Block Chain Use Cases

Master-Thesis von M. Rameez
Tag der Einreichung:

1. Gutachten: Gutachter 1
2. Gutachten: Gutachter 2
Betreuer: Rachid El Bansarkhani

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Abstract

In this paper, I explore different blockchain technologies and how they can be exploited for several use case scenarios. My main focus is finding use cases from the fields of Supply Chain Management, Internet of things, File Sharing and Machine to Machine. First, a general introduction of the blockchain is presented. Then, I discuss Ethereum and Smart contracts and how it differs in comparison to Bitcoin. I highlight some of the challenges facing blockchains today i.e. the scaling problem, and the transaction finality issue. Next, I look at possible solutions proposed to tackle these problems i.e. Payment Channels and State Channels. A possible extension to one of these solutions in the form of virtual channels and Perun is explored next. Finally, I explore several use case scenarios of blockchains in industry and how they are revolutionizing them in each case.

Contents

1. .... Introduction 3

2. .... Smart Contracts and Ethereum 3

2.1. Ethereum 3

2.2. Smart Contracts 3

3. .... A case for payment channels – blockchain scaling 4

3.1. Scaling debate 4

3.2. Payment channels – Lightning network 4

3.3. State Channels – Raiden Network 4

3.4. Virtual channels – Perun Network 5

4. .... Use case Scenarios of BlockChain 6

4.1. Internet of Things 6

4.2. Supply chain Management 7

4.3. File sharing 9

References 10

1. Introduction

"*Blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block contains typically a hash pointer as a link to a previous block, a timestamp and transaction data*" [1]. A blockchain can serve as a distributed ledger that can record transactions. The transactions stored on it are available to all parties and are easily verifiable. They are inherently resistant to data tampering as altering data in any one block breaks the chain and requires that all subsequent blocks be calculated again using the new data. Blockchain has the power to revolutionize how business is conducted in digital age. Some are calling it the most important innovation since the development of the internet. The first blockchain Bitcoin was invented by a person or a group of persons known only as Satoshi Nakamoto. Bitcoin is designed as an online digital currency i.e. mechanism to transfer value between two parties without involving any third parties e.g. banks or other financial and regulatory institutions. It was the first to solve the double spend problem in digital currency. Bitcoin paved the way for exponential growth in crypto currency market which together with other alt coins is worth over 120 billion dollars. The underlying technology which powers Bitcoin, Ethereum and other crypto currencies can be used for much more than just transferring X amount of crypto from Person A to Person B. Researchers are employing blockchain technologies to increase efficiency and reduce costs in industries such as Supply Chain Management, Networking and Internet of things, Banking and Finance. In this report I will look at some of the industries and business processes they are revolutionizing. I present several use cases from the fields of IoT, Supply chain Management and Distributed and decentralized cloud storage.

2. Smart Contracts and Ethereum

2.1. Ethereum

Ethereum is defined as *"an open-source, public, blockchain-based distributed computing platform featuring smart contract (scripting) functionality. It provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes"* [2]. It has its own programming language called solidity. Ethereum is special because each block in the chain represents a state in a virtual machine. Ethereum is Turing complete meaning it can be programmed to solve any computation problem.

2.2. Smart Contracts

"*Smart contracts are computer protocols intended to facilitate, verify, or enforce the negotiation or performance of a contract*" [18]. They allow us to automatically exchange goods and services be it money, property, shares or anything of value in a conflict-free way avoiding middlemen. Smart contracts have been called one of the killer applications of the blockchain. Smart contracts can be used in all sorts of scenarios like financial services, crowd funding (ICOs), credit enforcements etc. Consider the following example [19] which will demonstrate smart contracts in action.

Example

"*Suppose you rent an apartment from me. You can do this through the blockchain by paying in cryptocurrency. You get a receipt which is held in our virtual contract; I give you the digital entry*

key which comes to you by a specified date. If the key doesn't come on time, the blockchain releases a refund. If I send the key before the rental date, the function holds it releasing both the fee and key to you and me respectively when the date arrives. The system works on the If-Then premise and is witnessed by hundreds of people, so you can expect a faultless delivery. If I give you the key, I'm sure to be paid. If you send a certain amount in bitcoins, you receive the key. The document is automatically canceled after the time, and the code cannot be interfered by either of us without the other knowing, since all participants are simultaneously alerted" [19].

3. A case for payment channels – blockchain scaling

3.1. Scaling debate

Blockchain technology is still in its infancy. It is a novel idea to solve several interesting problems in a trustless and decentralized manner, however in order to compete with existing centralized platforms it needs to be able to scale to handle millions of transactions per second. Let us consider the use case where the block chain is used to make payments or transfer assets between users. Bitcoin can on average perform 3 to 4 transactions per second while Ethereum can handle up to 20 transactions per second. Compare this to Visa which on average handled over 1100 transactions per second in 2016 and has an estimated capacity to perform up to 100000 transactions in a second. The scaling problem is further amplified when we consider that Ethereum blockchain aims to be a platform for decentralized apps or dAPPs. In order to efficiently run dAPPs it needs to be able to handle so called nanotransactions. In most cases these nanotransactions need to be executed immediately and cannot wait for long block confirmation times. According to some estimates using current mechanisms *"we're roughly 250x off being able to run a 10m user app and 25,000x off being able to run Facebook on chain"* [3].

3.2. Payment channels – Lightning network

Lightning network is bitcoins proposed solution for the scaling problem. It advocates using payment channels to handle transactions off chain. *"Payment Channel is class of techniques designed to allow users to make multiple Bitcoin transactions without committing all of the transactions to the Bitcoin block chain. In a typical payment channel, only two transactions are added to the block chain but an unlimited or nearly unlimited number of payments can be made between the participants"* [4]. Simply put, a payment channel is a smart contract on the blockchain which is mostly executed off-chain after creation. In an ideal case, the two transactions that go on the block chain are the ones for opening and closing a channel. *"Security is enforced by blockchain smart-contracts without creating an on-blockchain transaction for individual payments. Payment speed measured in milliseconds to seconds"* [5]. This enables users to make off chain payments with confidence. If anything goes wrong blockchain can cryptographically verify the terms of the smart contract and enforce them on-chain. A good explanation of how this works technically can be found in this video [6].

3.3. State Channels – Raiden Network

Raiden network aims to solve the same scaling problem for the Ethereum blockchain. It uses State channels to perform transactions off chain. "*State channels are the general form of payment channels, applying the same idea to any kind of state-altering operation normally performed on a blockchain*" [6]. State Channels significantly enrich the functionality of payment channels. Consider **C** [11] which is a smart contract inside a state channel executed

by the users of the channel in an off chain way. This is achieved by letting channel state contain storage string õ as well as financial balance. Where õ describes the current state of **C** by storing values of all contract variables. As long as there is no conflict all parties can freely update õ. In the event that one of the users misbehaves the others can push the latest version of õ on the blockchain which will finish executing **C** starting from the latest agreed upon state i.e. õ. Please refer to [7] and [8] for detailed explanations on how this concept works. A brief summary based on [7] is given below.

1. Part of the state of blockchain is locked in a multi signature address, all participants must agree in order to update this state.
2. Instead of submitting updates to the blockchain participants update the state between themselves.
3. Each new fully signed update overwrites the previous one and is the only valid state for the channel that can be pushed on the blockchain.
4. In the event of a disagreement any participant can push the last fully signed state to the blockchain.
5. If nothing goes wrong participants submit the final state to the blockchain which closes the channel.

For greater technical understanding of how State Channels are implemented in the Raiden network please refer to [9] and [10].

3.4. Virtual channels – Perun Network

Lightning network introduced the concept of payment channels that allowed Off–chain transfer of tokens between two entities. Payment channels are realized using smart contracts on the block chain. Raiden Network introduces the concept of state channels which allow users to execute smart contracts within the channel in an off-chain manner. Both of these proposals call for creation of so called payment networks where by channels are linked together via a mechanism called “Payment Routing”. Informally this method calls for routing payments or transactions over chains of multiple channels linked together using “hash locked transactions”. Payment routing schemes require third parties or intermediaries to execute every single transaction between two unknown or unconnected users in the network. Perun offers a new technique for connecting channels which does not require interaction with intermediaries for every single update of the channel. In fact, in most common case when all parties are honest the only interactions with the intermediary would be made for opening and closing of the channel. Perun constructs a new primitive called virtual channels over so called multistate channels. Multi state channels are an extension of state channels presented in the Raiden network. Multistate channels allow for parallel creation and execution of several Nano contracts. Technical description for creating, updating, and closing multistate channels is given in section 4.2 of [11]. The scheme presented in Perun claims to be secure against arbitrary corruption of any of the communicating partners or intermediaries. In this scheme basic channels are connected via “virtual channels” which minimize interaction with intermediaries in channel chains. Consider an example where Alice and Bob establish a channel with each other with the help of intermediary Ingrid. In the case when they are honest each update to the channel can be made independent of Ingrid and the only interaction that involves Ingrid is for opening and closing of the channel. In the event that a dispute arises between Alice and Bob, they first try to resolve the dispute with the help of

Ingrid. Technical details of dispute resolution with the help of Ingrid are described in sections 4.3.2 and 4.35 of [11]. If that fails, then the dispute resolution is escalated to the block chain.

4. Use case Scenarios of BlockChain

4.1. Internet of Things

IoT is the next wave of automation promising to transform industrial and domestic lifestyles. The billions of smart devices coming online could transform homes, cities, offices and factory floors. "*IoT holds the promise to expand business processes and to accelerate growth. However, the rapid evolution of the IoT market has caused an explosion in the number and variety of IoT solutions, which created real challenges as the industry evolves, mainly, the urgent need for a secure IoT model to perform common tasks such as sensing, processing, storage, and communicating*" [12]. Currently IoT ecosystems are realized using brokered communication models based on client/system paradigm. Devices are connected through cloud servers using the internet even if they are few feet away from each other. Further more centralized models struggle to scale up to meet the demands of billions of users or devices. Blockchain offers an intriguing alternative as it is built for decentralized control. A solution based on blockchain should be more scalable then a traditional one. Blockchain is inherently resistant to data tampering hence it will prevent a rogue device from disrupting a home, factory or a transportation system. Two use case scenario examples are given below.

Smart Washing Machine

This example is described in [13]. "*Imagine a washer that autonomously contacts suppliers and places orders when it's low on detergent, performs self-service and maintenance, downloads new washing programs from outside sources, schedules its cycles to take advantage of electricity prices and negotiates with peer devices to optimize its environment*". If the machine is connected to some sort of ledger be it private or public, it can automatically pay the detergent suppliers and repairmen.

IoT enabled package transfers

This use case is described in [14]. Imagine a company orders a sensitive package for one of their suppliers. The business contract stipulates some guarantees about delivery time, and the conditions under which the package needs to be handled for example at no point should the package be exposed to temperatures above a certain threshold. The package will pass through multiple carriers. The IoT enabled package has embedded sensors to monitor package conditions throughout its journey from supplier to the factory floor. The sensor data is communicated from the package to a blockchain enabled smart contract. All parties have access to the same data. In the event that temperature target is acceded the smart contract will be triggered automatically and the responsible party in the supply chain will be charged with damages stipulated in the contract.

Blockchain in IoT sphere has the potential to revolutionize several industries and businesses. There are several exciting projects working towards this goal. Sections 5.1.1 and 5.1.2 describe two projects at the forefront of blockchain and IoT.

4.1.1. Adept

One proposal to connect Iot using blockchain is a project called Adept. It is joint venture between IBM and Samsung. They envision network of devices that are capable of autonomously maintaining themselves. Adept is working towards integrating IBMs Watson IoT platform with blockchain technologies. It is currently still in development stage but proof of concept has already been implemented ad described in [15]. It uses blockchains as the backbone of the system using a mix of proof of work and proof stake to secure transactions. The ADEPT architecture supports three foundational functions.

1) Peer to Peer encrypted messaging
   It uses a secure messaging protocol called TELEHASh.
2) Decentralized File Sharing
   For software updates, analytics reports etc this is achieved using Bittorrent protocol.
3) Decentralize device coordination and control
   In the absence of centralize controller device control and coordination becomes significantly challenging, it is using Ethereum blockchain to implement this in a trustless secure fashion.

Ultimately it will enable IoT devices to send data to private blockchain ledgers for inclusion in shared transactions with tamper-resistant records. Devices will be able to communicate with the blockchain in order to update or validate smart contracts. "*All business partners can verify each transaction, preventing disputes and ensuring each partner is held accountable for their individual roles in the overall transaction." [16]*

4.1.2. Filament

Filament is a technology stack that "*enables devices to discover, communicate, and interact with each other in a fully autonomous and distributed manner*" [17]. It is specifically targeting industrial internet of things. "*The Filament technology stack is built upon five key principles: Security, Privacy, Autonomy, Decentralization, and Exchange (SPADE)"* [17]. Filament uses **Telehash** for secure encrypted device to device communication. Secure Identity is provided by blockchain. Once a secure communication channel has been established between devices smart contracts are used to interact with them, or to enable them to transact with each other. Smart Contracts in Filament run directly on device and accept or run transactions from other devices based on contractual terms. It uses a protocol suite called "**JOSE**" (Javascript Object signing and Encryption) to implement smart contracts on the devices. In order to enable micro transactions on these embedded devices authors of the Filament project propose a solution called Penny Bank. It allows the devices to exchange small amounts of value with one another offline or online without involving the blockchain for every single transaction and avoiding heavy transaction fees.

4.2. Supply chain Management

Blockchains allow secure and permanent documentation of transactions in a decentralized ledger. They can be monitored transparently by all parties. This can improve efficiency and reduce human mistakes and time delays. It can also enable users to verify authenticity of products by tracking them from their origin. An example of this is securing supply chains of diamonds from mine to consumers. IBM hyperledger is one of the proposals working in this field. It is designed especially for handling supply chain management. Using blockchain

technologies customers can verify when and where a diamond was mined, all the places it passed through during its journey to the retailer, and whether or not during any step of the supply chain it crossed any moral or legal grey areas i.e. if it's a blood diamond.

4.2.1. SkuChain

Sku chain is a platform that uses blockchain to provide security, efficiency and transparency to supply chains. Today's supply chain management tools such as ERP systems, Inventory Management systems, Letters of credits, Purchase and Invoicing tools have significant friction and problems interfacing with each other. This causes delays and have costs associated with these delays. SKuchain proposes tools in order to resolve some of these issues.

IMT

"*IMT provides inventory financing that de-risks transactions and unlocks capital opportunities for the entire supply chain. The original contract between the buyer and seller is assigned to IMT in the blockchain. This acts as a Blockchain Based Security Interest that provides the collateral to an investor in the IMT fund. IMT uses its funds to purchase goods from the seller and stores them at a VMI warehouse. Finished goods are shipped pursuant to a purchase order from the buyer, a process covered by insurance. The buyer then pays IMT for the goods*." [20].

Brackets

Smart contracts on the skuchain are called brackets. They are cryptographically secured. They provide some key advantages.

- They are designed to release collateral as a result of being triggered automatically by real world events.
- They improve transparency for all participants by providing real time view of transaction state.
- "*It enhances liquidity of collateralized assets in a supply chain by improving upon current trade finance instruments such as Factoring, PO Financing and Vendor Managed Inventory Financing. It also creates the opportunity for Deep Tier Financing."* [20]

PopCodes

"*Popcodes are Proof of Provenance codes, a crypto-serialization solution to track flow of goods on SKU level. They provide bank-grade traceability to track physical value in the supply chain. Popcodes are sophisticated in their ability to track sub-assemblies, parts and raw materials used to make a finished product. Using Popcodes, an enterprise can gain JIT visibility across the entire supply chain ecosystem, enabling optimal agility and planning. It also provides end-consumer visibility into the entire history of the product*." [20]

4.2.2. Provenance

Is working on using blockchain technology to enable secure traceability of certifications and other salient information in the supply chain. It aims to become a platform for verifying authenticity of goods. "*Provenance enables every physical product to come with a digital 'passport' that proves authenticity (Is this product what it claims to be?) and origin (Where does this product come from?), creating an auditable record of the journey behind all physical*

products" [21]. They are creating a decentralized app for solving certification and chain of custody challenge in sustainable supply chains. It proposes a system to assign and verify certain properties of physical products using the blockchain. There are six differet actors involved in the proposed scheme namely.

- Producers (e.g cotton growers)
- Manufacturers (clothing brands etc)
- Registrars, they provide unique identity to other actors in the scheme
- Standards organizations, which define the rules of a certain scheme (e.g., Fairtrade);
- Certifiers and auditors
- Customers

The architecture in their white paper consists of number of modular programs. Namely Registration program, Standards programs, Production programs, and Manufacturing programs. Each one is deployed on the blockchain independently but since all of them work within the same blockchain system they can interact without friction. Principal functions of each of these programs can be found in [21]. Technologies such as NFC, RFID, barcodes, and digital tags link physical products to their digital representation on the blockchain. Furthermore, user facing application in the form of smart phone applications will facilitate access to the blockchain. They will aggregate and display information to customers in real – time detailing every step this product took in the complicated web of its supply chain.

4.3. File sharing

Filecoin, SiaCoin and Storj are some of the proposals for creating a decentralized platform for filesharing, storage and cloud computing using the blockchain. The idea is simple users instead of uploading files to a central cloud server hosted at google, Microsoft or Dropbox files are shredded, encrypted and spread across the distributed file storage network based on the blockchain. Only the uploader holds the keys to call smart contracts to decrypt and reassemble the files. People participating as hosts in the network rent out their storage spaces and get paid in return for the services they provide. One system offering decentralized file storage capabilities is given below

4.3.1. FileCoin

"*Filecoin is a decentralized storage network that is auditable and publically verifiable. Clients pay miners for data storage and retrieval. Clients offer data storage and disk space in exchange for payments. The network achieves robustness by replicating and dispersing content while automatically detecting and repairing replica failures*" [22].

Proof of Replication 

It is an extension of Proof of Storage protocol. It enables a miner to convince a user that some data D has been successfully replicated to its own unique physical storage S. it uses challenge/ response protocol to achieve this. It improves Proof of storage and Provable data possession by preventing Sybil attacks, Outsourcing attacks and Generation attacks.

Proof of Space time

Proof of storage allows a user to verify that data was being stored by the miner throughout a period of time. A natural way to verify this would be by repeatedly sending challenges to storage provider but due to communication complexity this would become a bottle neck in the system. Proof of stake requires a storage provider to produce a sequential proof of storage for a period of time. Technical details of this solution are presented in [22].

References

[1] https://en.wikipedia.org/wiki/Blockchain

[2] https://en.wikipedia.org/wiki/Ethereum

[3] https://medium.com/@FEhrsam/scaling-ethereum-to-billions-of-users-f37d9f487db1

[4] https://en.bitcoin.it/wiki/Payment_channels

[5] https://lightning.network/

[6] https://www.youtube.com/watch?v=MpfvhiqFw7A

[7] http://www.jeffcoleman.ca/state-channels/

[8] https://blog.stephantual.com/what-are-state-channels-32a81f7accab

[9] https://www.youtube.com/watch?v=JuVP4iDVkoQ

[10] https://www.youtube.com/watch?v=Statechannels-EthereumIsOpenforBuisness

[11] Stefan Dziembowski1, Lisa Eckey2, Sebastian Faust2, and Daniel Malinowski. PERUN: Virtual Payment Channels Over Cryptographic Currencies. https://eprint.iacr.org/2017/635.pdf

[12] https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain/

[13] https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/

[14] https://www.youtube.com/watch?v=ZKscEx2lO-4

[15] https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf

[16] https://www.ibm.com/internet-of-things/platform/private-blockchain/

[17] https://filament.com/assets/downloads/Filament%20Foundations.pdf

[18] https://en.wikipedia.org/wiki/Smart_contract

[19] https://blockgeeks.com/guides/smart-contracts/

[20] http://www.skuchain.com/about-us/

[21] https://www.provenance.org/whitepaper

[22] https://filecoin.io/filecoin.pdf