2-2022

Blockchain: Key Principles

Nadezda Chikurova
The Graduate Center, City University of New York

BLOCKCHAIN: KEY PRINCIPLES

by

NADEZDA CHIKUROVA

A master's capstone project submitted to the Graduate Faculty in Data Analysis and Visualization in partial fulfillment of the requirements for the degree of Master of Science, The City University of New York

2022

Blockchain: Key Principles

by

Nadezda Chikurova

This manuscript has been read and accepted for the Graduate Faculty in Data Analysis and Visualization in satisfaction of the capstone project requirement for the degree of Master of Science.

Date	Aucher Serr Capstone Project Advisor
Date	Matthew Gold Program Director

THE CITY UNIVERSITY OF NEW YORK

ABSTRACT

Blockchain: Key Principles

by

Nadezda Chikurova

Advisor: Aucher Serr

"Blockchain: Key Principles" is an interactive visual project that explains the importance of data privacy and security, decentralized computing, and open-source software in the modern digital world through the history of the underlying principles of blockchain technology. Some of these key concepts have their roots in the time before the Information Age. By explaining the history of these principles, I want to present the fact that over the past centuries, humanity has been fighting for their privacy, security, and the ability to efficiently express themselves one way or another. Blockchain technology, which was introduced to the public in 2008 through a White Paper and launched in 2009 as Bitcoin cryptocurrency, provides a possible approach to achieving these goals.

While initially blockchain technology was created to improve the financial industry, the structure of blockchain, which allows users to store, validate and transmit data, provides transparency, decentralization, and trust and could also be profitable in other economic, legal, and political systems.

Stable link of the project: https://nchikurova.github.io/history-of-blockchain/key-principles/.

TABLE OF CONTENTS

Abstract…….....……iv

List of Figures…….vi

Digital Manifest…….vii

A Note on Technical Specifications…….viii

Design Decisions and Challenges…….……ix

Content…….....ix

Structure…….....x

Style……..….....xiii

Introduction……...……..1

Foundation in Coursework……..2

Project Narrative……..4

Continuation of the Project……..7

The Mystery of Satoshi Nakomoto……..7

The Cypherpunk Movement……..10

The History of Digital money……...……11

Summary……16

Bibliography…..……17

LIST OF FIGURES

Figure 1: Initial webpage design. Timeline chart……..……....xii

Figure 2: Initial webpage design. Overview…….....…….…..…xii

Figure 3: Final webpage overview (screenshot)……..……xiii

Figure 4: Design decisions…….....…...……xiv

Figure 5: The Mystery of Satoshi Nakomoto…….……..……..……..9

Figure 6: The Cypherpunk Movement…….……11

Figure 7: The History of Digital Money……..……..13

DIGITAL MANIFEST

I. Capstone Project Whitepaper (PDF)

II. WARC File

a. Project Website

Archived version of https://nchikurova.github.io/history-of-blockchain/key-principles/

III. Code and other deliverables

Zip file containing the contents of GitHub repository at the time of deposit.

(https://github.com/nchikurova/history-of-blockchain)

A NOTE ON TECHNICAL SPECIFICATIONS

The project “Blockchain: Key Principles” is hosted on the GitHub pages and presented as a webpage. I used JavaScript programming language for most of the functionality, D3.js library for creating a timeline chart, and Scrollama.js to set the scrolling storytelling. D3.js library was chosen for the purpose of creating a visually simple but informative scatterplot. For Y-axis I used the Time scale (d3.scaleTime) to distribute years of the events chronologically, and for X-axis I used the Band scale (d3.scaleBand) to position the categories at the same distance from each other. While the user scrolls the page down, a few events happen simultaneously. The title of the category remains the same on the top left first (“sticky” position in CSS), and the title of the event included in this category on the right top changes according to the event displayed in the article. At the same time one of the articles on the left becomes “active”, changes the background color, and displays the description of the event, while the circle on the right side that corresponds to the year of that event changes color to black. This structure allows users to follow the story on the timeline while reading information about the event.

The repository on the GitHub pages is named **history-of-blockchain** and contains the following folders:

- key-principles (code)
- data (data used in the project)
- images (illustrations for the text)
- README.md (a brief description of the project)

Key-principles file includes the following code:

- .main.js (setting up Scrollama.js and event handles, includes the functionality of buttons)

- .scatterplot.js (contains code for drawing a scatterplot with data points as circles represented as a vertical timeline)
- .index.html (contains a structure of the webpage and short articles, links to resources)
- .style.css (includes the style of all elements in the webpage)
- .prettierrc (Prettier Code Formatter – automatically formats code to set conditions)

Data folder includes *data.csv* file, which has basic structure and contains the following data points:

- Type: the category names
- Name: the names of the events
- Year: the years the events occurred
- Step: consecutive count of the events

Design Decisions and Challenges

1. Content

For this project, I chose three key principles of blockchain technology: cryptography, open-source software, and decentralization, which I wanted to display through the main points of their history. The biggest challenge was to choose the most important points for each category that would provide chronological order, be connected to each other, be concise enough to be understandable for first-time readers and be informative at the same. I ended up including four key points in each category and providing extra sources so if the reader would be interested in more information, he/she will follow the links. For instance, if I had more time, I would have added a section about Morse code and telecommunications to the Cryptography category and a section about Microsoft, Bill Gates, and "An Open Letter to Hobbyists" (Gates) to the Open-source software category.

Originally, I wanted to include three key principles of blockchain only. However, it seemed

logical to me to add another path that led to blockchain technology – the Digital Money category. To visualize this path, I added five points: David Chaum (“DigiCash”), Adam Back (“HashCash”), Wei Dai (“B-Money”), Nick Szabo (“BitGold”), and Satoshi Nakomoto (“Bitcoin”). I gave lower opacity to the circles of this category and stated in the parenthesis of the title “coming next” to let the reader know there will be a continuation of this project. I wrote about the importance of the connection between digital money development and blockchain in chapter Continuation of the Project.

2. Structure

The idea of a timeline came to me instantly when I decided to create a project that includes chronological events. I think the timeline makes it visually easier for the human mind to follow the story, especially when the story contains multiple paths.

Initially, I planned to represent the timeline of the chart horizontally (Figure 1 and 2). However, after considering the wide use of mobile devices which are mostly vertical, and the different widths of the screens this project will be viewed on, I decided to switch the horizontal chart to vertical. I placed the earlier points of history at the top and modern data points at the bottom of the page. This direction also gives users a better sense of ‘scrolly telling’ since scrolling starts from the top of the page. In addition, the articles on the left side that represent every data point on the right side of the screen are significantly important content in the storytelling, and the vertical position of the chart allows text to obtain a larger portion of screen space. This decision brought up the biggest technical challenge: the responsivness of the webpage. Responsive web design is a web development approach that allows the content on the page to change dynamically depending on the size and orientation of the screen this content is viewed on. On mobile devices, the text of the articles and the timeline chart must be larger, but on computer screens the chart

should be smaller to fit vertically, and articles – wider. I solved this problem by setting the SVG of the chart as a viewBox and dividing the possible width of the screen into three sections (0 to 700px, 700px to 900px, 900px to max-width), where the smaller the width of the screen the larger the font of the text. Setting up the size of the article, margins, and padding I used a REM unit of CSS instead of pixel, which is relative to the font size of the html elements and automatically scales up and down elements on the webpage.

To represent the changes of data points on the timeline while scrolling, initially I wanted to make the size of the active circle larger. However, to save space visually, I decided to keep the size of the circles consistent and change the filling color of the circle instead. By hovering over the circles, users will be able to see the information about each data point: name of the event and the year this event occurred. Click on the circle would bring users to the article that corresponds to the circle. This would be helpful if users want to read the article again or follow their own sequence of the project. The clicked circle's border becomes thicker to let the user know which circles were clicked already.

In the future, I would like to make responsive design for mobile devices more accessible.

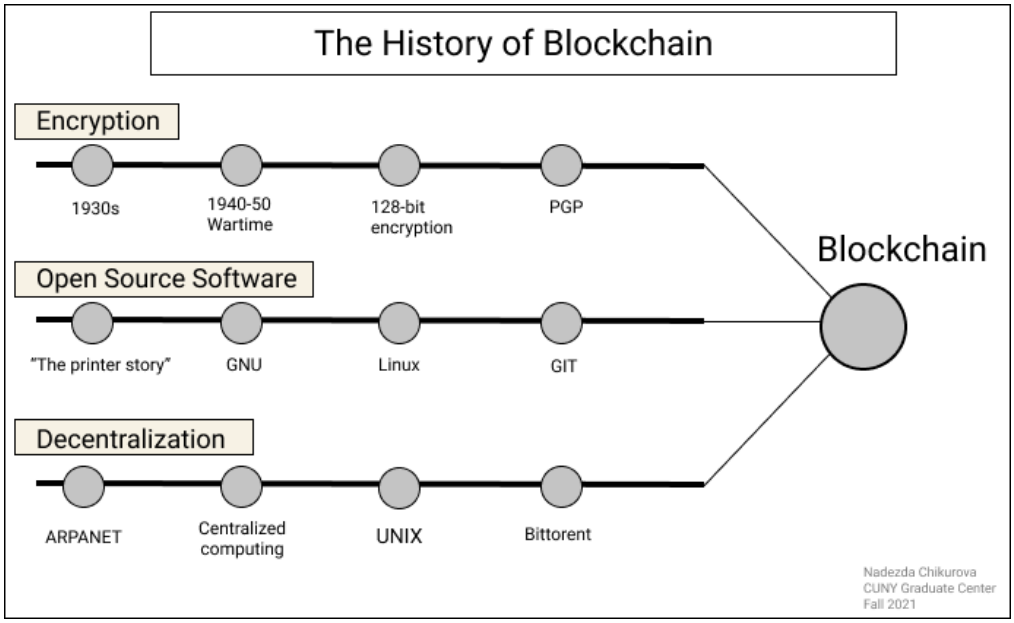

Figure 1: Initial webpage design. Timeline chart

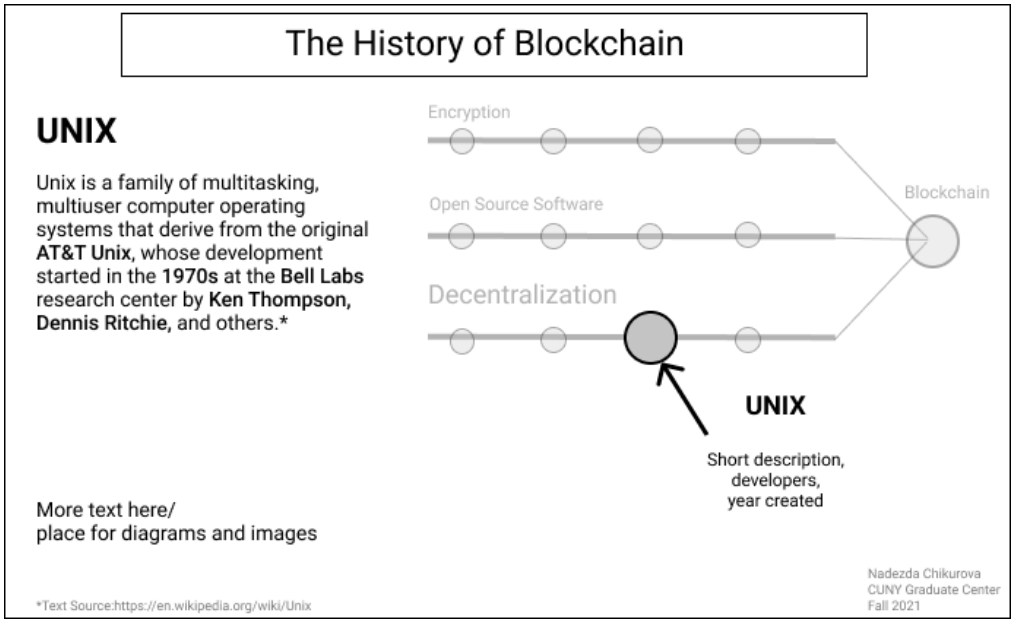

Figure 2: Initial webpage design. Overview.

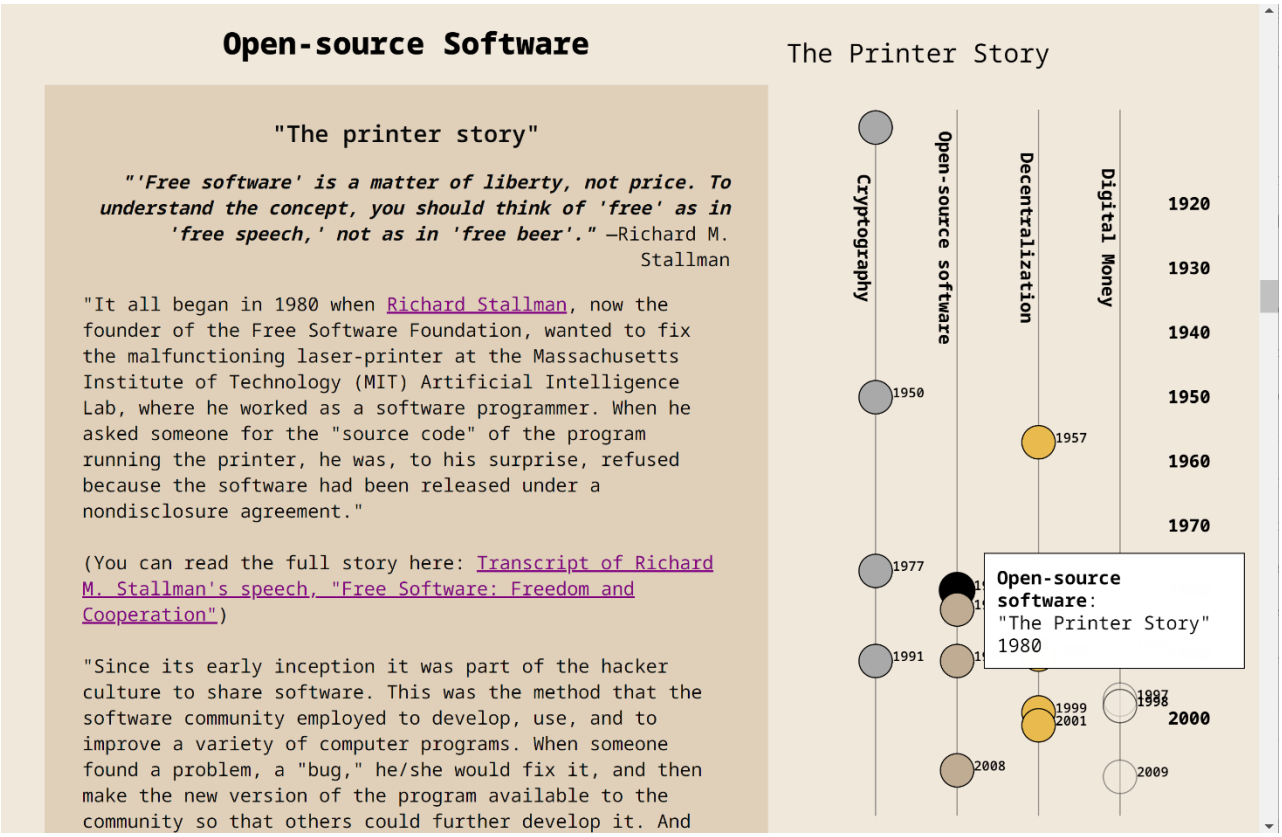

Figure 3: Final webpage overview (screenshot).

3. Style

The color scheme for the project was inspired by the color of Papyrus paper – paper that was used by ancient Egyptians for writing. Since one of the key principles described in this project is Cryptography which takes its roots in ancient times, I thought this color scheme would bring the presence of history and mentally would take users back in time. Instead of using bright modern colors, which might take the user's attention away from the content of the project, I decided to use pastel tones.

When thinking about the font, I wanted this project to be different from the modern articles in magazines and give the reader the association with the typewriter font. For this purpose, I chose Noto Sans Mono family fonts and used different weights on the text.

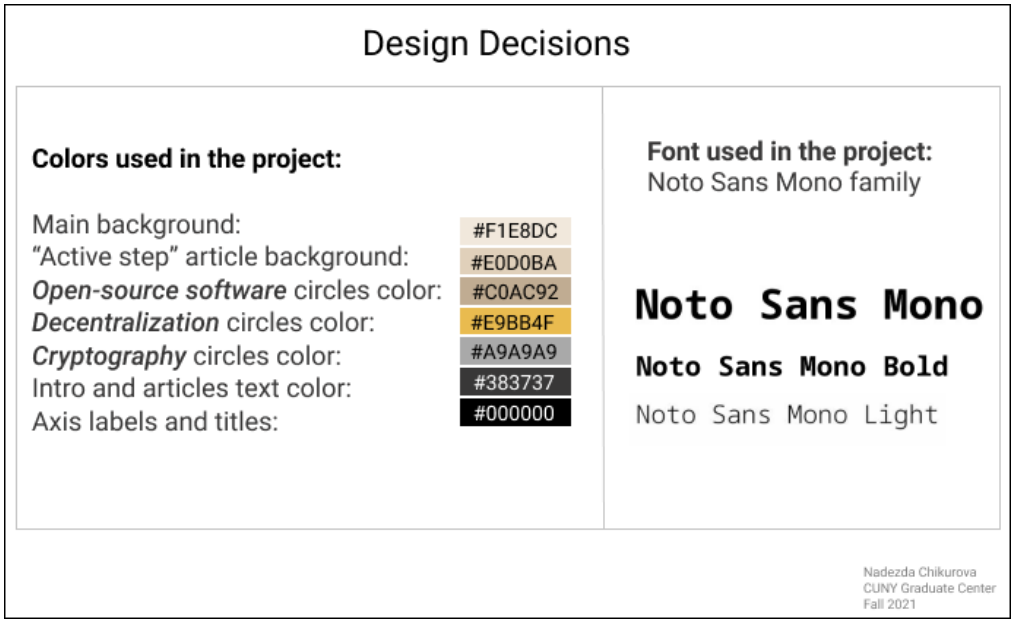

Figure 4: Design decisions

All figures for White Paper, except Figure 3, which is a screenshot of the webpage, were created in Figma.com.

Introduction

In October 2008 an unknown individual or a group of individuals under the name of Satoshi Nakomoto published a white paper "Bitcoin: A Peer-to-Peer Electronic Cash System," in which Bitcoin was described as "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (Nakomoto, 1). Bitcoin was launched in January 2009 and became the first successful cryptocurrency.

Nowadays there are thousands of cryptocurrencies in the world. However, despite the cryptocurrencies' popularity, not everyone understands what they are and how they can affect our future. There are two main questions I want to address in this project. First, what is the history leading up to the creation of cryptocurrencies? Second, do cryptocurrencies have real value? I believe the real value of cryptocurrencies is in the technology they are built on – blockchain.

"Blockchain: Key Principles" is an interactive visual project that explains the importance of data privacy and security, decentralized computing, and open-source software in the modern digital world through the history of the underlying principles of blockchain technology. Some of these key concepts have their roots in the time before the Information Age. By explaining the history of these principles, I want to present the fact that over the past centuries, humanity has been fighting for their privacy, security, and the ability to efficiently express themselves one way or another. Blockchain technology, which was introduced to the public in 2008 through a White Paper and launched in 2009 as Bitcoin cryptocurrency, provides the opportunity to achieve these goals. "The biggest threat to privacy that we face is that the power of computing is doubling every 18 months. The human population is not doubling every 18 months but the ability for computers to keep track of us is," says Phil Zimmerman, reminding us of Moore's Law ("A Short History of Cryptography"). Zimmermann is the inventor of Pretty Good Privacy, which is software that

provides data communication privacy through encryption. While initially blockchain technology was created to improve the financial industry, the structure of blockchain, which allows users to store, validate and transmit data, provides transparency, decentralization, and trust and could also be profitable in other economic, legal, and political systems.

Foundation in Coursework

"Blockchain: Key Principles" is the intersection of my experiences in the courses and workshops from the Data Analysis and Visualization program at the CUNY Graduate Center.

The course *Visualization and Design* introduced me to the fundamentals of data presentation, the techniques of communicating with the audience through data, design decisions, and storytelling. I have learned different approaches for working with qualitative and quantitative data, techniques for data cleaning and manipulation, strategies for identifying potential weaknesses in the collection methods, and the structure of the underlying datasets. I was able to apply these fundamental principles of presenting and manipulating data for every subsequent project I created.

The *Interactive Data Visualization* and *Advanced Interactive Data Visualization Studio* courses taught me how to create complex interactive data visualizations using JavaScript libraries, build web pages with HTML, CSS, and JavaScript and to host them on GitHub. These courses introduced me to web development and web design and showed me a way of manipulating and presenting data using programming and coding. Through both of these courses, I built a strong foundation in front-end development, web page design and structure, and the representation of large data sets through interactive visualizations. For the next semesters, I used this knowledge to present my projects for other courses, and to implement my own ideas through their digital representations, which are available to the public.

The idea of this capstone project came from my final project for the *Alternative Data*

Culture course. This course aimed to explore alternative approaches to representing and understanding data, searching for hidden interpretation, and embracing subjective perspectives to generate new knowledge and create new meanings. We studied the aesthetics of text, art, digital images, and movies as objects of data visualization. One of the concepts that stood out for me was the interpretation of human thought through digital representation. In her book *SpecLab: Digital Aesthetics and Projects in Speculative Computing*, Johanna Drucker argues that code is material, and every digital piece is the presentation of human thought:

> In every generation, some version of this question has been posted: If it were possible to understand the logic of human thought, would there be a perfect representation of it in some unambiguous, diagrammatic symbol set? This question, informed by classical metaphysics and philosophy, persists not only in contemporary struggles within the very different domains of visual art, information design, and computer graphics, but also in early formulations of cognitive science, with proximity to symbolic logic, and in debates over artificial intelligence (Drucker).

As the object of my research, I chose a relatively new at that time movement in digital art – NFTs. As my final project, I explored NFTs (Non-Fungible Tokens) as a form of the interpretation of the human mind in the digital environment. By creating this project, I learned that the main value of NFTs is their uniqueness. Each of these digital projects has a certificate of authenticity, which is provided by the technology they are built on – blockchain. By learning more about blockchain and what can be created with it, I became interested in the initial purpose of creating it as well as its impact on our future.

Lastly, attending numerous Python workshops and Python Users Group meetings led by Digital Initiatives prepared me for taking the *Advanced Programming Techniques* course at the School of Professional Studies. This course provides Python techniques in the context of data

manipulation, data analysis, and basic machine learning. One part of this course is applying Python to building blockchain. Through this assignment, I learned blockchain data structure and its hashing algorithm which provide the transparency and security of the stored data and the decentralization of the technology itself.

Project Narrative

The goal of this project is to present to the audience the significance of blockchain technology through the history of the development of its key principles.

"Two hundred years ago, all conversations were private. The right to a private conversation was a natural right, not just in a philosophical sense, but in a law-of-physics sense, given the technology of that time," writes Phil Zimmermann in "PGP User's Guide" (Zimmermann). The information age has transformed the approach towards data. Now, most of our conversations are conducted electronically, and therefore, could be easily accessed, and stored without our knowledge. Advanced technology takes control now of data acquisition, data manipulation, data security and data privacy. This is where blockchain technology would be able to assist data science. Data science, like every other industry, has its own limitations which include privacy issues and rogue data. In the article "How Blockchain Will Disrupt Data Science: 5 Blockchain Use Cases in Big Data", the author explains that "through decentralized consensus algorithm and cryptography, blockchain validates data making it almost impossible to be manipulated due to the huge amount of computing power that will be required" (Sarikaya). Therefore, blockchain technology ensures the security and privacy of data through its decentralized system.

The intended audience for this project is anyone who is interested in information technology, finance, web development, development of cryptocurrencies and blockchain or anyone who is curious about the history of cryptography, open-source software, and

centralized/decentralized computing. My goal is to make this project understandable and easy to navigate for people with different backgrounds. It is more difficult to accept something new without knowing where it comes from than to accept something we have been familiar with for years. If people understood the history of blockchain technology and the initial value behind it, it would be easier for everyone to see the potential and the future of this technology.

Like any new advanced technology, blockchain has its limitations. The high security of the ledger comes with high energy cost. New blocks on Bitcoin are mined through a decentralized consensus algorithm called Proof-of-Work (POW), which is used to generate a unique hash for every new block and confirm transactions through solving complex mathematical equations (Nakomoto, 3). Because solving the mathematical problem is only possible through numerous trials and errors, computers must run constantly to win the race of verifying the latest transaction of a new block and being rewarded with a bitcoin. While verifying a new block does not require much time and energy consumption, creating a new block is a much more difficult process and takes approximately ten minutes. Once a new block that satisfies the network's algorithm is created, the nodes are still competing while waiting for the final confirmation.

Since mining Bitcoin is becoming more profitable and, therefore, more popular, miners are drawn to places with low electricity rates: "While popular accounts of Bitcoin's energy usage describe the massive, abstract amounts of electricity that the network consumes, in practice, the geography of Bitcoin is highly uneven and intertwined with the infrastructural and ecological structures on which it depends" (Lally et. al. 1). Using not only electricity, but other natural sources of energy, Bitcoin mining becomes a deeper environmental issue. "As Bitcoin miners plug into existing electrical infrastructures to power their mining equipment, they become part of complex circulatory systems of electricity, resources, and capital that have been central to the production of the spaces of Central Washington" (Lally et. al. 9).

One of the solutions for this problem is using a newer consensus mechanism known as Proof-of-Stake (POS). POS algorithm substitutes staking for computational power, so users' mining power is limited to the percentage of ownership staked. It means that the percentage of the new blocks each miner can generate is proportioned to the percentage of coins they hold. Using POS drastically decreases the computational power which is needed to mine a block by a single piece of hardware. POS, however, is less secure than a decentralized POW algorithm.

The high energy cost is not the only limitation of blockchain technology. The high secure protocols slow down the transactions speed and the network in general and allow users to store only a limited amount of data. Decentralization of the network also has a drawback. It is very expensive and almost impossible to attack the ledger, however, there is a chance. It is called a "51% attack". "If a miner, or a group of them, has more than half the computing capability of the network, it can rewrite the blockchain" (Aponte-Novoa et al.). For this reason, bitcoin mining pools are being watched closely by the community to ensure that no one will gain such influence. Finally, the immutability of the ledger makes it hard to erase any human error or remove any piece of data once it is written.

While developers and scientists keep working on solving the problem of high energy consumption and maintaining security and speed of transactions on blockchain, this technology has already impacted the financial and technical world. Therefore, I think it is important to dive into the key principles of this technology and their history. For this project I chose three key principles of blockchain: cryptography, open-source software, and network decentralization.

Through decentralized algorithms and cryptography blockchain ensures data validation, immutability, identity verification, security, and transparency of the data records, as well as fraud and attack protection. Open-source software allows developers to access the source code, inspect and share it, therefore, to improve blockchain limitations and take this technology to the next level.

The variety of the features that compile with data in a new way allows blockchain to assist many different industries in multiple ways.

The Blockchain report "Forward Together" that draws input from 2965 conversations with C-suite executives, shows that in 2017 over one third of organizations across all industries and regions were already considering or were actively engaged with blockchain, and 66% of early adopters—or explorers—intend to adopt a new platform business model that breaks the boundaries of traditional market exchanges ("Forward Together").

Continuation of the Project

There are many different documentaries, videos, articles, and books that explain the history and timeline of the evolution of digital money. However, I haven't seen any interactive visual projects presented on a webpage that users can explore at their own pace. For viewers who are new to this topic, it might be difficult to understand information as fast as it is presented in the documentaries and videos. Also, those people who absorb information more easily through visual medium might find it hard to read long articles and books. Therefore, I plan to continue this project in the future to provide a more interactive approach.

Despite technological advancement, the future of Bitcoin and cryptocurrencies' is still uncertain, and the high natural resources consumption problem has yet to be solved. However, it is almost impossible to take control over Bitcoin mining, even for the government. One of the main reasons for it is the anonymity of Bitcoin's inventor. This leads me to the first possible project extension.

1. The Mystery of Satoshi Nakomoto *(Figure 5)*

While this topic is more entertaining than educational, the question of Bitcoin's inventor is one of the most discussed not only in the crypto community, but all over the world. It involves a lot

of research and logical thinking and remains unsolved. Satoshi Nakomoto is the name that was used by Bitcoin's creator. Pseudonymity allows the project to stay neutral since there is no charismatic leader behind Bitcoin, and the project cannot be associated with any personality. Pseudonymity also protects the founder from any type of attack or government control.

Satoshi Nakomoto was the first figure who worked on digital money and decided to stay unknown. All previous people who ever worked on digital money projects revealed their real names: David Chaum ("DigiCash"), Adam Back ("HashCash"), Wei Dai ("B-Money"), Nick Szabo ("BitGold"). A few years after announcing the project, Nakomoto disappeared leaving the code of Bitcoin as open-source software and giving the chance to other developers to work on and improve this code. There are many theories about who Satoshi Nakomoto is. Bitcoin's creator might be an individual, a group of individuals or even an organization.

The first possible candidate is Harold Finney. Hal Finney is a software developer who was advocating for cryptography and digital privacy, also known as the first person who helped Satoshi ("The Wall Street Journal"). The first-ever Bitcoin transaction was between Nakomoto and Hal Finney. In addition, Hal Finney was a neighbor of the person named Dorian Satoshi Nakomoto, who had no knowledge about the technical side of Bitcoin when asked. Hal Finney, however, denied being Satoshi Nakomoto (Finney). Harold Finney died from complications of Amyotrophic lateral sclerosis in 2014.

Another personality that some might think is behind the name of Satoshi Nakomoto is Adam Back. Adam Back is the founder of HashCash, one of the early attempts at creating digital money, which introduced the Proof-of-Work mechanism. Since Nakomoto communicated only digitally, his emails are one of the factors that are under close examination ("Bitcoin P2P E-Cash Paper"). Adam Back's email replies to other bitcoiners show that his technical understanding of blockchain was more advanced than others. Adam also had the right set of skills, experience,

writing patterns, and his absence in the time of Satoshi being around – all these facts are the evidence of the theory that Adam Back can potentially be Satoshi Nakomoto ("The Strange Story of Satoshi Nakomoto's Spelling Choices").

A third possible candidate is Nick Szabo, the creator of Bit Gold, another early attempt at creating digital cryptocurrency, and the idea of smart contracts, which was introduced in his paper "Smart Contracts: Building Blocks for Digital Markets" in 1996 (Szabo). He was also not as active as other cryptocurrencies activists in the time of Satoshi Nakomoto's presence, despite the fact that Bit Gold is one of the prototypes of Bitcoin. Interestingly, there is no reference to Bit Gold in Bitcoin white paper, even though there are clear similarities in between their systems used to process transactions and to secure the decentralized network.

Besides names mentioned above, there are several more personalities that are connected to Satoshi Nakomoto's name. However, the candidates above are the most well-known people who are related to Nakomoto and Bitcoin and all of them are members of the cypherpunk community, which leads me to the next possible extension of my project.

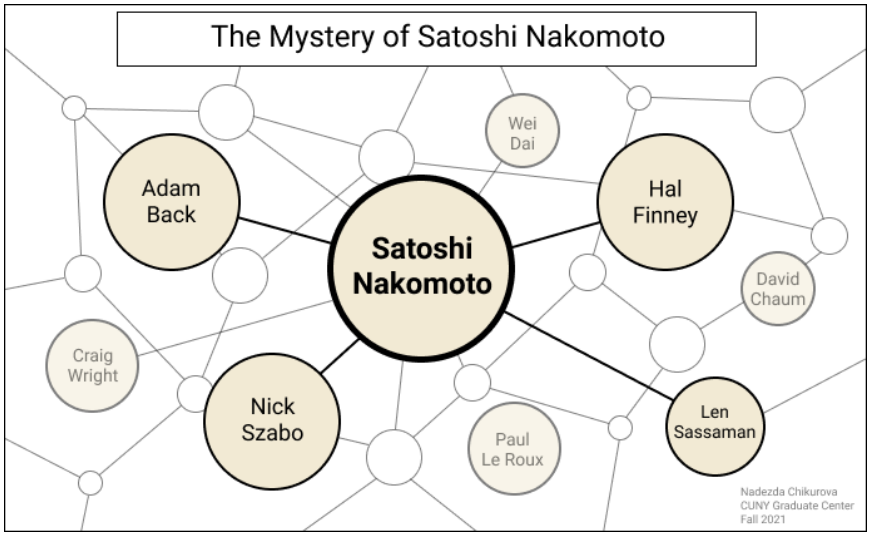

Figure 5: The Mystery of Satoshi Nakomoto

2. The Cypherpunk Movement *(Figure 6)*

The cypherpunk movement is the community that is advocating for the privacy of individuals through cryptography. This movement was founded in the early 1990s by a few scientists who started to meet regularly to discuss their work and related ideas. They also created the Cypherpunk mailing list in which many proposals and developments were discussed including the ones that later lead to Bitcoin. Eric Hughes, one of the first cypherpunks, wrote "A Cypherpunk Manifesto", where he describes the key principle of cypherpunk movement - the importance of privacy. "Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world" (Hughes)**.** The ideas explained in the *Cypherpunk Manifesto* became the fundamental concepts for early attempts of developing digital currencies. The concepts presented in the *Cypherpunk Manifesto* are as relevant today as they were in 1993:

> We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do (Hughes).

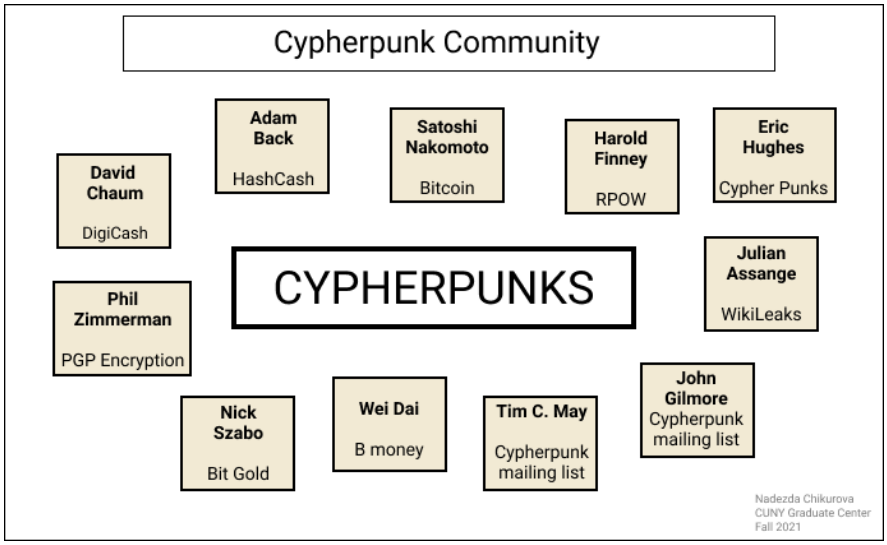

Figure 6: The Cypherpunk Movement

3. The History of Digital Money *(Figure 5)*

Is it a coincidence that Bitcoin was introduced the same year that the U.S. financial crisis happened? In that time many people started to reconsider the role of government and banks in the financial system, and, possibly, look for some type of alternatives.

To speak about digital money, we need to answer a few questions first: What is money? Where does money come from and what is its purpose?

Nineteenth century economist Carl Menger first described how money evolves naturally and inevitably from a sufficient volume of commodity barter (Menger 239-55). From ancient times till nowadays, money is just an exchange medium for goods. In ancient times many different objects were used as money: rocks (Rai stones), beads, seashells, cattle, and even salt. The English adjective *pecuniary* and noun *salary* were derived from the Latin words *pecus* (cattle) and *sal* (salt) (Fekete). Historical accounts show that the most salable seashells were usually the ones that were scarcer and harder to find, because these would hold value more than the ones that can be found easily (Szabo). According to Carl Menger, a good's salability across the time refers to its ability to hold value into the future, allowing the holder to store wealth in it (Menger 239-55).

Later, seashells, rocks and other objects were replaced by coins made from the rare metals: gold, silver, and copper. Due to metals' durability, they held the value of money across time better than any other goods (Ammous ch.1) To store money and wealth people needed a safe place to keep their coins – that is how the first predecessors of banks appeared. Since it was too heavy to carry metallic coins around, people would bring them to one place where the banker would store them in a safe and give out a paper that proved how many coins each holder had in the bank and how many were taken out.

Later, the bankers realized that almost no one was taking out all the coins they own at once, and, therefore, the bankers could use this money to lend it to someone else for compound interest or use it for their own purposes.

This realization was the first step for creating the banking system we have now – the fractional reserve system: banks are permitted to keep only a fraction of deposited money in the bank. The next step to exploit this system was understanding that nobody knows how much physical money is in a bank and the amount of money being lent to a third-party on paper could exceed the amount of physical money in the bank. The ratio of banks' total loans to its total deposits is called loan-to-deposit-ratio. For example, if the loan-to-deposit ratio is 0.9, it means that for every 10% of existing money in the bank (deposit), the bank can lend 90% of the money to someone else (loans), where 90% of loans are new money created by banks. According to the board of Governors of the Federal Reserve System, as announced on March 15, 2020, the Board reduced reserve requirement ratios to zero percent effective March 26, 2020. This action eliminated reserve requirements for all depository institutions (Federal Reserve Board - Accessed 16 Nov. 2021).

The only problem the banker can face is if all the customers decide to take out their money at the same time. This problem was solved by centralizing the banking system; if one of the banks

does not have enough money to give back to depositors, the Central Bank can always provide this money. This system has failed a few times in the history of the United States, including the financial crisis in 2008.

In the past, all created money needed to be registered on paper – declarations, statements, checks, nowadays most money is digital and even easier to create. The new money created by the Federal Reserve has formed the national debt. According to the U.S. Department of the Treasury, the national U.S. debt by November 2021 is $28.8 billion (United States Department of the Treasury - Accessed 16 Nov. 2021).

The ideology behind Bitcoin comes from the Austrian school of economy. They believed that an infinite supply of money is one of the factors that lead to inflation. "Followers of the Austrian school strongly believe in the need for a market-selected money-form with a finite supply, leading many of them to advocate for a return to the gold standard. For this reason, the upper limit is purposeful in the design of Bitcoin and derives from the Austrian school of economics' suspicions of fiat currency" (Lally et. al. 2). There will never be more than 21 million of Bitcoin. The upper limit of bitcoins is meant to provide a "known supply and a known inflation schedule, unlike fiat money" (qtd. Lally et. al. 5).

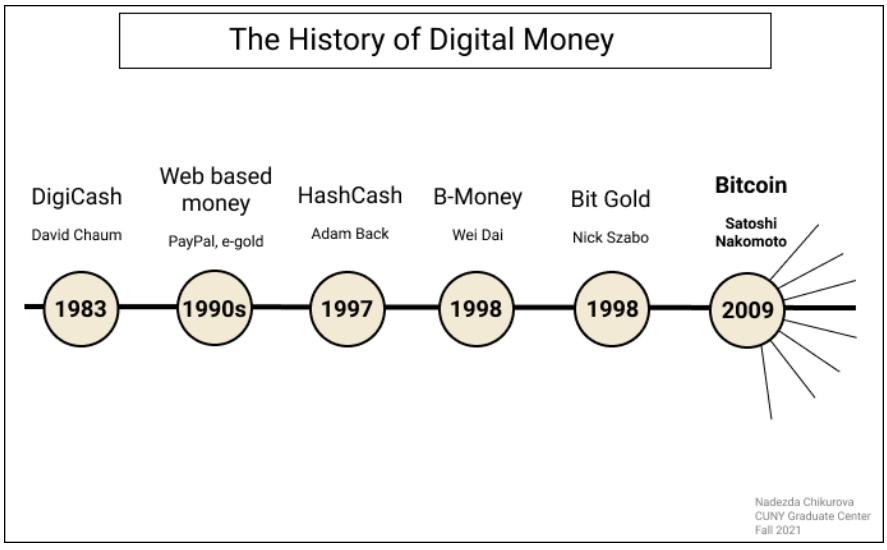

Figure 7: The History of Digital Money

The history of the development of digital money has a significant impact on the existence of the blockchain. Despite the importance of the blockchain key principles I describe in my project, blockchain technology would not exist if it were not for creating an alternative to the traditional form of money. The idea of creating digital money, or cryptocurrencies, enabled scientists to generate many ways of improving some features of the current financial system, especially in the digital world we live in now. Each attempt of creating digital money was bringing to the world more advanced technological mechanisms and concepts, that, one way or another, would better protect, store, record, or transmit data throughout the internet. While the focus of this project is not on attempts to substitute the current financial system and replace traditional money with cryptocurrencies, I think it is important to mention digital money when speaking of the blockchain.

Initially, the blockchain technology was developed to improve some aspects of the current financial system or/and introduce a new cash system. However, the technology itself already has had an impact on the other industries, like healthcare or supply management chain. Atzori suggests that it also has a potential to restructure society and government services. "The blockchain technology potentially allows individuals and communities to redesign their interactions in politics, business and society at large, with an unprecedented process of disintermediation on large scale, based on automated and trustless transactions" (Atzori 46). Some areas of our lives historically relied on third parties to establish a certain amount of trust.

> Reorganizing societies is of prime importance in poor countries. Wealth can be protected more effectively using the blockchain. These existential threats can be controlled by integrating land titles into the blockchain. Especially in the third world, landowners have problems to prove the ownership if for example the local government aims to expropriate

the population (Nofer et. al. 183 -187).

The identity verification through blockchain can also be used in the third world and by immigrants when the proof of identity is lost. The decentralized trust or trust-by-computation, ensured by proof-of-work protocol, makes presence of human intervention or controlling authority unnecessary. Atzori identifies this protocol as “a shift from trusting people to trusting math” and states that its “applicability goes far beyond the creation of decentralized digital currencies” (qtd. in Atzori 45).

Summary

Blockchain is a distributed ledger that holds, records, and transmits data. Blockchain is the underlying technology which Bitcoin was built on. Even though blockchain is still relatively new technology and needs to be researched and studied to utilize its best qualities and increase its efficiency, it has already impacted many industries, such as finance, healthcare, supply chain, manufacturing, and others.

The history of underlying principles of blockchain described in this project should help us to identify the most important features of blockchain and to understand the potential of this technology, and possible impact on the future.

Encrypted algorithms ensure the security and automated trust of the ledger, as well as the stability and immutability of the data records. Decentralization of the network provides protection, transparency, and verification of the data. Open-source nature of this software allows everyone to inspect, share and improve the code while maintaining the transparency of the data and changes on the platform.

In addition, one of the most important features of blockchain is that this technology allows users, businesses, and industries to build applications on top of the ledger which provides countless possibilities of beneficial utilization of blockchain in the future.

Bibliography

Ammous, Saifedean. *The Bitcoin Standard: The Decentralized Alternative to Central Banking.* John Wiley & Sons, Incorporated, 2018, ch.1.

Aponte-Novoa, Fredy Andres, et al. "The 51% Attack on Blockchains: A Mining Behavior Study." *IEEE Access*, vol. 9, 2021, pp. 140549–64. *IEEE Xplore*, https://doi.org/10.1109/ACCESS.2021.3119291.

Atzori, Marcella. "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" *Journal of Governance and Regulation*, vol. 6, no. 1, 2017, pp. 45–62. *DOI.org (Crossref)*, https://doi.org/10.22495/jgr_v6_i1_p5.

Bitcoin P2P E-Cash Paper | Satoshi Nakamoto Institute. https://satoshi.nakamotoinstitute.org/emails/cryptography/threads/1/?view=satoshi. Accessed 22 Dec. 2021.

Bostock, Mike. *D3.Js - Data-Driven Documents*. https://d3js.org/. Accessed 29 Dec. 2021.

Drucker, Johanna. *SpecLab: Digital Aesthetics and Projects in Speculative Computing*. Chicago; London: University of Chicago Press, 2009, pp. 1-126.

fb. *A Short History of Cryptography - A Brief History of Cryptography*. 2012. *YouTube*, https://www.youtube.com/watch?v=H9Cu36Qj3dQ.

Finney, Harold. *Bitcoin and Me (Hal Finney)*, 2013. https://bitcointalk.org/index.php?topic=155054.msg1643833#msg1643833. Accessed 22 Dec. 2021.

Gates, Bill. *An Open Letter to Hobbyists*, 1976. https://archive.nytimes.com/www.nytimes.com/library/cyber/surf/072397mind-letter.html. Accessed 21 Dec. 2021.

Goldenberg, Russell. *Russellgoldenberg/Scrollama*. 2017. 2021. *GitHub*,

https://github.com/russellgoldenberg/scrollama.

Hudges, Eric. *A Cypherpunk's Manifesto | Satoshi Nakamoto Institute*. https://nakamotoinstitute.org/cypherpunk-manifesto/. Accessed 23 Dec. 2021.

Jonathan Soma. *Building a Scrollytelling Site with Scrollama.Js (No D3, No Magic)*. 2021. *YouTube*, https://www.youtube.com/watch?v=d7wTA9F-l8c.

Lally, Nick, et al. "Computational Parasites and Hydropower: A Political Ecology of Bitcoin Mining on the Columbia River." *Environment and Planning E: Nature and Space*, Aug. 2019, p. 251484861986760. *DOI.org (Crossref)*, https://doi.org/10.1177/2514848619867608.

Menger, Carl. "On the Origins of Money", Economic Journal, vol. 2, (1892) pp. 239-55, https://socialsciences.mcmaster.ca/~econ/ugcm/3ll3/menger/money.txt. Accessed 23 Dec. 2021.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. https://nakamotoinstitute.org/static/docs/bitcoin.pdf

Sarikaya, Salih. *How Blockchain Will Disrupt Data Science: 5 Blockchain Use Cases in Big Data | Towards Data Science*. https://towardsdatascience.com/how-blockchain-will-disrupt-data-science-5-blockchain-use-cases-in-big-data-e2e254e3e0ab. Accessed 23 Dec. 2021.

Soma, Jonathan. *Jsoma/Simplified-Scrollama-Scrollytelling*. 2021. 2021. *GitHub*, https://github.com/jsoma/simplified-scrollama-scrollytelling.

Szabo, Nick. *Shelling Out: The Origins of Money | Satoshi Nakamoto Institute*, 2002. https://nakamotoinstitute.org/shelling-out/. Accessed 23 Dec. 2021.

---. *Smart Contracts: Building Blocks for Digital Markets*, 1996. https://fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Accessed 23 Dec. 2021.

Nofer, Michael, et al. "Blockchain." *Business & Information Systems Engineering*, vol. 59, no. 3,

June 2017, pp. 183–87. *Springer Link*, https://doi.org/10.1007/s12599-017-0467-3.

"Forward Together", IBM Institute for Business Value, 2017. https://www.ibm.com/downloads/cas/OX1JGX65. Accessed 20 Dec. 2021.

The Strange Story of Satoshi Nakamoto's Spelling Choices. https://ungeared.com/the-strange-story-of-satoshi-nakamotos-spelling-choices-part-1/. Accessed 22 Dec. 2021.

The Wall Street Journal, Finneynakamotoemails.Pdf. 2014. https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf. Accessed 22 Dec. 2021.

Zimmermann, Philip R. *Why I Wrote PGP | Satoshi Nakamoto Institute*. https://nakamotoinstitute.org/why-i-wrote-pgp/. Accessed 22 Dec. 2021.