## Features

### MongoDB Compatible

- Data is ultimately stored in MongoDB Atlas.
- MongoDB API and document format compatible.

### Blockchain Proofs

- The integrity and timestamp of database state can be proven on the bitcoin blockchain.
- ProvenDB can prove the integrity and timestamp of any database version or of any specific document.

### Bulk Load

- ProvenDB can be placed in a fast load mode in which only inserts are permitted.

### Compaction

- ProvenDB allows data between two proven versions to be compacted.
- This reduces storage overhead without compromising the integrity of any database proofs.

### Versioned Database

- ProvenDB keeps multiple versions of documents.
- Updates creates new versions of a document leaving the original intact.
- Deletes marks documents as logically deleted without destroying their content.
- ProvenDB users can query against any previous version of the database.

### Right to be Forgotten

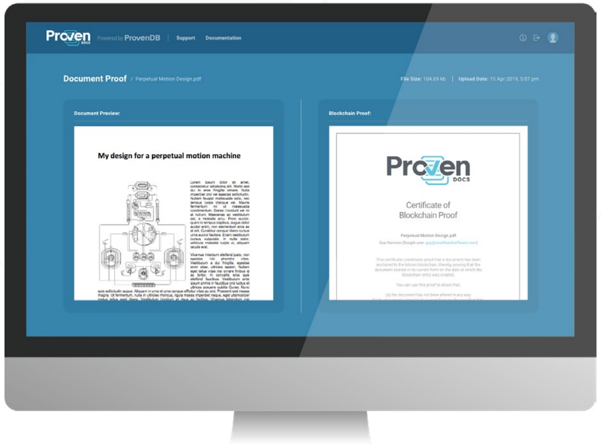
- "Forget" allows all data for a document to be redacted without compromising existing blockchain proofs.
- Viewing data from a forgotten document is impossible, however, other documents in the database version are still provable.

### Export

- Data in ProvenDB can be dumped in mongodump format.
- These dumps can be independently validated against the Blockchain independently of ProvenDB.

## ProvenDocs - A ProvenDB Application

ProvenDocs is a user friendly web application powered by ProvenDB. It allows users to upload their personal documents and receive blockchain proofs of ownership, timestamp and integrity. **provendocs.com**



Document Proof / Perpetual Motion Design.pdf

File Size: 104.69 kb | Upload Date: 15 Apr 2019, 5:07 pm

My design for a perpetual motion machine

Certificate of Blockchain Proof

Perpetual Motion Design.pdf

This certificate constitutes proof that a document has been anchored to the bitcoin blockchain, thereby proving that the document existed in its current form on the date at which the blockchain entry was created.

You can use this proof to attest that:

(a) the document has not been altered in any way

ProvenDB

Proudly partnered by

mongoDB

**info@provendb.com**
**www.provendb.com**

/provendb /provendb
/provendb /provendb

**Want to become a Blockchain developer?**

Sign Up for a ProvenDB early adoper account and recieve 1GB of free storage!

ProvenDB

*Take MongoDB.*
*Add Blockchain. Stir.*

datasheet

## Introduction to ProvenDB

Developing Blockchain applications is time-consuming and error-prone because familiar and well-established database development idioms are not available.

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.

## Why use ProvenDB?

To prove you created some content.

To prove that a document or data has not been tampered with or altered.

To prove the date of a legal or official document.

To prove the exact history (provenance) of some data.

## ProvenDB is particularly useful for:

- Document Management Systems
- Legal Records
- Accounting Systems
- Intellectual Property and Media Management Solutions
- Government and Regulatory Applications
- Audit and Access Management Systems

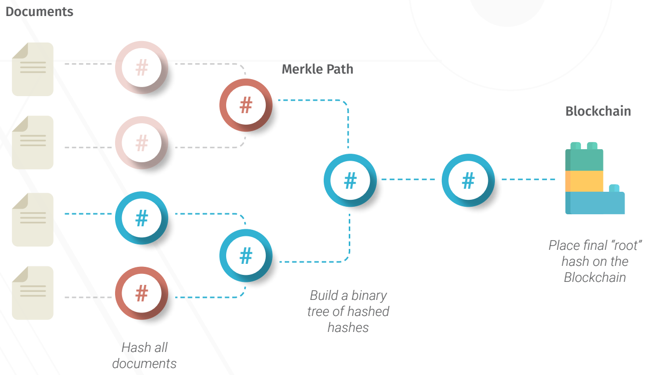
## How ProvenDB Works

ProvenDB can prove multiple documents with a single hash using a Merkle tree. We don't need a whole tree to prove an individual document that is included in the final hash - we only need the "Merkle path."

Thousands of documents can be included in a single Merkle tree - all anchored to a single Blockchain transaction.

***What's 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.*


Documents
#
#
#
#
#
#
#
#
Merkle Path
Blockchain
Hash all documents
Build a binary tree of hashed hashes
Place final "root" hash on the Blockchain

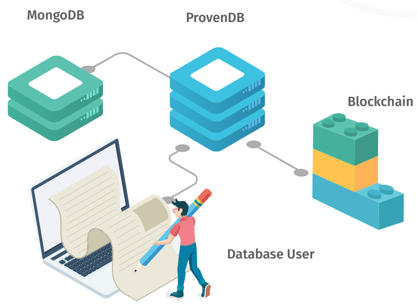
## Blockchain Proofs

ProvenDB can generate proofs for a database version or a single document. Although only the hash for a specific database 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.

## Architecture

ProvenDB presents a MongoDB compatible API to the database user. Every change to the database creates a new logical version within the database. The user can view the older versions at any time.

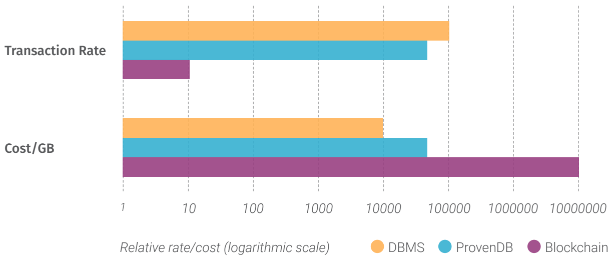
The database user requests a proof be placed on the Blockchain for a specific version. This proof can be used to prove the timestamp of that specific version or any document in that version.



## 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:


Transaction Rate
Cost/GB
Relative rate/cost (logarithmic scale)
● DBMS
● ProvenDB
● Blockchain