Data Integrity Verification Solution as key component of the business transformation

Technical Brief

Dmytro Haidashenko, CTO

Executive Summary

Mission statement about the solution

The mission of Data Integrity Verification Solution (DIVS) is to enhance control over the integrity of documents throughout their lifecycle as well as to monitor all changes and securely replicate them among the participants of the document processing systems.

Use Cases

- WORM (write once read many): proof of the documents immutability, metadata and signatures;
- Data provenance verification;
- Secure documents sharing;

Examples of solution

- Integrity and authenticity control of electronic health records (EHR) and documents;
- Approval of the financial documents correctness;
- Monitor changes in terms of customer contracts in CRM and other systems.

Key Features

- Secure storage and exchange of data;
- Provision of data existence, ownership, and integrity cryptographic proofs;
- Seamless integration with content services platforms;

Advantages of DIVS

- Vast software ecosystem with various ready-to-use auxiliary modules and reference implementations:
    - low entry threshold for developers;
    - short time to market;
    - no hidden fees;
    - low customization cost.
- Private blockchain network:
    - easy interconnection with external systems;
    - real-time secure backups;
    - predictable operational cost;
    - high level of privacy;
    - validators are known to the network owner;
    - full control over the decision-making rules.

Blockchain-Powered Data Protection Approach

Data Integrity Verification Solution (DIVS) is a TOKEND software platform-based (www.tokend.io) solution that consolidates the experience gained by Sakor LTD in building the production-ready blockchain-powered systems. DIVS enhances control over the integrity of data, monitors all changes and securely replicates them among participants of the network. DIVS would be suitable for the following use cases:

- WORM (write once read many): proof of immutability of documents, metadata, and signatures. Example of document metadata is depicted on Figure 1.
- Data provenance verification. In the data processing workflow, a certification authority can sign some data to prove that it has been certified at a given time
- Secure documents sharing. Users can anchor their documents to the DIVS solution and share the documents and signature requests with their counterparts.

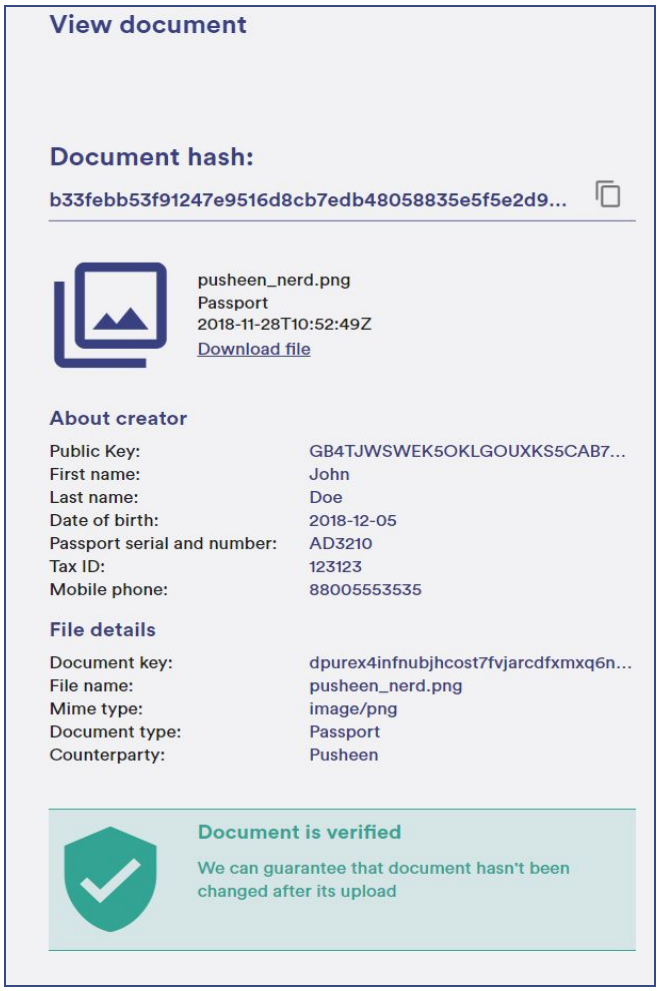

Figure 1. Example of document metadata

Key Features

Document Anchoring

Document anchoring is the process of creating cryptographic proof of data existence, ownership and integrity. To achieve this, a cryptographic hash of data and digital signature are recorded on the immutable blockchain. Combination of a secure cryptographic hash function and asymmetric cryptography allow for efficient verification of the document hash in case there have been any modifications to the document.

Anchoring to public chain

- Broadcast hashes of blocks to one or several public blockchains on the predefined schedule.
- Combine privacy and costs of a private blockchain with transparency and non-repudiation of a public chain.

Platform customization and Application development

DIVS is a highly flexible and configurable system that greatly facilitates the implementation of various use cases by a team that shouldn't obligingly have any experience in building the so-called DApps (Decentralized Applications). Development of custom MVP solutions does not require any changes to the core of the system which significantly reduces time to market and, at the same time, provides a high level of security.

Data agnostic approach allows for the secure exchange of custom data without having to introduce these changes to the core module. Intuitive REST API, SDKs as well as reference implementations of various modules and web applications significantly reduce the amount of resources needed to train a team with no experience in the development of blockchain applications.

DIVS concept

To illustrate the mission of DIVS - enhance control over the integrity of documents throughout their lifecycle, good examples were depicted below in Figure 2 and Figure 3:

DIVS for customer data and documents

Alice is sharing through Customer relationship management (CRM) system a document to Bob. Since the document is business critical, Alice wants to be sure that it won't be modified or corrupted. The figure shows how DIVS can help to achieve that:

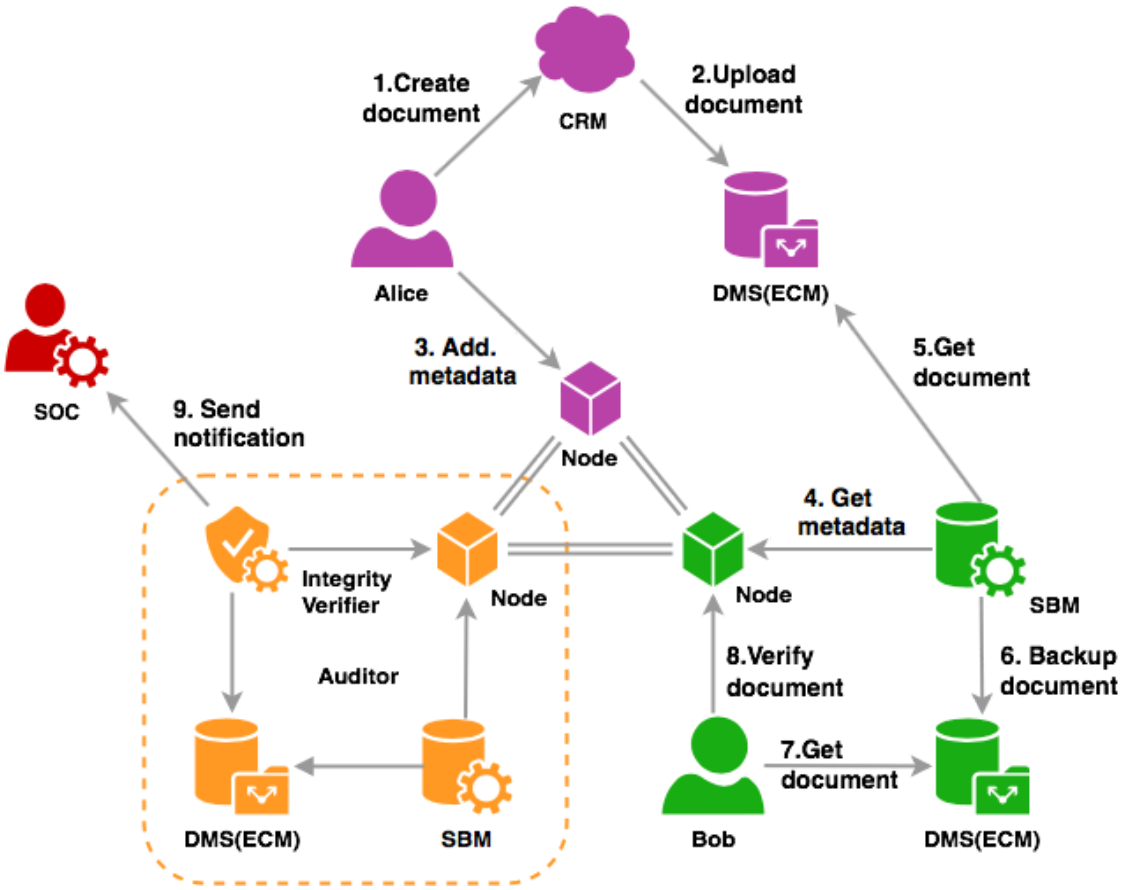

Figure 2. Data Integrity Verification Solution workflow

1. Alice creates the document in the Customer Relationship Management system (CRM).
2. CRM uploads the document into the selected Document management system (DMS) or Enterprise content management system (ECM).
3. Alice anchors to the Node her digital signature and a unique fingerprint of uploaded document (i.e., hash, which is a result of a cryptographic hash function application).
4. Smart backup module (SBM) notices that the new data has been anchored on the Node and extracts its metadata.
5. Having a hash extracted from metadata, SBM tries to find the document with the corresponding hash in Alice's DMS/ECM.
6. Once the document is found, SBM replicates to Bob's local DMS/ECM to ensure that each participant has their own verified copy of the document. SBM also notifies Bob that there is a new document in the system available for him to view.
7. Bob downloads the document from local DMS/ECM.
8. Bob verifies the downloaded document with the metadata that Alice anchored in Node.

DIVS real-time monitors state of the local storage or integrated DMS/ECM along with the blockchain, in case documents got somehow modified or corrupted

9. Integrity Verifier module notifies about document's state and tries to perform a local backup of the valid version of the document in question from other participants. In case document being tampered, Integrity Verifier will send an alert to Security Operations Center (SOC) . An example of alarm notification is specified in Figure 4.

DIVS for secure healthcare record

Proof of value:

- Ability to share clinical assays and medical histories in real-time can greatly help improve patient care and health outcomes.
- Proof of the medical documents immutability & data provenance verification (assays, CAT scans, EMR, MRI, x-rays).
- No central point of failure.
- Secure documents sharing.
- Creates a solid foundation for securely connecting EHR systems with PACS/EMR managed by separate entities while giving patients full control over their data.
- Customer identities increased security by using new blockchain-based digital identity applications.

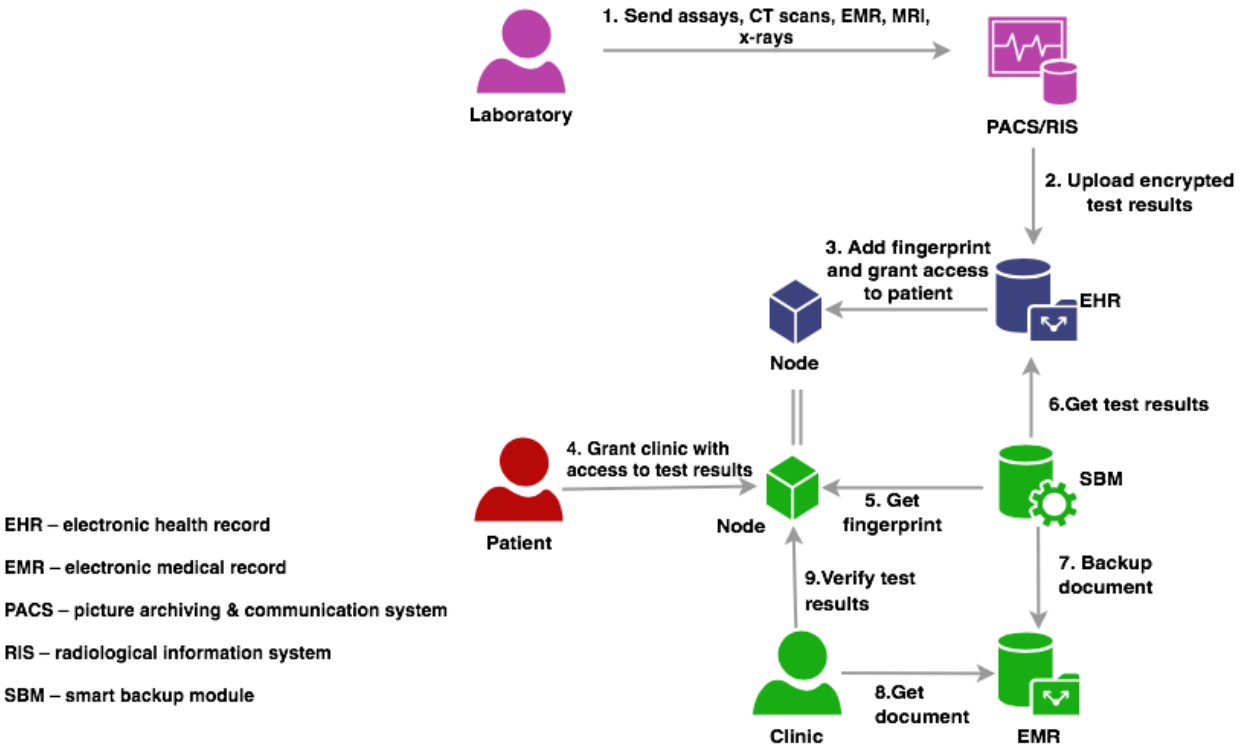

Figure 3. Secure healthcare record workflow

Solution overview

- Cryptographic hash function is used to generate a unique fingerprint of data;
- Data is encrypted on the client side during each data transfer.
- Hash value and digital signature of the data owner is anchored to the blockchain;
- Data is securely replicated off-chain among authorized participants.

A complete suite of DIVS

DIVS provides a unified platform of pre-integrated services that are extremely powerful when used together. A detailed overview of these modules and their connections is specified in Figure 2.

- **Node**
  Node is a key component of the platform. It processes transactions, manages history, and provides an easy to use API to access the blockchain data. It consists of two modules:
  - Core — a replicated state machine that maintains a local copy of cryptographic ledger and processes transactions against it in consensus with a set of peers. It implements the federated consensus protocol and is responsible for roles and anchored data management.
  - Horizon is the client-facing REST API server. It acts as an interface between the core and applications that want to access the network. It allows submitting transactions to the network, checking the status of accounts, and viewing transaction history.
- **Smart backup module (SBM)**
  This module replicates documents into its local storage or integrated DMS/ECM based on the commands successfully applied by trusted DIVS node. Such an approach allows to ensure that each of the participants has their own verified copy of the document and that any malicious actions performed on the node of one of the participants will not affect data stored by other participants.
- **Integrity Verifier**
  This module monitors state of the local storage or integrated DMS/ECM along with the blockchain and ensures that documents and metadata are up to date and have not been modified or corrupted. Otherwise, it notifies corresponding admin of the system and tries to perform a local backup of the valid version of the document in question from other participants.

DIVS uses the Federated Byzantine Agreement (FBA) consensus protocol, which provides a way to securely exchange information and ensure that all participants have the

same state of the ledger without relying on a closed system. FBA has a set of provable safety properties that prioritize safety over liveness — in the event of misbehaving nodes or partitioning, it halts the progress of network until the consensus is reached. FBA is a perfect solution for private permissioned networks. It simultaneously enjoins four key properties: decentralized control, low latency, flexible trust and asymptotic security. In other words, malicious actor needs to successfully attack the majority of nodes in network to have any significant effect on the business processes dependent on DIVS.

External Systems Integration

Modular architecture and open API allows DIVS to be integrated into any documents management systems and content services platforms (Open Text Content Suite Platform, Microsoft SharePoint, Hyland OnBase). Thanks to API provided by content services platforms integration can be fully seamless for the end user, making such solution even more beneficial.

DIVS provides a consistent sequence of all operations occurring in the system. It can be used to easily integrate various sets of event tracking tools, DMSs, CRMs, ERPs, PMSs and SCMs. Each operation also includes a set of changes applied to the ledger. They allow to calculate a partial state of the ledger at a specific moment in time. It can be used by the off-chain applications to perform real-time audit, and provides analytical insights like number of uploads per document type, activity of the users, document corruption attempts. What is more, Integrity Verifier module can be integrated with communication platforms to notify information security officer of the system via established channel if there any malicious actions were noticed that would corrupt documents.

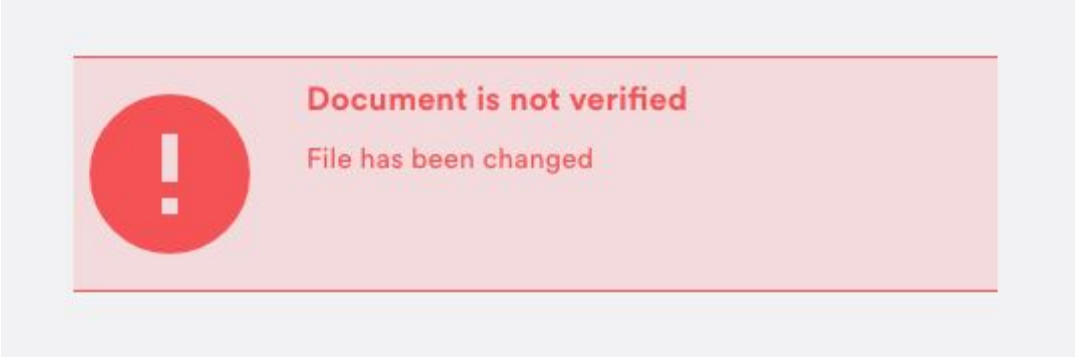

Figure 4. System's notification about corrupted document

Advantages of the DIVS

- Vast software ecosystem with various ready-to-use auxiliary modules and reference implementations:
    - low entry threshold for developers;
    - short time to market;
    - no hidden fees;
    - low customization cost.

- Private blockchain network:
    - easy interconnection with external systems;
    - real time secure backups;
    - predictable operational cost;
    - high level of privacy;
    - validators are known to the network owner;
    - full control over decision making rules.

System Requirements

DIVS is a highly modular system built using the microservices architecture. Such an approach used on top of FBA ensures high level of scalability and fault tolerance. The table below specifies software and hardware requirements for DIVS.

vCPU number	RAM (GiB)	Purpose	Additional requirements
4	8.0	Node	200 GB disk and S3-compatible object storage
2	8.0	Smart Backup Module	100 GB disk
2	8.0	Integrity Verifier	100 GB disk

Table 1. System requirements

Performance monitoring

System administrators must be able to proactively detect problems before they affect users, diagnose the root cause, and provide quick resolution to get the service back up and running. In DIVS system administrators can monitor problematic application code, database connections, slow queries, and external web service calls. Out of the box integration with Grafana/Prometheus/Loki or ELK stacks for performance monitoring, analytics and with Sentry for error tracking. Generally, any third-party services can create a seamless integration with DIVS using the API interface. Examples of performance monitoring services are depicted on Figure 5, 6,7.

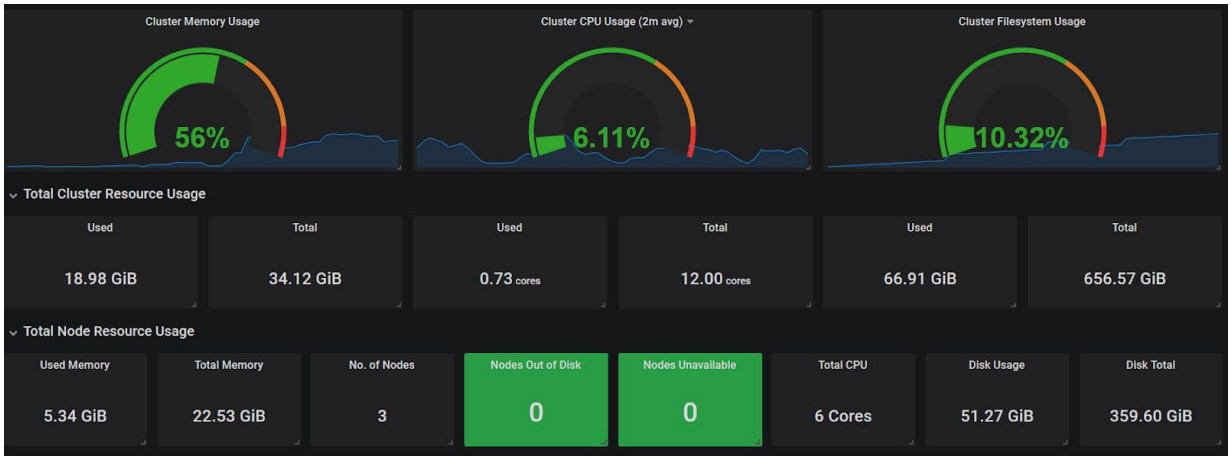

Figure 5. System's performance monitoring

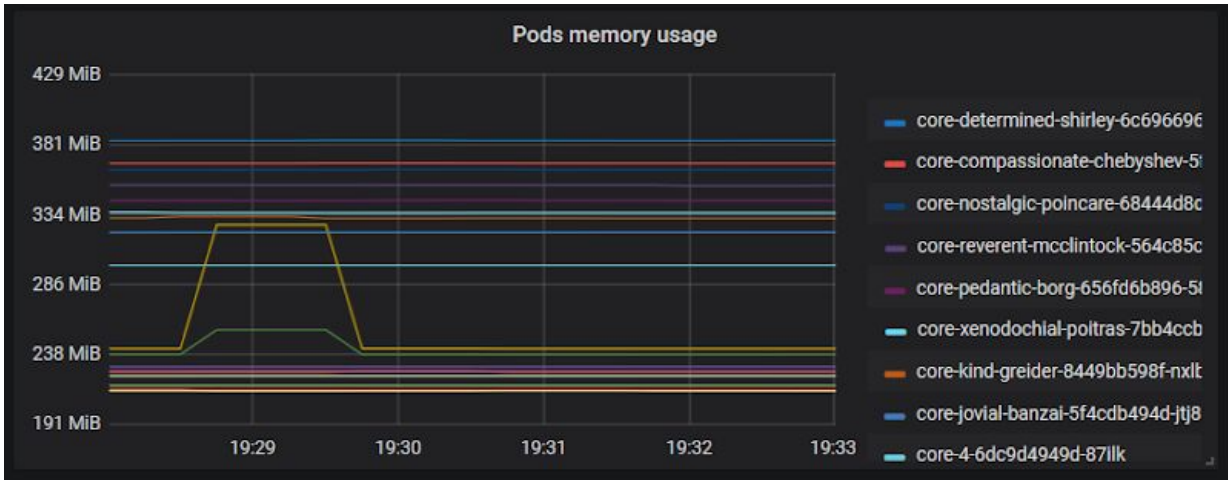

Figure 6. System's performance monitoring

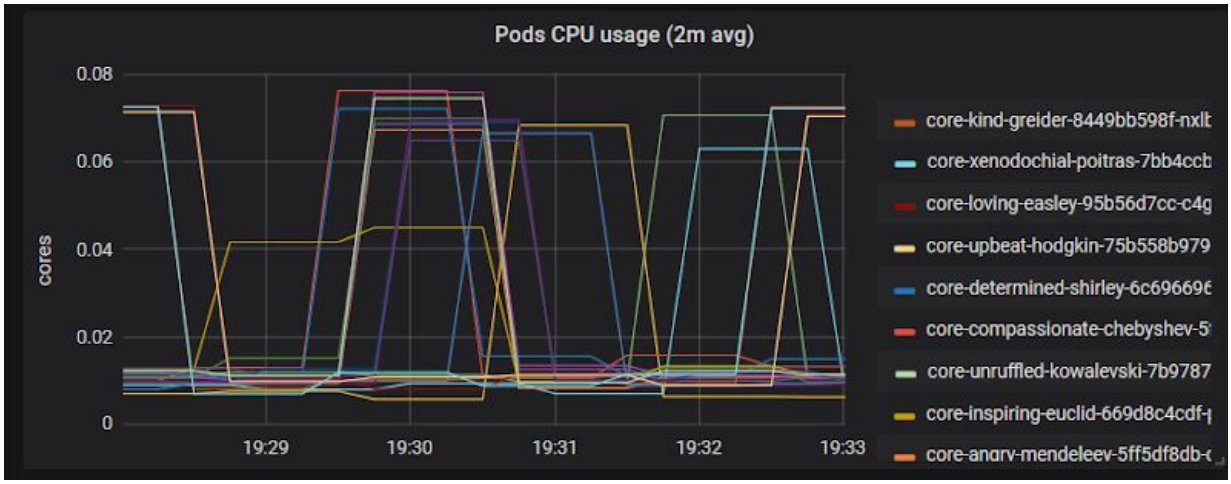

Figure 7. System's performance monitoring

Summary

Data Integrity Verification Solution (DIVS) provides tools to securely manage identities and encryption keys, assuring patient's health data integrity, authenticity, immutability and auditability. Seamless integration with content services platforms ensures best user experience and helps to build greater confidence in the data. DIVS is designed for enterprises who are willing to enhance security level of existing documents management systems by taking advantage of cryptography and blockchain technology without the need of maintaining an expensive team of blockchain experts and within the shortest time to market.

About the author

Dmytro Haidashenko, CTO.
Has over 5 years of practical experience in the development of blockchain powered solutions, 14 delivered blockchain projects.

Learn More

https://tokend.io/

enterprise@distributedlab.com

About TOKEND

TOKEND is a white label blockchain software platform that consolidates best practices of tokenization solutions. It allows you to issue, transfer and exchange your assets with high level of privacy, security and auditability while following regulations of your jurisdiction. TOKEND is designed for enterprises who are willing to take advantage of tokenization or experiment with the blockchain technology without the need of maintaining the expensive team of blockchain experts and within the shortest time to market.