Edzo Botjes [Follow]

A Shrek look a like and loves Coffee, Roadtripping, Zen, IT, Enterprise Engineering, SMACT, Group Dynamics, Business & IT Innovation, Food & American Football

Aug 11, 2017 · 5 min read

Pulling the Blockchain apart.. The transaction life-cycle

Popping the hood of something magical

Unraveling what the blockchain is, how it works and what the benefits are is pretty difficult. It took me many weeks to only get a rough idea on what is going on.

Therefore I will share my journey and understanding, to help others to get a bit more knowledge on this subject. So that we will not get sold snakeoil when talking to a blockchain consultant.

The ideas behind the Blockchain is a combination of various complex idea's and systems. While this combination provides significant value, its consequent complexity makes it difficult to grasp in a short period of time.

The Web — Blockchain
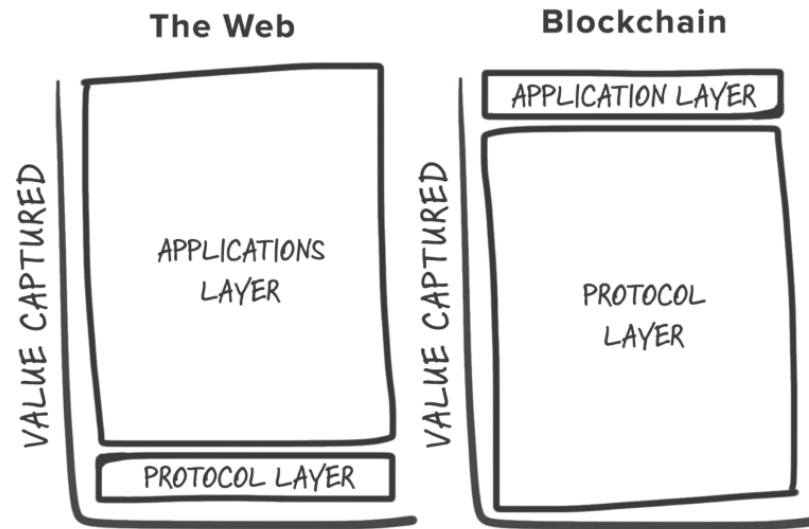
PULLING IT APART
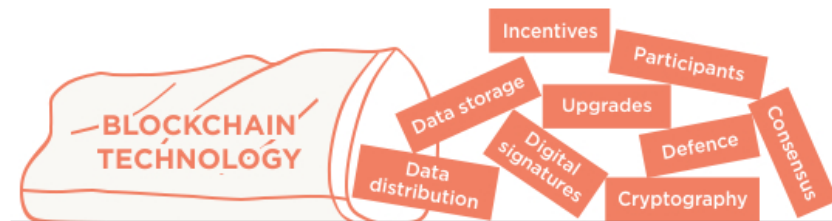
In the previous blog I stated that the blockchain is nothing more then a collection of transactions. Those transactions are sealt together in

packages of X number of transaction. Those packages are called blocks that are linked in a specific order, hence the name blockchain. A blockchain is comparable to a daisy chain :)

https://commons.wikimedia.org/wiki/File:Daisy_chain.JPG

To pull stuff apart it is important to know what the overall picture is, so that we can start pulling at the various parts of the whole. Lets start with looking at the life cycle of a transaction on a blockchain.

THE TRANSACTION LIFE CYCLE

Below we have a few Blockchain (and Bitcoin) transactions visualised.
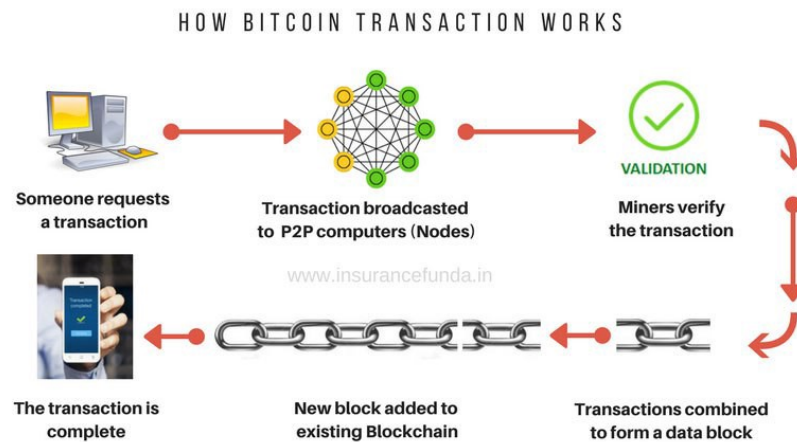
Overall the sequence of steps are;

1. Someone **Requests a Transaction** via something called a wallet.

2. **The transaction is send** (broadcast) to all participation computers in the specific blockchain network.

3. Every computer in the network checks (**validate**) the transaction against some validation rules that are set by the creators of the specific blockchain network.

4. Validated transactions are **stored into a block** and are sealt with a lock (hash).

5. This block becomes part of the blockchain when other computers in the network **validate** if the lock on the block is correct.

6. Now the transaction is part of the blockchain and can not be altered in any way.

In the following graphics the steps are illustrated and I have written down the steps also. You will see that everybody is using a different way of naming the steps but overall the content is the same.

Insurance Funda

HOW BITCOIN TRANSACTION WORKS

Someone requests a transaction

Transaction broadcasted to P2P computers (Nodes)

Miners verify the transaction

VALIDATION

www.insurancefunda.in

The transaction is complete

New block added to existing Blockchain

Transactions combined to form a data block

http://insurancefunda.in/bitcoin-cryptocurrency/

This is the most clear and easy to understand overview of the steps in the blockchain.

1. Someone requests a transaction

2. Transaction broadcasted to P2P computers (nodes).

3. Validation, miners verify the transaction.

4. Transactions combined to form a data block.

5. New block added to existing Blockchain.
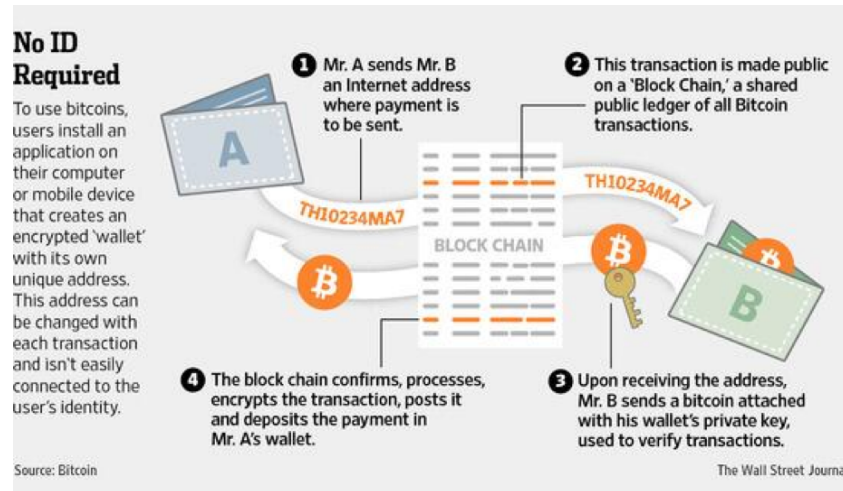
6. The transaction is complete.

Deloitte
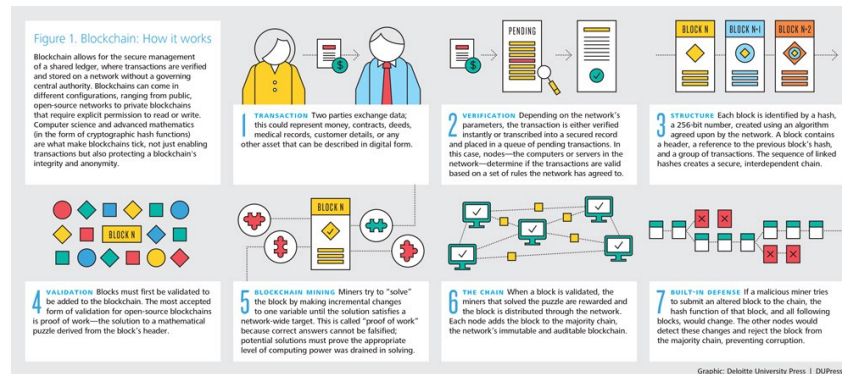
The image has a high resolution when you click on the source. The steps or elements depicted are

1. Transaction

2. Verification

3. Structure

4. Validation

5. Blockchain Mining

6. The chain

7. Built-in Defense.

Wall Street Analyst

No ID Required

To use bitcoins, users install an application on their computer or mobile device that creates an encrypted 'wallet' with its own unique address. This address can be changed with each transaction and isn't easily connected to the user's identity.

1 Mr. A sends Mr. B an Internet address where payment is to be sent.

2 This transaction is made public on a 'Block Chain,' a shared public ledger of all Bitcoin transactions.

TH10234MA7

BLOCK CHAIN

TH10234MA7

4 The block chain confirms, processes, encrypts the transaction, posts it and deposits the payment in Mr. A's wallet.

3 Upon receiving the address, Mr. B sends a bitcoin attached with his wallet's private key, used to verify transactions.

Source: Bitcoin

The Wall Street Journal

http://wallstanalyst.com/bitcoin-progression-towards-world-acceptance/

The description in this article is pretty clear. The steps identified here are.

1. Send payment destination address.

2. Payment destination address is published to the network for all to see.

3. Payment transaction is done securely from origin address to destination address.

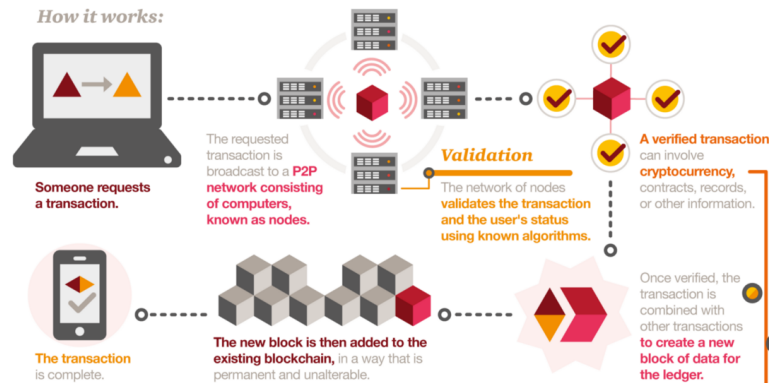4. The transaction is confirmed, processed and secured by the network and blockchain.
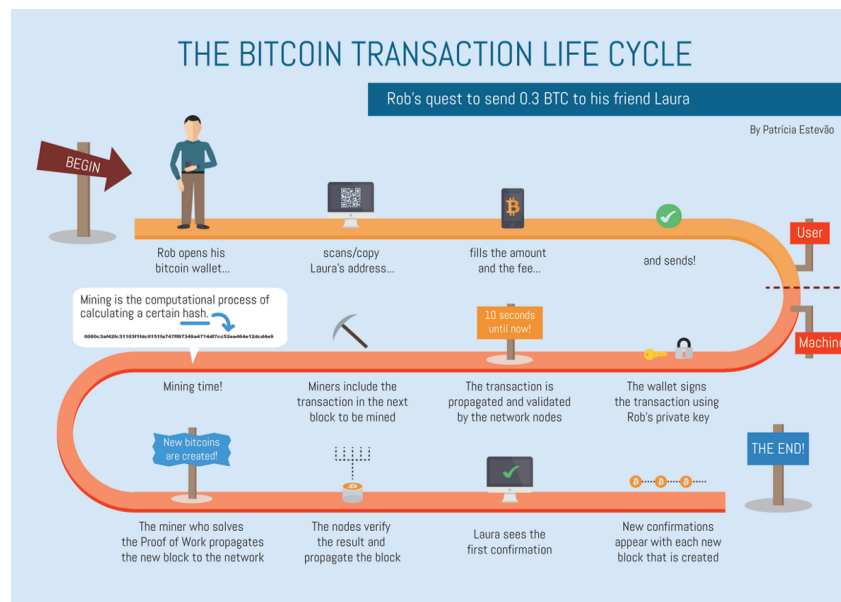
i-Scoop & Accenture

This image is a cut out from a larger infographic created by Accenture. The steps identified here are

1. Request of transaction is submitted to the network.

2. The transaction is validated by the network.

3. The verified transaction is combined with other verified transactions into a block in the blockchain.

4. Transaction is complete.

Bambora

THE BITCOIN TRANSACTION LIFE CYCLE

Rob's quest to send 0.3 BTC to his friend Laura

By Patrícia Estevão

BEGIN

Rob opens his bitcoin wallet...

scans/copy Laura's address...

fills the amount and the fee...

and sends!

User

Mining is the computational process of calculating a certain hash.

10 seconds until now!

Machine

Mining time!

Miners include the transaction in the next block to be mined

The transaction is propagated and validated by the network nodes

The wallet signs the transaction using Rob's private key

New bitcoins are created!

THE END!

The miner who solves the Proof of Work propagates the new block to the network

The nodes verify the result and propagate the block

Laura sees the first confirmation

New confirmations appear with each new block that is created

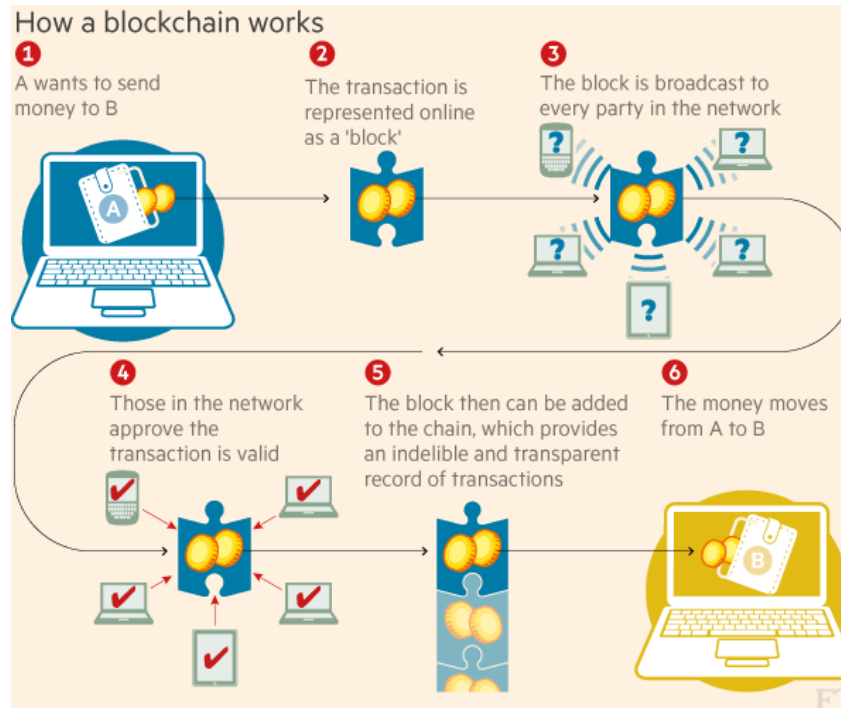https://www.bambora.com/en/ca/blog/bitcoin-explained/

1. Open your wallet and scan the address to which you want to send money.

2. Select the amount of money and send the transaction.

3. The wallet secures the payment so you know the sender of the money.

4. The transaction is validated by the network and made part of the mining process.

5. Mining is in progress and is done when a minder earns a bitcoin.

6. The network validates the result of the mining process.

7. The receiver of the money gets a confirmation of the successful transaction.

Techno Llama

How a blockchain works

1. A wants to send money to B
2. The transaction is represented online as a 'block'
3. The block is broadcast to every party in the network
4. Those in the network approve the transaction is valid
5. The block then can be added to the chain, which provides an indelible and transparent record of transactions
6. The money moves from A to B

http://www.technollama.co.uk/blockchains-and-the-challenges-of-decentralization
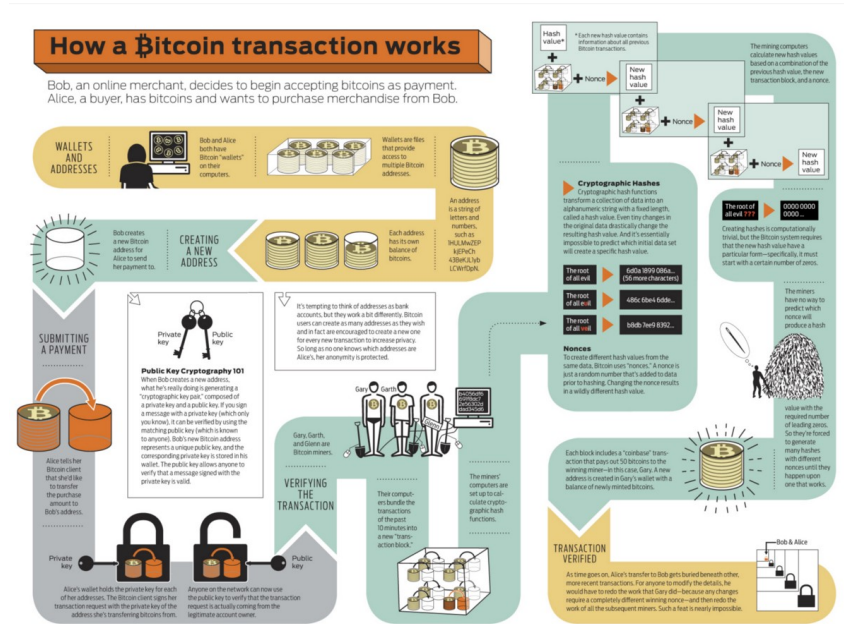
This blog is IMHO to abstract, but then this can also give new insights. The steps that are defined are.

1. There is intention to send money from A to B.

2. The transaction is put into a block.

3. The block is send to all members of the network.

4. The network validates the block.

5. The block is added to the chain.

6. The money is moved from A to B.

Zero hedge

This is a great roadmap, but to extensive for just someone without any knowledge to read.

1. **Wallets & Addresses**
   The sending and receiving party of the transaction have a wallet that contains addresses with money and can create new addresses when needed.

2. **Creating a new (receiving) address**
   create a new address for receiving the money for a transaction.

3. **Submitting a Payment**

   here the sender tells the wallet how much money is to be send to the receiving address and this is translated into a transaction.

4. **Verifying the transaction**

   in this step the transaction if being verified by computers in the network and bundled in transaction blocks

5. **Cryptographic Hashes**

   the blocks are locked together with cryptographic hashes.

6. **Transaction verified**

   The transaction is verified and part of the chain of blocks and therefor is it not possible to change this ever.