Vilnius University

FACULTY OF MATHEMATICS
AND INFORMATICS

HOMEWORK TASK 1

FINANCIAL TECHNOLOGY MODELS

INÉS CABRERA BETANCOR

2025-2026

INDEX

READING ASSIGNMENT

After reading *"Bitcoin: A Peer-to-Peer Electronic Cash System"* by Satoshi Nakamoto (2008), I gained a deeper understanding on how Bitcoin introduces a decentralized way to send payments without relying on trusted third parties. Below you can find my answers to the assigned questions:

a. How does the proposed payment system prevent double spending?

Double spending in Bitcoin is prevented by using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. Each transaction is timestamped and published in a chain secured by proof-of-work, causing it to be permanent and verifiable at any time in the blockchain.

The system as a whole is secure as long as nodes acting in good faith collectively control more CPU power than any group of nodes acting in bad faith. To change a previous transaction, an attacker would have to redo the proof-of-work for that block and all the blocks after it. This would require substantial computational power.

How do we eliminate the need to rely on a third party? The process eliminates the need for a trusted central authority by recording and broadcasting all transactions in a public chain visible to all nodes.

Lastly, Bitcoin also follows a "Longest chain rule" defining the history of valid transactions as the chain with the greatest amount of accumulated proof-of-work representing the majority of honest nodes.

b. How does the system ensure that nodes stay honest(i.e., do not propagate fictitious transactions)?

To ensure node honesty, Bitcoin relies on a combination of independent verification, consensus rules and economic incentives built into the network. Miners are given new coins and fees on valid blocks, incentivizing them to be honest which creates a strong financial incentive for rules-based behavior.

When a miner adds a block to the chain they perform a proof-of-work. If a miner includes invalid or fraudulent transactions in a block, the block will be rejected by the network because every node is verifying everything independently. Nodes verify the validity of each block before it is accepted by the miner, preventing complications with incorrect data spreading to nodes who may not have discovered the error and wasted their entire mining effort.

The network only accepts (as explained before) an existing longest valid block, so even if any attempted cheating is theoretically possible, it is practically a waste of economic, computational, and time resources.

c. What would you change in the Bitcoin white paper if you were Mr. Nakamoto?

Even though Mr. Nakamoto does a great job explaining how Bitcoin works, there are a topics i would add to the paper to make it richer in content:

- Scalability improvements

As mentioned in class, Bitcoin can only handle a limited number of transactions per second as blocks are small and added every 10 minutes. If I was Mr. Nakamoto, I'd add a section explaining the current protocol and how to make it faster and handle more users, so that it can process day-to-day transactions (small payments) more efficiently while keeping the system secure and decentralized.

In case there is a limit to transaction volume, I would also address it in this section, suggesting the need for future layers or solutions. It's important to first understand the problem of a Bitcoin bottleneck, so readers can maybe suggest ideas for solving it.

- Energy efficiency and environmental responsibility

The proof-of-work system is secure, but a lot of electricity must be used because miners compete by doing huge amounts of computation (trying different nonces until getting enough ceros as explained in class) . We know that the environmental impact of mining should be addressed, so I think making a section in the paper about possible ways to make Bitcoin greener, like using renewable energy or rewarding miners who use sustainable resources, it's necessary.

- Privacy for users

While the paper outlines how Bitcoin protects privacy by implementing public keys anonymously and encouraging the use of a new key for each transaction made, it doesn't fully address the risk long-term of linking transactions or patterns that could reveal identities.

If I were to write this paper, I would issue a more definitive statement about the importance of strong financial confidentiality and accept that, in the future, actions may be required to improve the security of the users' identity from sophisticated tracking or analysis.

Additionally, an example explaining how the system works under extreme circumstances, like nation-state attacks, network splits … should be discussed in the paper for future research and vigilance.

- Economic policy and future progress

The paper discusses Bitcoin's fixed supply and reward schedule and its role in economics, but does not fully elaborate the reasoning behind it. I would add a short description of how it works, how it avoids inflation and aligns incentives over time to give readers a sense of its monetary philosophy.

Further, some statements in the paper suggest that the current design is fixed. I would soften this a bit to invite the reader into thinking, regarding future innovations and how we expect it to evolve through new insights and technologies.

CALCULATION QUESTIONS

2. Perform the following calculations.

a) Using Euclidian algorithm calculated the greatest common divisor of 9357 and 5864.

Following the Euclidian algorith where $\gcd(a,b) = \gcd(b, a \bmod b)$ we get this trace leading to the result:

1. $\gcd(9357, 5864)$ $\Longrightarrow$

$$\begin{array}{r|l} 9357 & 5864 \\ -5864 & 1 \\ \underline{3493} & \end{array}$$

2. $\gcd(5864, 3493)$

$$\begin{array}{r|l} 5864 & 3493 \\ -3493 & 1 \\ \underline{2371} & \end{array}$$

3. $\gcd(3493, 2371)$ $\Longrightarrow$

$$\begin{array}{r|l} 3493 & 2371 \\ -2371 & 1 \\ \underline{1122} & \end{array}$$

4. $\gcd(2371, 1122)$

$$\begin{array}{r|l} 2371 & 1122 \\ -1122 & 1 \\ \underline{127} & \end{array}$$

5. $\gcd(1122, 127)$ $\Longrightarrow$

$$\begin{array}{r|l} 1122 & 127 \\ -1016 & 8 \\ \underline{106} & \end{array}$$

6. $\gcd(127, 106)$

$$\begin{array}{r|l} 127 & 106 \\ -106 & 1 \\ \underline{21} & \end{array}$$

7. $\gcd(106, 21)$ $\Longrightarrow$

$$\begin{array}{r|l} 106 & 21 \\ -105 & 5 \\ \underline{1} & \end{array}$$

8. $\gcd(21, 1)$

$$\begin{array}{r|l} 21 & 1 \\ \underline{0} & 21 \end{array}$$

Greatest common divisor $\gcd(9357, 5864) = 1$ //

b) Calculate

$15 \cdot 29 \bmod 13$

- $15 \bmod 13 = 2$
- $29 \bmod 13 = 3$

$\Big]$ $2 \cdot 3 = 6 \rightarrow$ result $= 6$

$2 \cdot 29 \bmod 13$

- $2 \bmod 13 = 2$
- $29 \bmod 13 = 3$

$\Big]$ $2 \cdot 3 = 6 \rightarrow$ result $= 6$

$-11 \cdot 3 \bmod 13$

- $3 \bmod 13 = 3$
- $-11 \bmod 13 = 2$

$\Big]$ $2 \cdot 3 = 6 \rightarrow$ result $= 6$

$\Downarrow$

$-11 + 13 = 2 \bmod 13 = 2$

c) Bob and Alice agreed to use RSA encryption scheme with n=11*3=33.

- What is the possible key space of this scheme?
- Assume decryption key of 3 was selected. What is the encryption key?
- Calculate the cyphertext of message 2.

(c) Bob and Alice use RSA with:

$$\boxed{\begin{array}{ll} p = 11 & n = pq = 33 \\ q = 3 & \phi(n) = (p-1)(q-1) = 10 \cdot 2 = 20 \end{array}}$$

The public Key is (e,n) where e is an integer such that:

(i) $1 < e < \Phi(n)$ (ii) $\gcd(e, \Phi(n)) = 1$ → $\boxed{e = \{\}}$

Now, let's find integers who satisfy both conditions:

Possible values of e that satisfy (i):

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19

Values of e that satisfy (i) and (ii):

- Factorization $20 = 2^2 \cdot 5$; So any number that shares a factor of 2 or 5 with 20 is not allowed in the Key space.

  – All even number do not belong since they are divisible by 2

  – 5, 10 & 15 are also excluded since they are divisible by 5

Result → $e = \{3, 7, 9, 11, 13, 17, 19\}$ → $|e| = 7$

- Assuming the decryption Key of 3 was elected ($d = 3$) The encryption Key is the modular inverse of the decryption Key.

$d = 3$

$n = 33$

$\Phi n = 20$

$e \to 3 \mod 20 = 1$

$\boxed{e = 7}$

$$\begin{array}{l|l} 20 & \underline{3} \\ 2 & 6 \end{array} \qquad \begin{array}{l|l} 3 & \underline{2} \\ 1 & 1 \end{array}$$

$$\begin{array}{r|l} 20 & 1 \\ 3 & -6 \\ 2 & -1 \cdot -6 + 1 = 7 \\ 1 & \end{array}$$

- Calculation of the cypertext of message $m = 2$.

$C = m^e \mod n =$

$2^7 \mod 33 =$

$128 \mod 33 = 29$

$$\begin{array}{r|l} 128 & \underline{33} \\ -99 & 3 \\ 29, & \end{array}$$

$\boxed{C = 29}$

3. Compute $\varphi(pq)$ when both p and q are primes.

$$\Phi(pq) = (p-1)\cdot(q-1)$$

Let p and q be two prime numbers. By definition Euler's totient function $\Phi(n)$ counts how many integers from 1 to n ($n = pq$) are coprime to n (that means that their gcd with n equals 1)

→ we want to find $\Phi(pq)$

- Total numbers to consider: all numbers from 1 to pq

  ↳ There are pq numbers in total

- Which numbers are not coprime with pq:

  A number will not be coprime to pq if it shares a factor with pq. Since pq only has the prime factors p and q, the numbers that fail to be coprime are those divisible by p or q.

  Multiples of p → $p, 2p, 3p, \dots, qp = pq$ → there q of them
  Multiples of q → $q, 2q, 3q, \dots, pq$ → there are p of them

  But the numper pq appears in both lists so we have to subtract 1:
  numbers not coprimes to $pq = p + q - 1$

  ↳ Substract from the total:

  $\Phi(pq) = pq -$ not coprime numbers
  $\Phi(pq) = pq - (p+q-1) = pq - p - q + 1$

  ↳ factorized → $\Phi(pq) = (p-1)(q-1)$ // Demonstrated.

4. Write a program which implements an RSA encryption/ decryption algorithm.

Calculate cyphertext of message m=12345678 when p=646253, q=953347, and e=508447791809.

The program can be found as an attached next to this file.

APPLICATION QUESTIONS

Your startup decided to start the marketplace for trading music creations. The idea is that the marketplace will enable song authors to sell the future royalties related to new songs to investors. Transfers of ownership rights to songs will be recorded on a blockchain.

a. Key considerations I would make in creating the business plan to ensure the future success of your startup

Market Research:

1. Research demand among artists who need upfront financing and investors seeking alternative assets.
2. Interview potential users to confirm pain points and interest in blockchain-based royalty trading. It's important to know our users' desires and features they would like to see in our product, so our solution fits real market needs.
3. Analyze competitors to identify differentiation opportunities like lower fees, simpler interface, clearer ownership verification…

Value Proposition:

Clearly design the core benefit for both sides:

- Artists → gain immediate capital to produce, promote or distribute new music while conserving creative ownership erasing record label dependence.
- Investors → access to a new alternative investment asset: transparent, traceable royalty income streams.

Revenue Model:

1. Establish a basic idea of how the platform will earn money.
2. Map potential partners and identify data sources needed to verify song ownership.
3. Develop a basic long-term marketing approach (suitable to change) to educate non-crypto users and expand the potential user base once the product is validated.

b. Business model (in terms of funding and pricing) options I would consider in this startup

FUNDING:

- Raise equity investment through seed or venture capital to develop the minimum viable product and secure legal compliance.
- Build strategic partnerships with music industry or blockchain companies to support growth and platform sustainability.

PRICING:

- Generate main revenue from variable transaction fees on each royalty trade, adjusted by trade size or user tier, keeping them low and competitive.
- Offer subscription plans for investors with premium analytics and early access to listings.
- Provide optional promotion fees for artists to feature their songs on the platform.

c. Possible effect of legal and regulatory environment on my business

- In the course of discussing Copyright and Intellectual Property laws, we need to ensure that we are selling royalties from legitimate rights holders, and that we have confirmed ownership, otherwise we could face legal issues or lawsuits.

- Selling royalties may also be interpreted as nothing different than selling securities, so it is important we investigate local laws and obtain any licenses necessary to operate them. Additionally, we need to follow the investment expectations in different countries.

- As we will also be processing personal and financial data, we also need to follow regulations for data protection in the countries where we launch the platform, and we will write contracts that will limit personal data stored on chains indefinitely.

- The artists and investors may be from any country, and the platform will need to consider varying copyright laws and tax implications from different jurisdictions, the exchange of divisas, and the control of electronic wallets.

- Ensure the legality of the contracts and ensure that legal professionals are engaged in the design process.

d. Key considerations to ensure success of my product from the blockchain technology implementation perspective

1. Select a blockchain platform that offers scalability, low transaction fees, strong security and supports NFTs or tokenized assets.
2. Making it compatible with existing music rights databases, royalty payment systems and external wallets (using APIs might be a solution).
3. Design a simple interface that hides blockchain complexity (letting users sign in with email, e-wallets …,, view transactions in normal currency, withdraw funds easily) this would help us enlarge our users base.
4. Implement robust security measures.
5. Think about efficient handling of large volumes of transactions without network overload.
6. Do regular security checks and keep the system updated with new blockchain versions to make sure it stays safe and reliable over time.

e. Advantages / disadvantages of using blockchain vs traditional database as the technological solution for this idea

BLOCKCHAIN

ADVANTAGES	DISADVANTAGES
- Each transaction is stored on an immutable public record, resulting in full transparency and traceability. - Removes intermediary, data integrity is mathematically verifiable. - Smart contracts allow payment or royalties to be processed instantly and automatically - Cryptograph protection significantly reduces the risk of data exposure or other unauthorized access - Enables asset tokenization and direct user to user access.	- Can be slower and more costly, especially on public chains - Data immutability can present challenges with correcting errors or enforcing compliance - Required higher setup costs and specialized knowledge - Bugs or vulnerabilities in contracts can cost you negatively and are irreversible.

TRADITIONAL DATABASES

ADVANTAGES	DISADVANTAGES
- Speed and cost efficient for high volumes or rapid transactions - Modification or deletion of records is simplified to meet regulatory standards - Backed by mature systems, standards, and people	- Subject to a single point of authority; prone to manipulation or data loss. - Internal audits are necessary and can limit transparency - Payments and updates are typically more time-consuming; require more human intervention - Considered closed systems; limited peer-to-peer interaction.

Despite being more complex and costly, blockchain is the best choice for our platform as it offers trust, transparency, and automation, which are critical to a platform dealing with digital ownership and royalty payments.

It also allows artists and investors to verify transactions without third-party intermediaries and also secure every transfer so that it is traceable. Such features make blockchain the best technology for a fair and transparent music marketplace.