Proven DB

Litepaper

Your trusted data integrity solution.

Databases and the Blockchain

Cryptocurrency and Blockchain technologies have the potential to be as powerful and disruptive as the internet itself. Database systems need to evolve to leverage Blockchain capabilities.

The Blockchain represents a new type of database:

Public
Transactions on the Blockchain are public.

Distributed
Not controlled by any central party.

Tamper Proof
Transactions cannot be altered.

Immutable History
The full history of all transactions are preserved.

Immutability is Revolutionary

They say history is written by the winners.

In databases, history is written by the developer or the DBA. There's no practical way to detect back-dating or tampering with historical data.

But there's no arguing with Blockchain data. Once sealed on the Blockchain, historical data is immune from modification.

> **Trust is a foundational feature of the Blockchain as the data written into it is immutable, and can never be changed, modified or removed.**
>
> **Wall Street Journal**
> *(https://on.wsj.com/2PJ1Wem).*

Blockchain Proofs and the Law

The immutability of data within a Blockchain constitutes a revolution in computer science. For the first time, we have a way of storing data which cannot be altered and whose creation data and integrity can be cryptographically proven. Data in a traditional database can be altered at any time by a database administrator or a privileged developer. In contrast, data in a public Blockchain is immutable. We now have an absolute mathematical proof of the veracity and provenance of a data item.

Blockchain cryptographic proofs are increasingly being recognized as legal proofs. We can foresee a day in which Blockchain records are held to the same evidentiary standards as DNA or fingerprint records.

> **A signature that is secured through Blockchain technology is considered to be in an electronic form and to be an electronic signature.**

Arizona Bill HB2603
(https://azleg.gov/ars/44/07061.htm).

> **Blockchain legislation pending or passed in at least 18 US states.**

National Conference of State Legislatures
(https://bit.ly/2L4Oksc).

> **A digital record electronically registered in a Blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902.**

2016 Vermont StatutesTitle12
(https://bit.ly/2OFHNtS).

> **The usage of a third-party Blockchain platforms that are reliable without conflict of interest providing the legal ground for proving the intellectual infringement.**

Hangzhou Internet Court (China)
(https://bit.ly/2R8dw3H).

Blockchain vs DBMS

Compared to a traditional DBMS (Database Management System), the Blockchain has many drawbacks:

Performance

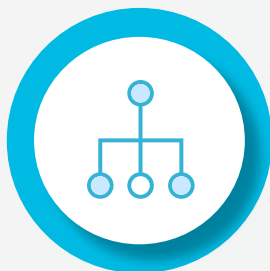High latency and low throughput.

Capacity

Limited data storage capacity.

Privacy

Transactions are publicly visible.

Structure

No Schema or data model.

Cost

Each transaction has a expensive cryptocurrency cost.

Productivity

Poor developer productivity.

Introducing ProvenDB

ProvenDB uses Blockchain technology to create the world's **first** genuinely **trustworthy** database. ProvenDB is for regulated industries or wherever impeccable data integrity is crucial.

ProvenDB layers on top of a standard database engine adding core Blockchain characteristics to the database. The resulting database respects all usual database "CRUD" operations (Create-Read-Update-Delete) but also provides the following:

Immutability

By default, all versions of a data item are retained. Previous versions of a data item can be superseded, but original versions are never destroyed.

Tamper Detection

Selected versions of the database are hashed upon the Blockchain. These versions can be proven to have been created at the specified time and can be proven to have been unaltered.

Point-in-time History

The state of a database at any point in time can be retrieved.

Data Provenance

The complete history of any item can be retrieved, showing its initial contents, and the changes made to the document at each point in time.
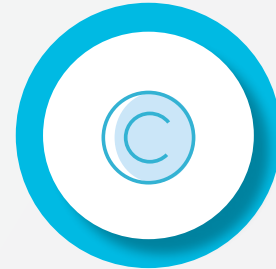
Where is ProvenDB useful?

Regulatory Compliance

Establish a tamper-resistant digital store for critical compliance information.

Finance and Accounting

Render financial records immune from malicious tampering or backdating.

Intellectual Property

Prove the ownership and creation date of intellectual property and eliminate authorship or prior art.

Legal Document Management

Prove the origin, integrity and ownership of wills, contracts, court papers, or any other legal document.

Government and Public Records

Eliminate counterfeiting and tampering for licenses, certificates, and public records.

Secure Systems

Build highly secure and tamper-resistant systems. Eliminate tampering or falsification of access logs and access control records.

Innovate with ProvenDB

Financial Services

Cyber Security

Government Regulation and Compliance

Accounting and Record Keeping

Legal Document Management and Intellectual Property

Supply Chain and Asset Management

Innovate Your Industry

Create Your Solution

Blockchain Proofs

ProvenDB can generate proofs for a database version or a single document. Although only the hash for a complete version is anchored on the Blockchain, ProvenDB can supply a Merkle tree path which provides cryptographic proof that a given document was included within the Blockchain hash.

In this way, users of ProvenDB may obtain proofs for individual documents that can be validated without the need to access any other documents within the database.

What is a hash?

A hash is a mathematical "signature" of a document - a digital fingerprint. The chances of two documents having the same hash are infinitesimally small. Hashes are far more precise proofs of document identity than DNA or fingerprints.

Performance and Economics

Blockchain is sometimes called "the world's worst database"; it offers truly terrible transactional throughput and storage costs. For instance, the Ethereum Blockchain can process only 15 transactions per second with a storage cost of hundreds of thousands or millions of dollars per Gigabyte.

The architecture of ProvenDB results in a penalty on storage overhead and throughout. However, this overhead is trivial compared to that of the Blockchain. While ProvenDB might be marginally slower and more expensive than a traditional database server, it is massively faster and cheaper than the Blockchain. ProvenDB offers a perfect compromise between the two technologies:
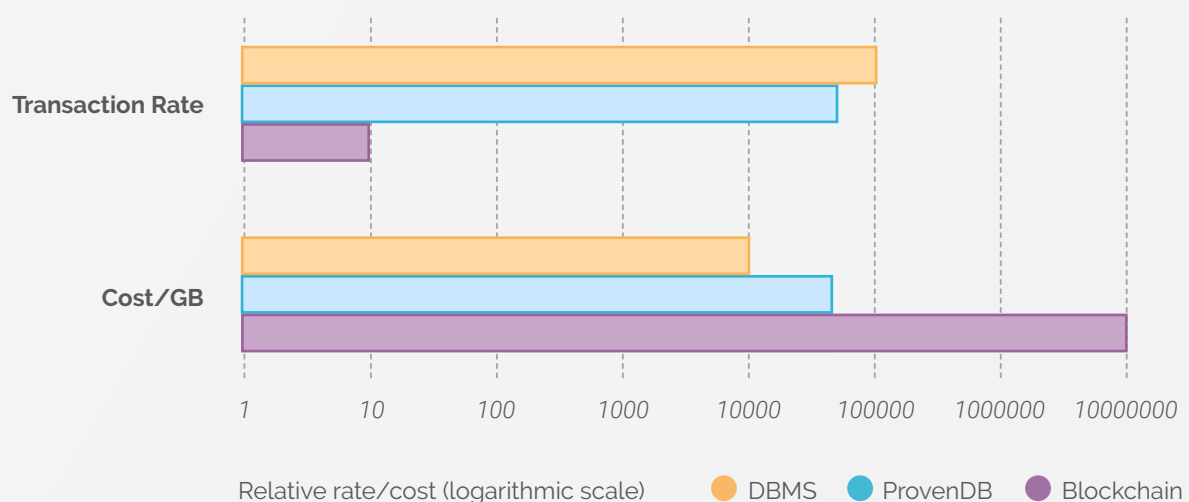
ProvenDB for Developers

ProvenDB for developers is a tamper-proof, highly secure Database system with best of breed database security and MongoDB compatible service. Gain a competitive edge for your products and upskill with Blockchain development.

Create your competitive advantage with Blockchain

- "Blockchain... is **revolutionary** and has the potential to revolutionise nearly every industry." - *Forbes (https://bit.ly/2Oc23C5)*.

- **Avoid the 95%** of of **Blockchain projects failing** due to either performance challenges or misapplication of the technology. Build your first successful Blockchain project with ProvenDB.

- Blockchain technology is poised to take over the way we work. Why not **empower your career** by becoming a Blockchain developer?

- Join ProvenDB today and start developing your project with a Blockchain-enabled database!

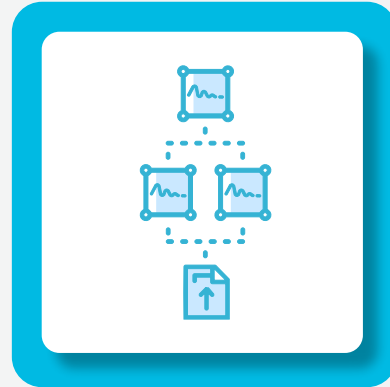> ❝ **Data written into th Blockchain is immutable, and can never be changed, modified or removed.** ❞
>
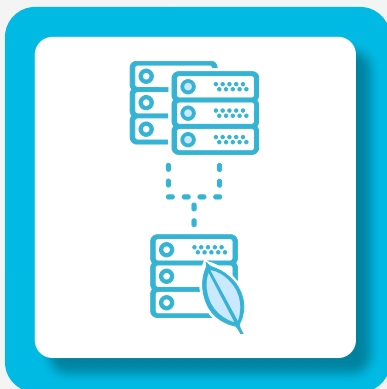> **Wall Street Journal**
> *(https://on.wsj.com/2PJ1Wem)*.

How developing with ProvenDB works

1. When information is added to ProvenDB, transactions are stored on a MongoDB database.

2. Digital signatures of these transactions are stored on an immutable Blockchain.

3. Each transaction creates a new version within the database. Explore older versions and their proofs at any time.

4. Finally request a proof to be placed on the Blockchain for a specific version. Prove the timestamp of an entire version or any document in that version.

Key features and benefits

MongoDB Compatible API

Connect effortlessly to your existing MongoDB applications or join millions of developers already using MongoDB. Speed up your development by learning Blockchain without a new language. If you know MongoDB, you know ProvenDB.

Versioning and History

Easily travel backwards and forwards through your data history with an immutable versioning system.

Proof Automation

Getting your data on the Blockchain has never been easier, and the scheduling interface allows you to automate the process.

Performance

By combining the best of a non-relational database with the best of the Blockchain, ProvenDB can achieve a balance of cost and performance.

Multi-Chain Support

Whether it's Bitcoin or Ethereum, testnet or mainnet, anchoring your data on one or more Blockchains is as easy as changing a single parameter.

Query Playground

The ProvenDB UI provides an interactive tutorial for easy onboarding. You can even write and execute queries directly in your browser.

ProvenDB
Compliance Vault

Compliance with regulation has always involved time consuming and costly reporting and recordkeeping requirements. This cost is justified by serious consequences of non-compliance: legal proceedings, fines and penalties, and the loss of income and reputation.

Compliance Vault is a cost-effective software solution that provides a tamper-resistant digital store for your critical compliance information. The ownership and creation date of information stored in ProvenDB Compliance Vault can be definitively proven by stringent industry standard cryptography. With ProvenDB Compliance Vault, you can be certain that your compliance data will satisfy the most rigorous compliance audit.

Compliance Vault allows you to:

Prove ownership of intellectual property.

Prove timestamps for legal instruments.

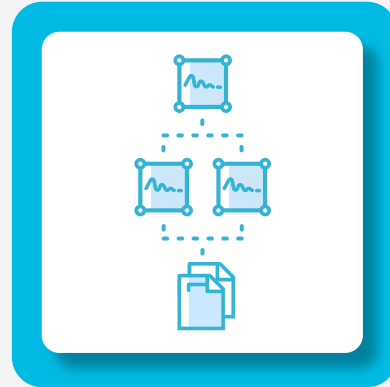**Prove that records have not been falsified or tampered.**

Create a log of all document changes.

![Proven DB logo]

How Compliance Vault works

1. Documents are uploaded to the Vault, directly from apps, file systems, or forwarded via emails.

2. Digital signatures for the documents are stored on an immutable, unhackable public Blockchain.

3. ProvenDB Compliance Vault continuously monitors the integrity of the data to detect any attempts at tampering or falsification.

4. Finally, verify the contents, creation date and origin of your documents to have certainty that your document integrity is maintained.

ProvenDB

ProvenDB Compliance Vault is for all your critical compliance documents:

Anti-Money Laundering and Counter-Terrorism Financing records

Receipts, invoices, and other documents supporting tax claims

Contracts, applications, and all materials that form a basis of financial credit assessments

Know Your Customer (KYC) documents

Board minutes and resolutions

Credit Reporting Privacy disclosures and activities

Timesheets and employment records

Professional certifications

Key features and benefits

Uploads compliance documents via webforms or bulk upload.

Accepts and stores critical email threads.

Integrates with existing application frameworks.

Provides a complete history of document changes.

Enables irrefutable proof of the origin date of the document.

Performs continual monitoring of data integrity.

Enforces non-repudiation of documents contents.

Enables audibility and transparency of all alterations.

Delivers complete tamper detection.

Generates cryptographic certificates confirming data ownership, date of origin, and integrity.

> **The average cost to organizations that experience non-compliance problems is USD $14.82 million.**
>
> **Ponemon Institute**
> *(Based on an analysis of 53 multinational organizations).*

> **The RegTech industry is on the verge of a move from 'Know Your Customer' to 'Know your Data'.**
>
> **KPMG**
> *(RegTech there's a revolution coming).*

ProvenDB
Secure Database

Secure Database is a tamper-proof, highly secure database system. Best of breed database security and encryption prevents any unauthorized database access, while Blockchain integration prevents any undetected tampering of data.

With Secure Database, you can have 100% certainty that your data integrity has been maintained and that no undetected manipulation of data has occurred.

Prevent these costly cyber threats

- Privileged insiders are capable of accessing and **tampering with data** in even the most secure systems.

- Outsiders may **compromise** insider credentials without their knowledge through malware or other exploits.

- In **72% of cases**, incident response professionals encountered destruction of logs to conceal security incidents.

> **The average cost of a Data Breach to organizations is USD $3.92 million.**

IBM
(Based on the analysis of 507 multinational organizations).
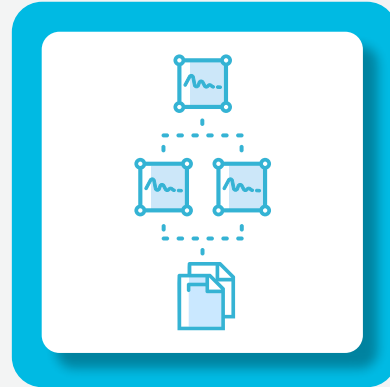
How Secure Database works

1. When information is added to Secure Database, digital signatures are created and stored on an immutable.

2. These signatures can prove the integrity, ownership, and creation date of your data. Data is securely encrypted with an enterprise MongoDB.

3. Secure Database continuously monitors the integrity of your data to detect any tampering or falsification attempts.

4. Finally verify the integrity and origin of the digital assets with their certificates at any time.

Key features and benefits

Create Secure and Tamper-resistant Systems

Build highly secure and tamper-resistant systems. Eliminate undetected tampering or falsification of your data.

Continuous Monitoring of Data Integrity

Continually monitors the integrity of your data to detect any tampering or falsification attempts.

Secure Access Logs and Access Control Records

Eliminate tampering or falsification of access logs and access control records. Any attempt to manipulate logs or records by an attacker can be quickly identified.

Detect Any Attempts to Manipulate or Destroy Data

Attackers cannot go undetected during data manipulation or destruction attempts. This includes attempts to "cover the tracks" of an intrusion.

Proofable API,
Powered by ProvenDB

Proofable is a framework for certifying digital assets to public Blockchains. You can anchor millions of digital assets quickly and economically in a single transaction.

Proofable certificates can be used to detect tampering or to prove the integrity and origin of any digital assets such as legal documents, financial instruments, intellectual property, and more.

Proofable includes

CLI

A command line interface to prove files.

SDK

Powerful SDK for JavaScript, GoLang and more to come.

gRPC

Modern gRPC wire protocol for integration into any language.
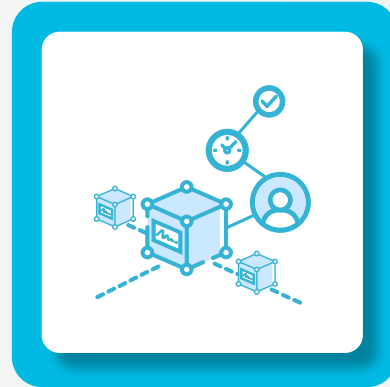
REST

Industry standard, cross platform interface.

How Proofable works

1. Create a trie structure containing up to millions of digital asset signatures.

2. Anchor the trie to a public Blockchain using a single API call.

3. Generate certificates from the trie that forever prove the integrity and origin of all or some of the digital assets.

4. Verify the integrity and origin of the digital assets with the certificates at any time.

Key features and benefits

Prove ownership of digital assets such as intellectual property or digital media.

Prove timestamps for legal, accounting or financial records.

Prove records are are not tampered with or falsified.

Anchor millions of digital assets in a single Blockchain transaction.

Highly efficient trie data structure allows for incremental updates and hierarchical proof structures.

Support for Bitcoin, Ethereum, Hashgraph, Elastos, Go Chain, and an increasing number of other Blockchains.

> **[Blockchain] is revolutionary and has the potential to revolutionize nearly every industry.**

Forbes
(https://bit.ly/2Oc23C5).

Summary

Blockchain technology represents a paradigm shift for applications and data management. The Blockchain allows data items to be anchored to a provable timestamp, allowing us for the first time, to prove the creation time of a data item and confirm its integrity.

ProvenDB provides a database service that combines the features of a familiar document database with the Blockchain characteristics of immutability and tamper-proof storage. By using ProvenDB, applications can easily provide incontestable proofs of data integrity, allow users to view any previous versions of the database and provide a complete and provable audit trail of data changes.