University POLITEHNICA of Bucharest

Faculty of Automatic Control and Computers,
Engineering and Management of Business Systems

RESEARCH REPORT

Blockchain for Business

Scientific Adviser:
Prof. Gabriel Neagu

Author:
Adriana Dincă

Bucharest, 2018

Contents

List of Figures

Chapter 1

Introduction

1.1 Project Description

The research report presents the actual state of Blockchain technology and business markets and identifies the fields that can benefit the most from the adoption of this technology in their current systems.

The report identifies all the areas that can make use of Blockchain by describing the existing system, the issues of it and how can Blockchain change and improve the users day-to-day activity. In order to be able to do such an analysis it's necessary to study the existing Blockchain businesses and their history from an idea to a successful startup. After determining the keys elements that made these businesses so popular we focus our attention to Decision Support System architecture and the technical aspects of Blockchain so that we can have a strong view of this technology. Last but not least we describe the areas that are not using Blockchain technology but if they would adopt it they will improve massively their work flows.

1.1.1 Project Scope

This report aims to determine if it would be useful to create a Decision Support System that assists project managers to adopt Blockchain technology in the projects they conduct. The DSS is going to be used in order to change the existing business system with a Blockchain solution that will simply the business processes and reduce the time of doing those activities.

1.1.2 Project Objectives

The list of objectives is the following:

- **Explore Decision Support System for architectural solutions** is needed in order to determine what is the current state and if there are systems that offer technical solutions for improving or innovating complicated and old systems.
- **Understand Blockchain technology** is the next step that we need to accomplish in order to be able to develop a DSS that offers particular solution for a defined business.
- **Discover Blockchain successful businesses** helps detect the main elements that made these projects so popular. This step of market analysis is important in determining what are the target groups of these type of business, what is the size of a Blockchain business or what is the revenue of these startups in a certain period of time.

- **Determine the fields that could be innovated by the adoption of Blockchain** is the step when we identify the possible markets that would benefit from the DSS that we propose. Understanding their needs and limitations helps us offer the best version of a DSS.

1.1.3 Related Work

This report focuses on the research work conduct during the first semester of master for determining if a DSS for Blockchain architectural solution is useful and is worth to develop. The logical steps after selecting the research topics were to discover the existing DSS for architectural solutions, investigate the technical details of Blockchain, determine the main elements that made certain Blockchain businesses so successful and the possible fields where Blockchain can innovate.

Decision Support System is defined as "an extensible system, capable of ad-hoc analysis and decision modeling, focused on future planning and used as unplanned and irregular timestamps" accordingly to Moore and Chang [13]. An important aspect of decision support systems is to improve effectiveness, rather than the efficiency of decisions [4]. A DSS that helps managers make decisions regarding the architectural solutions was proposed before. An example of such a system that decides between certain web framework is described in the article [3] but there is no DSS that offers solutions that uses Blockchain as a requirement for designing the project's architecture.

Before getting into the technical aspects of Blockchain is useful to investigate the impact of Blockchain on different areas of our life and the first step is to determine the areas that would benefit most from the Blockchain innovation.

In John Rampton's article [10] are listed the five directions where the Blockchain technology could make a difference. The Blockchain is closely linked with Bitcoin, a project published in 2009 by Satoshi Nakamoto as an alternative to traditional currency. The innovation brought by Bitcoin consists in the use of Blockchain as a storage for financial transactions in a distributed system. Since 2009, the Blockchain technology was used for different purposes and these are the five directions of innovation:

- Smart Contracts are a concept introduced in the Ethereum project that allows applications to run as programmed without the possibility of downtime or fraud.
- Cloud Storage on Blockchain is a secure cloud storage solution that decreases the dependency of big market players such as Google or Amazon.
- Supply-Chain Communications and Proof-of-Provenance can benefit from Blockchain that offers the possibility to record digitally the state of a product along its chain to the final consumer.
- Paying Employees via digital assets reduces the time and money spent and is highly secured. The money have an unique identification(public key) and in each moment we can identify where they are in the network. The owner is the one that holds the private key.
- Electronic Voting using the consensus model of Blockchain is offering a solution to the voting manipulation issues and it protects all participants by assuring anonymity.

Chapter 2

Background

2.1 Decision Support Systems Architecture

Developing Decision Support Systems requires high costs, human effort, time and the success of the system cannot be guaranteed. These system can be affected by many risks like system design, data quality and old technologies. Their purpose is to assist managers in decision making such as investments, budgeting, cash flows or financial planning.

Level 1 (bottom-tier) – data management

Level 1 (bottom-tier) is the level of data management and it involves data, metadata, DBMS, data warehouses and marts, data dictionaries and metadata dictionaries. The data that comes from operational databases and external sources is transformed using different types of filtering tools and predefined procedures. At this level of the architecture a series of tasks should be implemented in order to load data in a data warehouse such as collecting and extracting from external data, data cleaning and transformation and than loading the data in the data warehouse. The processes performed at this level are very important for the success of the DSS. A faulty design could lead to the failure of the DSS.

Level 2 (middle-tier) – model management or analysis level

The second level of the DSS architecture is involved in modeling and analysis. At this level the data is transformed and the necessary information is extracted. In order to get that information architects are using data analysis, simulation and forecast models that achieves the business requirements. An example of technology used at this level is OLAP. The OLAP tool is using multidimensional data representation that allows quick data analysis by using rool-up or slice operations. Data mining techniques are present at this level so they are extracting knowledge from that data not reports of the data. In [1] the authors state that 'very often, the success of a DSS is determined by the discovery of new facts and data correlations and not by building reports that presents data'.

Level 3 (top-tier) – The interface or the presentation layer

The level 3 contains the interaction between users and the system. The user interface should be specially designed to make the interaction more user friendly. This level involves queries and reports building tools, data viewing tools, data publishing and presenting tools. On this level, the human resource has an important role because he/she need to make the final decision. To facilitate the interaction between the system and the end-users the architects developed also smart portals using portal-based web technologies. BI portals offers users a good end-to-end experience by including nice graphics, report generation features, etc.

Level 4 – Telecommunications

The telecommunicationslevel interconnects all three levels and it contains web servers, computer networks, communication devices, etc.

2.2 Blockchain technical details

The blockchain is a public ledger of all transaction sent through the network that is known by every one that holds a blockchain node. More precisely, each node has a copy of the blockchain in order to validate or invalidate a transaction. The majority of nodes decide if a transaction is valid and if so that transaction is added in the latest created block by one of the miners. The choice of using blockchain for data storing is related with the fact that the blockchain's deep history is immutable so it ensures the protocol security.

The blockchain has no central authority for managing assets flow along the network. This technology is recognized as the "fifth evolution" of computing, the missing trust interface of the Internet as stated by Laurence [7].

The blockchain structure has the following components as described in Figure 2.1:

• **The block** is an array of transactions recorded into a ledger. Depending on the blockchain the transaction has assigned a different type of value. Each block has its own hash and a merkle tree with hashed transactions. Storing transactions in a merkle tree is a design decision that saves disk space. Nakamoto [9] explains the reason why using a merkle tree makes disk space recover possible. The explanation for this is that "once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree, with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored" according to Satoshi [9].

• **The chain** is simply a hash that connects two blocks in chronological order. The hash for a new block is generated based on the data that was in the previous block. The hash algorithm used by Bitcoin is Secure Hash Algorithm 256 [5] that creates an unique (collision probability is negligible), fixed-size (256 bits) hash.

• **The network** is represented by full nodes. We can think of it as a computer that runs an algorithm for securing the network. Mining is expensive and it requires a lot of computer power so the blockchain algorithm rewards miners for their service. The payment is usually a currency or a token.

2.3 Blockchain properties

2.3.1 Proof-of-work

The idea of using a proof-of-work [8] system to legitimate the user of an application was used before in other software systems. For example, Hashcash [2] is a proof-of-work system introduced by Black that was invented to limit email spam and denial-of-service attacks. The idea is quite easy to follow: a legitimate sender needs to spend a reasonable amount of computing time in order to issue an email. If a legitimate user sends a reasonable number of emails, a spammer wants to send thousands of emails making the spamming effort very expensive. The

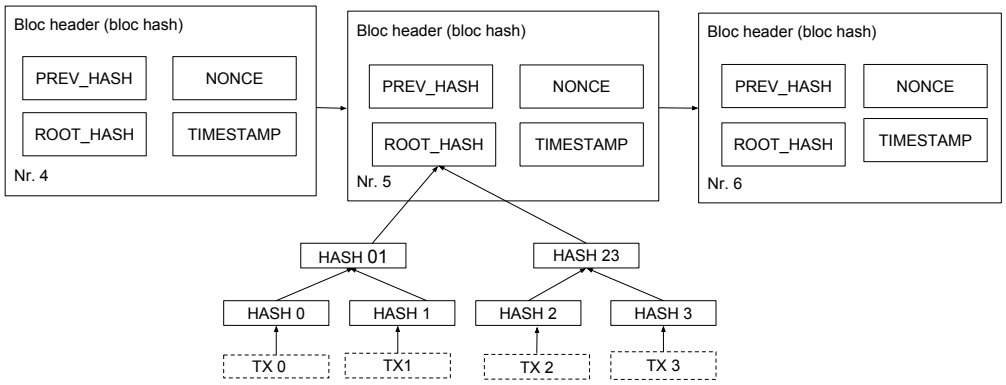

Figure 2.1: Blockchain Structure using Merkle Tree

receiver's role is to validate the hash, which is quite easy. Hashcash is conceptually similar to the proof-of-work system used by Bitcoin miners.

Solving the problem of double spending using a proof-of-work system provides security guarantees for naming/identity registration and transfer.

2.3.2 Consensus Protocol

Based on prior work, the Bitcoin technology introduces a consensus protocol based on the Byzantine Generals' Problem [6] to eliminate double-spending by transaction validating process.

When a new transaction is broadcasted to the network, nodes have the option to add the transaction in their copy of the Blockchain or not. The majority of nodes which compose that network decides the single state of a transaction (valid or not) and the consensus is achieved.

2.4 Bitcoin project

The Bitcoin is the first cryptocurrency developed using blockchain technology. The unique attributes of the blockchain and the cryptographic principles brought Bitcoin a huge popularity. Satoshi Nakamoto is the pseudonim of the Bitcoin inventor. The real identity of Satoshi was never revealed. There are many suppositions but not of them was confirmed. He claimed to be a Japanese male around forty years old.

One interesting aspect about Bitcoin technology is how it solves both the problem of double-spending and mining in a decentralized system. The protocol is developed on "sound cryptographic" principles that guarantee proof-of-work, proof-of-ownership and classic currencies attributes such as fungibility and scarcity.

Chapter 3

Blockchain based projects

Don and Alex Tapscott [12] define Blockchain as *an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.*

The Blockchain technology has a huge potential of development and the number of areas that it could innovated is impressive. In [11], Ameer Rosic gathers a complete list of fields that could be innovated by Blockchain technology.

3.1 Financial

Blockchain and the financial world involve trading, money transfer and mortgages. Right now the economic world releases on banks, governments and other financial institutions to transfer money from an account to another. Financial information transfer is monitored by governmental institutions and this type of information can be used to banks advantages in trading operations.

3.1.1 Cryptocurrencies

The Bitcoin project is a popular blockchain based application but there are other blockchain projects that deserves to be brought to attention such as Ethereum, Namecoin or Ripple. The Ripple project started before Bitcoin in 2004 and it passed through many changes over time. Today, Ripple is a solution that enables banks and clients to exchange value. Similar with Bitcoin, Ripple is a distributed system with its own blockchain and a native currency called ripple. Ethereum is another blockchain based application that has its own Turing-complete programming language which makes it more powerful than Bitcoin by allowing users to create their applications on a new programming language. Namecoin was the first fork of the Bitcoin project. It offers a domain name registry similar to the Internet's DNS. It is an alternative domain name service for the root domain *.bit*. The project has its own currency called namecoin (symbol *NMC*) which is used to pay transactions fee for registration, update and transfer of domains name.

3.2 Smart contracts

The smart contracts are applications that run as independent nodes in the Blockchain network and execute actions when special conditions are accomplished. Ethereum is an open-source

project that have its own operation system and programming language that have the potential to leverage the usefulness of Blockchain projects. Using Ethereum we can program a smart contract to pay out a derivative when a financial instrument reaches a certain benchmark and the payout is automated.

3.3 Sharing services

The sharing economy is a successful field in the modern world. Companies such as Uber and AirBnB are flourishing and users are becoming interested in sharing services. The change that can be made by the use of Blockchain is to remove the power from centralized systems such as Uber or other platforms that allows sharing by using a peer-to-peer network for sharing services. An example of such a system is OpenBazaar that is a Blockchain project for a eBay peer-to-peer.

3.4 Crowdfunding and Voting Systems

Companies like Kickstarter and Gofundme are examples of Blockchain projects that are creating crowd-sourced venture capital funds for different projects. The popularity of these companies highlights that people are willing to get involved in product development and make a difference in a challenging industry such as IT&C. Another experiment is the Ethereum-based DAO (Decentralized Autonomous Organization) that raised $ 200 million USD in a few months in DAO tokens. People bought tokens to vote on smart contract venture capital investments. The project was hacked due to insufficient diligence with disastrous consequences.

3.5 Public sector

The public sector activities can benefit from blockchain technology by changing the asset registration, citizen identification process, medical records and medicine supply chain. The real power of blockchain consists of creating new solutions of performing old processes that are inefficient in the modern world. Checking paper records for validating the ownership of an asset had become very difficult and time consuming activity. The number of population is increasing at a high rate and public sector employees are forced to perform lucrative and repetitive tasks. Having all properties stored in a blockchain repository eliminates the problems mention above and offers the guarantee of security and privacy.

Another problem of the public sector is protecting critical data. Despite governmental institutions effort to protect their systems, criminals manage to get access to their databases and manipulate their records. Using encryption methods to protect personal information is 100 percent safer than storing data in DBMS. There is an application called Keyless Signature Infrastructure (KSI) that uses Blockchain to protect all public sector data in Estonia. The KSI project uses hash values to identify records. The values are unique and there is no possible way to reconstruct the information for that record(file). Right now, the electronic health records of all Estonia citizens uses KSI technology.

3.6 Digital property ownership

The process of owning and selling assets involves multiple interaction and a long paper trail. To improve this difficult process in Sweden, Lantmäteriet the government is exploring ways to

digitize it. A mobile prototype app was launched that offers transaction mechanism for sellers and buyers as well as for real-estate agents and banks. The basic technology used is Blockchain that stores all information about existing properties and it will improve the communication among all the parties involved in the process. The time reduction is expected to be from three-to-six months to days or hours.

3.7 Retail

In the retail field blockchain can change the way the supply process, fidelity programs are implemented or the information sharing process is done (from supplier to retailer and the other way around).

3.8 Insurance

There are many activities in the insurance industry than can be innovated such as risk provenance, claims processing, asset usage history or claims files.

3.9 Manufacturing

Another industry that can benefit from blockchain technology is the manufacturing starting with the supply chain, product parts or maintenance tracking. In tech and telecommunication manufacturing all big players vies for the IoT dominance. IBM, AT&T and Samsung are researching to detect the best solution to predictive maintenance of mechanical part or data analytics. Monitoring these systems is hard and expensive but Blockchain is offering a cheaper solution for keeping track of IoT applications components.

3.10 Prediction markets

Making prediction based on event probability was proven to have a high degree of accuracy. Augur is an example of sharing offering project for the prediction market that is based on the outcome of real-world events. The people that uses Augur can earn money buy buying into the correct predictions.

Chapter 4

Conclusion

In conclusion, in this report we presented the Blockchain technical details, what is Blockchain, how does this protocol works and what makes it so powerful and we determine the fields that could be improved by the adoption of Blockchain. The number of processes that can make use of this technology is large and the impact of Blockchain is massive. From financial applications to identity management, land title registration or crowd funding, the Blockchain is going to revolutionize everything we knew and complained about.

The Decision Support System aims to offer clear architectural solutions for improving old and unreliable systems. The DSS is going to collect all the project specifications and it will create solutions that are Blockchain based and meet the old system requirements. The DSS uses logical design model of successful Blockchain based systems from the same field. The limitation of the DSS is that it can be used only for fields well described by logical models.

Taking into account all the fields that can be innovated using Blockchain technology, the project of developing a Decision Support System for assisting managers in innovating their product with the power of Blockchain is going to be a successful idea.

Bibliography

[1] Ion Lungu Adela Bâra. Improving decision support systems with data mining techniques. 2012.

[2] Adam Back. Hashcash-a denial of service counter-measure. 2002.

[3] Olaf Zimmermann Cesare Pautasso and Frank Leymann. Restful web services vs. "big"' web services: making the right architectural decision. https://dl.acm.org/citation.cfm?id=1367606&preflayout=flat, Originally published in 2008. Accessed: 2018-01-28.

[4] M. Bohanec D. Mladenić, N. Lavrač and S. Moyle. Data mining and decision support: Integration and collaboratio. *Kluwer Academic Publishers*, 2002.

[5] Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva. Bicliques for preimages: Attacks on skein-512 and the sha-2 family. http://eprint.iacr.org/2011/286.pdf, Originally published in 2011. Accessed: 2018-01-25.

[6] Leslie Lamport, Robert Shostak, and Marshall Pease. *The Byzantine generals problem.* ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3, 1982.

[7] Tiana Laurence. *Blockchain For Dummies.* 2017.

[8] Ben Laurie and Richard Clayton. *Proof-of-work proves not to work; version 0.2.* Workshop on Economics and Information, Security, 2004.

[9] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *The Cryptography Mailing list at metzdowd.com*, 2008.

[10] John Rampton. 5 applications for blockchain in your business.

[11] Ammer Rosic. What is blockchain technology? a step-by-step guide for beginners. https://blockgeeks.com/guides/what-is-blockchain-technology/, Originally published in 2017. Accessed: 2018-01-28.

[12] Don Tapscott and Alex Tapscott. Blockchain revolution. https://www.linkedin.com/pulse/whats-next-generation-internet-surprise-its-all-don-tapscott/, Originally published in 2016. Accessed: 2018-01-28.

[13] Chang E. Koh Watson H., R. Kelly Rainer. Executive information systems: A framework for development and a survey of current practices. *MIS Quarterly*, 15, 1991.