**Introduction**

Blockchain technology has the potential to redesign how computational resources interact in an automated and decentralized society. This technology was invented by a person (or group of persons) named Satoshi Nakamoto in 2008 to be used as a public transaction ledger for a cryptocurrency called Bitcoin (reference\_1). On a high-level, the ledger is a self-governing list of records called blocks (reference) which are linked cryptographically using a hash algorithm. Each block is then connected to the previous block containing a timestamp and the transaction data. Here’s a high-level diagram to illustrate the transaction flow:

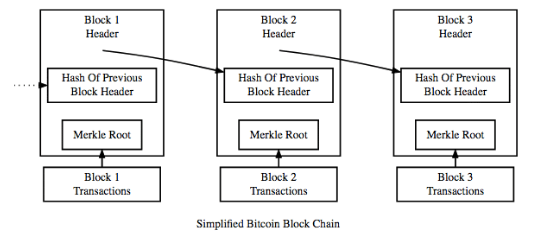


Figure 1 – Blocks linked to one another

**How does Blockchain Works?**

The following will use Bitcoin, a cryptocurrency, to explain how blockchain technology works – it is important to note that this framework can be used in non-finance related applications as well. Owner A wants to send his Bitcoin to Owner B – which in reality assigns Owner B’s identification to that specific transacted Bitcoin. For this to take place, the transaction is inserted as a ‘block’ which is then broadcasted to the peer-to-peer network for verification. If successful, the transaction will be recorded in a public ledger. These ‘blocks’ are all linked to one another (hence, Blockchain) in a linear and chronological sequence with every block containing the hash of the previous block (reference\_2) – shown in Figure 1. Refer the following diagram so visualize the flow of how a transaction is processed for Bitcoin:

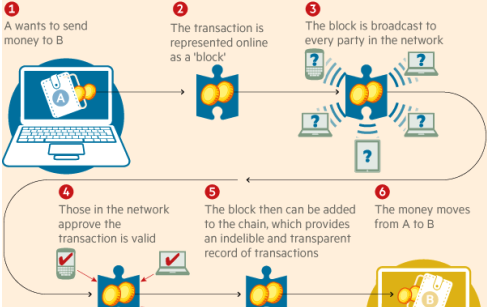


Figure 2 – Flow chart of Bitcoin Transaction

**What is a Cryptographic Hash Function?**

A cryptographic hash function protects sensitive information, either at rest or in transit. In the case of Blockchain, it prevents the double-spend problem (definition: the act of using the same coin more than once) from occurring with the use of public-key cryptography (reference\_4). A transaction is first initiated by future owner of the cryptocurrency by sending his public key to the current owner. The cryptocurrency is then transferred by the digital signature of a hash – the public keys (i.e. the assigned address of the cryptocurrency) are stored in the blockchain. In the case of Bitcoin, it utilizes a SHA-256 hash function which take an input of a random size and produces an output of a fixed size – pre-image resistant. What makes SHA-256 powerful is that it is nearly computationally infeasible to reconstruct a given input from the output value.

**Immutability of Blockchain**

Immutability is one of the most important (and defining) features of blockchain. As explored in the section above, blockchain is a one-way hash function making the records irreversible without community consensus. This eliminates reconciliations and establishes trust in the system (reference\_3). Only the owner of the record who has the proper credentials could make changes to the records.

**Industry Applications of Blockchain**

Since 2008, blockchain technology has been considered for many use cases outside of cryptocurrency (i.e. finance related). The following are industries where blockchain technology could be applied:

1. Insurance: With the use of a blockchain application called ‘Smart-Contracts (reference), insurance claims could be processed without the aid of an adjuster or physical inspection. Users would provide the information and the smart-contract would determine if it satisfies the criterions prior to distributing funds to the insured.
2. Internet of Things (IoT): There are new security vulnerabilities since these devices are sending and receiving data. Blockchain would add an additional layer of security insuring only the owner is receiving access and information of his IoT devices.
3. Healthcare: The encryption blockchain provides would be of importance to medical records, prescriptions, and supply management – offering extreme privacy.
4. Voting: Voter fraud could be prevented since a vote recorded in the blockchain would be immutable and would provide an audit trail if there is evidence of tampering. Since each voter would have his own lock and key, authentication of user would virtually be impossible to fake.

**Conclusion**

Although created for the financial world, the implications of Blockchain technology can affect applications in wide range of areas outside of finances. One of the main purposes of blockchain is to eliminate the need for an intermediary to verify and process a transaction – making it decentralized and distributed. The main objective is that the blockchain establishes a new standard and model by creating a distributed consensus in a digital world (reference\_2). In order to accomplish this, the designers made blockchain immutable and/or resistant to data modification – any change would require all subsequent blocks to be altered. Since these public ledgers are managed by peer-to-peer network (reference\_2), mass collaboration governs whether a transaction can be changed. This headwind hits directly at one of the central tenants of GDPR (reference\_5).

As one would expect, the supporters of blockchain believe the advantages of it outweigh the regulatory issues – the inverse applies for those who hold data privacy in higher regards. Before moving on to evaluating possible solutions that can satisfy both worlds, lets dive deep into GDPR.

Reference\_1 : <http://www.academia.edu/download/54517945/Bitcoin_paper_Original_2.pdf>

Reference\_2 : <https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf>

Reference\_3 : Olleros, F. , Zhegu, M. (2016) Research Handbook on Digital Transformation. Pilkington, M. (2016). Research on Blockchain Technology: Principles and Applications

Reference\_4 : <http://discovery.ucl.ac.uk/10043048/1/Aste_BlockchainIEEE_600W_v3.3_A.doccceptedVersion.x.pdf>

Reference\_5 : <https://jbba.scholasticahq.com/article/3554.pdf>