

# Databases in the Era of Ledger currency



*BlockchainDB failure overcome by  
BigchainDB*

*Khushboo Singh  
Database Management  
Systems Research Report  
NEUID: 001684376  
Information systems  
7/29/2016*

## Table of Contents

<b>1. Abstract.....</b>	<b>3</b>
1.1. Introduction.....	3
<b>2. Journey of Decentralized database .....</b>	<b>3</b>
2.1 Decentralized database over the years.....	5
<b>3. Bitcoin and the mechanism which drives it .....</b>	<b>6</b>
3.1 How it works.....	6
3.2 Acquiring Bitcoins and making payments .....	7
<b>4. Blockchain in the era of Decentralized computing.....</b>	<b>8</b>
4.1 Problem driving the implementation .....	9
<b>5. BIGCHAINDB securing Bitcoin industry.....</b>	<b>10</b>
5.1 Why use BigchainDB .....	10
5.2 Working model of BigchainDB.....	11
<b>6. Conclusion.....</b>	<b>12</b>
<b>7. References .....</b>	<b>13</b>

**1. Abstract:** It was difficult to even think about currency over internet but “Satoshi Nakamoto” in 2008 not did think but made it possible to introduce transaction between two users without the involvement of a third party. In 2009, he introduced a software for peer-to-peer transaction without an intermediary which brought evolution in databases. Bitcoin transaction uses Traditional BlockchainDB to BigchainDB [1]. This paper focuses on how and why the evolution happened and what is the current situation even after small failures.

### ***1.1 Introduction:***

Due to the introduction of Bitcoin, decentralized databases came into a picture in a better way. Even if it was used earlier but Bitcoin presented the Decentralized database in a different way. Before getting into the depth of the Bitcoin model we need to first understand the Decentralized database.

### **2. Journey of Decentralized database [2]**

If we talk about databases, then we need to categories them into the way they are managed. The DBMS (Database management systems). DBMS helps to create, update, read and delete data in the database. When we talk about data, we need to understand how is it being located over the network. The below three systems help to categorize the database systems.

#### ***Centralized database:***

It has all the files located, stored and maintained at one physical location.

#### ***Decentralized database:***

A big database is partitioned in such a way that each smaller database represents a particular data subject.

#### ***Distributed database:***

Those databases where storage devices are not at all attached to a common storage unit. These databases are controlled by distributed database management systems.

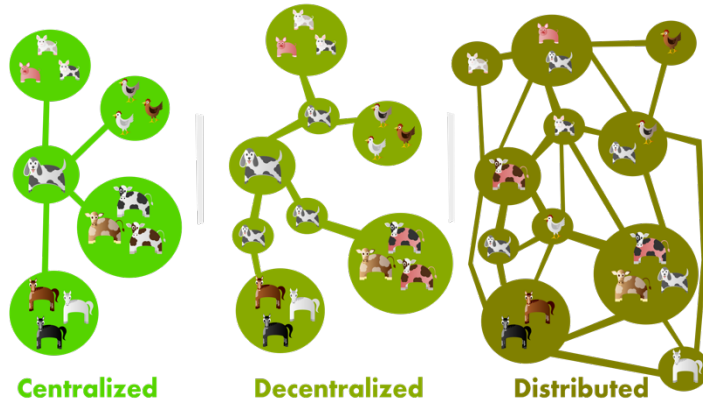


Fig 1: Database systems

The above figure mentions the three kind of database structure over the network. Centralized database is quite famous, old and even used recently by a lot of companies including all the industries. Distributed and decentralized systems came later but are being used where large number of related transactions is involved. Below table describes the differences between all three of them.

<u>Properties</u>	<u>Centralized</u>	<u>Decentralized</u>	<u>Distributed</u>
Points of failure/maintenance	Easy to maintain as they have only a single point of failure.	It has more but still finite.	They are most difficult to maintain.
Fault tolerance/ Stability	It can become highly unstable because the main system failure can create chaos.	Even if the main system is killed, you will have many other systems to support.	It is the most stable system and failure doesn't harm much.
Scalability	Low	Moderate	High
Ease of development	One consistent framework is used so it is quite easy to create centralized systems.	Creation of the system needs resource sharing and communications details that is why it is difficult to create.	Due to the lower lever details before creation it is difficult to create.
Evolution/Diversity	No diversity as they follow single framework.	After basic infrastructure evolution is enormous.	It is also quite enormous [3].

Table 1: Table for data processing systems.

We talked about the way data is being processed. Whenever transaction over the network gets involved we need to set up a secure and organized level of data processing, we need to consider the way data is being managed. Due to advancement in information technology, specific database software's are coming into picture. In the past it was common to have centralized database systems due to data integrity and less expensiveness. But due to advanced hardware which are cheap when speed and efficiency is considered, decentralized database has become better choice [4].

## 2.1 Decentralized database over the years

The development of decentralized infrastructure is as follow [5]:

<u>Year</u>	<u>Inventions</u>	<u>Inventors</u>	<u>Systems</u>
1970s	TCP/IP	Vint Serf/Bob Kahn	Decentralized communications
1989	WWW	Tim Berners Lee	Decentralized communications(current forms)
2009	Bitcoin	Satoshi Nakamoto	Decentralized ledger with a cryptocurrency
2015	Interplanetary file system	Juan Benet	Decentralized file system
2015	Ethereum	Vitalik Buterin et al	Decentralized processing
2016	BigchainDB	Trent McConaghy et al	Decentralized database

Table 2: Decentralized infrastructure development over the years.

If the output is handled by only one central database, then the failure possibility becomes high. This force the business to stop processing results in the revenue loss. This is where decentralize database becomes helpful. Partitioning the data as per the subject user and providing ownership to the subject area solves the failure problem. Each of the database partitioning is managed by a specific user or group like financial group or sales group. This kind of setting helps to maintain **data integrity** more securely. If you have to look for a simple report, the database will scan all the database when centralized systems are used but in decentralized we can search a specific group or user which boosts **access and processing speed**.

### 3. Bitcoin and the mechanism which drives it

It is time to control our own digital information and control our assets. The same thinking was ignited for the development of Bitcoins. It is a digital asset and a payment system introduced in 2008. It involves peer-to-peer transaction between two users without involving intermediary. The transactions are verified by network nodes and are recorded in a public distributed ledger called the Blockchain. It works without a centralized repository or administration that is why US Treasury marked it as *decentralized virtual currency*. It is also called the first cryptocurrency. A cryptocurrency or crypto currency is a medium of exchange where security is provided using cryptography known as digital currency. Bitcoin is largest as per the total market value.

#### **3.1 How it works [6]:**

In layman term, Bitcoin is just a mobile application or computer program which provides a personal wallet which is used to send and receive bitcoins to other users.

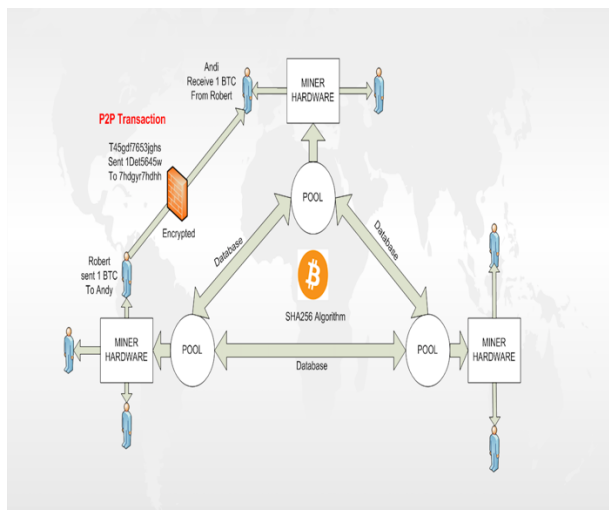


Fig 2: Bitcoin working model

Technically, it's a network of bitcoins which is used to share public ledger called "block chain". The ledger contains every processed transaction and allow the user to validate each transaction. Digital signatures are used to protect the authentication of the sending address, provides full control to the user over the bitcoins they send from their own address. As well users can earn reward points by using computing power of specialized hardware which is called "mining".

### 3.2 Acquiring Bitcoins and making payments

You can use for exchange and acquire it for payments. Below are the way which mentions the details of Bitcoin acquiring process:

- Bitcoin for payment of goods and services.
- Use Bitcoin for Bitcoin exchange.
- Can exchange Bitcoins with others who are nearby.
- Mining- By competitive mining, you can earn Bitcoins.
- Chargeback- Sell Bitcoins in exchange of credit card or PayPal payment.

Bitcoin payment is one of the most attractive properties about Bitcoins. This is the reason for big customer pool as it is quite easy to make Bitcoin payments in comparison to credit cards and receiving payment without the involvement of a third party and that too free.

 Deposit now FREE	 Deposit now 4.95% fee	 Deposit now 4.95% fee	 Deposit now 4.95% fee	 Deposit now 4.95% fee	 Deposit now 4.95% fee
 Deposit now 4.95% fee	 Deposit now FREE	 Deposit now 3% fee	 Deposit now 9.9% fee	 Deposit now FREE	

Fig 3: Bitcoin comparison with other transaction methods




Carrier 8:07 PM		
BLOCKCHAIN		
0.41434437 BTC		
\$115.43		
5 minutes ago RECEIVED	pending	0.03745095 BTC
9 minutes ago TRANSFERRED	pending	0.04541474 BTC
3 hours ago SENT		0.06431428 BTC
4 hours ago RECEIVED		0.03785096 BTC
4 hours ago RECEIVED		0.04221302 BTC
4 hours ago SENT		0.0130906 BTC
  		

Fig 4: Bitcoin wallet structure.

The payments are made using the wallet application by entering the address of the recipient and amount. Address can be easily retrieved by scanning the QR code or NFC technology.

<u>Advantages of Bitcoin:</u>	<u>Disadvantages of Bitcoin:</u>
<i>Payment freedom</i> – It is easy to send and receive Bitcoins.	<i>Degree of acceptance</i> – Less people and business are aware of it.
<i>Fewer risk for merchants-</i> The transactions are secure and irreversible and don't contain personal information.	<i>Volatility</i> – It will decrease as the market matures.
<i>Security and control</i> – Difficult for merchants to force unwanted and unnoticed charges.	<i>Ongoing Development-</i> New tools and services are being developed to support Bitcoins.
<i>Transparent and Neutral-</i> Can't manipulate as it is cryptographically secure.	

Table 3: Bitcoin and how it is surviving in the market.

#### 4. Blockchain in the era of Decentralized computing [7]

When someone try to understand Bitcoin, Blockchain which is the technology behind Bitcoin always pop up our mind with a lot of questions. Blockchain is a type of *decentralization technology* which try changing the way our industry works. Due to this technology the user has direct control to their asset via their password.

Blockchain is a transaction database participates in a Bitcoin protocol. It contains all the transactions ever executed by the currency and helps to find out the value and the history of each address.

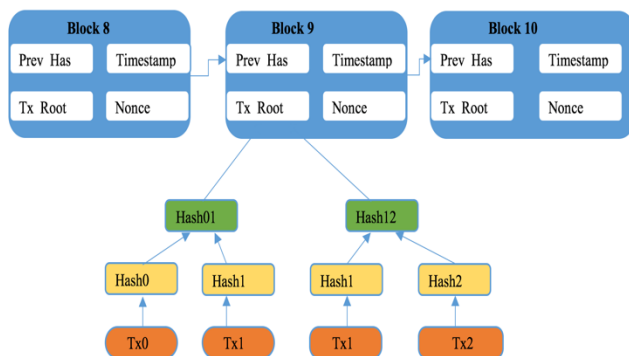


Fig 5: Decentralized Blockchain working example



In the above figure, timestamp is the block found time, Prev\_Has is the reference to the parent, Tx\_Root represents the set of the transactions which has been closed. All of the above items get hashed into the block hash and referenced by the next block.

Each block contains a hash of the previous block hence it creates a chain of blocks from the previous to the current block. Each block chronically comes after the previous block to obtain the previous block's hash. It is difficult to modify as the block attached to it needs to be regenerated. A valid chain is one which has all its transactions valid. This is what makes double-spending of Bitcoins difficult.

There is only one path to the parent chain which is also known as "genesis chain" but it can have forks. Two blocks are created in few seconds where as one-block forks are created time to time. This results in node generation which belongs to the block which receives first. Hence they keep becoming part of the block chain. Shorter chains are not used whereas these chains when switched to longer chains, blocks inside the shorter chains are added to the pool of the transactions which are queued and later it will be included in another block. The rewards given to shorter chains are lost. The shorter chain blocks are called orphan blocks as during generation it lost the parent block in the new longest chain whereas these blocks can have a parent block and might have children as well. It is impossible for 2 forked chains to merge as they belong to different parent block.

Blockchain has brought a new way to deal with your own money and thrilled the financial Industry. Other industries like pharma, automotive and natural resources have also started using it. But in the banking sector, decentralization technologies pose some significant risk as well.

#### ***4.1 Problem driving the implementation [8,9]***

When money gets involved, security becomes the main point of focus. Same thing happened with Bitcoin Blockchain.

- "In 2016, \$1.6 million of value was drained from Ether Blockchain and added to a new account". It was said that this happened due to unpatched security hole. After that, different patches have been released but none of them helped to fix the security issue of the Bitcoin Blockchain database.

- If the key is compromised anytime then it can be used to access the other chains connected to the parent chain.

To fill the gaps, BigchainDB was introduced as well database introduced new characteristics which helped the Bitcoin industry not only to survive but also a secure and safe transaction was introduced in the field of technology.

### **5. BIGCHAINDB securing Bitcoin industry**

BigchainDB is a decentralized scalable database which performs 1 million writes per second as well stores petabytes of data and sub-secondary latency. It starts with a distributed database and keeps adding Blockchain characteristics:

- Decentralized Control
- Immutability
- Movement of digital assets with their creation.

As well it adds modern database characteristics:

- Linear scaling for throughput per node
- NoSQL query language
- Querying
- Permissioning – Enables configuration from private to public database.

#### **5.1 Why use BigchainDB:**

The below table describes the reason to switch to BIGCHAIN from Bitcoin Blockchain database [10].

	<u>Bitcoin</u> <u>Blockchain</u>	<u>BIGCHAIN</u> <u>database</u>
Immutability	Yes	Yes
No Central Authority	Yes	Yes
Assets Over Network	Yes	Yes
High Throughput		Yes

Low Latency		Yes
High Capacity		Yes
Rich Permissioning		Yes
Query Capabilities		Yes

## 5.2 Working model of BigchainDB :

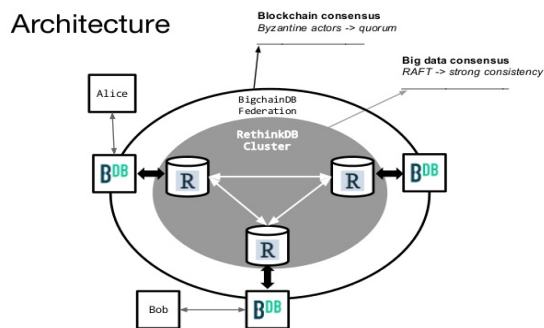


Fig 6: BigchainDB Architecture

Not only the above benefits but it also embeds enterprise-hardened code for its codebase. Legal certificates can be directly stored on the Blockchain database.

The BigchainDB architecture simply specifies that the assets are provided with crypto-conditions:

- Private-public key
- Multi-signatures
- **Crypto condition – Owner define condition, new user to take over need to fulfill the conditions.**
- Smart-Contracts

Last but not least, the specific properties will explain why is it BigchainDB

<u>Throughput</u>	<u>Latency</u>	<u>Capacity</u>	<u>Scalability</u>	<u>Query</u>	<u>Decentralization</u>
> 1, 000, 000 /sec	<100 ms	Petabytes each node adding 48TB	Nodes addition increases performance	Database fully queryable	Non- anonymous participation

## **6. Conclusion:**

Ledger systems come and go. Even Bitcoins came with some of its disadvantages but over others it was better which made it famous with time resulting in high revenue and market share but a system is successful till a hacker doesn't cracks it. The same scenario decreased the market share of Bitcoin using Blockchain. No one was aware that a small change can change the picture. Though BigchainDB is just not a small chain but one of the best examples of scalable decentralized database which can perform 1 million writes per second. That's not the end, it complements the decentralized processing and file systems.

## **7. References**

- 1) <https://en.wikipedia.org/wiki/Bitcoin>
- 2) <http://ib2012-itgs.wikispaces.com/file/view/Centralised+Vs+Distributed.pdf>
- 3) <https://medium.com/@bbc4468/centralized-vs-decentralized-vs-distributed-41d92d463868#.j1t0adliy>
- 4) <http://www.learn.geekinterview.com/data-warehouse/dw-basics/decentralized-database.html>
- 5) <http://blogs.lse.ac.uk/businessreview/2016/04/14/blockchain-will-usher-in-the-era-of-decentralised-computing/>
- 6) <https://bitcoin.org/en/faq#how-does-bitcoin-work>
- 7) [https://en.bitcoin.it/wiki/Block\\_chain](https://en.bitcoin.it/wiki/Block_chain)
- 8) <http://techportfolio.net/2016/07/will-blockchain-revolutionize-the-world-of-financial-contracts/>
- 9) <http://www.csoonline.com/article/3050557/security/is-the-blockchain-good-for-security.html>
- 10) <https://www.bigchaindb.com/whitepaper/>