BLOCKCHAIN TECHNOLOGY

Created by Momdzhiyan Edward
Taganrog 2018

Contents

- Glossary
- Technology in Brief
- Blockchain Consensus Protocols
- Major problems with Blockchain
- Popular Applications of Blockchain Technology
- Bibliography

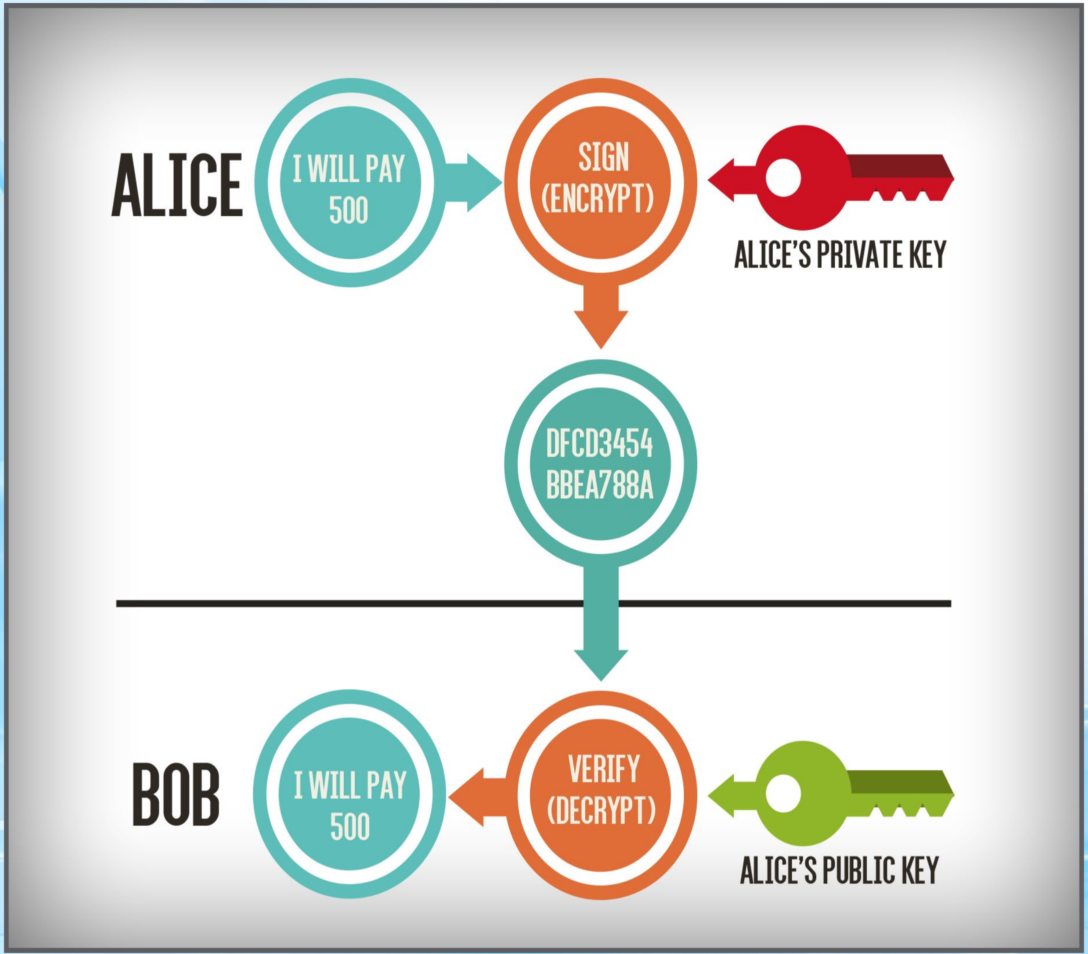
Glossary

Blockchain – It is a chain or records stored in the forms of blocks which are controlled by no single authority. A blockchain is a distributed ledger that is completely open to any and everyone on the network. Once an information is stored on a blockchain, it is extremely difficult to change or alter it.

Hash – it is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function which is infeasible to invert.

Cryptography keys – *public keys* which may be disseminated widely, and *private keys* which are known only to the owner. This accomplishes two functions: authentication, where the public key verifies that a holder of the paired private key sent the message, and encryption, where only the paired private key holder can decrypt the message encrypted with the public key.

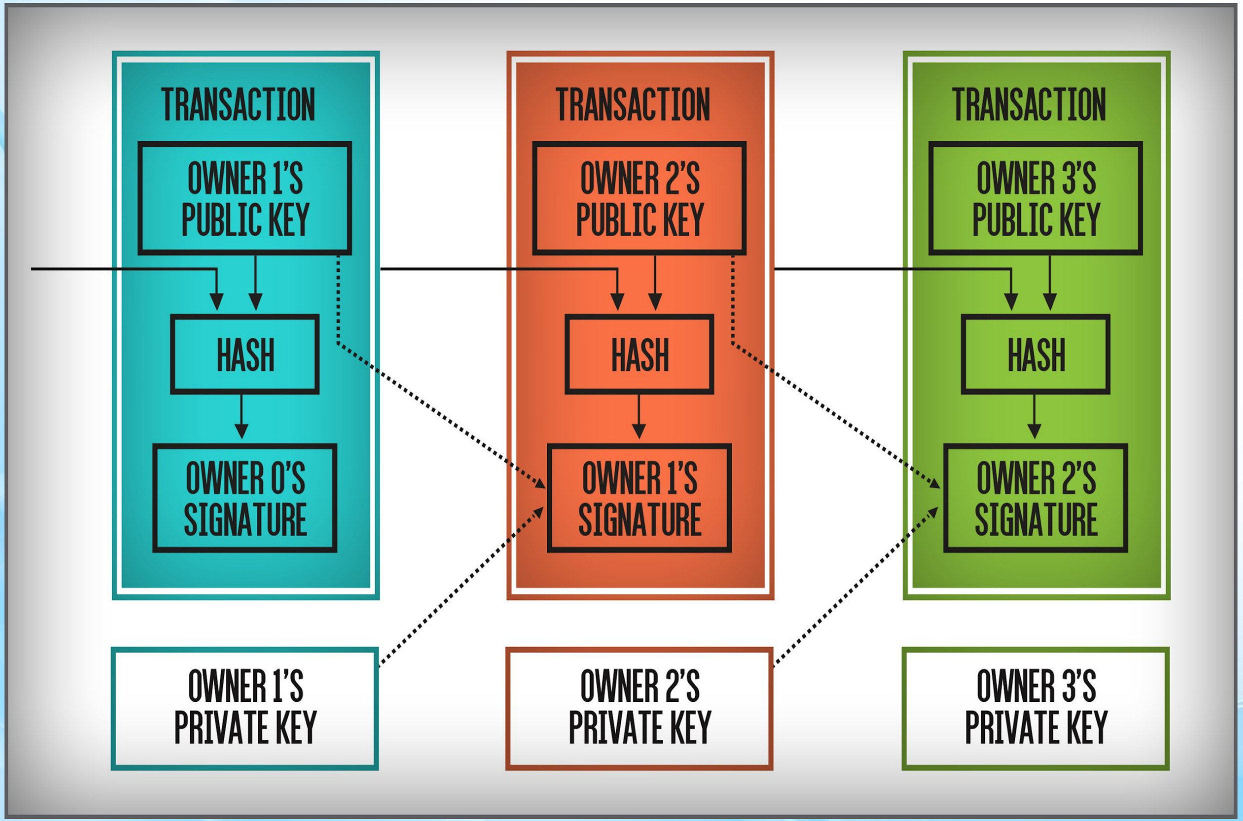
Technology in Brief



To begin, we need to explore the concept of “keys”. With a set of cryptographic keys, you get a unique identity. Your keys are the Private Key and Public Key, and together they are combined to give you a digital signature. Your public key is how others are able to identify you. Your private key gives you the power to digitally sign and authorize different actions on behalf of this digital identity when used with your public key.

In the cryptocurrency world, this represents your wallet address (public key) and your private key is what let’s you authorize transfers, withdrawals, and other actions with your digital property like cryptocurrencies. As an aside, this is why it’s so important to keep your private key safe — anyone who has your private key can use it to access any of your digital assets associated with your public key and do what they want with it!

Technology in Brief



Each block in a blockchain network stores this information along with the hash of its previous block. A hash is a unique mathematical code which belongs to a specific block. If the information inside the block is modified, the hash of the block will be subject to modification too. The connection of blocks through unique hash keys is what makes blockchain secure.

While transactions take place on a blockchain, there are nodes on the network that validate these transactions. In Bitcoin blockchain, these nodes are called as miners and they use the concept of proof-of-work in order to process and validate transactions on the network. In order for a transaction to be valid, each block must refer to the hash of its preceding block. The transaction will take place only and only if the hash is correct.

Technology in Brief

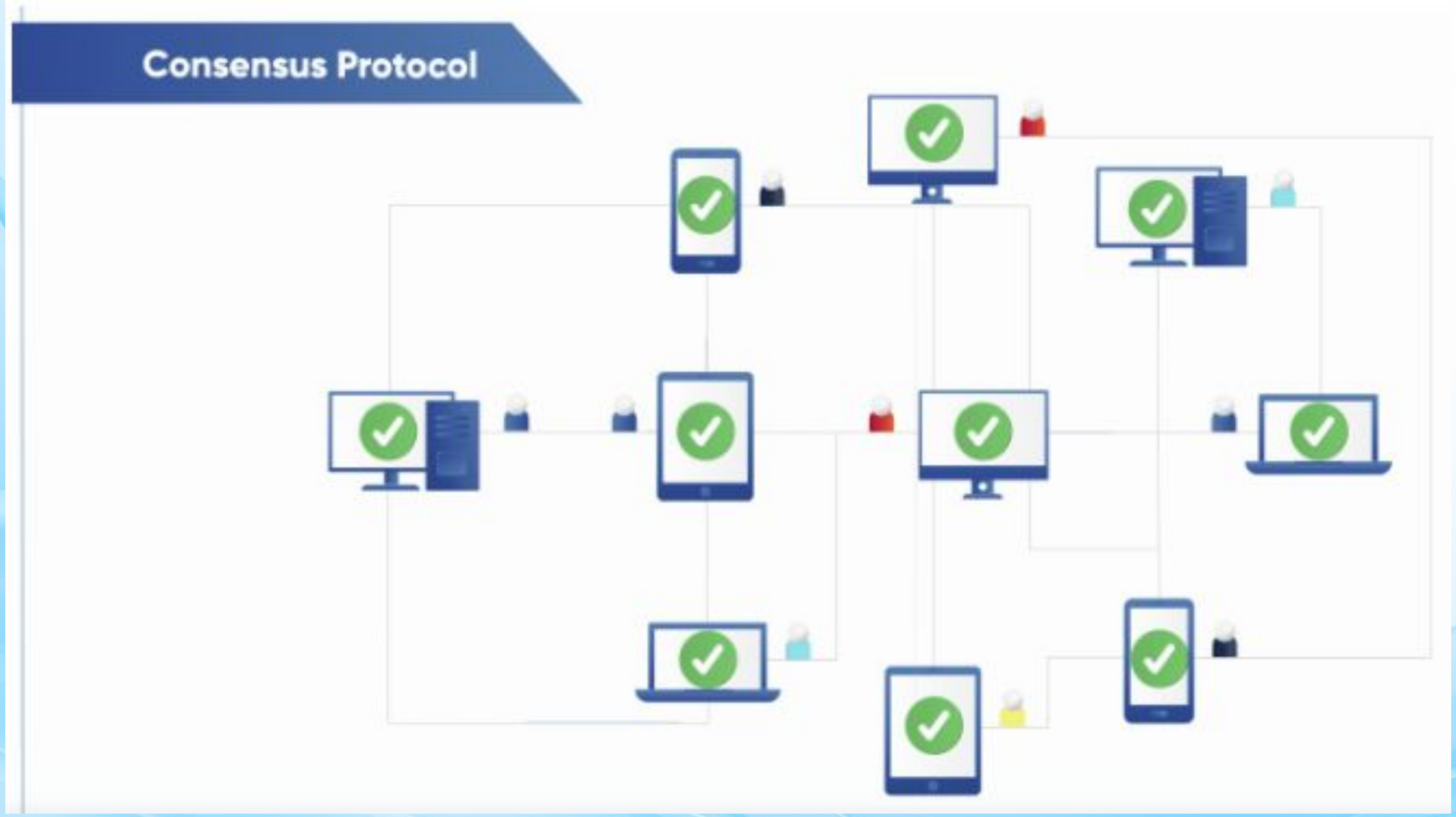
Blockchain features

Decentralised - Blockchains are decentralized in nature meaning that no single person or group holds the authority of the overall network. While everybody in the network has the copy of the distributed ledger with them, no one can modify it on his or her own. This unique feature of blockchain allows transparency and security while giving power to the users.

Peer-to-Peer Network - With the use of Blockchain, the interaction between two parties through a peer-to-peer model is easily accomplished without the requirement of any third party. Blockchain uses P2P protocol which allows all the network participants to hold an identical copy of transactions, enabling approval through a machine consensus

Immutable - The immutability property of a blockchain refers to the fact that any data once written on the blockchain cannot be changed. If you try to change the data of one block, you'll have to change the entire blockchain following it as each block stores the hash of its preceding block. Change in one hash will lead to change in all the following hashes. It is extremely complicated for someone to change all the hashes as it requires a lot of computational power to do so. Hence, the data stored in a blockchain is non-susceptible to alterations or hacker attacks due to immutability.

Blockchain Consensus Protocols

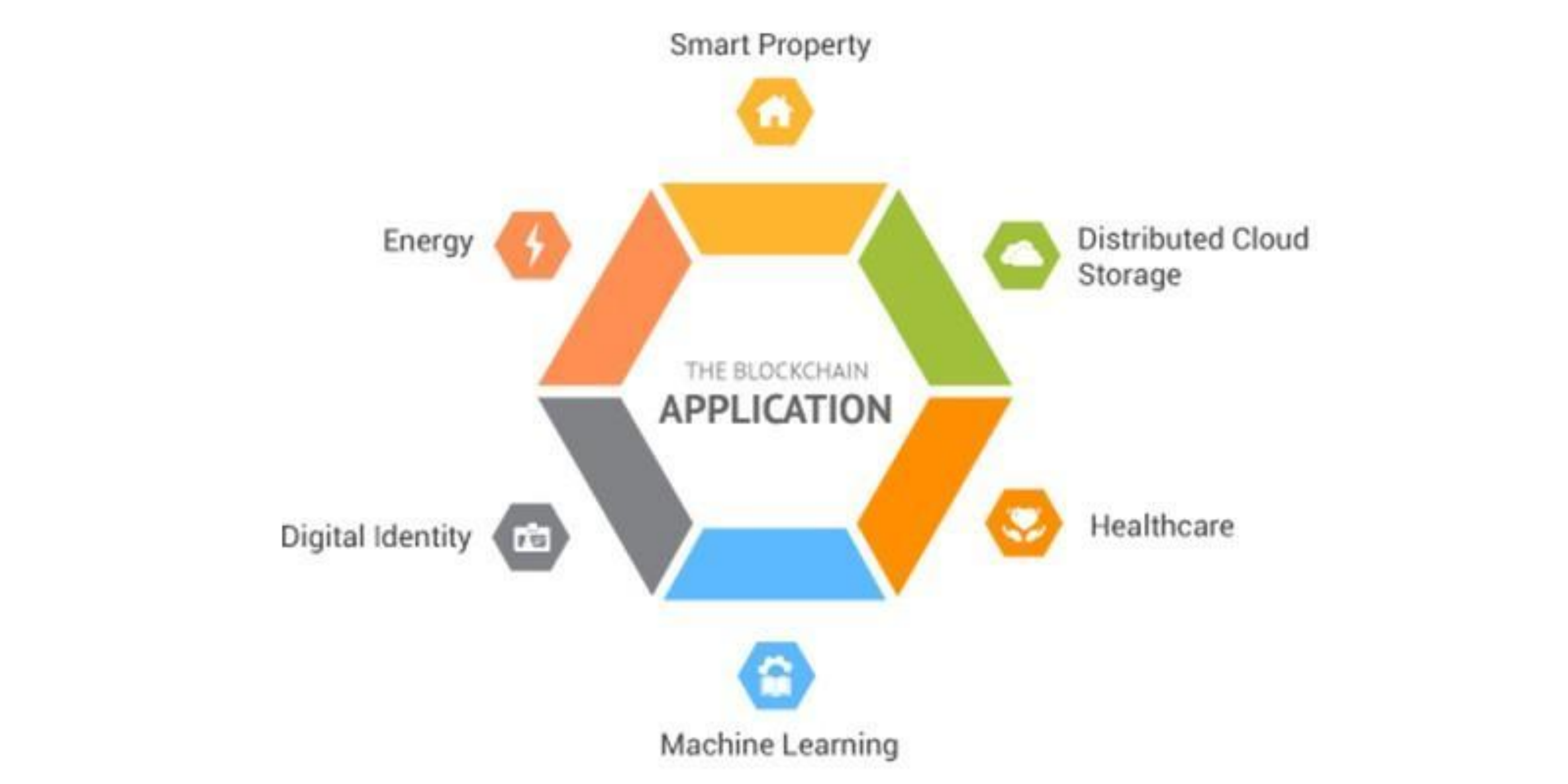


- Proof of work
- Proof of stake
- Proof of activity
- Proof of burn
- Proof of capacity

Major problems with Blockchain

- Blockchain has an environmental cost
- Lack of regulation creates a risky environment
- Its complexity means end users find it hard to appreciate the benefits
- Blockchains can be slow and cumbersome

Popular Applications of Blockchain Technology



- Cryptocurrency
- Smart contracts
- Government Elections
- Identity management
- Intellectual Property Protection

Bibliography

1. https://hackernoon.com/blockchain-technology-explained-introduction-meaning-and-applications-edbd6759a2b2
2. http://hackeducation.com/2016/04/07/blockchain-education-guide
3. https://www.investinblockchain.com/what-is-blockchain-technology/
4. https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#539f1a791670
5. *Jaikaran, Chris (February 28, 2018). Blockchain: Background and Policy Issues. Washington, DC: Congressional Research Service. Retrieved 2 December 2018.*