2018 Update

image credit: shutterstock.com

A brief introduction to Blockchain

October 24, 2013 | 2018 Update

by Sascha C. Röber

SMAC Consulting

Table of Contents

1 Blockchain: A distributed ledger

2 Tokens

3 Applications of Blockchain: Bitcoin

4 Crypto Currencies: A State of Affairs

1

Blockchain: A distributed ledger

Definition and Elements

Definition of a ledger

- A ledger is the principal book or computer file for recording and totaling economic transactions […], with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account. Source: wikipedia
- The special form of the distributed ledger in a blockchain is that every participant holds an updated and exact copy of this ledger and is distributed by the blockchain‘s algorithm.

Elements of a Blockchain transaction

- Sender ID
- Receiver ID
- Amount of transaction
- [Nature of transaction]

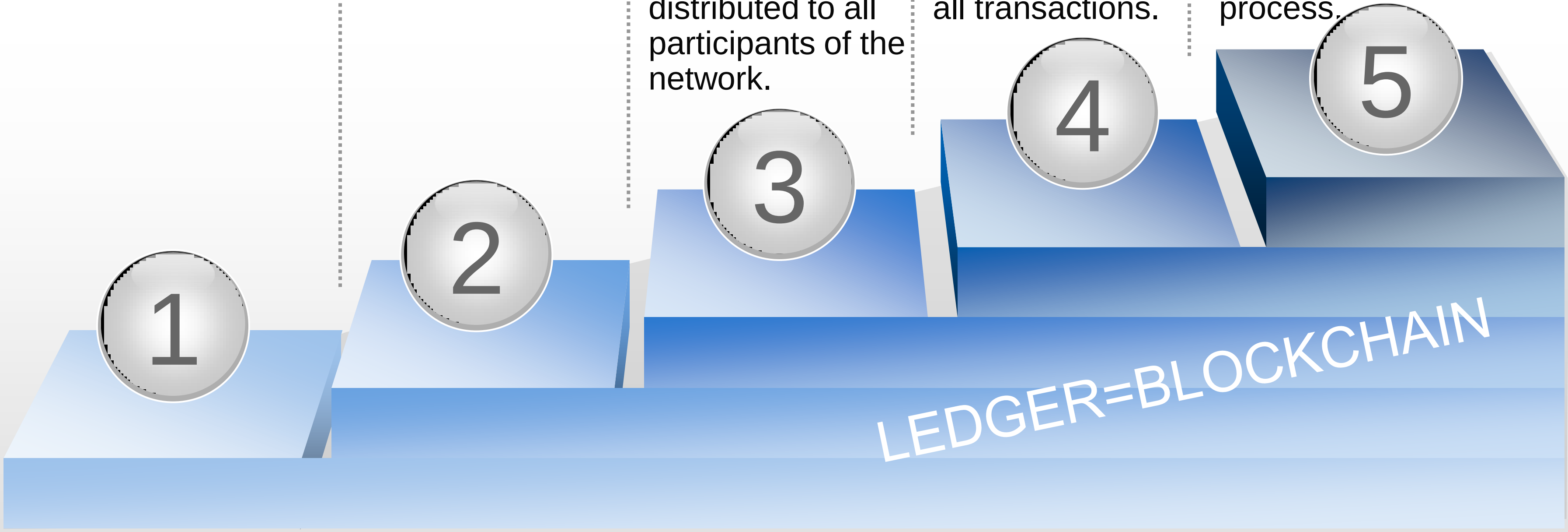
1

Blockchain: A distributed ledger

How the Blockchain is Built

The blockchain is a growing ledger containing all past transactions

Transaction 1	Transaction 2	Transaction 3	Transaction n-1	Transaction n
A transaction can be a transfer of funds from one person to another.	For each single transaction, a new entry is made in the ledger.	All entries are added to the ledger (= „block-chain“), which is distributed to all participants of the network.	Therefore, each participant has the same entire ledger containing all transactions.	The creation of a transaction is a mathematical and highly complex process.



The blockchain is a special form of a growing database.
Each participant of the network holds an exact copy of the entire blockchain.

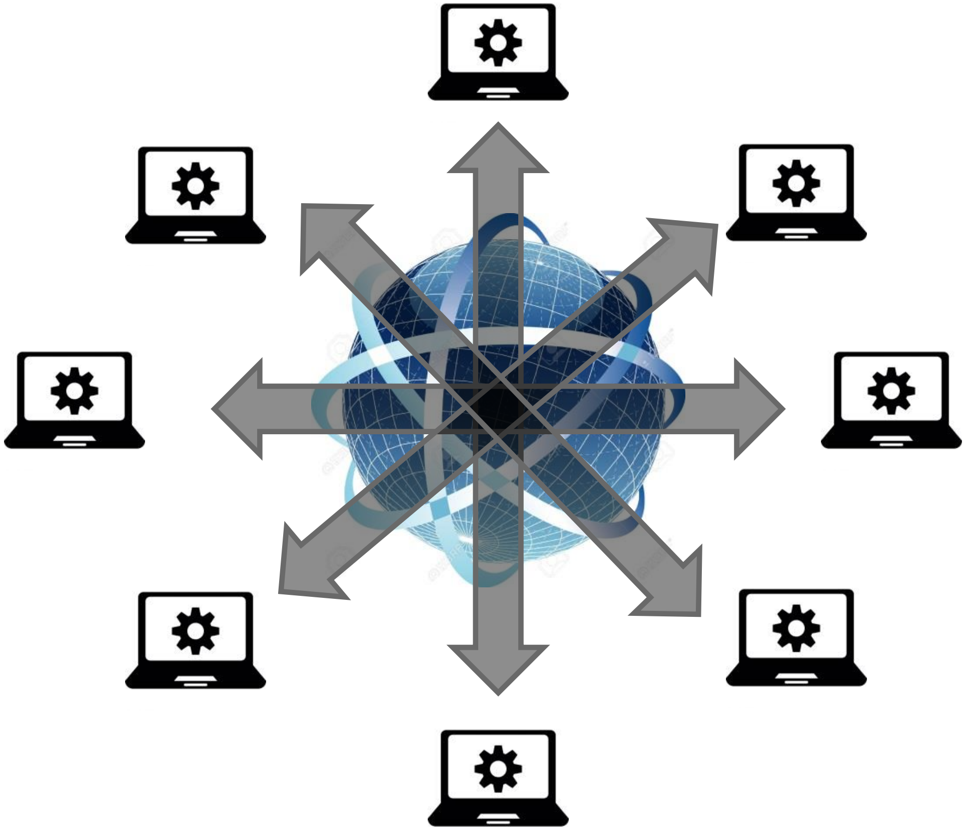
1

Blockchain: A distributed ledger

The Four Steps of the Blockchain

Four Steps

1. A new transaction ("block") is broadcast to the entire network
2. Every node (computer) verifies the new transaction based on an identical algorithm
3. When verfied as valid, the new transaction becomes the latest block in the blockchain (ledger)
4. The transaction is complete once the blockchain is updated.



SMAC Consulting

1 Why the Blockchain is Safe

The principles of hash values (1/3)

Hash Values are one way functions

Hash values are mathematical functions with a very helpful feature: They work only in one direction („one way functions“).

This means: The value of a function (algorithm) is easy to calculate, but it is extremely difficult, if not impossible to „reverse engineer“ the initial value.

Imagine it like the recipe for a lemon cake: It is easy to compose the cake‘s dough from various ingredients and bake it in order to have, as the end product, a delicious lemon cake. But it will be extremely hard to disassemble the cake and crack it down to separately receive its original ingredients (butter, milk, flour, sugar etc.).

1

Why the Blockchain is Safe

The principles of hash values (2/3)

Hash Values are deterministic

The algorithm to compute a hash value will always produce the exactly same result as long as the initial value is the same.

In other words, if the cake recipe is used without changing any of its ingredients and baking it for the exactly same length of time at the same temperature, the cake will be and taste just like the previous one.

There is, however, a major difference between the cake and the hash value of the blockchain: If you just add a teaspoon of addtional sugar to the original recipe, the new cake will just taste a bit sweeter, while just slightly changing the initial value of a hash calcuation, the resulting hash value will be **completely different**!

1

Why the Blockchain is Safe

The principles of hash values (3/3)

Hash Values are resistant to collision

This means that it is close to impossible to find two different initial values of any one given hash value. In other words, different initial values will not result in identical hash values.

1

Why the Blockchain is Safe

The application of hash values

The legacy of a block is handed down to its successors

Every single transaction, which is recorded in a blockchain, contains a **header** and a **body**.

While a block‘s body contains the details of a specific transaction (e.g. the transfer of bitcoin from one account to another), the header always also contains the hash value of its direct predecessor. So, every new block shares a bit of any of its predecessors‘ „DNA“.

In consequence, the modification of a single block‘s header would lead to a mismatch of all other blocks in the ledger as the tampered block would neither fit together with its predecessor and any of its successors would not fit with the tampered block.

This is why the blockchain technology is considered to be extremely safe.

2

Tokens

Definition and Types

The Distributed Ledger Technology (DLT) is built upon the use of digital assets (=Tokens). Tokens can represent values, rights, or claims.

At this time, there are three main types of tokens, i.e.

- Crypto Currency Tokens
- Utility Tokens
- Security Tokens

In the future, other types of tokens may be created as the blockchain technology evolves.

2 Tokens

Crypto Currency Tokens

Crypto Currency Tokens (CCTs) are used for effecting payment transactions within a specific blockchain network / universe.

Popular forms of crypto currency tokens are Bitcoin, Ethereum, Ripple, etc.

Many of these CCTs are traded via crypto exchanges. Most CCTs were created by software engineers or mathematicians, without the interference of a goverment, a central bank, or a regulator. So far, only the „Petro“ in Venezuela is a crypto currency issued by a government (in 03/2018).

2

Tokens

Utility Tokens

Utility Tokens (UTs) grant to their owners a form of a functional use.

The uses may vary from granting access to a specific network (which, at the time of issue of the UT may not even exist yet), to granting rights to receive certain services or products. In the latter form, the money spent on UTs can be used as seed financing. UTs may also grant rights under a contract.

UTs can also be issued to grant voting rights, for example to have a say over the design of certain products etc.

SMAC Consulting

Tokens

Security Tokens

Security Tokens (STs) are digital forms of securities.

There are abundant forms of securities in today‘s economies, such as bonds or shares. Such securities can also be digitalized and appear in the form of a blockchain. Their features are similar or equal to those regulated by the EU‘s MiFID II directive and can be debt or equity titles.

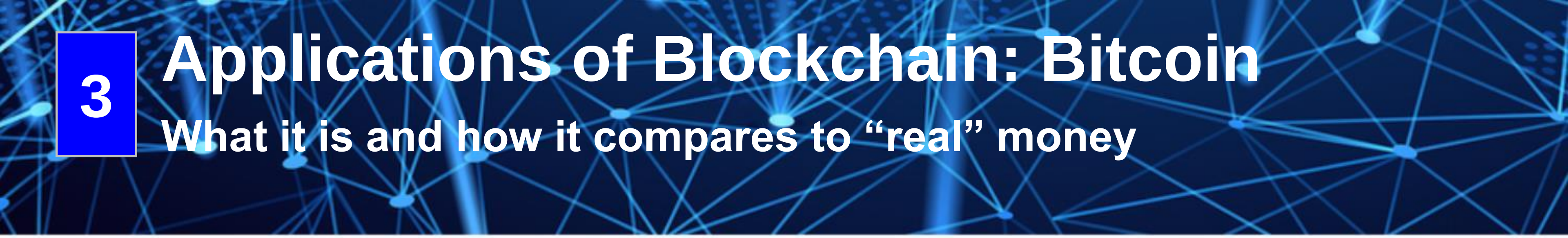
3

Applications of Blockchain: Bitcoin

What it is and how it compares to “real” money

What is Bitcoin?

- According to the Token types, Bitcoin is the archetype of a Crypto Currency Token.
- The Bitcoin system works “**permissionless**”. No state body or authority approves the creation of Bitcoins or the execution of a transaction. The algorithm alone is the “judge” of the system. Bitcoins as a crypto currency are not subject to politics or national laws.
- Bitcoin is a „**trustless**“ system. There is no federal or international body who has to be trusted in order to invest into or accept this currency for payment.
- Bitcoins are traded on a “**peer-to-peer**” basis. This means that there is no intermediary like a bank, whose technical infrastructure would be required to execute a transaction. Therefore, Bitcoin transactions work without paying commissions (unless traded thru internet platforms).
- Bitcoins are **safe from inflation**. Since only a predetermined number of Bitcoins can be mined, no uncontrolled multiplication of Bitcoins is possible.



3 Applications of Blockchain: Bitcoin

What it is and how it compares to “real” money

How does Bitcoin compare to physical money („fiat currencies“)?

- While you may have seen some actual coins with the Bitcoin symbol impregnated on them, these only serve as a factice and are for demonstration purposes only. Bitcoin is a 100% digital currency and only exists in the distributed Bitcoin ledger. You cannot touch Bitcoin.
- However, it has features of fiat money in as that there are thousands, if not millions of online traders and platforms willing to accept Bitcoin for payment. Especially in Asian countries (Japan, South Korea), Bitcoin and other crypto currencies enjoy widespread acceptance.
- Like other fiat currencies, Bitcoin‘s value is subject to change and volatility.
- However, the total number of Bitcoins which can ever cirulate was limited from its start in 2008. This is a major difference to regular currencies, which can be reproduced by mere decisions of central banks and / or governments.

3 Applications of Blockchain: Bitcoin

What it is and how it compares to “real” money

- The **mining process** (the creation of new Bitcoins within its limitations) gets more and more complex as the total number of Bitcoins mined increases. The algorithm for creating additional Bitcoins requires more time with ever new Bitcoin as the computations become incrementally more complex. While initially it was possible to mine new Bitcoins with regular desktop computers, now special hardware (mainly extremly fast graphics boards) is required. This is very expensive and energy consuming. If electricity does not get extremly cheap, mining will soon be more expensive than the value of the newly generated bitcoin.
- The ever growing size of the Bitcoin‘s distributed ledger increasingly slows down the **transaction speed**. While originally, the transfer of Bitcoins from one wallet to another took just fractions of a second, transactions nowadays can take hours before they get verified by the netword and added to the distributed ledger.
- The **value of Bitcoin has skyrocketed** towards the end of 2017 to prices of around USD 20,000, while currently it has come back to to approx. USD 6,800.

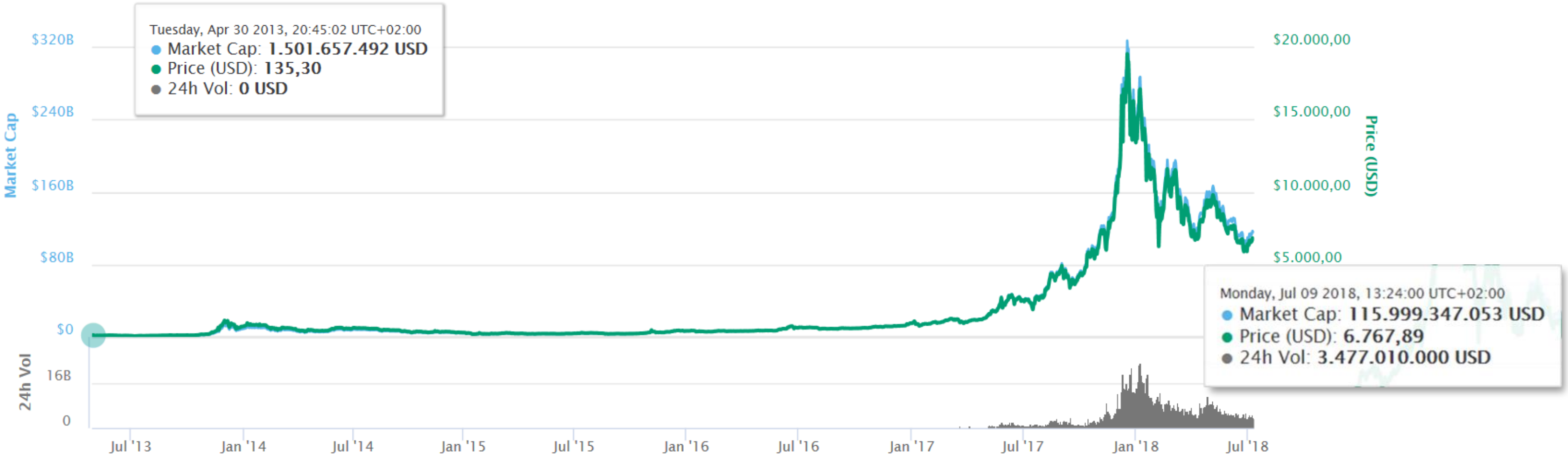
SMAC Consulting

3

Applications of Blockchain: Bitcoin

What it is and how it compares to “real” money

- Fears of a major investment bubble were the result. Especially small investors are likely to have lost massively following the steep price decline since early 2018.



- Unless the system receives a **major overhaul**, Bitcoin will soon lose all of its advantages over fiat money.

4 Crypto Currencies: A State of Affairs

- Almost all crypto currencies were and are being issued by **non-governmental bodies**, such as affiliated groups, individuals, or corporations.
- The **lack of control** over these Crypto Currency Tokens (CCTs) is becoming an increasing concern to central banks and governments around the world. Some countries are starting to impose regulations on CCTs. Especially China has been cracking down on CCTs and has recently forbidden ICOs and Bitcoin mining.
- The overall argument against CCTs in most countries is that so far, CCTs have been used mainly for **illegal activities** such as drug and weapons trafficking via the dark net. CCTs are not being recoreded in regular bank accounts, but by the underlying DL technology and, therefore, cannot be controled like funds flows from fiat currencies.
- In a counter move and with the objective of **cirumventing sanctions** imposed against its country, Venezuela‘s central bank launched an official crypto currency, the Petro, and has pegged it to the price of one barrel of BTI crude oil. Given its galopping inflation, Venezuela has been a heavy user of Bitcoin in the past years.

4 Crypto Currencies: A State of Affairs

- The **mining process** (the creation of new Bitcoins within its limitations) gets more and more complex as the total number of Bitcoins mined increases. The algorithm for creating additional Bitcoins requires more time with ever new Bitcoin as the computations become incrementally more complex. While initially it was possible to mine new Bitcoins with regular desktop computers, now special hardware (mainly extremly fast graphics boards) is required. This is very expensive and energy consuming. If electricity does not get extremly cheap, mining will soon be more expensive than the value of the newly generated bitcoin.
- The ever growing **size of the Bitcoin‘s distributed** ledger increasingly slows down the transaction speed. While originally, the transfer of Bitcoins from one wallet to another took just fractions of a second, transactions nowadays can take hours before they get verified by the network and added to the distributed ledger.

4 Crypto Currencies: A State of Affairs

- Bitcoin was the first crypto currency, but is by far not the only one. Meanwhile there will be hundreds, if not thousands of different crypto currencies. coinmarketcap.com is a platform showing the price developments of the 100 most traded crypto currencies. At this time, **Ehtereum and Bitcoin Cash** are most likely the two other most popular and known crypto currencies.
- An entire market of developers for crypto currencies and other blockchain tokens has developed around the initial idea of Bitcoin. Even market giants such as IBM have entered into the blockchain realm.
- First serious **capital market transactions** were based on the blockchain technology (e.g. in the German „Schuldschein“ market). However, none of them was based on crypto currencies given the lack of a safe „crypto to Euro conversion“.
- **There is still a far way for any crypto currency to be a full equivalent to any major fiat currency, such as USD, EUR, or YEN.**

A APPENDIX

- To practically understand the mechanism of hash values and transactions in a blockchain, you can visit a demo @ https://blockchain.adesso.ch/

About

(c) 2013/2018
SMAC Consulting
Sascha C. Röber
Frankfurt am Main
www.sascha-roeber.com

SMAC Consulting has no affiliation of any kind to adesso.ch or any other platform or company named in this presentation.