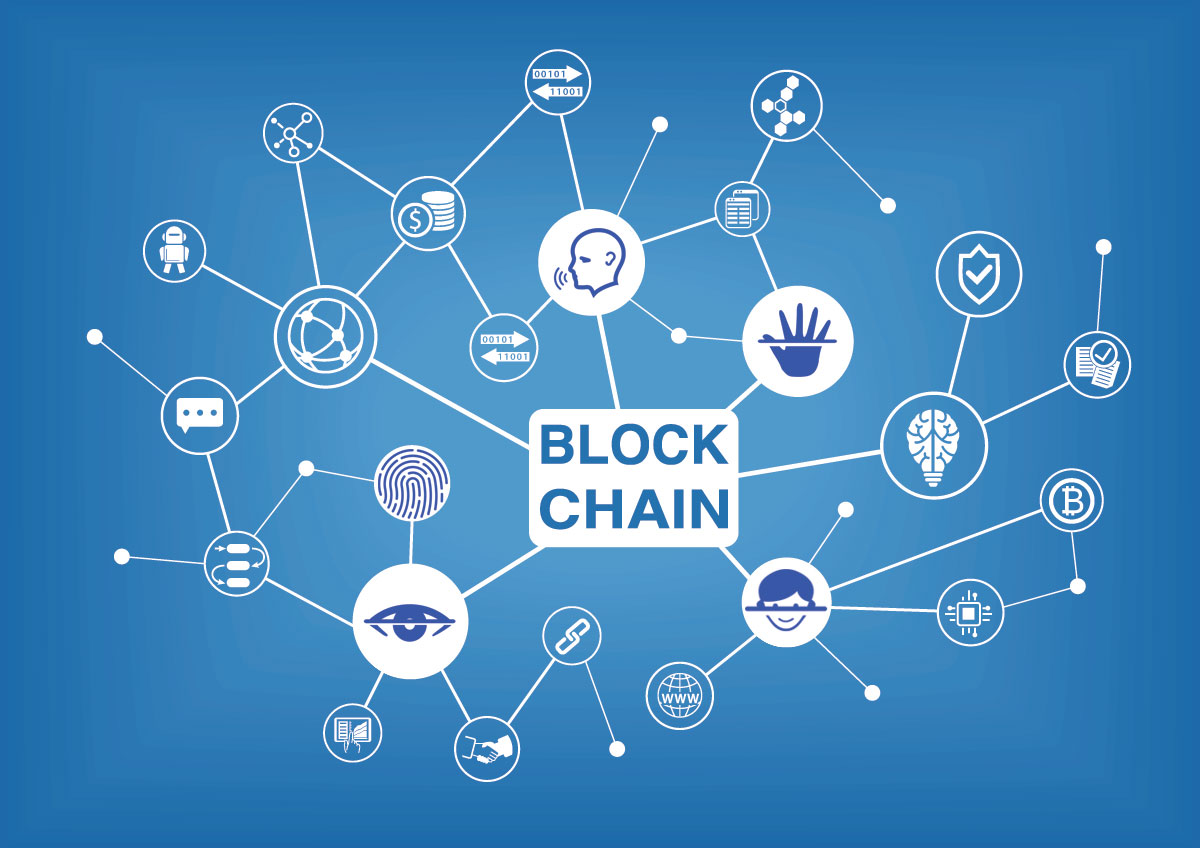
Blockchain Series

Part 1: What is blockchain?

# Introduction

2017 is a pivotal year for blockchain technology due to the rise of cryptocurrency and many startups base on it. However, people do care more about the cryptocurrency such as Bitcoin, Ethereum, … and forget the technology underlying of them: Blockchain.

Blockchain is not a brand new technology as rumors, it is a combination of many familiar technologies we all know about: **Peer-to-Peer Architecture**, **Decentralization concept** and **Hash Algorithm**. You can image that Blockchain is just like a book where any line is a transaction and a page is a block. We will talk more about them later.



# Elements of Blockchain

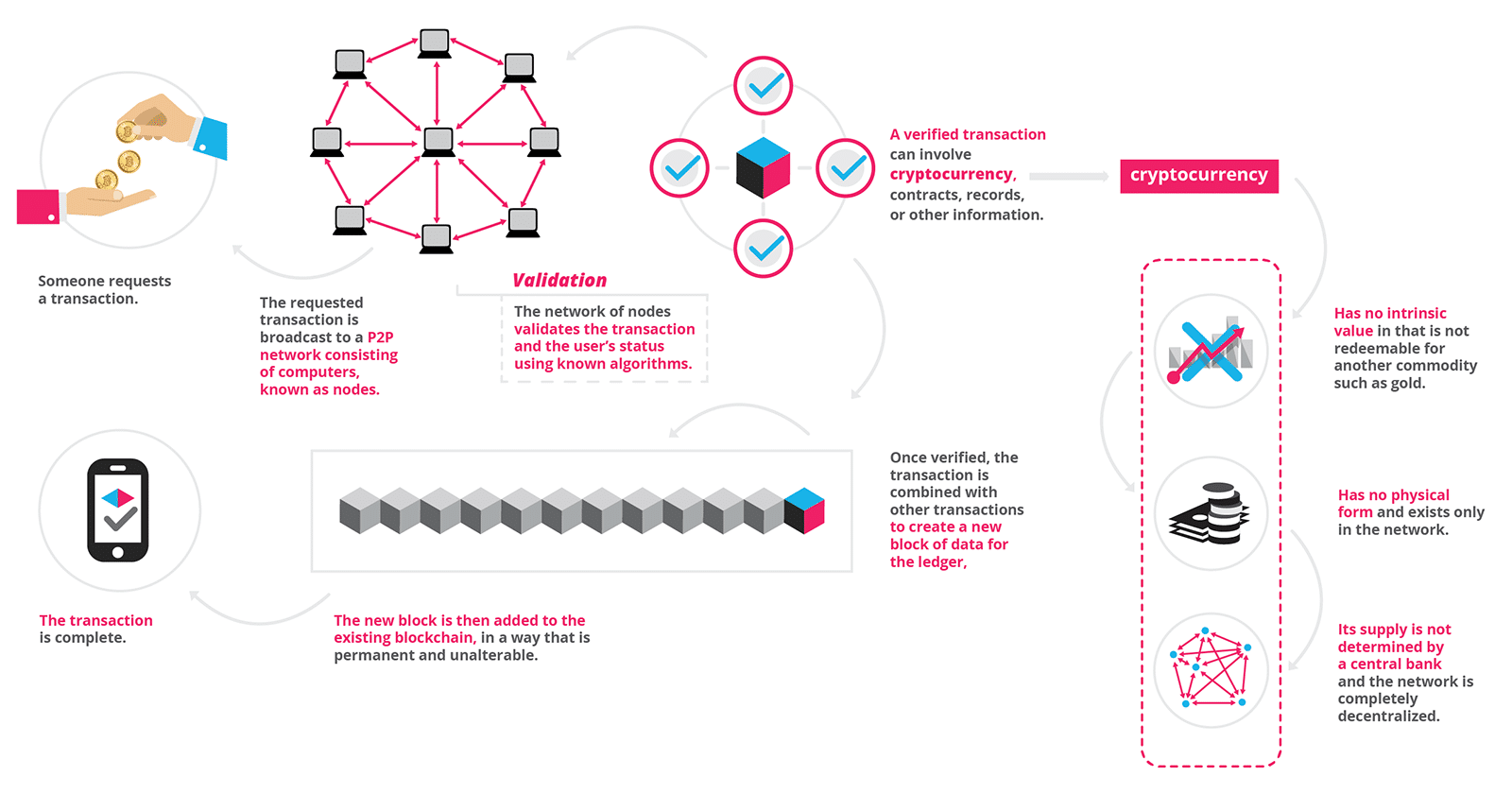
In these days, applications or services based on Server – Client model are so popular that people let the provider do all stuffs for them without any concern about their information. This is a big problem, people depends on these companies so much and can’t control what belongs to them. Blockchain is created to solve this issue. By using blockchain technology to build applications, everything is so clear to everyone on the blockchain network that don’t need an existence of a central certifying authority.

As I have described above, blockchain technology is just a new way of using old technologies or concepts. Let’s take a look at some concepts in blockchain:

* Transaction: Anything you make in the blockchain network will be recorded, this is **a transaction**. You buy a car from BWM, it is a transaction; you send money to your friend, it is a transaction.
* Block: A place where all transactions are collected and put into.
* Blockchain: A chain of blocks works as a database.
* Node: Any devices which have an internet connection and connect to the blockchain network is called **Node**. A Node works as both client and server, every node gives a hand to host this network.
* Hash: Generate the input and return a random string. With a same input, there is only one output. ([Give a try](http://passwordsgenerator.net/sha256-hash-generator/))

Blockchain is basically a distributed and shared database of transactions that facilitates exchange of value. To be simple: “Node is a pen, Transaction is a line in a page, Block is a page in a book and Blockchain is a book.”

# How Blockchain Works

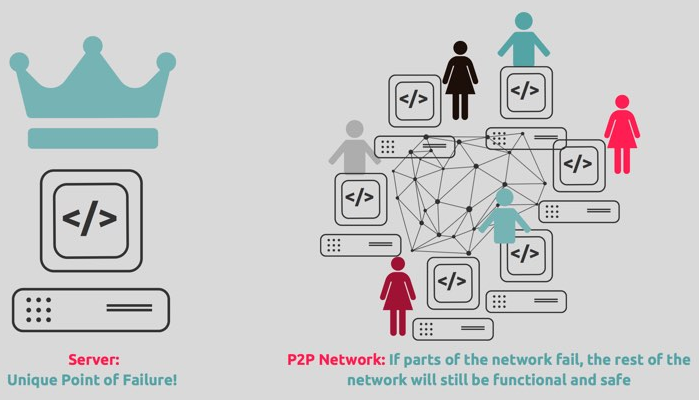
There are 5 steps to complete a transaction:

* **Transaction**: Two persons, Bob and Alice, both are in a same blockchain network. Bob want to send Alice some money. Bob initiate the transaction and broadcast to the network.
* **Block**: The transaction is packaged with other pending transactions thereby creating a block. The block is sent to the blockchain system’s network of participating computers.
* **Verification**: The participating computers (called “miners” in the Bitcoin blockchain) evaluate the transactions and through mathematical calculations determine whether they are valid, based on agreed-upon rules. When “consensus” has been achieved, typically among 51% of participating computers, the transactions are considered verified.
* **Hash**: Each verified block of transactions is time-stamped with a cryptographic hash. Each block also contains a reference to the previous block’s hash, thus creating a “chain” of records that cannot be falsified except by convincing participating computers that the tampered data in one block and in all prior blocks is true. Such a feat is considered impossible.
* **Execution**: The money moves from account of Bob to the account of Alice.

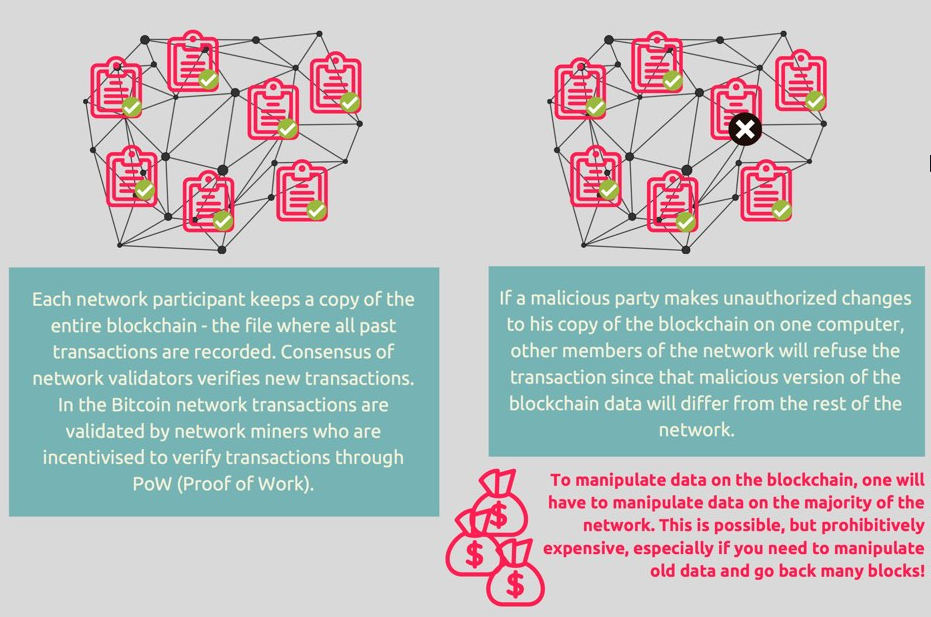
# Key Benefits

Blockchain is powerful for applications which focus on **Decentralization**, **Security** and **Trust**.

- **Decentralization:** Everyone who joins in the blockchain network have to download all the database and keep it up-to-date after a period of time (10 minutes in Bitcoin, 15 second in Ethereum). That means whenever there are new transactions, they have to update their ledgers to make them the same. There is no single point of failure in the network. Since someone ledger is lost or damaged, they can easily recover the ledger from the others. (**Robustness**)



- **Security:** When a user makes a transaction, they have to broadcast to all nodes in the network and put it in a block. After being validated by other nodes, the block is added into the database like a chain of blocks (that why it’s called Blockchain). At this time, everyone will update their own database and there is no way to change or remove the transaction have made (**Immutable**). If the database is not match with many other nodes, you will have to change the database to look like the others to be able to make transactions.



- **Trust:** Since everybody has a same database, users can access and check their transactions (**Transparency**). That means no one can change or tamper the data secretly. There is technique called [Merkle Tree](https://brilliant.org/wiki/merkle-tree/) to detect which block has been changed.

# Potential

* **Automotive:** Consumers could use the blockchain to manage fractional ownership in autonomous cars.
* **Financial services:** Faster, cheaper settlements could shave billions of dollars from transaction costs while improving transparency.
* **Voting:** Using a blockchain code, constituents could cast votes via smartphone, tablet or computer, resulting in immediately verifiable results.
* **Healthcare**: Patients’ encrypted health information could be shared with multiple providers without the risk of privacy breaches.

# References

<https://www.digitalpulse.pwc.com.au/wp-content/uploads/2016/07/PwC-What-is-blockchain-infographic.png>

<https://blockchainhub.net/blog/infographics/what-is-a-blockchain/>

<https://www.icicibank.com/managed-assets/images/blog/blockchain-infographic.png>

<https://blockgeeks.com/guides/what-is-blockchain-technology/>