[redacted]

Reasons, advantages and disadvantages of transitioning from a centralised bank system to a distributed bank system using blockchain technology

Niccolò Barbini

[redacted]

Contents

List of Figures

Chapter 1

Introduction

Ever since their initial foundation, banks have changed how they function. Born as institutions to lend money to kingdoms and states throughout history (Hildreth, 1837)), banks have constantly evolved their manner of conducting business (Mollan, 2021). Two examples of change include the establishment of the Bank of England in 1694 (Kynaston, 2020) and financial deregulation between 1970 and 1990, which revolutionised the banking sector (Buch, Eickmeier, and Prieto, 2022). Even though the banking system, structure and service have changed over different eras, the banking sector has preserved three essential services: payment services, intermediation for lending and borrowing money, and insurance (Davies et al., 2010). An advanced technology for banking today, would be to provide bank services using blockchain technology (BC) (Ammous, 2016). Despite being a recent, but well-advanced technology tool, BC, with its characteristics as a distributed database, privacy, transparency, security, and authenticity, offers an efficient vehicle for banks to improve their service offering (Garg et al., 2021a).

1.1 Report goals

In this report, the author examines the advantages and disadvantages of the implementation of blockchain technology within a bank which uses a centralised system (see Appendix A, section A.1). A critical analysis of current challenges and limitations of current banking technology status is presented. The author has examined Banco BPM SpA due to its importance in the Italian banking context.

1.1.1 Banco BPM SpA

Operating in Europe and Asia, Banco BPM SpA is the third largest Italian bank in Italy (FitchRatings, 2022) with varied income sources. The bank's main activities include managing deposit and saving accounts, debit and credit cards, private and liquidity mortgage loans, life insurance and automobile policies (BancoBPM, 2021a).

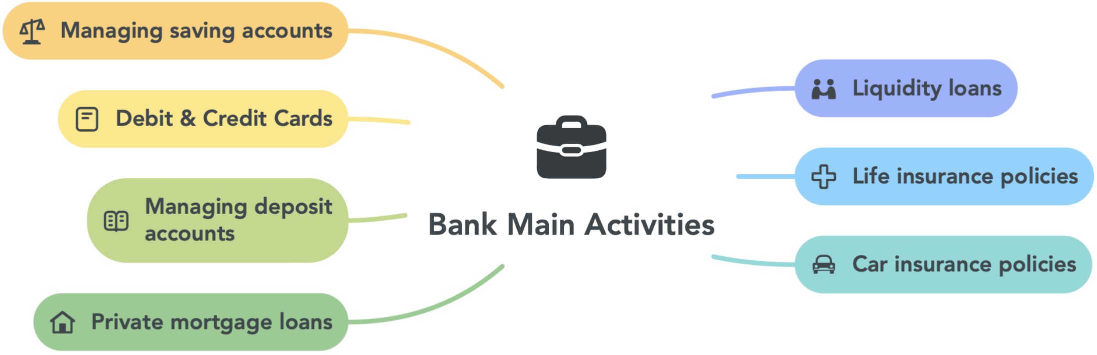

Figure 1.1: Banco BPM's main activities

BPM's principal objectives are to provide the best possible services, to operate with a correct and transparent process for the country's development, and to generate sustainable value creation over time (BancoBPM, 2021a). Banco BPM's principal goals in their strategic plan 2021-2024 (BancoBPM, 2021b) are to successfully develop an innovative digital-driven service model and facilitate business growth.

Chapter 2

Centralised bank structure

In order to provide services, Banco BPM uses technological tools, physical infrastructures and human resources. The bank uses a centralised system, which means it owns each client's data, and the management takes decisions for everyone within the bank's environment. Data is saved on servers which belong to the bank; thus, these servers are distributed within different geographical areas and not located in a single area to guarantee security, safety (Ko and Rubenstein, 2004) and load-balancing traffic to increase response time and throughput between multiple devices (IBM, 2021).

2.1 Technologies, Physical Infrastructure and Humans

Physical devices, software suites, networks, and databases are all tools which are necessary for the bank to provide its services for each customer, to enable operating 24/24 hours a day. Physical infrastructures such as branch sites, servers, security hardware, and security access devices are the base of bank services' operability. The human element is essential because employees are the first point of contact with the bank (Tomer, 2016). Today, without employees, it would be challenging for the bank to successfully provide services to its clients.

2.2 Centralised bank system

Banco BPM uses a centralised system to provide its services, where the company board and management decide the rules, factors and services which the bank needs to provide. Figure 2.1 illustrates the main areas of the bank's centralised bank structure.

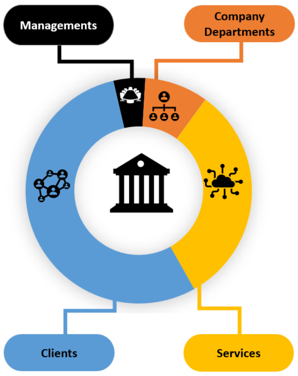

Figure 2.1: Banco BPM's centralised structure

2.3 Bank Security Risks

Digitisation of the bank sector has brought numerous advantages (e.g., customers demanding and receiving services anytime) and disadvantages concerning security (Alzoubi et al., 2022) and privacy (e.g., internet fraud and data leakage)(Brar, Sharma, and Khurmi, 2012). A recent attack, concerning UK customers, emanated from a web service called iSpoof (MET, 2022), which offered services to steal money from bank customers. The attackers' modus-operandi aimed to steal the bank's customer information, access the client's bank account, and transfer money. Two social-engineering techniques of identity theft and vishing (voice phishing attack) were deployed to perform attacks (MET, 2022). iSpoof used a vulnerability common within digital banking, which is identity theft (Wewege, Lee, and Thomsett, 2020). This attack contributed to reveal how fragile banks' cyber security measures and policies are, and how it is relatively easy for attackers to exploit vulnerabilities and use threats. In iSpoof's case, the vulnerabilities were identity theft and human error, the attack's success depended only on human trust exploitation (Wang, Zhu, and Sun, 2021).

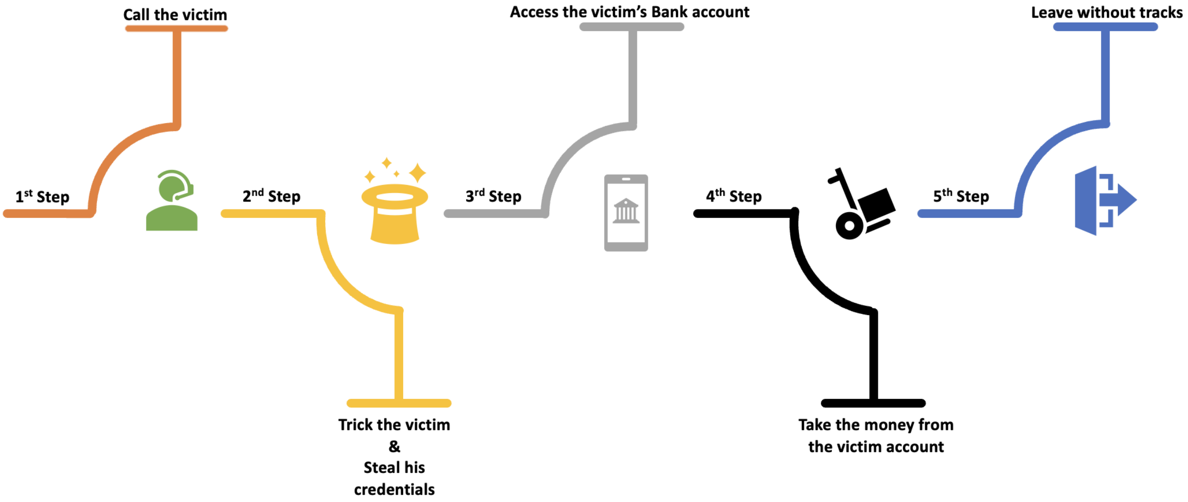
Call the victim
1st Step
2nd Step
Trick the victim & Steal his credentials
Access the victim's Bank account
3rd Step
4th Step
Take the money from the victim account
Leave without tracks
5th Step

Figure 2.2: iSpoof attack steps representation

Chapter 3

Blockchain and Decentralised Autonomous Organisations (DAOs)

In classic network architecture, devices are interconnected with the purpose of sharing the same information. The network is managed by a single central authority which regulates the activities and behaviours of the network's elements. One key risk with this architecture is the chance of data alteration by network elements. One of the advantages of introducing blockchain technology is to de-risk this possibility (Di Pierro, 2017) through the practice of saving this information on all the nodes of the network (Ammous, 2016). Thus, the introduction of Decentralised Autonomous Organisations (DAOs) helps the blockchain structure to increase its security level, enhance the privacy of the users and introducing smart contract to regulate the structure (Andolfatto, 2018).

3.1 Blockchain Technology

A distributed, decentralised database of records which enables fast transactions without being managed by a single entity is defined as blockchain (Sheth and Dattani, 2019); the elements of blockchain are called nodes or blocks. To achieve successful blockchain characteristics the blockchain architecture should be subdivided into seven different layers: physical, data, network, consensus, incentive, contract and application layer (Homoliak et al., 2021).

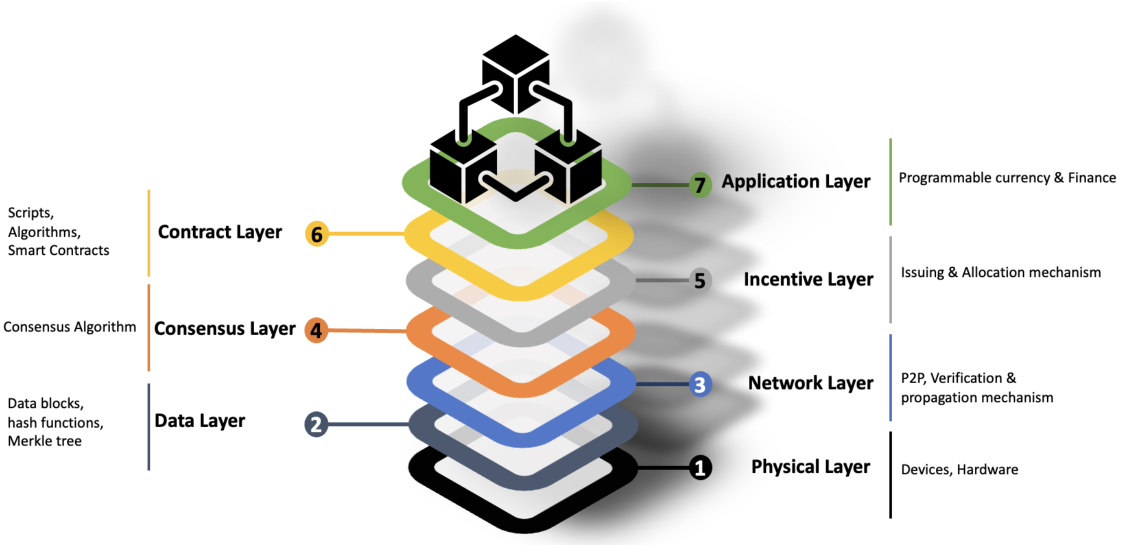

Figure 3.1: The seven key blockchain layers

These blocks, which communicate via peer-to-peer (P2P) protocols (Sheth and Dattani, 2019), are responsible for validating, storing and synchronising the content of a transaction ledger; thus, it is nearly impossible to modify or alter the data without the entire network's approval (Ali et al., 2021). To ensure the immutability and security of blockchain, HASH mathematical encryption is used, the most common HASH used is HASH-256 (Fu et al., 2020).

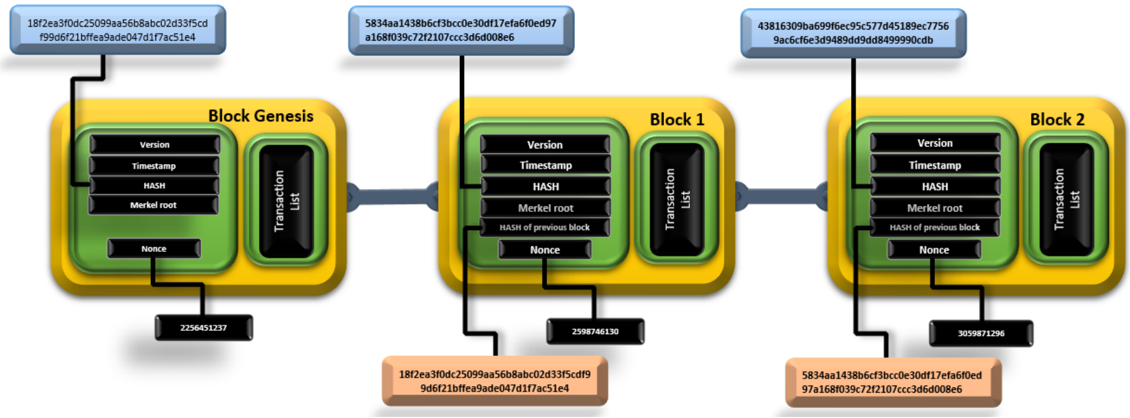
18f2ea3f0dc25099aa56b8abc02d33f5cd
f99d6f21bffea9ade047d1f7ac51e4
5834aa1438b6cf3bcc0e30df17efa6f0ed97
a168f039c72f2107ccc3d6d008e6
43816309ba699f6ec95c577d45189ec7756
9ac6cf6e3d9489dd9dd8499990cdb
Block Genesis
Version
Timestamp
HASH
Merkel root
Nonce
Transaction
List
2256451237
Block 1
Version
Timestamp
HASH
Merkel root
HASH of previous block
Nonce
Transaction
List
2598746130
18f2ea3f0dc25099aa56b8abc02d33f5cdf9
9d6f21bffea9ade047d1f7ac51e4
Block 2
Version
Timestamp
HASH
Merkel root
HASH of previous block
Nonce
Transaction
List
3059871296
5834aa1438b6cf3bcc0e30df17efa6f0ed
97a168f039c72f2107ccc3d6d008e6

Figure 3.2: Blockchain Structure Representation

3.1.1 Block Description

A block is a file where data are continuously (Sheth and Dattani, 2019); a set of blocks constitutes a blockchain. A block is composed of seven attributes such as version (it is an indicator about the current version of the block), its hash value (which is the identifier), the previous block's hash (it is a link to the previous block, the hash cannot be changed, and it enhances the security and immutability of the block [Golosova and Romanovs, 2018]). Merkle root tree is a tree data structure to store the transaction, via using HASH, and is used for verifying data and synchronising the blockchain (Garewal, 2020), time is used to indicate when the block data has been written. The number of transaction, and the nonce which is a random or semi-random value used to ensure the uniqueness of each block (Bellare and Tackmann, 2016).

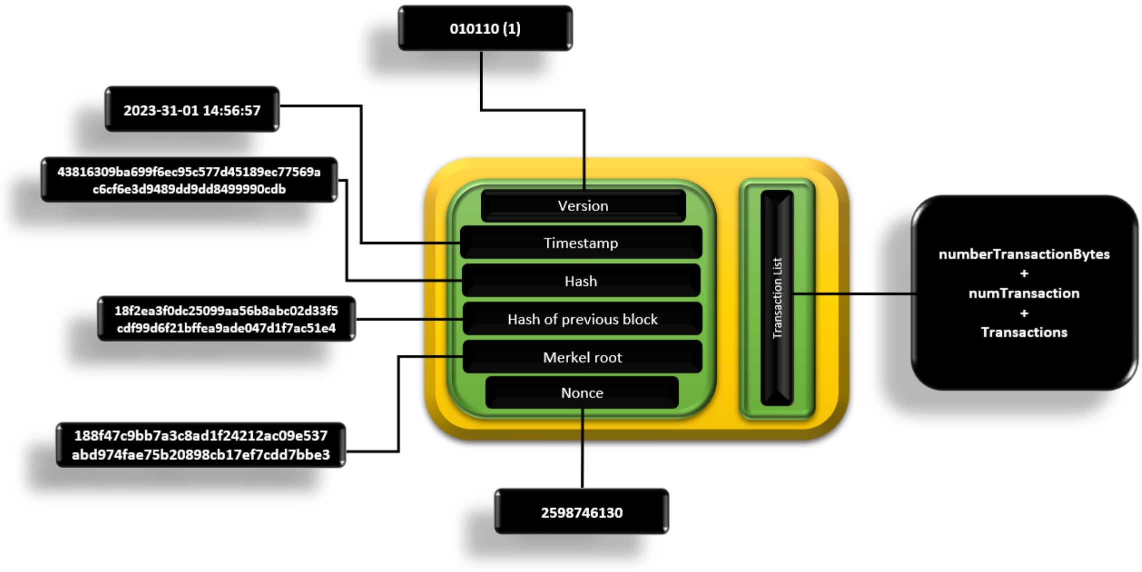
010110 (1)
2023-31-01 14:56:57
43816309ba699f6ec95c577d45189ec77569a
c6cf6e3d9489dd9dd8499990cdb
18f2ea3f0dc25099aa56b8abc02d33f5
cdf99d6f21bffea9ade047d1f7ac51e4
188f47c9bb7a3c8ad1f24212ac09e537
abd974fae75b20898cb17ef7cdd7bbe3
Version
Timestamp
Hash
Hash of previous block
Merkel root
Nonce
Transaction List
numberTransactionBytes
+
numTransaction
+
Transactions
2598746130

Figure 3.3: Block Structure Representation

3.2 Different Types of Blockchain

A blockchain can be permissionless or permissioned (Helliar et al., 2020), the most significant difference is that everyone can join the permissionless network without restrictions (Ayesha et al., 2022). Whereas, permissioned blockchains have set rules that regulate access, increase privacy and security. In general, permissioned blockchains are used by specific organisations (e.g., financial institutions) (Sarmah, 2018). Additionally, there is a deep differentiation within BC structure, such as open, private and consortium blockchains (Ayesha et al., 2022).

3.2.1 Open, Private and Consortium Blockchain

A blockchain is defined as open when anyone can read and write without authorisation from a central jurisdiction in the network (e.g., Bitcoin [Nakamoto, 2008]) (Panicker, Patil, and Kulkarni, 2016). However, a blockchain is considered private when a single body or bodies decide which nodes are allowed to be part of, and active within the network (e.g., Corda3 [R3.Corda, 2014)(Oliveira et al., 2019). Thus, when a private blockchain is permissioned, a few nodes can participate in the consensus process (Oliveira et al., 2019). In a consortium blockchain, a group of individuals dictate the rules of the network (Dib et al., 2018); usually, this kind of blockchain is used for a group of companies that operate in the same sector (e.g., Hyperledger Fabric [Hyperledger.fabric, 2014])(Ye and Chen, 2016).

3.3 Distributed Ledger (DL)

Scientific literature has a variety of definitions for distributed ledger technology (DLT)(Rauchs et al., 2018). The Bank of England defines a DLT as a *"distributed database, in a sense that each node has a synchronised copy of the data, but departs from the traditional distributed database architectures in three essential ways: decentralisation, reliability in trust-less environments and cryptography encryption"* (quoted in Rauchs et al., 2018, page 19) adding the use of validation consensus algorithms and digital signature. On the other hand, DLT has been defined as a distributed database where multiple identical records are distributed between several participants

(Romero Ugarte, 2018). It is essential to distinguish DLT from blockchain technology, giving the definition that a blockchain is a particular data structure where data are stored in a specific format (Chowdhury et al., 2019), and used in some DL and not vice-versa (Natarajan, Krause, and Gradstein, 2017).

3.4 Decentralisation

Decentralisation is a concept that is applied to multiple fields and disciplines, the two most important areas where this notion applies, is to blockchain and networking (Bodó, Brekke, and Hoepman, 2021). In networking, systems are decentralised where a single authority manages the network. In a blockchain, the network is composed of a decentralised physical structure with a logically distributed authority (Bodó, Brekke, and Hoepman, 2021). Some reasons to utilise a distributed system are because this structure increases the network's resilience; and, because the traffic congestion on the nodes decreases in relation to the augmentation of nodes in the network (Bodó, Brekke, and Hoepman, 2021). Other reasons are related to the diminishment of risks linked to network failure, an incremental growth of trust in the service (e.g., service always active) and the authority in the system is distributed among each node (Tharaka, Mika, and Madhusanka, 2021).

3.5 Consensus Algorithms

Major concerns regarding blockchain systems are how to obtain an accord between entities, to balance the load within the network and how to validate the block. To solve this problem, consensus algorithms are used (Bamakan, Motavali, and Babaei Bondarti, 2020). It is possible to define the consensus as a process between bodies in a blockchain to reach agreement even though some of these bodies are untrustworthy or misleading (Bach, Mihaljevic, and Zagar, 2018). This can be the Byzantine Generals Problem, where the question is whether a defined number of generals (or nodes) can agree to attack a fortress considering that they can communicate only with messengers and they are in different locations (Bach, Mihaljevic, and Zagar, 2018). To achieve resolution, Byzantine Fault Tolerance (BFT) and other implementations of this algorithm (e.g., Delegated Byzantine Fault Tolerance (dBFT)) have been introduced to resolve the dilemma (Bach, Mihaljevic, and Zagar, 2018).

3.5.1 Delegated Byzantine Fault Tolerance (dBFT)

In dBFT, there are two categories of nodes: bookkeepers and ordinary nodes. To define bookkeeper nodes, it is necessary that the ordinary nodes elect them. Once elected, it has the chance to be part of the consensus process; and, in that process, a random bookkeeper node is chosen to spread its recorded and validated data to the entire network (Bach, Mihaljevic, and Zagar, 2018).

3.5.2 Proof of Work (PoW)

The first utilisation of PoW dates back to 2009 when the bitcoin blockchain was introduced (Nakamoto, 2008). PoW is based on the solution of complex mathematical calculation where the objective is to find the nonce (see Appendix A, section A.2). Once the nonce has been identified and the consensus problem is satisfied, the new block is added to the blockchain (Bach, Mihaljevic, and Zagar, 2018). The first block in the network is called Genesis; its previous hash value is equal to zero, whereas all the other blocks on the blockchain have the hash value of the previous block (Bach, Mihaljevic, and Zagar, 2018). After the validation and the addition of the new block on the blockchain, all nodes will append the new block to the chain (Bamakan, Motavali, and Babaei Bondarti, 2020).

3.5.3 Proof of Stake (PoS)

Proof of Stake (PoS) is a consensus algorithm where adding a block to the blockchain does not require solving mathematical problems as in PoW (Bach, Mihaljevic, and Zagar, 2018). The coin age of a coin or token is defined by the period of time after it was generated. Holding a coin for a long time enables the owner to have more rights in the network (Mingxiao et al., 2017). In order to mint a new block for the network, the validator needs to use his coin age, this value is calculated considering the proof hash (a hash value formed by weight, unspent output value and the sum of current time) (Mingxiao et al., 2017), number of coins, age and the target. The formula is $(coins \times age \times target) > proofhash$ (Bach, Mihaljevic, and Zagar, 2018). For example, PoS is implemented on the Ethereum blockchain (Smith, 2023).

3.5.4 Proof of Importance (PoI)

PoI takes the PoS structure, adding new features such as the importance of score, which affect the chance of obtaining a small financial price for appending a user transaction on the network. PoI has three main attributes: vesting (the higher the number of the owned coins, the bigger the score), transaction partnership (the user that makes a considerable number of transactions within the network will get a better score) and size of transaction and number in the previous thirty days (Bamakan, Motavali, and Babaei Bondarti, 2020). PoI is used on the NEM blockchain (NemOrganisation, 2014).

3.6 Smart Contract

Executable code script that runs on a blockchain to ease, perform and administer agreements between unethical parties without the engagement of a third party is called smart contract (SC) (Khan et al., 2021); Technically, an SC is composed of four attributes: an address, state, function and value (Mohanta, Panda, and Jena, 2018). Consequently, SC is traceable, tamper-resistant, and it is not possible to reverse its actions once it is executed. SC behaves as a decentralised program within the blockchain network, this program is permanent, and its standing is certificated by trusted hash cryptography techniques on the network (Tharaka, Mika, and Madhusanka, 2021). An SC can be used to improve accuracy and transparency between parties (Tharaka, Mika, and Madhusanka, 2021)) in categories such as supply chain, real estate, healthcare, financial systems, digital management and insurance (Mohanta, Panda, and Jena, 2018).

3.7 Decentralised Autonomous Systems (DAOs)

As described in the previous sections, the blockchain can have an open, private or consortium structure. Since decentralisation is the key for this kind of network, it has been challenging to maintain a decentralised structure while governing it (El Faqir, Arroyo, and Hassan, 2020). A solution to this problem could be the utilisation of Decentralised Autonomous Systems (DAOs). Despite being a recent technology, different definitions of what a DAOs exists, while its structure is well-defined (Wright, 2021). DAOs is a structure which can operate without a central organisation or defined hierarchy, it uses smart contracts as management (Sims, 2019) and consensus algorithms to administrate operations, governance and evolution of itself (Wang et al., 2019). DAOs use on-chain and off-chain collaborative governance modes; the difference between these governance modes is that the first one is used to update and maintain the consensus using smart contracts. Whereas off-chain is used to guarantee, distribute, recognise and regenerate the consensus (Wang et al., 2019). In summary, DAOs can be integrated with a blockchain where smart contracts play a vital role in keeping the decentralised and distributed system working (Hassan and De Filippi, 2021).

Chapter 4

Using blockchain in Banco BPM

Based on the treatise in the previous sections regarding blockchain technology, the author suggests that there are advantages to implementing a blockchain structure in Banco BPM. Using blockchain technology in the banking system can positively affect how data are stored and offer new ways of providing new tools (e.g., services for clients)(Cucari et al., 2022). From a technical perspective, using blockchain enhances the security of transactions between entities, reduces the frictions between them, and minimises the risks and errors behind data processing (Garg et al., 2021b)); in addition to offering standardisation of the process, the risks associated with operations, cost and time are reduced (Cucari et al., 2022). Moreover, the capability of this technology to keep records on significant and distributed databases results in enhanced information quality (Chowdhury et al., 2021), speed and time of each operation. Thus, the database is kept updated by the users (Cucari et al., 2022). For example, the blockchain can improve the activity of lending and borrowing money between users (e.g., using a lending scheme)(Cucari et al., 2022; Garg et al., 2021b).

4.0.1 Blockchain structure in Banco BPM

Banco BPM should use a private blockchain as architecture because this will provide the opportunity to keep a minimum level of control over the network. The bank should use the Polygon blockchain with PoS as consensus algorithm; the main reason for Polygon is the use of Ethereum's blockchain as a decentralised and distributed network. While Ethereum transaction fees (gas fee) are expensive, Polygon has reduced this cost using a sidechain structure, which increases the scalability of the network, maintaining its security (Polygon.Technology, 2021), and compared to PoW it consumes less energy and computer power. Although blockchain brings advantages to the banking sector, it is vital to analyse its potential disadvantages. There are different points-of-view in examining the disadvantages of using blockchain, areas such as the cost of implementing this technology (Chang et al., 2020) and the lack of people with expertise in developing and managing it (Cucari et al., 2022) representing a significant obstacle. Alongside these two areas, the delays in developing legal frameworks (Sulik-Górecka, Strojek-Filus, and Maruszewska, 2018), the issues related to scalability, governance and personal data protection acts (e.g., GDPR) represent a constraint to using this technology (Sulik-Górecka, Strojek-Filus, and Maruszewska, 2018).

4.0.2 A look into the future

In the long term, the private blockchain has the potential to become too centralised due to its desire to have control over the network and who can access it. Consequently, the DAOs system represents a positive solution related to this concern. The utilisation of DAOs can increase the speed of execution and decision-making progress for the organisation (Wagener, 2022);); a vital role in this process is played by the new kind of structure, which is no longer hierarchical. Consequently, it becomes flat (MacDonald, Allen, and Potts, 2016), which allows everyone to have the same privilege in participating (Bellavitis, Fisch, and Momtaz, 2022). The cost of transactions will diminish considering the removal of intermediaries (Bellavitis, Fisch, and Momtaz, 2022). Thus, the members (e.g., managers, customers, senior management) of the network get a reward, which is regulated by transparent code (e.g., SC) (MacDonald, Allen, and Potts, 2016). Despite presenting itself as a flat decision-making environment, DAOs can be transformed into a hierarchical structure where voting power is not equalised between members (Schneider et al., 2020). For example, it could be possible to have two types of token owners, where one group is allowed to make decisions and the other one not (Bellavitis, Fisch, and Momtaz, 2022). DAOs are a recent technology, and there are many areas of this structure that need to evolve to overcome some of the challenges, such as external forces which intervene in the network or, even worse, when the structure is wholly dependent on them (Schneider et al., 2020). Another disadvantage deriving from DAOs' principle of no central management is that when facing a crucial situation, the response to this situation is delayed since every entity of the network needs to be active in the decision-making process (Schneider et al., 2020).

4.0.3 Cost of implementing Blockchain

Based on the previous chapter's discussion, it is possible to suggest that blockchain can have a powerful cost-cutting impact, such as removing third-party services as intermediaries (Osmani et al., 2021). However, it is necessary to consider the expenditure in implementing such technology in Banco BPM, which can include energy, storage and transaction costs (Osmani et al., 2021). Thus, costs can be categorised in the short and long term. In order to implement the blockchain structure, Banco BPM should allocate enough funds to buy high-performance devices (e.g., servers, computers), hire skilled staff and management (for studying, implementing, running and maintaining the new network) and minimise risks concerning natural disasters (e.g., earthquake, flood, fire), security protocols to guarantee the cooling of the operative machines and a plan to face energy cuts or issues(Chang et al., 2020). Additionally, new policies to regulate security, and interaction between clients and the bank, must be studied and implemented. Banco BPM must think about its long-term expenditures regarding the cost of use and maintenance of this new architecture. Regarding long-term cost, it is necessary to train all of the relevant company teams, from people working on implementing, running and maintaining the BC structure to employees interacting with customers. Also, different teams with varying types of expertise need to be employed. Energy cost and supplies represent a significant expenditure considering the requirement of huge energy consumption (these costs increase with the augmentation of the transaction volume)(Osmani et al., 2021) and the necessity to have supplies available in any necessity (Chang et al., 2020).

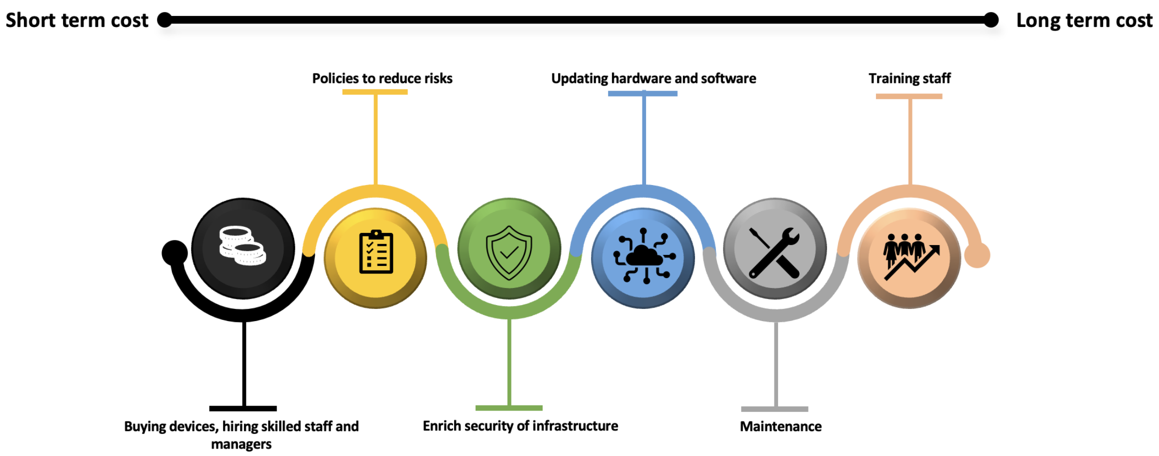
Short term cost
Long term cost
Policies to reduce risks
Updating hardware and software
Training staff
Buying devices, hiring skilled staff and managers
Enrich security of infrastructure
Maintenance

Figure 4.1: Short and Long Term costs

4.1 Blockchain attacks

Despite representing a more secure infrastructure, blockchain remains vulnerable to attacks. For example, the 51% Attack is conducted against the consensus algorithm where the adversary tries to control the network through the ownership of the majority of nodes. If the attacker achieves the majority goal, he has the possibility to dictate new rules in the blockchain (e.g., no validating and adding new blocks) (König et al., 2020). On the other hand, a Sybil attack is a category of network-based attack with the aim of compromising the BC through the installation of dummy software in different nodes (Vokerla et al., 2019); Sybil attack is used in blockchain for SC, financial services (Vokerla et al., 2019).

4.2 Smart Contract Vulnerabilities

Even though SC is considered secure due to its nature as script code, it is vulnerable to human error. For example, Forcible Balance Transfer is a vulnerability in the code where an SC transfers the balance without using the fall-back functions; without that function, it is possible to have a failure in the transaction, and the money spent is not refundable (König et al., 2020). Reentrancy Attacks are performed on Ethereum where an attacker claims the total balance of a specific address, and recursively calls a function of the ERC20 token (König et al., 2020). This attack can be conducted on a selected target, and the withdrawal of funds can be performed more frequently than allowed by the system (König et al., 2020).

Chapter 5

Conclusion

The purpose of this report is to examine the reasons and to study the advantages and disadvantages of implementing blockchain technology in Banco BPM SpA. As a result of this study, overall, it is advisable to transition from a centralised structure to a decentralised one using blockchain technology. The main advantages are related to increasing the speed of processes (e.g., money transactions), cutting costs (e.g., no third-parties involved in the process), enhancing the security of the platform using cryptography algorithms and improving the privacy of the users. As a future suggestion, the utilisation of DAOs on the BC and the use of Smart Contracts as regulators can enrich the qualities of the blockchain. Implementing and maintaining this new architecture would involve an initially expensive outlay, however, this paper demonstrates that in the long term, the introduction and implementation of blockchain would repay the investment. Figure 5.1 is a Gantt chart which estimates the activities, time and stages of studying, implementing and testing the new network structure.

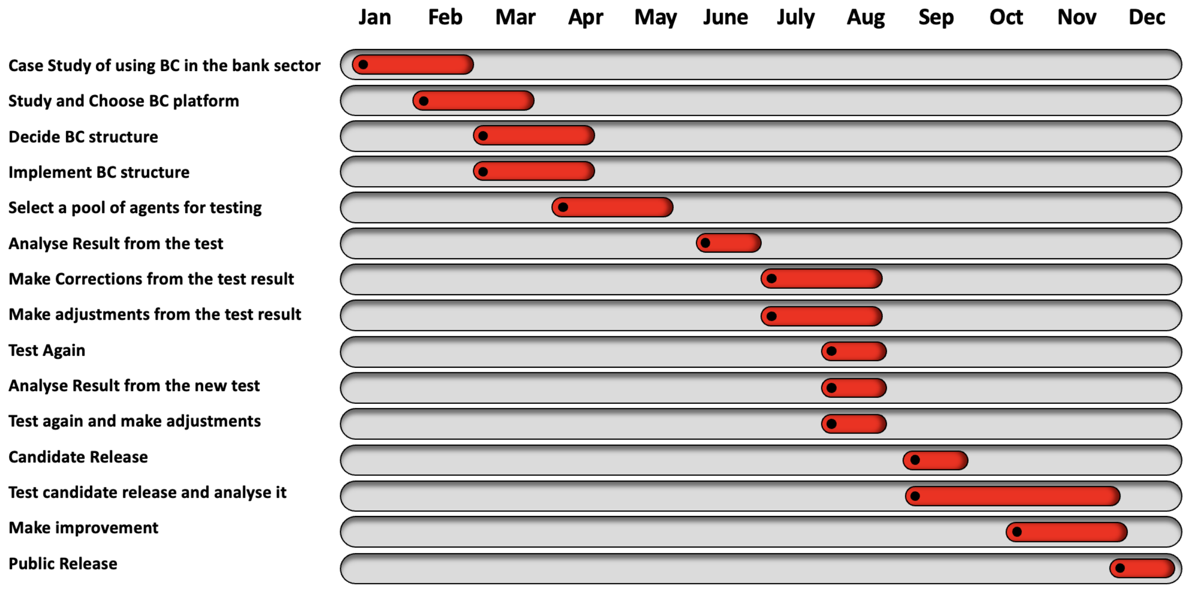

Figure 5.1: Gantt chart implementation blockchain in Banco BPM

Chapter 6

Future Recommendation

Banco BPM should consider using sharding as a solution for anticipated future expansion challenges (e.g., an increase in the number of transactions in the network). Transactions within the blockchain will increase over time, consequently, it is necessary to find a solution to this problem. Sharding offers a suitable solution to address this challenge, considering its characteristics of enhancing speed, increasing the decentralisation of the network and its scalability (also known as the triangle problem [Liu et al., 2022]); sharding can be applied to communication, storage and computation. Regarding communication, nodes are split into several specific numbers of shards (in each shard, the amount of nodes is the same)(Wang et al., 2022), where users can understand the state of the blockchain by liaising with intra-shard nodes (Liu et al., 2022). In computation-sharding, every shard manages the processing of its own transaction, this action contributes to a better load balance in computing power (Liu et al., 2022). Storage sharding is applied where non-identical nodes from distinct shards are required to store data (e.g., transaction history and unspent transaction output), and they do that by storing within their corresponding shard (Liu et al., 2022).

Appendices

Appendix A

Definitions

A.1 Centralised bank system

In this architecture, the central management takes all the decisions regarding bank services, how to provide these services and what kind of services. To provide these services and deliver them, the bank needs to hire personnel. Bank's employees are the intermediary between the bank and the customers.

A.2 Nonce

It is a random number that miners need to find by solving complex mathematical problems.