WITH ETHEREUM

BLOCKCHAIN TECHNOLOGIES

AJIT SINGH

BLOCK TECHNOLOGIES

First edition. June 14, 2019.

Written by Ajit Singh.

10 9 8 7 6 5 4 3 2 1

eBook Edition:

Produced by 
1827 Walden Office Square Suite 260,
Schaumburg, IL 60173, USA
Enquiries:
info@ebooks2go.net
www.ebooks2go.net

ePUB ISBN: 978-1-5457-4702-5

CONTENTS

Chapter 1

Introduction-Blockchain

This chapter introduces the blockchain data structure, the problem of its continual growth, a problem statement, delimitations, and relevant previous academic and industry e orts made to manage this problem.

Background

At the end of 2008, the alias Satoshi Nakamoto introduced Bitcoin [1], a peer-to-peer system hosting a cryptographic currency. The system was released to the public in early 2009, and soon became famous due to claiming and proving to be both trustworthy and decentralised, two properties previously considered almost being antonyms within the software community. The Bitcoin system has up until this day largely withstood the tests of time and scale, and has gone from globally processing about 100 transactions per day in 2009, to more than 200 000 at the time of writing [2].

The creation of Bitcoin was allegedly driven by an ambition to create a monetary system without a single regulatory entity, such as a central bank or clearing house. In the process, however, the feasibility of relying on multi-stakeholder consensus systems for applications where reliability is critical was clearly demonstrated. It was realised that the family of technologies that underpin the scalability and robustness of Bitcoin could be used to automate any kind of task where trust and negotiation is integral, a category of tasks previously assigned almost exclusively to humans. The blockchain data structure, even though not complex enough in itself to facilitate such trust automation systems, became the poster child of this novel combination of mostly familiar technologies.

It has been proposed, such as in [3], that blockchain technology could be used to create smart property, where device loyalty is determined by machine agents owned by multiple stakeholders, decentralised autonomous organisations, or other kinds of systems that traditionally would rely on a trusted middle-man.

Banks, traders, postal services, or other cooperating entities, could use blockchain systems to automate contract handling, trading of commodities, or tracing of assets. In short, blockchain systems could have the potential to replace human labour in domains where, generally, it was previously thought not to be feasible.

At the time of writing, there are already plenty of blockchain systems in varying levels of production, such as [1] [4] [5] [6]. These systems are, however, commonly suffering from some important scalability issues (e.g. [7]), among one is potentially significant storage requirements. The total size of the Bitcoin blockchain is well over 100 Gb [8], and has been growing exponentially since the system started in 2009. This stems from the fact that past transactions are used to prove the validity of future such. A sacrifice made in history held is also a sacrifice in system reliability, to some degree.

What is blockchain?

A blockchain is a decentralized, distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block. By design and by purpose blockchains are inherently resistant to modification of the data. Functionally, a blockchain can serve as ‘an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.’ [9]

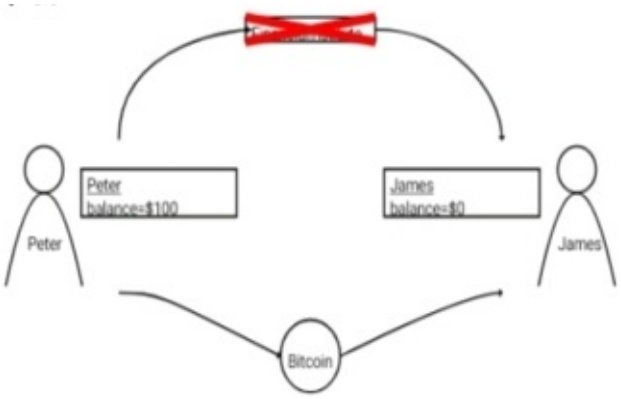

Figure 1.1: With blockchain a centralized third party is no longer needed

What does this mean and how does this work?
Well, lets take a crypto valuta like Bitcoin (for more information on Bitcoin

see subsection 3.1.1). The crypto valuta is built on blockchain so it doesn’t need a third ’authority’ (such as a bank) anymore.

Running Example 1

Peter wants to give $100 to James (see Figure 1.1).

Without blockchain

Peter would send his bank a request to send $100 of his account to his friends’ acount. The bank would check a few things like whether Peter actually has the $100. If everything checks out the bank will send Peters $100 to James’ account.

With blockchain

Peter creates a transaction of $100 to James and sends this transaction over the internet. This transaction is included in a block. All miners check whether this is a valid transaction. If it is, James has the $100 of Peter.

The Running Example on page 2 illustrates the use of blockchain. Instead of the transaction being checked by a third authority like a bank, it is being ’checked’ by everyone who takes part in the system and everyone who will join the system in the future. Thus releasing the need of a centralized third party, this has several advantages like less transfer costs (after all, there are no more man hours needed to check everything). It has the potential of being more anonymous while making it both easier to pay globally and nearly impossible to ’reverse’ transaction (which the third ’trusted’ party could decide to do).

All of this while maintaining the promise of the same certainty of getting your money as one would get from a Financial Institute.

Because blockchain is decentralized and distributed all current nodes and all future nodes to come can check whether every transaction follows some given rules. This makes sure someone can’t promise money to two people at the same time.

Removing the need of a third authority who has the monopoly on all the information and can make decisions which are very hard to check.

How can blockchain achieve this certainty of one getting their promised money, without a third party which checks this?

To answer this: let's continue the Running Example on page 2.

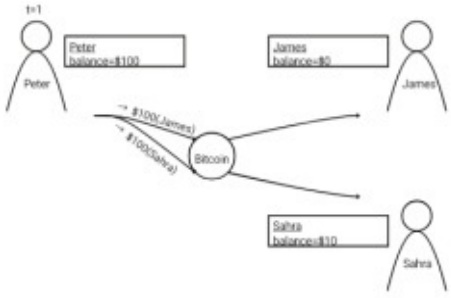

Figure 1.2: Peter promised his $100 to both James and Sahra!

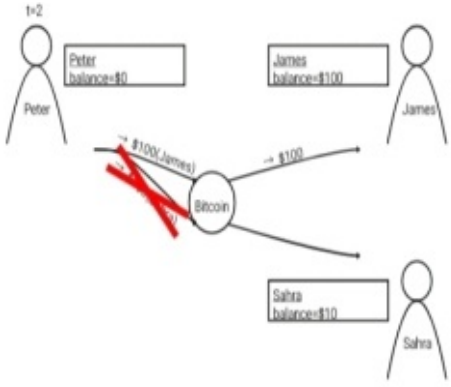

Figure 1.3: Blockchain checks this, and only the first promised, will receive the money Running Example 2

In Figure 1.2 Peter promised both James and Sahra his $100!

Since both promises are done in between the same two blocks, arbitrarily one of them is chosen to be included into the next block (say block number 433). This happens to be the promise toward James.

Now when block 434 is created (at time t=2 Figure 1.3) every node verifies that Peter does not have the required $100 anymore to give to Sahra. And thus Peters promise towards Sahra is not kept.

When James checks his balance, he sees that the promis Peter made to him has been kept.

This example shows that the order of blocks in the chain conclusively determines the order in which the transactions take place.

Blockchain is named that way because it is basically an endless chain of blocks. The order of this chain defines the order in which the transaction in the blocks took place. In Figure 1.4 an example of such a chain is given. The different colors indicate different 'types' of blocks. The chain 'grows' so to speak from bottom up. The first block is a special block, because it is the only block in the whole chain which has no preceding block. That's why it is the only one colored green.

The black blocks are the 'normal' blocks. These are the blocks which form the longest (and thus official) chain. The purple blocks form so called 'forks'. These form when two blocks are found at exactly the same moment. For a short moment in time there are two chains of equal length. Until for one of the chains a new block is found quicker than for the other chain it is undecided which of the two is the 'official' chain.

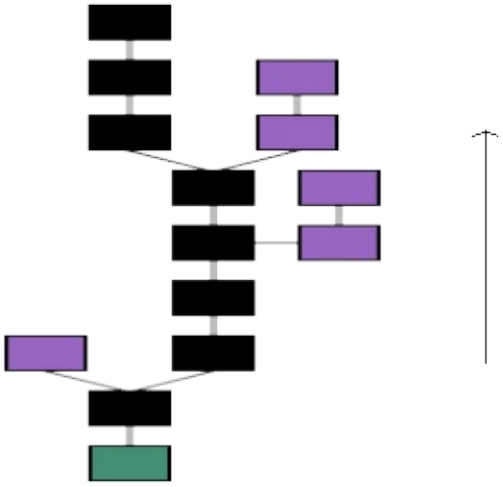

FIgure 1.4: An example of blocks in a chain

What problem does blockchain solve?

The creator of blockchain created blockchain with a very specific problem in mind to solve: the *double spending problem*.

> "What is needed is an electronic payment system based on cryptograhpic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms

> could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.”−Satoshi Nakamoto [6]

In other words: a growing problem in an ever more globalizing world is trust. People do business with people they have never met - and probably will never even meet face to face. How can you be sure the other person will pay you what he/she promised? And if he/she doesn’t, is there anything you could do against this? Or are you just gambling all your merchant wares? All sorts of authorities (like Pay-pall) have been brought into life to help solve these type of problems. But they do have the power to for instance reverse the payments made.

Blockchain solves all of these problems. Because the database is distributed, it is extremely transparent: everyone on this planet could check for him- or herself if all the rules have been followed until now.

There is no longer one party that can decide to reverse a payment: once a payment is done, it’s done.

Added bonus is that the blocks can’t be changed anymore because of the proof-of-work (section 2.3).

History of blockchain technology

Blockchain seemingly came up out of no where together with Bitcoin in 2013. Ever since it has been of interest to an increasing number of people. Currently a momentum around blockchain has been formed now the ’big four’ are investing in it . Chances are blockchain is going to be of growing importance in the future. Dubai is even planning on being ”the first blockchain powered government in the world by 2020” [22].

What path did blockchain follow before it so spectacularly appeared to the wider public? Both blockchain and Bitcoin are a creation of ‘Satoshi Nakamoto’. Until now it is unclear who this is, it could theoretically even be a group of people. He himself claimed to be a man living in Japan, born on 5 April 1975. However, there is still some doubt and quite some names have already passed as possible real identities [5].

In Nakamoto’s paper ‘*Bitcoin: A Peer-to-Peer Electronic Cash System*’ from 2008 he introduces Bitcoin to the world and explains how it works [6].

As with most inventions he used and combined many already present theories / techniques. Especially his encryption methods have been around for a while. For instance the way blockchain works with public and private keys stems

from a paper from 1980 by R.C. Merkle ”*Protocols for public key cryptosystems*”. A lot of the cryptology, and techniques that make blockchain so secure date from the 90-ies, as can be deduced from Nakamoto’s literature list [6].

According to some the only new part that sets blockchain apart is that every transaction is being hashed and carefully ’braided’ together with every new transaction [17].

Blockchain Versions

Blockchain 1.0: Currency

The implementation of DLT (distributed ledger technology) led to its first and obvious application: cryptocurrencies. This allows financial transactions based on blockchain technology. It is used in currency and payments. Bitcoin is the most prominent example in this segment.

Blockchain 2.0: Smart Contracts

The new key concepts are Smart Contracts, small computer programs that "live" in the blockchain. They are free computer programs that execute automatically, and check conditions defined earlier like facilitation, verification or enforcement. It is used as a replacement for traditional contracts.

Blockchain 3.0: DApps:

DApps is an abbreviation of decentralized application. It has their backend code running on a decentralized peer-to-peer network. A DApp can have frontend code and user interfaces written in any language that can make a call to its backend, like a traditional Apps.

Blockchain Variants

Public:

In this type of blockchains, ledgers are visible to everyone on the internet. It allows anyone to verify and add a block of transactions to the blockchain. Public networks have incentives for people to join and free for use. Anyone can use a public blockchain network.

Private:

The private blockchain is within a single organization. It allows only specific people of the organization to verify and add transaction blocks. However, everyone on the internet is generally allowed to view.

Consortium:

In this Blockchain variant, only a group of organizations can verify and add transactions. Here, the ledger can be open or restricted to select groups. Consortium blockchain is used cross-organizations. It is only controlled by pre-authorized nodes.

Limitations of Blockchain technology

- Higher costs: Nodes seek higher rewards for completing Transactions in a business which work on the principle of Supply and Demand
- Slower transactions: Nodes prioritize transactions with higher rewards, backlogs of transactions build up
- Smaller ledger: It not possible to a full copy of the Blockchain, potentially which can affect immutability, consensus, etc.
- Transaction costs, network speed: The transactions cost of Bitcoin is quite high after being touted as 'nearly free' for the first few years.
- Risk of error: There is always a risk of error, as long as the human factor is involved. In case a blockchain serves as a database, all the incoming data has to be of high quality. However, human involvement can quickly resolve the error.
- Wasteful: Every node that runs the blockchain has to maintain consensus across the blockchain. This offers very low downtime and makes data stored on the blockchain forever unchangeable. However, all this is wasteful, because each node repeats a task to reach consensus.

Challenges of blockchain

Despite it’s many useful properties, there is a need to make some cautionary remarks on Blockchain.

First of all ‘There is a tradeoff between performance and security with blockchain: faster blocks mean more forks mean less security.”[15]

CHALLENGES OF BLOCKCHAIN mining. Only when they receive a new block where the previous block is not the block they were working on will they know there was a fork. This means that for as long as it is unresolved which

part of the fork will be the ’final’ (black) chain, it is still not certain in what order the transactions will have taken place officially.

Example 3

Let’s say there are two blockchains: chain A and chain B, that find a new block every 10 minutes, 15 seconds resp.

A fork occurs when two blocks are found within lets say a second. Furthermore the assumption is made that the distribution of the time between two blocks found is exponential. Some simple math will show that chain B has many more forks:

<u>Chain A</u>

$X \sim Poisson\left(\frac{1}{10 \times 60}\right)$ *= the number of blocks found in one second*

$$\begin{aligned}\mathbb{P}(X > 1) &= 1 - \mathbb{P}(X = 0 \text{ or } X = 1) \\ &= 1 - \Big(\mathbb{P}(X = 0) + \mathbb{P}(X = 1)\Big) \\ &\approx 1 - \Big(0,999998613\Big) \\ &\approx 0,00000138735\end{aligned}$$

<u>Chain B</u>

$Y \sim Poisson\left(\frac{1}{15}\right)$ *= the number of blocks found in one second*

$$\begin{aligned}\mathbb{P}(Y > 1) &= 1 - \mathbb{P}(Y = 0 \text{ or } X = 1) \\ &= 1 - \Big(\mathbb{P}(Y = 0) + \mathbb{P}(Y = 1)\Big) \\ &\approx 1 - \Big(0,997874117\Big) \\ &\approx 0,002125883\end{aligned}$$

For both chains the probability of a fork is very small. However chain B has rougly 1532 times more probability of a fork than chain A.
