that blockchains are the future. For the past years, **SERA** has been working around the clock to develop a new generation of ERP. An ERP that runs on a layer-2 blockchain, combining all the existing benefits of a regular ERP with the added privacy and security of a public blockchain.The only condition here is getting a share of **SERA**'s token. By taking this approach, we are teaming up with our investors so that they can also benefit when the price for the token gets higher.

SERA's Tokenomics

- Symbol: **SERA**
- Total supply: 500,000,000


Seed
6%
Private
20%
Public
4%
Team
14%
Advisors
5%
Reserve
6%
Marketing
7%
Development
14%
Liquidity
8%
Staking
16%

Project Roadmap



Conclusion

Former ERP on blockchain projects were heavily dependent on private networks. And because of that, the lack of understanding regarding the way public blockchain networks operate was greatly widespread. But with the support of new technologies, a number of corporations have been able to embrace public blockchains.

SERA is a complete digital/blockchain transformation platform, and your best investment option. **SERA** offers 35+ extensive business modules suitable for a number of different industries. With the help of layer-2 rollups and both on and off-chain data and by focusing on security and privacy, we help companies achieve their goals.

Reference:

ey-public-blockchain-opportunity-snapshot.pdf