Managing Risk and Non-Compliance with ProvenDB

Introduction

ProvenDB is a trustable database storage service that prevents tampering and manipulation of databases, information and documents. ProvenDB quickly integrates with traditional database and application technologies and leverages Blockchain technology to guarantee the origin, ownership, versioning and integrity of your important data.

The Problem: The Increasing Cost of Rick and Non-Compliance

Information integrity is crucial for establishing trust with business partners, customers, and regulators. It requires that Information is complete, consistent, and correct.

All businesses today are data and information driven. Interactions between consumers and providers are increasing across digital channels and the documentation that supports orders, invoices and services are also increasingly electronic. The same holds true for regulators and business partners. All businesses with employees or revenue are subject to regulation, and compliance with regulation can only be established by accurate information.

The Information Age has brought many benefits to society and business. However, in a world of fake news, cyberattacks, document fraud and identity theft, trust in information is on the decline.

This is partially because digital documents and data are too easy to copy and falsify. In the world of paper documents, copying or tampering would generally leave tell-tale signs that could reveal the fabrication. However, in the digital world there's usually no way to distinguish a falsified document from the original.

> *The average cost for organizations that experience non-compliance problems is $14.82 million.*
>
> *Ponemon Institute - 2017*

Fabricated or falsified digital information is an increasing problem for almost all industries, at all levels of scale. The consequences of falsified information can be severe, ranging from loss of consumer confidence, fines and other legal penalties and in the most extreme cases complete business failure.

Consequently, Business partners, customers, and regulators are increasingly unlikely to take digital information at face value: they need proof of information integrity.

Organizational Remedies

Organizations have at their disposal a variety of procedural mechanisms for increasing data integrity. Many of these procedures are incorporated into Information Security Guidelines or in regulatory frameworks such as Sarbanes Oxley. Some of the typical procedures include:

- Fine-grained control over document and information access
- Segregation of duties
- Physical access management
- Access control and authentication procedures
- Monitoring and logging of data access
- External audit
- Dual sign off

Unfortunately, while robust organization policies are necessary for information integrity, they are not sufficient for establishing the validity of any existing data item.

The existence of audited and comprehensive policies and procedures may improve the credibility of an organization and help "trust me" get over the line. Nevertheless, they do not establish any sort of definitive proof about the origin or integrity of data provided by an organization. Furthermore, most of these procedures are unable to mitigate insider threats – where an individual with superuser or "root" authority is involved – and raise obvious questions of "who watches the watchers".

Technology Solutions

There are technological solutions that can provide definitive proof of data integrity. We do have the ability to use cryptographic techniques to establish the "who, what and when" for any data item.

Document hashing can be used to prove that the contents of a document have not been modified. A hash is a mathematical "signature" of a document - a digital fingerprint. The chances of two documents having the same hash are infinitesimally small, and the hash itself is very compact – typically 256 bits (64 characters) long.

A digital signature is a special type of hash that is created by someone in possession of a PKI private key. A digital signature can prove the identity and integrity of a document. By comparing the digital signature with the document's contents and a public key, you can verify that the signature was generated by someone in possession of the private key and that the document contents have been unaltered.

Hashes and digital signatures can be used to prove the "who and what" of a digital document. However, until recently we haven't had a strong solution for proving the "when" aspect of digital integrity. Digital signing proves that a document has not been changed since signing, but does not establish the date of the signature.

Blockchain Technology provides the missing piece of the "who, what, when" puzzle. Data items posted to a public Blockchain are immutable and timestamped. Once created, public Blockchain records cannot be redacted, removed or repudiated.

By placing a hash or digital signature on a public Blockchain, we can irrefutably establish a date for the document or data item.

The storage capability of the public Blockchain is relatively low, and the transaction costs high – if we had to create a transaction for every document signature the costs would be prohibitive. Luckily, cryptographic structures – Merkle trees and the like – allow us to aggregate the hashes for millions of documents in a single "root" hash. By placing the "root" hash on the Blockchain we can prove the veracity of the digital signatures of millions of documents in a single transaction.

Obstacles to Adoption

Unfortunately, while the elements of the solution are available, in practical terms they are out of reach for almost all enterprises. The complexity involved in the implementation of Blockchain and cryptographic technologies is daunting. These technologies are not easily integrated with existing software frameworks. Furthermore, there is no existing solution that integrates the Blockchain and cryptographic proofs with the storage and management of digital documents and data. Consequently, Gartner estimates that 95% of Blockchain data managements project will fail (Gartner report G00325744).

Introducing ProvenDB

ProvenDB is a trustable database storage service that prevents tampering and manipulation of databases, information and documents. ProvenDB quickly integrates with traditional database and application technologies and leverages Blockchain technology to guarantee the origin, ownership, versioning and integrity of your important data.

ProvenDB delivers value in three ways:

- By reducing the cost and risk involved in managing the documents and data required to prove compliance, and by delivering definitive proof of data origin date and integrity.
- By reducing the cost and schedule risk involved in developing bespoke applications that seek to leverage Blockchain and cryptographic technologies to improve data integrity.
- By allowing Independent Software Vendors, System integrators and others to deliver competitive advantage through the provision of superior data integrity.

How it Works

By combining digital signatures and immutable public Blockchain transactions ProvenDB solves the increasing problem of tampering and falsification of digital documents. As a result, enterprises can again have faith in the integrity, ownership and origin of our digital assets.

ProvenDB augments a widely used database engine (MongoDB) with Blockchain Data Management capabilities. When a data item is added to a ProvenDB database cryptographic signatures of the item are automatically created, aggregated and anchored to a public Blockchain such as Bitcoin or Ethereum.

When data in a ProvenDB database is modified, the original item is preserved, ensuring that Blockchain proofs created against that version of the data are preserved and allowing you to view a complete history of changes for a data item.

ProvenDB allows you to

- Prove ownership of intellectual property
- Prove timestamps for legal instruments
- Prove that database records have not been falsified or tampered with
- Create a log history of all document changes

ProvenDB in Action

ProvenDB is applicable across a variety of industries, and scenarios. In particular:

- In heavily regulated industries, ProvenDB Compliance Vault can be used to create a repository of compliance information that is secure, tamper-proof and completely provable. Regulators can be shown that the information in the vault is completely immune from falsification, backdating or tampering. Within the organization, the possibility of insider manipulation of compliance data will be eliminated. The costs and risks involved in compliance audits and regulatory reviews will be minimized.
- Independent Software Vendors can use ProvenDB to improve the competitive advantage of their solutions. Solutions built on ProvenDB can use any industry standard development framework that supports MongoDB without modification, so there is virtually no additional development overhead. Applications built on ProvenDB automatically gain all the data integrity advantages of ProvenDB
- Consulting and services firms that wish to develop solutions for customers can enhance both enhance their competitive advantages and reduce development costs using ProvenDB. Solutions developed with ProvenDB have superior data integrity, while developing applications with ProvenDB is massively faster and cheaper than programming solutions directly against the Blockchain.

ProvenDB's data integrity is directly applicable across many industries and user cases that require best practice management of risk and non-compliance - for example:

- Accounting and finance
- Government
- Healthcare
- Legal
- Intellectual property
- Regulated industries
- Any industry where impeccable data integrity is required

Reduce the costs and risks involved in regulatory compliance with ProvenDB Compliance Vault.
Visit www.provendb.com to sign up for a ProvenDB cloud service, or email us at support@provendb.com to explore options for deploying ProvenDB within your organization.