UNIVERSITY OF TARTU
Institute of Computer Science
Software Engineering Curriculum

Sven Mitt

Blockchain application - case study on Chain

Master's Thesis (30 ECTS)

Supervisor(s): Luciano García-Bañuelos
Fredrik Milani

Tartu 2017

Blockchain application - case study on Chain

Abstract:

Blockchain and smart contract based systems are slowly gaining more foothold. There is research how it impacts the software architecture and what can be done with smart contracts. In this paper we study how implementation of blockchain based system called Chain core compares to other system. As a result we implement a parking spot application fir multisided market using Chain core and smart contract language called Ivy and compare it to iterative language contract. In the end we have a working prototype covering predetermined use cases.

Keywords:

Distributed Ledger Technology, Smart contract, Blockchain Technology, Chain infrastructure, Chain core, IVY language

CERCS:

Pealkiri eesti keeles

Lühikokkuvõte:

Blockchain tüüpi rakendused on vaikselt hakanud maad võtma ning .

Võtmesõnad:

Kujundus, paigutus, mall

CERCS:

Table of Contents

1 Introduction

1.1 Scope

Scope of this thesis is to research blockchain suitability for parking spot application and implement using predetermined use cases. Result is a research how to implementation of parking business model as software. Platform for blockchain is Chain core.

1.2 Motivation

Current parking applications are divided into two categories.

In first ones where you show up, find a parking spot and buy a ticket for predetermined time. This is done using separate machine to get the parking ticket or app on a phone. In Estonia, 32 cents is the fee for parking app platform owner.

In the second type, you get a ticket before you enter through a barrier gate. Paying for parking time is done before leaving the parking lot. The fee is included in the parking price.

Both of those solutions is driven by a third party that has built a platform for managing the app and machines and takes a hefty cut when you use their service.

We are interested in searching a cheaper solution. One that has smaller mediator fee and does not include vendor lock-in. That means the platform is shared between the companies that are interested providing parking spots.

Chain core is a relatively young company founded in 2014 and it provides an opensource system to transfer financial assets with permission handling on a blockchain to provide immutable transactions and data. It supports also smart contracts using language Ivy. In this paper we implement a parking lot solution using this framework and see how that compares currently used system.

What if you are in a hurry and need a parking spot and you do not have time to lose. There is no reservation possibility in current business models nor assigning specific parking spot per veichle.

1.3 Research problem

We define research questions accordingly:

1. Is blockchain viable for implementing parking solution?
2. Is Chain core viable for implementing parking solution?
3. Is Chain smart contract language Ivy powerful enough to implement parking solution on its own?

To answer these questions we have research whitepapers that deal with differences of software systems used today and compare them to blockchain based solutions. Before implementing such solution, we need to know if blockchain is at all appropriate for these kind of systems.

1.4 Summary of contribution

In the end of this theses we have implemented selected use cases for parking application and shown that it is possible to provide a viabale system using Chain core as a blockchain platform.

2 Related Work

2.1 Search strategy

Searched strings:

- Blockchain
- Smart contract
- Distributed Ledger Tehnology
- Product-centric blockchain
- Blockchain software connector
- Two sided and multisided markets

Search was conducted in digitaal libraries to find any whitepaper related to search string. Databases used:.

1. Scopus
2. Web of Science
3. IEEE Xplore
4. ACM Digital Library
5. SpringerLink
6. ScienceDirect
7. Google Scholar

2.2 Technology for two- vs multi-sided markets

To understand how blockchain enables to provide better business value, we have to understand how it is produced currently [1].

Most business models today depends on two-sided platforms, where a trusted third party is involved for mediating the interaction between end-users. End users do not trust each other, so they need a third party that can be trusted by all. Transactions and resolving data left on the shoulders of the mediator and its platform. The platform must kee records and use patterns to resolve transaction problems. All that also involves cost since the third party must develop a platform for mediating and will charge end users for using it.

Multisided platform enables end users trust each other since data is decentrialized and all parties have a full copy of database. The problem is how to get data synchronized to all parties.

That is the reason blockchain is multisided platform enabler. It allows to create specific datastore that contains immutable blocks and gives order to transactions. To bring down costs a multisided-platform is used, to enable interaction between multiple end-users and reducing cost. Mediator in this case will monitor the trading and revenue is split according to contract and business rules.

2.3 Blockchain

Blockchain datastructure is list of blocks that are timestamped, immutable and in strict order. All transactions are immutable and that allowes us to be certain that no data that already has been sumbtired to blockhain, is not tampered with. Blockchain enalbes this behaiviour by requiring consensus from interested parties and only committing the transaction after reaching consensus.

Allows technology enables to create distributed database that guarantees that simulations modification of data will not. If there is concurrent changes, the consensus algorithm will

guarantee that only one version of database will be in use. That provides companies the insurance that they can see the entire database in and they will be included in vote for consensus.

Criteria's for platform to be blockchain enabled [2]:

1. Must be durable or capital good – parking spot is an example
2. Fully shared database, cannot be fragmented
3. Multiple concurrent writers
4. Need for one absolute version (not like git)
5. Must depend on previous modifications
6. Need for trust for untrusted parties and permissions on items
7. Need to remove intermediation (someone who maintains joint database and enables trust and multiversion concurrency)
8. Blockchain mining mechanism increases latancy – since parking spot app is not realt time system, then it is not a issue
9. Data stored in block chain is limited and should be minimal

There can be other technologies for implementing the solution for parking platform, but this theses concentrates on enabling platform on blockchain and specifically Chain infrastructure and using Ivy language

2.4 Distributed Ledger Technology

Initially blockchain, later blockchain was generalized to distributed ledger that uses blockchain to verify and store transactions in distributed manner.

2.5 Smart contract

Smart contract [3]adds functionality to blockchain as it is a computer program that can access blockchain blocks and the history. Functionality was added to second generation of blockchain

Smart contract is a computer program that is stored in distributed database – their operation logic can trigger some functionality in before happened events in blockchain. They can act like database triggers, conditionals and add business logic to transactions. Quite powerful tool, but they are usually very simple and lack the tools that programmers are used to. For example Chain core Ivy language for smart contracts is not Turing complete and lacks loops and conditionals.

Since smart contracts move digital values that also have real monetized value in the real world, a bug in a contract will be costly. Writing even a simple smart contract need economic thinking and can lead to unexpected results [1].

2.6 Chain core

Chain core is blockchain based enterprise software for issuing and transferring financial assets [1]. It also includes role based permission handling, a must have capability for private and for enterprise usage. It is open source software licenced under AGPL [2].

The product owners place chain core in between decentrized cryptocurrencies like Bitcoin and two-side market platforms like banks. Contrary to cryptocurrencies, the tehnology allows defining of assets – it can be capitalized goods like parking spot or also monetary values.

It has built in federated consensus mechanism for automatic transaction confirmation. It also allows you to hide the details of transactions.

Data model:

- **Asset** – any type of capital or durable goods. Issuing and retiring assets is supported by the platform. Each asset has an immutable identifier and 256 bit string designed to be globally unique.
- **Transaction** – move value from inputs to output. Input can be previous transaction output or in case of assignment of new Asset, a new issuance of unit
- **Blocks** –multiple transactions are batched into blocks and those make up the block-chain. New block is written when a consensus program is executed successfully.

Functionality:

- **Program** – customable logical software pieces written in bytecode and executed in Chain Virtual Machine:
  - Issuance programs define rules for creating new assets
  - Control programs define rules for transactions
  - Consensus programs are used when a transaction is completed and block is written to blockchain
- **Chain Virtual Machine** – responsible for running programs, instruction set is Tu-ring complete and has built in support for parallel processing and limited runtime.
- **Introspection** – allows issuance or control program define who, how and when can spend asset.

Different consensus programs are supported. Default is federation consensus protocol that makes sure that blockchain cannot fork unless more than 2M - N -1 block signers violate the rule that all block must have unique height (M is number of valid signature and N is number of public keys). To ensure that one block gets signed, only one generator of block is used. Since it can crash or deadlock, the block generator is the weakest link in the system, but the design of this technology is built on top of that there is on company that is responsible for running the network and infrastructure. The generator can be replicated and set behind load balancer.

All the transaction are public in Chain core, privacy is achieved by signing transaction with a new key and that makes hard to link transaction with actor.

3 Background

4 Conclusions

5 References

6 References

[1] T. S. J. H. Juri Mattila, “Product-centric Information Management: A Case Study of a Shared Platform with Blockchain Technology,” UC Berkeley, Minneapolis, 2016.

[2] M. A. A. K. A. M. a. E. S. Kevin Delmolino1(B), “Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab,” 2016.

[3] R. M. G. M. B. Kewell1, “Distributed ledger technology: Applications and implications,” John Wiley & Sons, Ltd, 2017.

[4] “Chain core brochure,” 2017. [Online]. Available: https://chain.com/assets/brochure.pdf.

[5] “Chain core licence,” 2017. [Online]. Available: https://github.com/chain/chain/blob/main/LICENSE.

[6] C. P. L. Z. V. G. A. P. Xiwei Xu, “The Blockchain as a Software Connector,” 13th Working IEEE/IFIP Conference on Software Architecture, 2016 .

[7] K. C. L. W. N. K. Daniele Magazzeni and Peter McBurney, “Validation and Verification of Smart Contracts: A Research Agenda,” *COMPUTER ,* no. september, pp. 50-57, 2017.

Appendix

I. Glossary

II. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Sven Mitt**,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

Blockchain application - case study on Chain,

(title of thesis)

supervised by ,

(supervisor's name)

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **23.10.2017**