NATRIX

Lightpaper

Executive summary

What is the Natrix Platform and how does it provide a unique opportunity for companies that operate in regulated environments?

The innovative and versatile Natrix provides the missing technological guarantees without sacrificing legal security.

Natrix is actually the stable bridge which helps organizations implement innovative, 21st century services. It is a unique hybrid solution in the blockchain world, and with its help, from now on we don't have to live with the restrictions and built-in risks of the classic closed-, consortium-, and open source blockchain systems.

What does this mean in practice?

According to the law, blockchain based services need to be stoppable at any time (by the way it contradicts the Satoshi principles). To be able to stop a service over a blockchain network, the network operator needs to possess the necessary legal and technological tools which may sound simple, but in practice it is really not. However, in Natrix this is a very simple task which can be achieved via our validator and authority nodes.

The authority nodes enable supervisory authorities to suspend financial institutions' operations with one click (multiple four eyes available), and thanks to validator nodes, attacks against the system (from both inside and outside of the organisation) can be effectively strained off.

We believe in the power of change

We could see several scary examples of data abuse and property loss caused by human failure in the past few years. In closed blockchains the user is not in possession of its own private key. This could seem safer at first, but unfortunately the technological risk for misuse cannot be eliminated. Therefore, a high level of trust is essential. At Natrix, we believe in a dual system: there is a centralized key storage (part of the platform), and there is also a public-private keypair at the user (only known by the user), so only he or she is able to initiate and manage transactions, no one else. At the same time the system itself has its own public-private keypair with which any access right can be immediately suspended. The flexibility of Natrix is provided by the fact that clients can pick the most suitable construction for themselves, while all public keys can be validated transparently over the keychain.

There are countless notarial, governmental, and even public administrative scenarios to which our hybrid blockchain platform could add serious value to.

Learn more about our next generation hybrid blockchain: THE NATRIX!

Sign up for a free demo

Table of contents

1. Introduction

The Natrix: blockchain is only a tool, it's not the purpose on its own!

There is a huge gap between the classic financial world and the world of open blockchains. The Natrix Platform is the bridge which provides a set of modern and easy-to-use tools for building secure, yet fast applications for innovative companies wanting to operate in a regulated environment.

Why is it needed?

For example, the financial industry has its own legal controls and regulations, but recently there are still no technological guarantees. Organizations still try to secure money handling and usage with complex human processes and IT systems. But from now on, the missing technological guarantee is available for every actor of the regulated market: it is called Natrix.

Learn more about this next generation hybrid blockchain which is suitable for enterprise and government use as well!

1.1. Connecting worlds

It is obvious that the Natrix Platform has its place on the market. In order to understand its role and values, we need to know the two worlds that Natrix is positioned between.

The controlled world

The first world is centrally controlled and generally supervised by an authority. Solutions therefore are legally secured, just like in the case of the classic financial system.

This world (the bank system) is already known and accepted. Its operation was improved and elaborated during the centuries, and it has always been based on central control. This control was only a legal control however, as most of the processes are carried out optionally, through non-digitalized or non-computerized methods.

It is important to see that the supporting IT systems were created separately (regarding time and location), and their integration is far from being smooth. Nowadays, the complete financial ecosystem of a classic financial institution generally consists of even more than a hundred tightly integrated systems. That is why these systems are rather complex, hard to operate, inflexible, and that is why their substitution/replacement is extremely difficult, expensive and risky.

Furthermore, these systems are planned to provide legal guarantees only. This is the reason why financial systems vendors also contribute to banks' responsibility towards the controlling authorities for handling a large amount of sensitive (financial and personal) data.

Here comes the question: where is the technological guarantee which could ensure appropriate data handling?

World without control

The second world - the other extreme - is the world of open blockchain platforms, which are 100% decentralized, peer-to-peer and are based on cryptography and math algorithms. Trust between users is unnecessary, the required software (and its source code) can be downloaded freely and anonymously. Users must trust only to these software. But there is no legal and flow control which could help preventing fraud, stealing, lying etc.

This means that the technological guarantee is given, but the supervision of open source blockchains is problematic. This might be the reason why this kind of technology is not popular and widespread in the supervised field at all.

1.2. The Natrix Platform: bridge between the crypto and the financial world

Natrix incorporates the biggest advantage of the supervised world: legal security. So, the platform exists as a hybrid between the two universes. The technological guarantee provided by blockchain technology is already available for those who require not only legal assurance, but transparency as well. Optimized for the supervised field, with approx. 8.000-10.000 business transactions per second, this next generation platform is a unique hybrid solution within the blockchain world. From now on, we don't have to live with the restrictions and built-in risks of the supervised, classic closed-, consortium- and open blockchain systems. Learn more about it!

Sign up for a free demo

2. Overview of the consortium blockchain landscape

Consortium blockchain: where “I” becomes “us”!

The consortium blockchain is a semi-private system which has a controlled user group but can work across different organizations. If more market participants (companies) join their forces during a process, e.g. delivery or sales, some kind of collaboration and trust will be essential. Contrary to open blockchains, consortium blockchains provide a necessary level of trust between consortium members. But how?

2.1. Speed, simplicity, integrability

A consortium blockchain needs to be faster than a public one for obvious reasons. Thanks to the simplified consensus algorithms this can be easily achieved. The price of the system being 5-10 times faster is that there must be a central actor who supervises the network. The open source Hyperledger and Corda, which both almost completely fulfill the base requirements of the finance sector, are both based on consortium blockchains.

2.2. Consortium heroes: Quorum, Azure, Hyperledger and Corda

Quorum is an Ethereum-based system by J. P. Morgan. The open source solution developed for enterprise applications is not only fast, but it is among the best in terms of private transactions and private smart contracts.

Microsoft could not be left out: they managed to develop a three-step blockchain method in Azure with which almost anybody can easily build a consortium system, simplify company management and surveillance and can integrate the blockchain technique with their legacy systems and devices.

Naturally, Linux did not want to miss out on the “game”, so the successful incubator initiative was born: the Hyperledger project. It is an open source, collaborative effort created to advance cross-industry blockchain technologies. Among its framework, inter alia, can be found a modular blockchain platform (Fabric), a built-in blockchain framework that is capable of automatic system control (Sawtooth), a framework developed for mobile phones (Iroha), a service ideal for digital identification management (Indy) and a solution for combining access control with Ethereum smart contracts (Burrow).

We cannot forget about Corda, established by R3 in 2014. In 2016, R3 launched Corda as an open source blockchain platform with the support of an energetic community of organizations and developers. They created a consortium including more than 200 members. Corda performed well with its special inter-participant (part-synchronized) ledgers, and smart contracts that can contain “legal prose”.

It is apparent that the different consortium blockchains offer many possibilities but concerning regulations, there are still many issues to be solved.

2.3. GDPR & KYC

In contrast to open blockchain systems – where users are identified by a “randomly” generated number – consortium blockchains generally use digital identification systems to identify actors (users, transactions etc.). These processes generate some serious data protection related issues and challenges (just think of GDPR and KYC regulations) to which the Natrix Platform provides truly comforting answers.

Sign up for a free demo

3.Design principles

We can say that Natrix is a hybrid platform between the blockchain world and the classic systems that are supervised by an authority, but this is not completely true as some features go beyond the system itself. Let's see what these outstanding features are:

- **Financial industry focus** – The strengths of our hybrid blockchain solution are really beneficial for the financial industry. During the development process we focused on the weaknesses of financial and other supervised institutions.
- **Auditable** – Corporations operating in a supervised field need a fully transparent and easily auditable platform. Natrix provides a solution for this as well, as every state (both current and historical) of every entity is available in the blockchain itself.
- **Legally bound** – Just as in the case of private blockchains, legal guarantees are available, provided.
- **No internal tokens or cryptocurrencies** – No internal token belongs to our system, therefore it can be operated independently, based on the supervised corporations' demands.
- **Modular and configurable access control system** – Customization is essential. That is why Natrix was designed to provide multiple solutions, based on the corporations' demands.
- **Privacy by design** – It is hard to create a system that takes care of privacy and provides the opportunity to meet magisterial regulations at the same time. But it is not impossible using math and cryptographic solutions.
- **Data encryption by design** – Highest level of data security is guaranteed via Elliptic Curve Integrated Encryption Scheme (ECIES). Just few algorithms which are the base of the system: EC-SECP256K1, AES, HMAC, SHA, bcrypt and scrypt, data partitioning based on Galois Fields (GF8).
- **Microservice architecture** – Microservice architecture enables rapid, frequent and reliable delivery of large and complex applications. It also eliminates the burden of long-term commitments to technology stacks.
- **Safe smart contract execution and data distribution** – Natrix enables safe smart contract execution via sandbox environment and data distribution via distributed ledgers.
- **Safe authentication** – Natrix uses strong, cryptography based, passwordless customer authentication and authorization with mandatory two-factor authentication and device verification.
- **Digital signatures 2.0** – Natrix's strict access- and ownership control is based on digital signatures and key fragmentations for maximum safety.
- **Traceable communication** – The platform is transaction based: everything can be traced. Each and every user request must have a valid digital signature from a registered device of the transacting user. This signature travels through the system and eventually gets saved with the processed request to the blockchain.
- **Encrypted by default** – The data in the blockchain is encrypted so only the entitled is able to access it, but the blockchain's integrity can be verified by anyone without having to decrypt its content.
- **Secure, group-based sharing** – Only the actors who have the necessary cryptographic keys can read the contents of the blockchain. The data model can be segmented (via annotations) so every actor can access (read) only the segments (groups) they are allowed to access. Data access can also be granted post-factum.

- **Zero-knowledge like verification** – The Natrix Platform can prove the existence of a given record without having to reveal the record itself. It is also possible to reference these records in transactions.
- **User-friendly API** – The platform's API is an easy to use key-value based API with only a few operations so interacting with the blockchain is pretty straightforward. The platform has all the necessary development libraries to easily create business related APIs.
- **Bridge between worlds** – The smart contract execution runtime is powerful and secure. Users (developers) can run custom codes from the blockchain through a user-friendly API, offering the best of both worlds: secure and trusted code execution combined with hassle-free, easy development.
- **Active & passive validation** – Smart contracts are guaranteed to be trustworthy, every transaction is validated and signatures are checked. Passive validation is running in the background and checks illegal data insertion and modification to the blockchain. So even the leader (RAFT leader) cannot mislead the network.
- **Multitenant by design** – Run multiple blockchain clusters parallel in a single network, share data between clusters, and manage your own smart contract runtime.
- **Support for authority groups** – Authority groups allow certain authorized members of the network (and also third-party actors e.g. central, governmental and supervisory authorities) to access predetermined data groups stored in the blockchain in read-only mode. It is also possible to put the whole blockchain network (or only a cluster of the blockchain) into read-only mode.

3.1. Short comparison

	Open Blockchain	Closed Blockchain	Classic supervised systems	Natrix
Identity	Anonymous / Pseudonymous	Known KYC/KYB	Known KYC/KYB, strict legal requirement	Cluster: Known KYC/KYB, Network: pseudonymous
Asset	Native	Any asset	Any asset, but with multiple systems	Any asset
Mutability	Immutable	Immutable	Mutable	Immutable
Speed	Slower	Fast-Fastest	Fastest	Fast
Security Consensus	Proof of work Proof of stake	RAFT Multi digital signature PBFT	Through workflows and legal and internal regulations	Proof of Identity - Extended RAFT - Leader validation - Member validation - Multi Digital signature
Network	Distributed	Decentralized or Distributed	Centralized	Distributed
Stoppable	No	Yes	Yes	Yes
Upkeep	Public ownership	Managed upkeep	Centralized and managed upkeep	Cluster ownership private or paid for
Ledger access	Open	Private membership	Only the institute	Can be open for read
Trust level	Trust-free	Trusted	Fully trusted	Supports trust-free Setup
Legal	Without legal security (allegal)	Legally binding	Legally binding	Legally binding
Anchoring	No	Yes (somewhere)	Not applicable	Yes (in public BC or somewhere)

Microservice support	No	Available after design and development	Multiple big systems, very heterogeneous and like “macroservice”	Yes
Smart Contracts	Solidity or Custom language	Multiple language Without SDK	Does not exist, and the software code is separated and supervised	Typescript with Full-fledged SDK With business objects
Data Encryption	No	No	Based on requirements, usually only partially	Yes
Durability	Significant amount of time	Depending on parameters <10ms or <120sec	Depending on parameters <10ms	Eventual consistency <300ms
Generic data structure	No	Yes, low level	Yes, usually full SDK support	Full, by design, full SDK support
Credible data schema version control on blockchain	No	No	No, schema versioning is outside of the systems, and using upgrade and migration scripts to update database	Yes, with mapping smart contracts
Multi cluster encryption and data sharing with privacy	No	No	No	Full, by design, full SDK support
ZKProof of data existence	No	No	No	Full, by design, full SDK support
PKI module	Limited	Limited, full after developing	Based on requirements, but usually only on API layer	Full, by design, full SDK support
Custom client key management	Only client	Usually centralized	Usually centralized	Both, client and centralized together

Sign up for a free demo

4. More about Natrix's advantages

Not open, not closed: it's more

How does user identification/authentication work? Instead of the extremely strong control (KYC, KYB) used in closed blockchains or classic supervised systems and the anonym/pseudonym methods used on open platforms, the owner of The Natrix cluster can give permission to a another cluster to identify a user without allowing access to the user's personal or other data. Also, it is important to note that the identification process is based on cryptographic and mathematical algorithms (such as Merkle proofs).

It is no surprise that in Natrix, you can create as many assets as you want. However, thanks to the Extended RAFT consensus algorithm, one can reach a throughput of 8.000-10.000 transactions per second (TPS), which is an outstanding result. Even our lightweight demo system is scaled up to a 2.000 TPS throughput.

But what is the real power of the Extended RAFT and how can it do more than the "simple" RAFT?

Everyone agrees on that the RAFT consensus algorithm is an understandable, easy to implement consensus protocol. However, creators of the Natrix Platform were not satisfied with its possibilities. Therefore, they complemented the algorithm in a way that did not change it fundamentally but made it possible to use it in enterprise environment with the highest level of transparency possible.

Thanks to our engineers Natrix has the following special superpowers:

- **ESB** – Due to our extension of the original algorithm it is not necessary to send the same messages for each participant of the network. It is enough to send out a message only once and the built-in message bus takes care of the rest. Fewer messages mean less bandwidth so communication can become a lot faster.
- **PreVote or PreRequestVote** – When a single node or a part of the blockchain network gets isolated, members may not be able to reach a consensus in choosing the leader, so "term" starts to grow in a large measure. This could cause problems when the network gets back together again. The extended algorithm offers an elegant solution for this problem: it creates ideal conditions for leader election in a time efficient way.
- **Managing changes in configuration** – In opposition to static configuration, changing the configuration of the blockchain network (e.g. adding a new ledger node) in Natrix is dynamic. When a new server arrives and wants to join the network – only one new node can join at a time – the leader can only change the configuration of the blockchain network if all current members gave their blessing. From this point onwards the candidate member becomes a full member (it can receive data from the leader, it can vote, it can be elected as leader etc.).
- **Two-phase log replication and parity** – Before becoming a full member, candidate nodes need to synchronize their state to the state of the network (learner status). Only up-to date nodes are allowed to join and participate in the network.
- **Leader stepdown, leader election** – In case for some reason the leader node of the network becomes unavailable or considers itself no longer eligible for the leader role and steps down, the remaining nodes of the blockchain network automatically choose a new leader from among themselves. This algorithm makes impossible for the leader node to monopolize (hijack) the blockchain network.
- **Leader lease** – There are no more inconsistent responses in case of network separation. Leader lease offers an elegant solution for this problem.
- **Leader validation** – When a client turns to the blockchain network with a request, besides the response from the leader, validator nodes also respond to the client's request

with the fingerprint of the original request. This validation takes approximately up to 300 milliseconds. This fingerprint proves that the leader has not modified the request in any way. If a validator node detects that someone altered a request, it instantly switches the network to read-only mode in order to prevent malicious activities and minimize damage.

- **World State Machine conception (WSM)** – Natrix stores the most recent value of every key in a separate cache database (World State Machine, or WSM) so there is no need to dig into the blockchain in order to find the actual value of a key. This way, read requests are extremely quick. (based on RAFT State Machine)
- **Snapshot function 2.0** – Unlike the conception outlined by RAFT, taking a snapshot on the Natrix Platform means that the current WSM fingerprint gets written into the blockchain. This means that any state of the blockchain can be anchored (in newspapers or in public blockchains) which enables independent third-party entities to validate the content of the blockchain.
- **Transaction monitoring** – Operations executed by the same transaction can be marked with a unique identifier which enables validator nodes to detect and report incomplete transactions and other anomalies (e.g. when an operation is missing from the blockchain).

According to the law, blockchain based services need to be stoppable at any time (which by the way contradicts the Satoshi principles). To be able to stop a service over a blockchain network, the network operator needs to possess the necessary legal and technological tools which may sound simple but in practice it is really not. However, in Natrix this is a very simple task which can be achieved via our validator- and authority nodes.

The authority nodes enable supervisory authorities to suspend financial institutions' operations with one click (multiple four eyes available), and thanks to validator nodes, attacks against the system (from both inside- and outside of the organisation) can be effectively strained off.

4.1. Financial- and legal security is hardcoded into the core of the Natrix Platform

Usually when speaking about blockchains, trust issues arise. The experts behind Natrix created something special and unique to address these issues. Thanks to the Extended RAFT algorithm and the extensive use of digital signatures, zero trust is required by the parties towards each other.

Accounts can be frozen so legal security is established. Certain parts of digital keys can be revoked in order to ban the transactions of certain actors. The revoked parts can be restored later but only with the assistance of the original participants (the system itself and the account owner). This way in case of theft we can return the stolen assets to their rightful owners.

4.2. Privacy and customizability by design

Data encryption in Natrix is unique on the market. It is not an overstatement to say that with our powerful developer tools our partners can effectively model and implement their business functions in a truly flexible and generic way. With the platform's analytics engine, effective data mining and further data processing is not a big problem anymore.

There is a disturbing issue which neither open nor closed blockchains could offer a satisfying solution for. The issue in question is the managing of inevitable data model changes. In Natrix on the other hand there is an easy and elegant way to introduce new data models or alter existing ones. Developers can even define custom data mapping routines which run automatically when accessing data with stale data model version, auto upgrading it to the current version.

ZKProof is an open industry academic initiative that seeks mainstream zero-knowledge proof cryptography through an inclusive, community-driven standardization process that focuses on data security. Natrix offers a 100% GDPR compatible solution, with comprehensive developer and business support in regards to provable data possession and validity as well. This way privacy and data security is guaranteed while the end users still obtain the adequate safeguards. One of the biggest benefits of the Natrix Platform is that it lets you certify data fingerprints and proves data possession (existence). It can also prove validity without revealing any information about the original data itself.

One of the biggest concerns with the crypto exchange market from user aspect is that during the registration process one needs to go through a mandatory KYC procedure, that besides uploading photos, also requires submitting lots of personal data. With the Natrix Platform's innovative proof system, this problem can be completely eliminated, while taking GDPR directives entirely into account.

4.3. Blockchain-based solutions for enterprise challenges

Imagine an enterprise grade platform with a built-in blockchain and all necessary security related components. This is Natrix. What happens for example when there are three companies in a network and one of them would like to share certain information with only one of its partners? Fortunately, we have a solution for this scenario as well! On the Natrix Platform every cluster has its own set of encryption keys (public and private key pairs).

The PKI of The Natrix is 100% eIDAS compliant. Besides, in the field of custom client key management we managed to incorporate advantages provided by both open and closed blockchains. The freedom of these systems (e.g. users are solely responsible for keeping their private keys safe) can unfortunately backfire in some cases. If a private key is lost (or stolen), the assets are lost as well and there is no way to recover them. We could see several scary examples of data abuse and property loss caused by human failure in the past few years. In closed blockchains the user is not in possession of its own private key. This could seem safer at first, but unfortunately the technological risk for misuse cannot be eliminated. Therefore, a high level of trust is essential. At Natrix, we believe in a dual system: there is a centralized key storage (part of the platform), and there is also a public-private keypair at

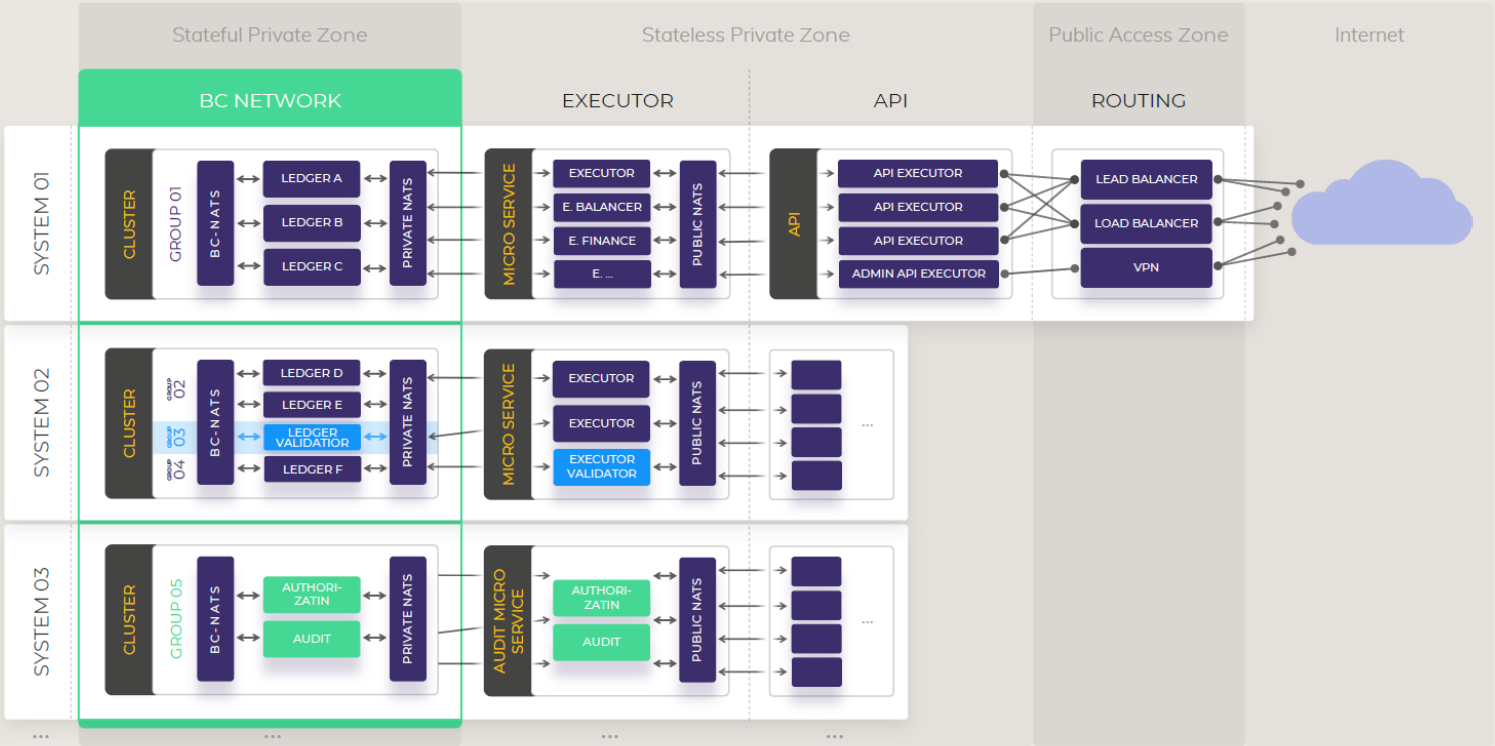
the user (that only the user knows about), so only he or she is able to initiate and manage transactions, no one else. At the same time, the system itself has its own public-private keypair with which any access right can be immediately suspended. The flexibility of Natrix is provided by the fact that clients can pick the most suitable construction for themselves (while all the public keys can be validated transparently over the keychain). This way it is possible to give users their own private keys and yet keep the ability to freeze their accounts. Also, this way assets cannot be transferred without the explicit consent of their owners, so no asset can be lost within Natrix and no one can tamper with them.

4.4. Architecture

Open blockchains are basically monolith applications with all the classic layers. Closed blockchains can be implemented as microservices, but not in a cost-effective way, as it requires heavy design and lots of extra development. However, Natrix is an out-of-the-box cloud native, event-based and uses microservices by default.

Natrix being written in Typescript is also special because it supports both object oriented and functional programming with its own SDK and business objects, so the developers can easily create simple solutions to complex business problems by defining custom business objects and securing important data without having to know a thing about blockchains.

A simplified architecture diagram of a multi cluster network. The diagram shows a the physical, logical and a microservice view, too.



5. Business is business

We believe that blockchain is an excellent tool for various business requirements and challenges on the market. There are countless notarial, governmental and even public administrative scenarios to which our hybrid blockchain platform could add serious value to. This could be important not only because of the challenges we're facing in this current pandemic situation, but also because we need to shift to the new era of digitalization.

In the data model we can out-of-the-box designate data as GDPR data, which automatically prevents sharing it with unauthorized parties. This method also works with other kind of private data (financial data, TAX, police and health care records, etc).

In case of access control, cryptographical algorithms guarantee that unauthorized actors cannot access data. How does it work in practice? The system cuts the digital keys into four parts. The delegator (the actor who delegates a role) gets the first fragment, the delegate gets the second one, and the two remaining fragments are kept by the system (one of them will be GDPR-level encrypted). In order to reset a digital key from key fragments, three corresponding key fragments are necessary.

In Natrix every user has its own set of encryption keys for their own data. This way in case someone hacks the system, it only can access the data of a single client, not more. At the moment the platform operates with the standard secp256k1 encryption (which is a 256 bit elliptic curve based encryption that complies with a 3000 bit RSA) recommended by the NIST.

Many solutions promise multitenant operation but companies that chose the Natrix Platform are able to create more clusters in a single network, thus providing the ability to customize or change some parts of their application (e.g. the interface).

A digital signature is valid only with a trusted timestamp. The Natrix Platform can operate with network-wide trusted timestamps and able to integrate trusted timestamp providers easily.

The Natrix: blockchain is only a tool, it's not the purpose on its own!

Sign up for a free demo