THE USE OF BLOCKCHAINS. AN R APPROACH

Nicolae-Marius JULA[*]
Nicoleta JULA[**]

Abstract

The cryptocurrency is a hot topic and understanding the blockchain is very important. Also, understanding what blockchain may lead to more decentralized services and applications to be used, not only in relation to financial applications. Today, blockchains can be used to for smart contracts, decentralized networks, governments and non-profit organizations, banks and even photography copyright recordings and smart contracts for music artists. Even World Economic Forum predicted that by 2015 about 10% of global GDP will be stored on blockchain technology. The blockchain technology cosists in creating a chain of blocks, validated with a hash function and under a "proof of work" concept, which limits speed of creating new blocks. The new technology is open source, but recently has attracted the attention of big software players, like Microsoft and other companies (BBVA, UBS). In this paper, we present a simple R implementation of a blockchain, containing a initial block, creation of each blocks (including hash and proof of work) and the creation of the chain. Data validation and the lack of so-called middle man, minimization of the fees, increasing the speed of transactions, security and anonymity provided by this technology are good arguments for ensuring the continuous development of the technology and its spreading in everyday activities.

Keywords: *blockchain, cryptocurrency, R, proof of work, technology.*

1. Introduction

1.1. History of blockchain

One cannot start an analysis about blockchain without mentioning its public debut: when Satoshi Nakamoto, whose true identity is still unknown, released the whitepaper Bitcoin: A Peer to Peer Electronic Cash System in 2008 that described a "purely peer-to-peer version of electronic cash" known as Bitcoin. Many years the two concepts (blockchain and Bitcoin) were seen together. Of course, without blockchain, there will be no Bitcoin, but blockchain technology is a lot more than just cryptocurrency: it has potential to impact every industry, from financial, manufacturing to education and evan creative arts.

It is worth mentioning that, from the beginning, the technology behind blockchain was offered as an open source. The term "open source" describes the practice of producing or developing certain finished products, allowing users to access the production or development process freely. Some specialists define the "open source" as a philosophical concept; others think it is a pragmatic methodology.

The most important aspect that blockchain brings to the masses is that it records important information in a public space and doesn't allow anyone to remove it, it's transparent, time-stamped and decentralized. Sally Davis, a reporter from FT Technologies states that "Blockchain is to Bitcoin, what the internet is to email. A big electronic system, on top of which you can build applications. Currency is just one". At its core, blockchain is an open, distributed register that records transactions between two parties in a perpetual way without needing third-party authentication. This creates an extremely efficient process and one people predict will dramatically reduce the cost of transactions. When entrepreneurs understood the power of blockchain, there was a surge of investment and discovery to see how blockchain could impact supply chains, healthcare, insurance, transportation, voting, contract management and more. It is estimated thatn early 15% of financial institutions are currently using blockchain technology.

It was in 2013 when Vitalik Buterin wanted to expand beyond the limitations found in Bitcoin technology and cretated the second public blockchain, called Etherum. The major difference between the two is that Ethereum can use other assets such as loans or contracts, not just currency. Ethereum launched in 2015 and can be used to build "smart contracts"—those that can automatically process based on a set of norms established in the Ethereum blockchain. This technology has attracted the attention of companies such as Microsoft, BBVA and UBS, who are interested in the potential of the smart contract functionality to save time and money.

Today, Bitcoin is just one of the several hundred applications that use blockchain technology. It's been a remarkable decade of transformation for blockchain technology and it will be interesting to see where the next decade takes us.

[*] Lecturer, PhD, Faculty of Economics and Business Administration, Nicolae Titulescu University, Bucharest (e-mail: mariusjula@univnt.ro)
[**] Professor, PhD, Faculty of Economics and Business Administration, Nicolae Titulescu University, Bucharest (e-mail: nicoletajula@univnt.ro)

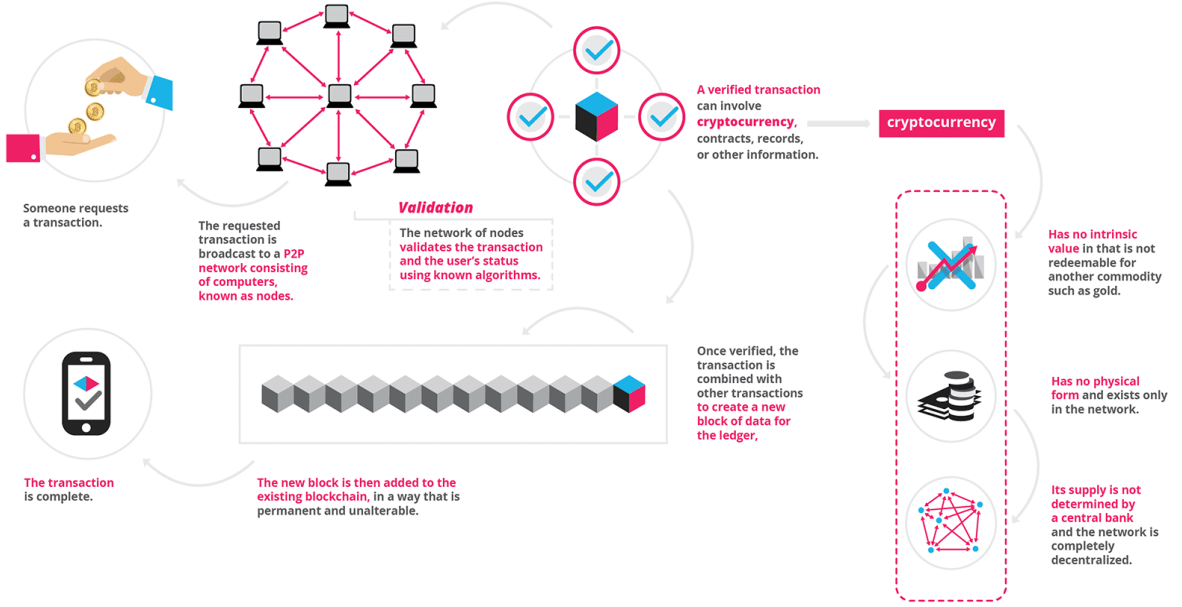
2. The use of blockchains

2.1. Validation

Presently, blockchain works on the "proof of work" concept, where a powerful computer calculation or "mining" is done in order to create a block (or a new set of trustless transactions). Currently, when you initiate a transaction, it is bundled into a block. Then the so-called "miners" confirm the transactions are authentic within that block by solving a proof-of-work problem—a very difficult mathematical problem that takes an extraordinary amount of computing power to solve. The first miner to solve the problem gets a recompense and then the verified transaction is stockpiled on the blockchain. Ethereum developers are interested in changing to a new consensus system called proof of stake.

2.2. Popular Use Cases of Blockchain

Figure 1 – Blockchain use (source: https://blockgeeks.com/guides/what-is-blockchain-technology/)



Notary

It is a fact that most records are stored on paper ledgers, but these can be tampered, lost, destroyed and so on. The data in blockchains cannot be tampered. Even the name suggests the two main components of the blockchain: a block and a chain. Data is stored in blocks and these blocks are all connected in a chain. The secure system is contained in the hash information from each block. In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length. In the context of cryptocurrencies like Bitcoin, the transactions are taken as an input and run through a hashing algorithm (Bitcoin uses SHA-256) which gives an output of a fixed length. Every successive block will contain the previous block's hash. This is what binds them together.

Smart contracts

Usually, two parties can agree and sign a contract that legally binds them. For exemple, for renting or other services. What if one of the parties don't want to pay when the limit expires? Of course, there are legal ways to follow, but usually in a court the time lost is hard to compensate. So, the blockchain solution is to create a code that is deployed on both parties' computers. Also the banks of both parties should be part of this private blockchain. When the conditions are met, a trigger enforces the bank to make the payment:

Pseudo code of the smart contract between Person 1 and Person 2:

If today's date is 30th and rent is not paid then

Transfer $500 from Person 1's account to Person 2's account

Digital Voting

Blockchain helps overcome the biggest issue with digital voting: security. The technology can make the votes anonymous and provide better security. The latest drop in voting turnout may be changed using this system.

Distributed Storage

We are heading to an era when storage is more and more seen as a cloud option. We do not discuss here about the pros and cons regarding cloud versus local storage options, but more and more people rely on internet services for their files. It is also a big issue with the privacy and more people start to care and demand security and privacy for their private files. Using blockchains, the data is stored descentralized, with high encryption

Other uses, as Ameer Rosic describes in the article from BlockGeeks, are:

The sharing economy

With booming companies such as Uber and AirBnB, the sharing economy is already a proven success. Currently, however, users who want to save a

sharing service must rely on an intermediary such as Uber. By allowing peer payments, the block opens the door to interact directly between the parties - resulting in a truly decentralized economy.

An early example, OpenBasear uses the block to create a peer-to-peer eBay. One can download the app on the computing device and make transactions with OpenBazzar retailers without paying transaction fees. The "no rule" philosophy of the protocol means that personal status will be even more important for business interactions than is presently on eBay.

Crowdfunding

Crowdfunding initiatives, such as Kickstarter and Gofundme, are working in advance on the emerging peer-to-peer economy. The popularity of these sites suggests that people want to have a direct say in product development. Blockchains take this interest at the next level, creating potential venture capital funds with multiple sources.

In 2016, such an experiment, DAO based on Ethereum (Decentralized Autonomous Organization), generated a surprise of $ 200 million in just two months. The participants bought the "DAO chips", allowing them to vote on intelligent risk capital investments (the voting power was proportional to the number of DAOs they held). Subsequent hacking of project funds has shown that the project was launched without proper diligence, with disastrous consequences. Indirectly, the DAO experiment suggests that the bloc has the potential to introduce "a new paradigm of economic co-operation".

Governance

By making the outcomes fully transparent and available to the public, distributed database technology could bring full transparency to elections or any other way of polling. Intelligent contracts based on ethereum help automate the procedure.

The Boardroom application allows organizational decisions to be taken in block. In practice, this means that businesses' governance becomes fully transparent and verifiable when managing digital assets, equity or information.

Supply chain auditing

Consumers are increasingly keen to know that companies' ethical complaints about their products are real. Distributed records provide an easy way to certify that the history of the things we buy is genuine. Transparency comes with temporal marking of a date and location - for example on ethical diamonds - that correspond to a product number.

Provenance in the UK offers supply chain audit for a wide range of consumer goods. Using the Ethereum blockchain, the Provenance pilot project guarantees that fish sold in Japan's Sushi restaurants has been harvested sustainably by its Indonesian suppliers.

Prediction markets

The agglomerated screening of predictions about the probability of the event proves to be of a high degree of precision. The significance of the previous attitude cancels the unexamined disagreements that distort the judgment. Predicted markets that pay according to event results are already active. Blocks are a "crowd wisdom" technology that will undoubtedly find other applications in the years to come.

However, in Beta, the Augur Market Demand Demand offers bids to participate in the outcome of real-world events. Participants can earn money by buying in the correct prediction. Most of the shares purchased in the correct result, the bigger it will be. With a small commitment (less than one dollar), anyone can ask a question, create a market based on a predictable outcome, and collect half of all market-generated trading fees.

Protection of intellectual property

As is well acknowledged, digital information can be replicated infinitely - and widely distributed through the Internet. This has given global users a goldmine of free content. However, copyright holders have not been so lucky, losing control over intellectual property and financially suffering consequently. Smart contracts can protect copyright and automate the online sale of creative works, eliminating the risk of copying and redistributing files.

Mycelium uses blockchain to create a peer-to-peer music distribution system. Founded by British singer and songwriter Imogen Heap, Mycelium allows musicians to sell songs directly to the public, as well as to issue licensing samples to producers and to hold copyright for composers and musicians - all of which are automated by smart contracts. The use of blocks to issue payouts in fractional cryptocrats (micropayments) suggests that this case of use for the blockchain has great chances of success.

Internet of Things (IoT)

What is IoT? Network management of certain types of electronic devices - for example, monitoring the air temperature in a storage facility. Intelligent contracts make it possible to automate remote management. A mixture of software, sensors and networking simplifies the exchange of data between objects and mechanisms. The result increases system efficiency and improves cost monitoring.

The biggest players in the manufacturing, technical and telecommunication industries are fighting for IoT supremacy. Think of Samsung, IBM and AT & T. A natural extension of the existing infrastructure, controlled by current operators, IoT applications will run ranges from predictive mechanical maintenance to data analysis and large-scale automation systems management.

Neighbourhood Microgrids

Blockchain technology allows the acquisition and sale of renewable energy created by neighborhood microgrids. When solar panels produce excessive energy, smart contracts based on Ethereum redistribute it automatically. Similar types of intelligent contract automation will have many other applications as the IO becomes reality.

Located in Brooklyn, Consensys is one of the world's leading global companies that develops a wide

range of applications for Ethereum. A project that they partner with is the Transactional Network, working with the distributed energy equipment, LO3. A prototype of a project currently in use, and uses smart deals from Ethereum to automate the monitoring and redistribution of microgrid energy. This so-called "smart grid" is an early example of IoT functionality.

Identity management

There is a clear need for better identity management on the web. The ability to verify your identity is the connection between financial transactions that occur online. However, remedies for the security risks associated with web trade are imperfect at best. Shared spreadsheets provide improved methods to prove who you are, along with the ability to digitize personal documents. Having a secure identity will also be imperative for online interactions - for example, in the sharing economy. Good reputation, after all, is the most important condition for online transactions.

The development of digital identity standards proves to be an extremely complex process. Apart from the technical challenges, a universal online identity solution requires cooperation between private entities and government. Add to this the need to navigate in the legal systems of different countries and the problem becomes exponentially difficult. Internet e-commerce is currently based on the SSL (low green block) certificate for secure web transactions. Netki is a startup that aspires to create a SSL for blockchain. After announcing a $ 3.5 million seed round recently, Netki expects to launch a product in early 2017.

AML and KYC

Anti-money laundering (AML) and know your customer (KYC) have a strong potential to adapt to the block of flats. Currently, financial institutions need to carry out a multi-step process for each new client. KYC costs could be reduced by customer checking within an institution and, at the same time, increasing the effectiveness of monitoring and analysis.

Startup Polycoin has an AML / KYC solution that involves transaction analysis. These transactions identified as suspicious are passed on to compliance agents. Another startup command develops an application called Trust in Motion (TiM). Characterized as a "Instagram for KYC," TiM allows customers to take an instant image of key documents (passport, utility bill, etc.). After verification by the bank, these data are stored cryptographically on the block of blocks.

Data management

Today, in exchange for personal data, users can use free social platforms like Facebook. In the future, users will have the ability to manage and sell the data generated by their online activity. Because it can be easily distributed in small quantities, Bitcoin - or something like that - will most likely be the currency used for this type of transaction.

The MIT Enigma project understands that user privacy is a prerequisite for creating a personal data market. Enigma uses cryptographic techniques to allow splitting of individual data sets between nodes and at the same time to perform bulk calculations across the entire data group. Data fragmentation also makes the Enigma scalable (as opposed to blockchain solutions where data is repeated on each node). A Beta release is promised in the next six months.

Land title registration

As registers accessible to the public, blocks can make all sorts of more efficient registrations. Property titles are a case in point. They tend to be susceptible to fraud, as well as costly and forced labor efforts for administration.

Several countries are building land registry projects based on blocks. Honduras was the first government to announce such an initiative in 2015, although the status of this project is unclear. This year, the Republic of Georgia has reached an agreement with the Bitfury Group to develop a block system for property titles. According to him, Hernando de Soto, the high-ranking economist and property rights attorney, will advise on the project. Most recently, Sweden has announced that it is experiencing a blockchain application for property titles.

Stock trading

The potential to increase efficiency in the stock settlement process makes the use of trading blocks strongly used. When running peer-to-peer, commercial confirmations become almost instantaneous (as opposed to taking three days for clearance). Potentially, this means that intermediaries - such as clearing houses, auditors and custodians - are eliminated from the process.

Numerous stock and commodity exchanges are application prototypes for the services they offer, including ASX (Australian Securities Exchange), Deutsche Börse (Frankfurt Stock Exchange) and Japan Exchange Group (JPX). The highest profile because the first known in this area is Linda Nasdaq Linq, a platform for trading on the private market (usually between companies that started to engage with investors). A partnership with the blockchain technology group, Linq, announced the completion of its first volume of transactions in 2015. More recently, Nasdaq announced the development of a block block test project for the proxy vote on the Estonian stock market.

3. A simple blockchain in R

The algorithm is detailed in the CorrelAid blog and describes a simple R implementation of a blockchain, containing a initial block, creation of each blocks (including hash and proof of work) and the creation of the chain.

3.1. Creating the BLOCK

At minimum, a block must contain: data, timestamp, index and self-identifying hash:

block_example <- list(index = 1,

```
timestamp = "2018-01-05 17.00 MST",
    data = "Some data",
    previous_hash = 0,
    proof = 9,
    new_hash = NULL)
```

3.2. Hash

As stated before, a hash helps to ensure the integrity of a block by connecting it to the other blocks in the chain. A hash function takes something as an input and gives us a unique, encrypted output**.**

In the hash function, it is not included only the current information contained by the block, but also the hash of the previous block. This means, the algorithm calculates the valid hash only if it knows the hash of the previous block, which was created using the hash of the previous and so on. This ensures the sequntiality of the blockchain.

```
#Function that creates a hashed "block"
hash_block <- function(block)
{
block$new_hash <- digest(c(block$index,
    block$timestamp,
      block$data,
    block$previous_hash),          "sha256")
return(block)
}
```

3.3. Proof of work

There is a need to control the maximum numbers of blocks that can be created (for example, in cryptocurrency this is due to value loss if unlimited number of coins cand be crated). To control that, a so-called “proof of work” is defined. The work that is to be done by the computer, for example – solving a mathematical problem, which should be hard to solve but easy to verify, is to be rewarded. In Bitcoin mining (which is the name of the problem solving for this currency) the reward is in Bitcoins. When a new block must be created, a computational problem is sent out to the network. The miner which solves the PoW problem first creates the new block and is rewarded in bitcoins (this is the way new BitCoins are actually created). This "lottery" of finding the new correct proof ensures that the power of creating new blocks is decentralised. When a new block is mined it is sent out to everybody so that every node in the network has a copy of the latest blockchain. The idea that the longest blockchain in the network (the one which "the most work was put into") is the valid version of the blockchain is called "decentralised consensus[1]".

As suggested in a blog regarding block creation, one can define a PoW like find the next number that is divisible by 99 and divisable by the proof-number of the last block**:**

```
library("digest") #Loading the hash-algorithm
### Simple Proof of Work Alogrithm
proof_of_work <- function(last_proof)
{
proof <- last_proof + 1
# Increment the proof number until a number is found that is divisable by 99 and by the proof of the previous block
while (!(proof %% 99 == 0 & proof %% last_proof == 0 )){
   proof <- proof + 1
 }
return(proof)
}
```

3.4. Adding new blocks

First, one should define the start block, the first block in the chain:

```
# Define Genesis Block (index 1 and arbitrary previous hash)
block_genesis <-  list(index = 1,
    timestamp = Sys.time(),
    data = "Genesis Block",
    previous_hash = "0",
    proof = 1)
```

Now, adding blocks to the chain cand be done with a function like:

```
#A function that takes the previous block and optionally some data (in our case just a string indicating which block in the chain it is)
gen_new_block <- function(previous_block){
#Proof-of-Work
new_proof <- proof_of_work(previous_block$proof)
#Create new Block
new_block <- list(index = previous_block$index + 1,
    timestamp = Sys.time(),
    data = paste0("this is block ", previous_block$index +1),
    previous_hash = previous_block$new_hash,
    proof = new_proof)
#Hash the new Block
new_block_hashed <- hash_block(new_block)
return(new_block_hashed)
}
```

3.5. Building the Blockchain

To build the blockchain, the algorithm should start with the first block, previously defined:

```
# Create blockchain
blockchain <- list(block_genesis)
previous_block <- blockchain[[1]]
# How many blocks should we add to the chain after the genesis block
num_of_blocks_to_add <- 20
# Add blocks to the chain
for (i in 1: num_of_blocks_to_add){
print(system.time(block_to_add <- gen_new_block(previous_block))) # Evaluate time it takes for PoW
```

[1] https://correlaid.org/blog/posts/blockchain-explained

```
    blockchain[i+1] <- list(block_to_add)
    previous_block <- block_to_add
    print(paste0("Block ", block_to_add$index, " has
been added"))
    print(paste0("Proof: ", block_to_add$proof))
    print(paste0("Hash:                    ",
block_to_add$new_hash))
    }
```

4. Conclusions

Blockchains are a revolutionary solution for a such variety of industries. The data validation and the lack of so called middle man, minimizing the fees, increasing the speed of transactions and the security and anonymity provided by this technology are good arguments for ensuring the continuous development of the technology and its spreading in every day activities.

References

- Dusa A., Oancea B., Caragea N., Alexandru C., Jula N.M., Ciuhu(Dobre) A.M., 2015, *R cu aplicatii in statistica*, Editura Universitatii din Bucuresti
- https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/2/#1411e3d773bc
- https://blockgeeks.com/guides/what-is-blockchain-technology/
- https://correlaid.org/blog/posts/blockchain-explained