Department of Business & Management

Bachelor's degree in Management and Computer science

Football meets Blockchain: an innovative ticketing solution

Supervisor:

Prof.

Massimo Bernaschi

Candidate:

Leonardo Scalzi

234191

ACADEMIC YEAR 2020/2021

Contents

Chapter 1

Abstract

Football is the most followed sport worldwide and due to its popularity has to continuously face challenges related to innovation. Fraud and secondary market are the main problems football event ticketing needs to improve. Blockchain technology can be a game changer, providing security and transparency to both actors: event organizer and event consumer. Reviewing some studies, companies and application, a merge of two blockchain-based business models can be a valid ticketing solution for big and small football events. The final proposal is defined by a permissioned system.

Chapter 2

Acknowledgement

This thesis is the result of the constant support of my family and friends. Mother, you made me free, free to undertake, I give you a special thanks. To my father and my brother, you have always listened to what I thought. To the closest friends, those who count on their fingers. To my grandparents, number one supporters. Last but not least, a warm thanks to the teacher who shared with me a short but intense path of personal growth, Massimo Bernaschi, with whom I went into the heart of blockchain technology, giving me a further way of thinking and inspiring my creative and reflective vein. Without Professor Bernaschi, you wouldn't be reading this thesis.

Chapter 3

List of Figures

Chapter 4

Introduction

Football, with an estimated 3.5 billion fans worldwide, is the most followed sport, surpassing second-ranked cricket by one billion supporters. A significant part of football's appeal revolves around the passion that captivates various continents. To showcase this, data from FIFA states that, in 2018, 3.57 billion people watched the FIFA World Cup in Russia. To put that into perspective, at the time, this accounted for 50 percent of the global population aged four and over. Given such popularity, for football events, the demand for tickets is often way higher than the supply. The pricing of tickets also differs from other items. Most people would probably not say that tickets are cheap, yet on primary market the tickets are usually sold at a price below market value. The reason that they are underpriced is that event promoters want to make sure that the event is successful and sold out. They also want to show goodwill before upcoming events by not being too greedy towards the fan. Another reason to keep the prices low is that audience visits the event with a more positive vibe, which helps players to perform better and makes the event visitors more likely to buy merchandise. The combinations of high demand, low supply, and underpriced tickets makes many that are not interested in the event to see a business opportunity by buying tickets with the intention of reselling them at a higher price. This behavior is called 'scalping'. To be able to buy as many tickets as possible, the scalpers are using software called 'bots' that can purchase the tickets faster than a human can do. The tickets that are sold via the promoters are said to come from the 'primary market'. When the scalpers, or people with other reasons than making a profit from a bought ticket are reselling their tickets, they are creating what is called a 'secondary market'. Since a ticket most often is a pdf-file or a piece of paper with a barcode on it, it is most often impossible for buyers on the secondary market to verify that the ticket they are buying is authentic and not sold in multiple copies to other customers and on other platforms. Nowadays the overall ticketing system is trying to exploit the best technologies available in order to offer the best service as possible. Tickets represent a mechanism to demonstrate entitlement to access to any football match. They come in many forms, ranging from physical paper to electronically readable codes on paper or chips embedded in smart cards or wristbands (Waterson, 2016). The increasing use of electronic ticketing systems in recent years has greatly improved the efficiency of ticketing, management, and reduced the cost of storage of the ticketing information, compared to traditional paper tickets (Qteishat et al., 2014). Although over time football ticketing has improved its processes, some problems related to online ecosystem arose. In the next section I am going to give you an overview of the "dark practice" used when tickets are released, describing with accuracy the analysis of the problem that football industry is facing. In Chapter 6 there will be an explanation that is useful to well understand the basis of what this thesis is going to cover and use as principles, such as the different types of blockchain: public and permissioned, with a focus on the last one I have mentioned. Chapter 7 is characterized by the analysis of two different blockchain applications, and both will be essential for my final proposal, in fact the contribution I am going to provide is a mixture of the two, an innovative solution which is a merge of multiple existing blockchain based applications, more specifically a permissioned blockchain as a result.

Chapter 5

Problem Definition

Why football ticketing frauds are frequent? The problem of ticket fraud is not exactly small: An estimated 12% of ticket buyers get scammed, which amounts to an estimated yearly damage of USD 2 bn (Waterson, 2016; Leonhart, 2018). Ticket resale is a growing business globally, totaling 8 billion USD in revenue per annum (Courty, 2017). Those are problems this section wants to define, but to approach those statistics, we should have an overview about all the existing problematics event ticketing is facing. At first, before going deeper into problem definition, we should take a look at problems visualization.

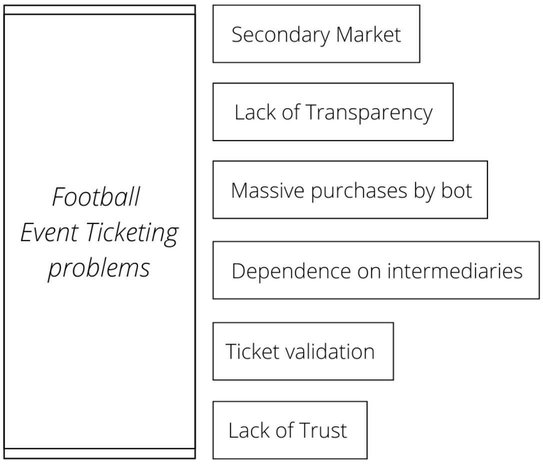


Fig.1 - Football Event Ticketing problems

Secondary Market

There is no control over secondary market prices. Consumers ticket prices on secondary markets are taken to extremes, partially through the use of bots which automatically drive-up prices to earn a profit by reselling them at the highest possible markups (Courty, 2017). From the event organizer's point of view, a major problem is the limited control over secondary transactions.

Lack of Transparency

A lack of transparency in the secondary market is evident in the event ticketing industry (Waterson, 2016). Spectators but also clubs aren't able to define if the number of tickets sold exceed the number of tickets issued because of the fraud in secondary markets.

Massive purchases by bots

Bots are becoming a problem because of their massive purchases, depriving football fans from the possibility to buy tickets on primary market and charging huge markups on secondary market is becoming a challenging problem.

Dependence on intermediaries

Event organizers are dependent on intermediaries and bear financial risks while being cut off from windfall profits and direct relations with event attendees.

Ticket validation

Until attendees physically arrive at the event for the entrance check, they cannot easily verify if their tickets are valid (Tackmann, 2017).

Lack of Trust

Consumers have to trust third parties when buying tickets on secondary markets and thus face the risk of purchasing fraudulent or invalidated tickets, that face the risk of being cancelled or are counterfeits (The Australian Government the Treasury, 2017).

Although ticketing has improved some features along the time, those problems are still persistent. This thesis aims to fill the gap of the actual football event ticketing system architecture, trying to give an innovative point of view and concrete solutions to the football ticketing world, addressing the problems illustrated in Fig.1. The objectives are to provide a solution to secondary markets, giving to event organizers full control over tickets management, being as transparent as possible with fans and spectators, limiting the massive purchases by bots. This thesis wants to combine different business solutions to reach a ticket verification mechanism that prevents scalping in such a way to solve the well-known lack of trust problem, faced by event participants when buying tickets on secondary market. Tickets can be bought on the primary market directly from the event organizer or from authorized sellers, mostly for a fixed price. Secondary markets exist, with the notable difference that any price can be charged, and buyers and sellers often directly engage in business or rely on secondary ticket sale platforms, which typically take 25-30 percent of secondary sales in fees (Waterson, 2016). However, while platforms and third parties do well, the status quo is not satisfactory for the two central stakeholders – the event organizer and the consumer(spectator) –. Consumers have to trust third parties when buying tickets on secondary markets, hence facing the risk of purchasing fraudulent or invalidated tickets, which are counterfeits or might be cancelled (The Australian Government the Treasury, 2017). Using QR-codes or barcodes, which encode information, but do not encrypt it, is not sufficient to make tickets truly tamper-proof. In various cases, the same barcodes have been sold multiple times or been obtained by extracting it from pictures of a ticket posted online (Tackmann, 2017). This problem could be addressed to lack of consumer "buying education", meaning that they are not well informed and educated about all types of fraud happening online (going from barcodes theft to buying tickets on unofficial websites) and this is also a problem of event organizers, lacking in transparency and security, often falling on bad brand reputation. Ticket prices on secondary markets are taken to extremes, partially through the use of bots which automatically buy and drive-up prices to earn a profit by reselling them at the highest possible markups. Thus, multiple governments are considering bans of ticket resale for profit altogether, however, economists remain skeptical about outright resale bans (Courty, 2017). For football associations and clubs, it is really a hard challenge to avoid these kinds of fraud by continuing to use not so updated technology; neither does the use of static codes on a ticket permit to link a ticket to the owner if it is resold, nor is it desirable to strictly bind a ticket to a person and prohibit reselling completely as costly and time-consuming entry checks must be performed (Waterson, 2016). Summing up, a clear lack of transparency and trust is evident, and stakeholders are currently in search of efficient and effective solutions to tackle this problem (Waterson, 2016; Tackmann, 2017). Now I want to give an overview of what are the design goals to make the ticketing service innovative with preserving all the "friendly-features". Digitalization go hand to hand with portability, digital storage of all data and exchange of those data is a requirement for present and future generations. Portability for tickets, independently from a physical medium, should be achieved. The event organizer should be able to manage ticket transaction and earn transaction fees from any paid ticket transfer among attendees. Management policies should be determined by the ticket issuer (Fujimura et al., 1999). This means more control over charging power of secondary markets is needed. Clubs should be independent, being able to conduct business with no intermediaries or at least the trusted intermediary should provide the most recent technology in order to face cyber-threats. In fact, a secure environment is characterized by the accessibility of resources (availability), the authenticity of data (integrity), and the prevention of access to illegitimate users (privacy) (Vacca,2013). To increase trust in the integrity of the system, ticket ownership should be verifiable in a simple way at any time. For clubs and fans, Transparency is needed to trace ticket transactions history and so to minimize frauds; current ownership status and any state change, from the creation and transfers between attendees to end of its lifecycle, should be publicly viewable. Automation is also an important design objective; the event organizer should not be required to perform any manual action after an initial setup. Any policies set by the organizer should be enforced automatically. The fixed and variable cost of the system should be economical from the event organizers point of view.

Chapter 6

Literature Review

This section reviews the origin of the blockchain technology, the working principle of the Bitcoin Blockchain and of the Ethereum blockchain, the comparison of the different blockchain types and different consensus mechanism, then going through Smart Contract and Non Fungible Token. Concluding with an explanation and discussion about UEFA blockchain-based football event ticketing system and Socios.com application; reading both is essential in order to understand the merging solution between the two architectural design and processes in the next section.

6.1 Blockchain

The concept of blockchain technology was originally introduced by Nakamoto Satoshi in a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” in 2008 (Nakamoto, 2008). Nakamoto presented a novel peer-to-peer network system to solve the problem of double-spending in a decentralized peer-to-peer electronic cash system where payment transactions do not need to be verified by a third party. In the network, a submitted transaction is verified before being accepted by the network. The network verifies whether the submitted transaction has already been spent based on the history of all the transactions. All the verified transactions within a period of time are hashed into a Merkle Tree (Becker, 2008) to generate a new block. In the same transaction block and for transactions from the same payer, only the first-in transaction will be accepted in order to avoid double spending. Each block contains a hash of the previous block as a clue in forming a chain of blocks. A new generated block is broadcasted to all the nodes in the network for verification, and the verified block will be added into a growing chain of blocks. Each node in the network always accepts the longest verified chain received and attempts to generate a new block in the longest chain. As a result, once a transaction has been recorded in a block in the chain, it cannot be changed. If an attacker wants to forge a transaction, the attacker must regenerate a block containing the fabricated transaction and all the blocks after it to catch up and become the longest chain. This requires the attacker to have the majority of the computing power in the network, because the nodes in the network generate blocks through a proof-of-work mechanism which is based on computing power. In order to avoid this situation, Nakamoto (2008) also designed an incentive mechanism in his network system. A node that generates a new block will receive a new coin as a reward.

6.2 Bitcoin Blockchain

In “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto, 2008), the author uses a proof-of-work mechanism to ensure that the decision making of a new block generation is based on computing power. This section reviews the implementation of the proof-of-work mechanism and the composition of a block given in Bitcoin blockchain. The methodology used in Bitcoin blockchain to implement the proof-of-work mechanism is that when a node attempts to generate a new block, it has to constantly generate nonce until it generates a nonce which can make the hash value of the block (composed by the previous block hash, the root hash of the Merkle tree (Becker, 2008) of transactions in the block, and the nonce) starting with a certain number of zero bits. In this method, the node with more computing power, has faster processing speed, which will allow it to have higher probability to be the first one finding the nonce that meets the condition. After a node finds a nonce that meets the requirement, it will send the found nonce with the generated new block to the other nodes in the network. The other nodes will verify whether the nonce meets the condition when they receive a new block. If the requirement is met, they will stop working on the current block generation and add the received new block to the current longest chain they have. After this, they will start to attempt to find a new nonce that meets the condition to generate a new block based on the lengthened chain. The interval of the generation of a new block can be controlled by the difficulty of proof-of-work. The more digits of zero bits required at the beginning of the hash value of the nonce, the greater the difficulty of the proof-of-work, and thereby it will take longer for nodes to find the nonce to generate a new block. With this mechanism, once a transaction is recorded in a block on the chain, it cannot be changed. If an attacker wants to change a previous transaction, they must regenerate the block where the transaction resides and all the subsequent blocks until the forged chain is longer than the current chain, which requires the attacker to have more computing power than all the other nodes combined. The process of generating a new block is also called mining (Chung et al., 2019). A block in the Bitcoin Blockchain has a Block Header and a Merkle Tree (Becker, 2008) formed by transactions. The Block Header is composed of three elements, Previous Hash, nonce, and Root Hash of the Merkle Tree. The Previous Hash is a hash value of the previous block which is used as a clue to link a block to the previous block. The nonce is a found nonce, meeting the condition of proof-of-work. The Root Hash is a Merkle Tree’s root. The Merkle Tree in a block is formed by all the transactions recorded in that block. The workflow of the Bitcoin Blockchain Network can be described using the following steps.

- Step 1: The workflow starts with a transaction being submitted to a node of the Bitcoin Blockchain.
- Step 2: After a node receives the submitted transaction, the node (Node A) verifies if the transaction is valid and if the coins in it have been spent or not.
- Step 3: If the submitted transaction passes the verification in Step 2, Node A will accept the transaction by adding it to the block Node A is generating. If not, Node A rejects the transaction.
- Step 4: Node A broadcasts the verified transaction to other nodes in the network.
- Step 5: Node A continues to collect new transactions and repeats the previous steps for each received transaction while working on finding the nonce that meets the condition of proof-of-work.
- Step 6: If Node A finds a nonce that meets the condition of proof-of-work, it will generate a new block with the found nonce and all the verified transactions. Then it will broadcast the new generated block to the other nodes and start to work on generating a new block. If other nodes find the nonce faster, Node A will receive the generated new block broadcasted by other nodes.
- Step 7: After Node A receives a new block from other nodes, it will first verify the nonce in the new block. If the nonce is correct, Node A will do the following steps. If not, Node A will reject the received block and keep working on generating its current block.
- Step 8: After the nonce of the received block is verified, Node A will verify all the transactions inside the received block. If all the transactions are valid and have not been spent, Node A will do the next step. If not, Node A will reject the received block and keep working on generating its current block.
- Step 9: After all the transactions in the received block are verified, Node A will accept the received block, and start to work on generating the next block based on the accepted block by using the hash value of the accepted block as the previous value in its generating block. The nodes in the network will keep collecting new transactions to add to the generating block it is working on until it generates or accepts a new block. However, according to a publication by Gobel Krzesinski (2017), in the actual Bitcoin blockchain, the size of a block is limited to 1MB and the number of transactions contained in a block cannot exceed 4000 transactions (Gobel Krzesinski, 2017)

6.3 Ethereum Blockchain

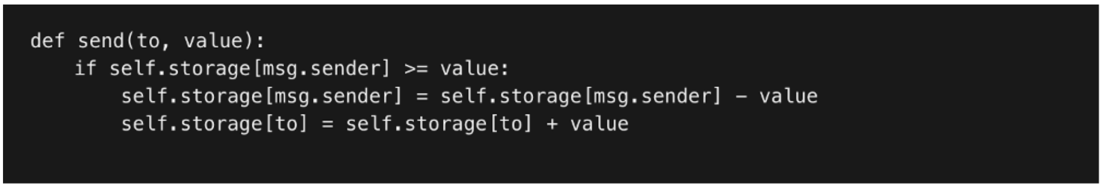
The intent of Ethereum is to create an alternative protocol for building decentralized applications, providing a different set of tradeoffs that will be very useful for a large class of decentralized applications, with particular emphasis on situations where rapid development time, security for small and rarely used applications, and the ability of different applications to very efficiently interact, are important. Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions. Smart contracts, cryptographic "boxes" that contain value and only unlock it if certain conditions are met, can be built on top of the platform, with vastly more power than that offered by Bitcoin scripting because of the added powers of Turing-completeness, value-awareness, blockchain-awareness and state. The Ethereum blockchain is in many ways similar to the Bitcoin blockchain, although it does have some differences. The main difference between Ethereum and Bitcoin with regard to the blockchain architecture is that, unlike Bitcoin (which only contains a copy of the transaction list), Ethereum blocks contain a copy of both the transaction list and the most recent state. Aside from that, two other values, the block number and the difficulty, are also stored in the block. The basic block validation algorithm in Ethereum is as follows:

- 1. Check if the previous block referenced exists and is valid.
- 2. Check that the timestamp of the block is greater than that of the referenced previous block and less than 15 minutes into the future.
- 3. Check that the block number, difficulty, transaction root, uncle root and gas limit (various low-level Ethereum-specific concepts) are valid.
- 4. Check that the proof of work on the block is valid.
- 5. Let S[0] be the state at the end of the previous block.
- 6. Let TX be the block's transaction list, with n transactions. For all i in 0...n-1, set S[i+1] = APPLY(S[i],TX[i]). If any application returns an error, or if the total gas consumed in the block up until this point exceeds the GASLIMIT, return an error.
- 7. Let S_FINAL be S[n], but adding the block reward paid to the miner.
- 8. Check if the Merkle tree root of the state S_FINAL is equal to the final state root provided in the block header. If it is, the block is valid; otherwise, it is not valid.

The approach may seem highly inefficient at first glance, because it needs to store the entire state with each block, but in reality, efficiency should be comparable to that of Bitcoin. The reason is that the state is stored in the tree structure, and after every block only a small part of the tree needs to be changed. Thus, in general, between two adjacent blocks the vast majority of the tree should be the same, and therefore the data can be stored once and referenced twice using pointers (i.e. hashes of subtrees). A special kind of tree known as a ”Patricia tree” is used to accomplish this, including a modification to the Merkle tree concept that allows for nodes to be inserted and deleted, and not just changed, efficiently. Additionally, because all of the state information is part of the last block, there is no need to store the entire blockchain history - a strategy which, if it could be applied to Bitcoin, can be calculated to provide 5-20x savings in space. A commonly asked question is ”where” contract code is executed, in terms of physical hardware. This has a simple answer: the process of executing contract code is part of the definition of the state transition function, which is part of the block validation algorithm, so if a transaction is added into block B, the code execution spawned by that transaction will be executed by all nodes, now and in the future, that download and validate block B.

6.3.1 Token System

On-blockchain token systems have many applications ranging from sub-currencies representing assets such as USD or gold to company stocks, individual tokens representing smart property, secure unforgeable coupons, and even token systems with no ties to conventional value at all, used as point systems for incentivization. Token systems are surprisingly easy to implement in Ethereum. The key point to understand is that a currency, or token system, fundamentally is a database with one operation: subtract X units from A and give X units to B, with the provision that (1) A had at least X units before the transaction and (2) the transaction is approved by A. All that it takes to implement a token system is to implement this logic into a contract. The basic code for implementing a token system looks as follows:



```
def send(to, value):
    if self.storage[msg.sender] >= value:
        self.storage[msg.sender] = self.storage[msg.sender] - value
        self.storage[to] = self.storage[to] + value
```

Fig.2 - Basic code for Token System

This is essentially a literal implementation of the ”banking system” state transition function described further above in this document. A few extra lines of code need to be added to provide for the initial step of distributing the currency units in the first place and a few other edge cases, and ideally a function would be added to let other contracts query for the balance of an address. But that's all there is to it. Theoretically, Ethereum-based token systems acting as sub-currencies can potentially include another important feature that on-chain Bitcoin-based meta-currencies lack: the ability to pay transaction fees directly in that currency. The way this would be implemented is that the contract would maintain an ether balance with which it would refund ether used to pay fees to the sender, and it would refill this balance by collecting the internal currency units that it takes in fees and reselling them in a constant running auction. Users would thus need to "activate" their accounts with ether, but once the ether is there it would be reusable because the contract would refund it each time.

6.4 Types of Blockchain

In the previous sections, this thesis reviewed the origin of blockchain technology and the working principle of the Bitcoin Blockchain and the one of Ethereum Blockchain.

According to Peck (2017), as well as Wust and Gervais (2018), although different blockchains are based on a variety of consensus algorithms, they can be divided into two general types according to the rules of nodes joining the network. One type is the public blockchain, where anyone can choose to join the network by becoming a node to read and write transactions, as well as mining new blocks, or can exit the network at any time by abandoning its nodes. The other type is the permissioned blockchain, which only allows limited designated participants to join the network or become a node. Mingxiao et al, (2017) divided blockchains into three categories. In addition to the public blockchain and the permissioned blockchain, Mingxiao et al. (2017) also introduced a type of private blockchain which is a centralized system where an owner has the highest authority over all the data. However, Wust and Gervais (2018) considered this type of blockchain as a special form of the permissioned blockchain.

6.4.1 Public Blockchain

Public Blockchain is also called permissionless blockchain, which is a totally decentralized peer-to-peer system where no trust is required for any node since each node has the same read and write authority as well as a complete ledger of all the past transactions on the blockchain, and all the nodes participate in the process of mining blocks. Similar to the original Bitcoin blockchain, most of the public blockchains reward the node that mined a new block with an incentive mechanism. The Bitcoin blockchain is an example of public blockchain. Besides the proof-of-work of the Bitcoin blockchain, Mingxiao et al. (2017) reviewed several other public blockchain consensus algorithms, including Proof-of-Stake (PoS) introduced by King and Nadal (2012) and Delegated Proof-of-Stake (DPoS) introduced by Larimer (2014). The proof-of-stake is an algorithm that introduced a new concept of coin age based on the proof-of-work. The privileges of a coin will be increased over time from the time of its creation. The node which owns more coins with longer coin age will have more rights in the decision-making of the network. In this way, the waste of resources in proof-of-work will be reduced. The delegated proof-of-stake algorithm is a public blockchain algorithm with improved efficiency and reduced resource wasting, based on the proof-of-stake algorithm. In general, the consensus algorithms of the public blockchain must be able to allow nodes the freedom to join and leave the consensus progress in the network. According to Peck (2017) and Wust and Gervais (2018), there are four features of the public blockchain and three applicable scenarios for choosing the public blockchain as the desired system. The features are:

- Feature 1: The system does not have any limitations for the participants joining the system, or becoming nodes involved in reading and writing in the system, which usually results in public blockchains having a large number of nodes. This also ensures that public blockchains are not vulnerable under attacks.
- Feature 2: There is no need for any trust among all the participants and nodes in the system. It can be inferred from Feature 1 and Feature 2 that everyone can join, leave, become a node or abandon a node at any time in the system.
- Feature 3: The efficiency of the system in processing transactions is low (using the number of transactions processed per second (TPS) as the evaluation standard). As mentioned, different public blockchains use various consensus algorithms. However, the efficiency of these algorithms in public blockchains is low due to the magnitude of the nodes, which in turn results in relatively low efficiency of the public blockchains compared to the centralized systems. As explained, centralized systems do not need to make consensus over the network. And the permissioned blockchains make consensus more efficient than the public blockchains since their smaller scale network of limited nodes. Therefore, it is not recommended to use the public blockchains for operations that require high efficiency.
- Feature 4: The system is completely decentralized, which means that all the nodes have the same authority and the same operations.
- Feature 5: Once the data is written into an accepted block in the system, it cannot be changed (including modification and removing), which ensures the traceability of the data in the system.

Based on these features, according to Peck (2017) and Wust and Gervais (2018), the applicable scenarios of the public blockchain are as follows:

- Scenario 1: There is no trusted third party in the target system that can be trusted by all the participants. Feature 2 and Feature 4 are corresponding to this scenario.

- Scenario 2: The Data in the target system needs to be distributed and stored to ensure that it will not be lost or tampered under attacks. Feature 1 and Feature 5 are corresponding to this scenario.

- Scenario 3: The data in the target system should be public, transparent and traceable to all the participants in the network (the data can be encrypted ciphertext). Feature 5 is corresponding to this scenario.

6.4.2 Permissioned Blockchain

The permissioned blockchain is a system that can be considered both centralized and decentralized according to different roles it plays. For the nodes in the network, the permissioned blockchain is a decentralized system whose decision-making is based on the consensus of the nodes in the network instead of a central role that can decide everything. For the participants, other than nodes, the permissioned blockchain is a centralized system which is a black box with no transparency. The permissioned blockchain is composed of a limited small number of nodes where every node in the network is authorized and known. Therefore, the nodes in the permissioned blockchain can reach consensus by direct voting, which is not feasible for the public blockchain where the nodes are unknown and limitless. If direct voting was adopted to reach consensus in the public blockchain, a malicious attacker could increase its possibility of tampering with data by having more nodes, without incurring a huge cost. This characteristic determines that the permissioned blockchain is suitable for a limited scale network with limited number of nodes instead of a global scale network. The limited scale and the nodes being known make the consensus algorithm of the permissioned blockchain more efficient than the public blockchain. Mingxiao et al. (2017) reviewed a consensus algorithm widely used in the permissioned blockchain called Practical Byzantine fault tolerance (PBFT) which was introduced by Castro and Liskov (1999). The PBFT is developed based on the Byzantine Generals problem which was introduced by Lamport (1983). The Byzantine Generals problem described a problem that existed in a distributed system network whose nodes reach consensus by passing messages to each other. However, some of the nodes can be unreachable, and furthermore, there could be dishonest nodes sending tampered fake messages, all of which may result in failure for the network to reach a correct consensus to make the right decision. If a distributed system network can keep reaching consensus to make right decision in such a situation, then this system network is considered a Byzantine Fault Tolerance (BFT) system. In the PBFT, for a network with n nodes, a malicious attacker needs to control more than (n-1)/3 nodes in the network to be able to tamper with the data. The data will be secure and the network is BFT as long as (2n+1)/3 of the nodes in the network are reachable and honest. The nodes in the network are divided into two types. One type of the node can receive, reply to client requests, and initiate and participate in the consensus reaching process. The other node type can only participate in the consensus reaching process. There are five stages for process of nodes in the network to reach consensus on accepting a client request which include request, pre-prepare, prepare, commit and reply. In the request stage, a master node receives and timestamps a client request. Then, the master node initiates the consensus process by sending messages to the other nodes in the network to permit them to make a decision on whether to accept the broadcasted client request. This is the pre-prepare stage. In the prepare stage, if a node (including master node and the other nodes) makes a decision to accept the client request, it will broadcast a message of its acceptance to all the other nodes. When a master node receives the acceptance messages from more than (2n+1)/3 nodes (including itself), it will start the next stage. The nodes in the commit stage will broadcast a commit message to the other nodes in the network. Similar to the previous stage, after a master node receives the commit message from more than (2n+1)/3 nodes (including itself) in the network, the master node executes the client request for the network to accept and the next step begins once the execution is completed. In the reply stage, the master node in the network responds to the client with the result of the execution of the client request.

According to the characteristics of the permissioned blockchain, the applicable scenarios of the permissioned blockchain were introduced and discussed by Peck (2017) as well as Wust and Gervais (2018), which can be generalized as shown in Figure 3.

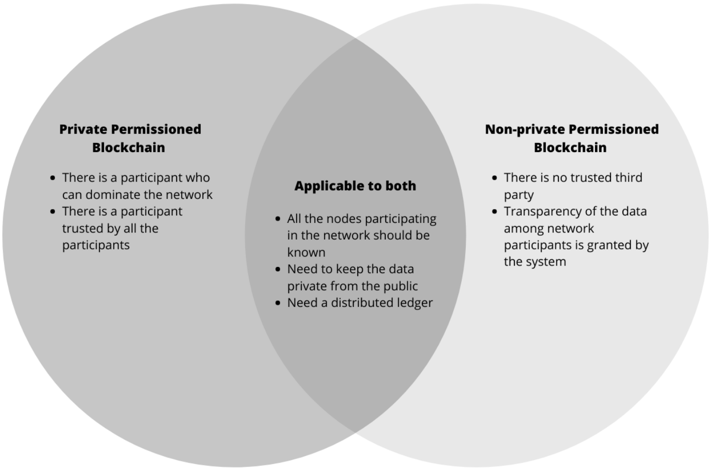

Private Permissioned Blockchain
• There is a participant who can dominate the network
• There is a participant trusted by all the participants
Applicable to both
• All the nodes participating in the network should be known
• Need to keep the data private from the public
• Need a distributed ledger
Non-private Permissioned Blockchain
• There is no trusted third party
• Transparency of the data among network participants is granted by the system

Fig.3 - Applicable Scenarios of Permissioned Blockchain

As can be seen in Figure 3, the applicable scenarios of the permissioned blockchain discussed by Peck (2017) and Wust and Gervais (2018) can be generalized as follows.

- 1. The data in the system needs to keep its privacy from the public. The system should be a black box to the public.

- 2. There are limitations for becoming a node in the system. Every node participating in the network should be known and authorized.
- 3. The system needs a distributed ledger to ensure the transparency or the security of the data (Private permissioned block uses the distributed leger to enhance the security of the data).

The above scenarios are applicable to all types of permissioned blockchain. According to Peck (2018), the permissioned blockchains can be categorized into two types, which are the non-private permissioned blockchain and private permissioned blockchain. In addition to the above three applicable scenarios for all types of permissioned blockchains, these two different types of permissioned blockchain have their own specific applicable scenarios.

For the non-private permissioned blockchain:

- 1. The system needs to ensure the transparency of the data among a group of participants.
- 2. There is no such third party that is trusted by all the participants in the network.

For the private permissioned blockchain:

- 1. There is a participant that is trusted by all the other participants.
- 2. There is a participant who has the highest authority that can dominate the network and dictate the authorization

Proof of Authority (PoA)

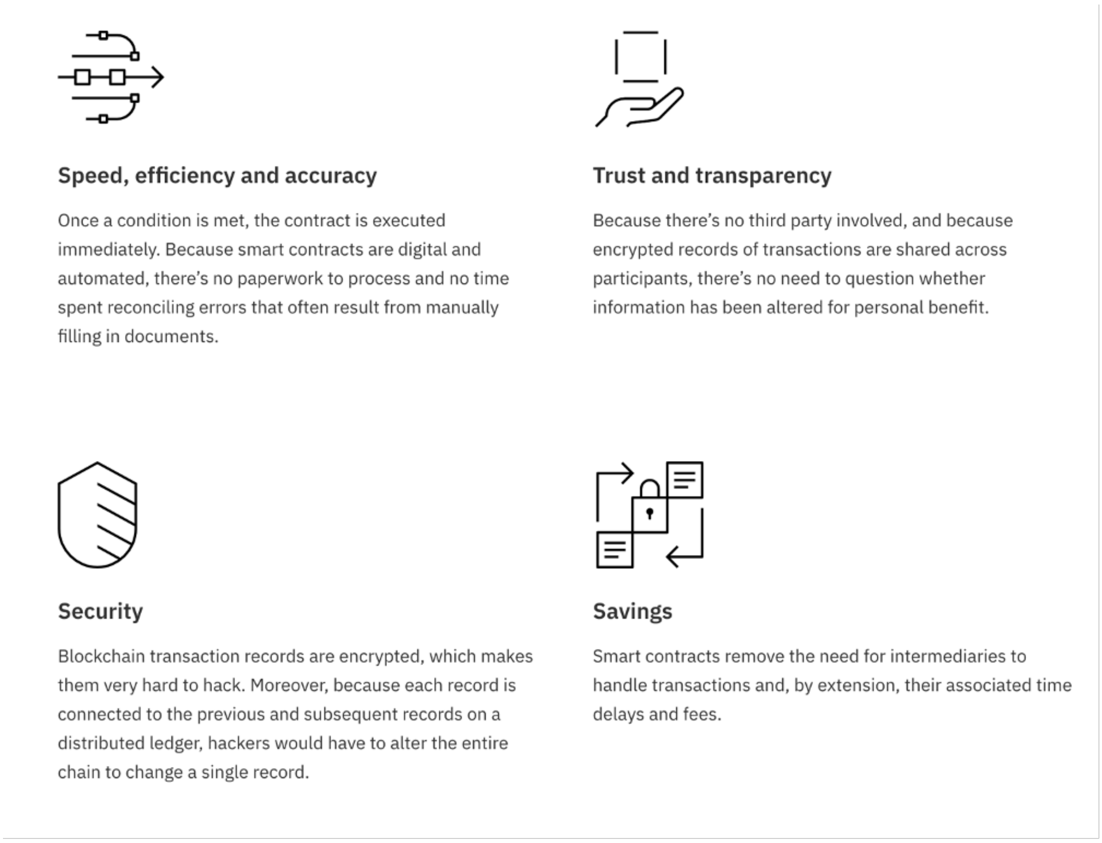
Proof-of-authority (PoA) is a reputation-based consensus algorithm that introduces a practical and efficient solution for blockchain networks (especially the private ones), hence relies on known and reputable validators to produce blocks, providing computational power to a network. It enables relatively faster transactions using a Byzantine Fault Tolerance (BFT) algorithm with identity as a stake. PoA is a type of consensus mechanism geared towards enterprises or private organizations who want to build their own chains that are essentially closed in nature and don't require participation from general users. Since a network running PoA is permissioned, it doesn't require any "mining" activity. However, network participants can still deploy redundancy by running multiple nodes under the same identity. This type of consensus mechanism isn't resource intensive, but requires validators to preserve the integrity of their nodes. It can be understood as a mechanism, which provides incentivization to act honestly and in accordance with the proper functioning of a network, due to user identity and reputation at stake.
PoA requires three conditions to be met:

- Formal identification on-chain for validators.

- Eligibility based on certain criteria, including but not limited to, association with the organization or good reputation, etc.
- Complete conformance to defined procedures required for producing blocks and validating on the network.

6.5 Smart Contract

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met. Smart contracts work by following simple "if/when. . . then. . . " statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results. Within a smart contract, there can be as many stipulations as needed to satisfy the participants that the task will be completed satisfactorily. To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the "if/when...then. . . " rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes. The smart contract can be programmed by a developer – although increasingly, organizations that use blockchain for business provide templates, web interfaces, and other online tools to simplify structuring smart contracts. Smart contracts can bring real benefit for individuals, businesses and organizations in terms of speed, efficiency, accuracy, trust, transparency, security, savings.



Speed, efficiency and accuracy

Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there's no paperwork to process and no time spent reconciling errors that often result from manually filling in documents.

Trust and transparency

Because there's no third party involved, and because encrypted records of transactions are shared across participants, there's no need to question whether information has been altered for personal benefit.

Security

Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.

Savings

Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays and fees.

Fig.3 - The Benefits of Smart Contract

6.5.1 Non Fungible Token (NFT)

NFT stands for Non Fungible Token. In order to easily understand what exactly they are and how they can be used, we should clarify the main difference between fungibility and non-fungibility. Fungibility refers to an asset's ability to be exchanged with a similar asset without sacrificing its value. Fungibility also defines an asset's characteristics, such as divisibility and value, for example, one $10 dollar bill is identical to another $10 dollar bill in terms of value. In the cryptocurrency sector, one BTC has the same value as any other BTC. However, the game changes when we cross over to Non Fungible Tokens. An NFT has a distinct value from any other similar token. Individual characteristics dictate their uniqueness, hence, they are non-fungible, much like real-world assets like rare stones, works of art and football match tickets (a VIP seat is more expensive than a popular seat), this last example will be discussed later. One of the main benefits of owning a digital collectible versus a physical collectible like a Pokemon card or rare minted coin is that each NFT contains distinguishing information that makes it both distinct from any other NFT and easily verifiable. NFTs create scarcity among otherwise infinitely available assets — and there's even a certificate of authenticity to prove it. This makes the creation and circulation of fake digital asset pointless because each item can be traced back to the original issuer. If we pay attention to the reason why digital artists started selling digital artwork through NFTs, we understand that it is the first digital technology allowing artists to provide authenticity and property thanks to the blockchain architecture, being non-fungible brings immutable uniqueness, and this feature is valuable for any activity and business that is able to adapt to technological innovation, converting physical objects into digital assets, scaling security, efficiency and reputation. Non-fungible tokens bring a new dimension to digital interactions. The three leading advantages of NFTs are:

- They're transferable – Unlike exchange-traded fungible tokens, NFTs are bought or sold on special marketplaces. However, their value depends on their uniqueness.
- They're authentic – Blockchain technology powers Non Fungible Tokens. Therefore, you know that your NFT is genuine, since it's nearly impossible to create counterfeits with a decentralized immutable ledger.
- They preserve ownership rights – Again, this refers to an NFT's use of decentralized platforms where no owner can alter the data once committed.

Chapter 7

Merging Architectural Design

7.1 Uefa Blockchain-based Ticketing System

In November 2013 UEFA signed a partnership with SecuTix, a ticketing solution to implement UEFA's new ticketing and hospitality management system. The SecuTix 360° solution will be the technology backbone of UEFA's future ticketing and hospitality management system. (Secutix, 2013). This section will introduce the overall UEFA ticketing project with a focus on how they implemented Blockchain Technology, pointing out the benefit and improvement this technology concretely brought to the UEFA event organization. Before going deeper into the blockchain model applied, we should have an overview of the scope of UEFA Ticketing project. There are six important scope of Ticketing project:

- Access Control: interface with stadium access control system, troubleshooting at the gates and entrances, liaising with SSNS.
- Onsite Operations Pre-event: training for staff volunteers, ticket Centre and clearing point, volunteers management, liaison with venue management.
- Printing Distribution, Data Management: security features on tickets, mobile ticket delivery, monitoring of the delivery and the return.
- Seating, Quota Management: per target group, per block, per category, conditional matches
- Inventory Management: validation of real situation on-site, mapping of overlay, assessment of seat quality and categories, pre-seating of target groups, buffer zones mapping.
- Sales, Promotion Customer Service: online sales and promotion, lotteries implementation, group sales (hospitality, VIP, host, sponsors, broadcasters, UEFA family), participating teams, in-house customer service and FAQs.

The SecuTix system was first used for the 2015 Champions League and Europa League Finals and, following that success, for the UEFA EURO 2016. Because it's one system, UEFA could easily move around inventory between hospitality and ticketing. Returns of hospitality tickets has always proved problematic, but now it was an easy process to take back inventory and trigger further general sale ticket availability. SecuTix is an enterprise-class ticketing software solution that combines ticketing and CRM in one unified platform delivered as a service. SecuTix is delivered as Software/Service in the cloud, which means no infrastructure or maintenance costs. SecuTix manage ticket sales across any channel (box office, internet, mobile), boost B2B sales and increase hospitality revenues. Attract a wider audience and generate brand loyalty, delivering a modern fan experience across mobile and digital channels and improving operational agility. If we think about existing blockchain applications, we notice that the scalability can be a problem when facing high number of transactions per second, but this problem is more relevant on public permissionless blockchain, in fact on private permissioned blockchain the scalability increases consistently as in the case of SecuTix, which one is able to combine efficiently CRM services and the blockchain on the back-end.

"Considering the diversity of what we offer, the challenge is to segment our client base very carefully so that the right message can be targeted at the right person. SecuTix allows us to define the segments using many different criteria (age, date of last purchase, member or not, etc.) and then target each sub-segment with offers and benefits that we think will interest them. This fine-tuning in terms of targeting means we can improve in both relevance and speed."

(Olivier Ouf, Head of Ticketing - LE HAVRE ATHLETIC CLUB)

In the next section we will go through the relevant fraud problem, analyzing how e-wallet works and how e-tickets are able to substitute "old barcode-based tickets". Proceeding with the analysis of SecuTix we will see how this company is facing the black market, security, customer trust and the lack of industry protocol.

7.1.1 Fraud Problem

Fraud has long plagued the ticketing industry, forcing true fans to pay extortionate prices, while posing security threats for event organisers. With recent technological advances, ticketing bots have caused chaos, enabling online touts to buy tickets in bulk and sell them on secondary markets at a high profit margin. The result is evident, customer trust in the industry is at an all-time low and legal steps are being considered in some countries to combat the effects of bots. However, it's fair to say that the ticketing industry itself has been frustratingly slow at responding to the issue. Vincent Larchet, ex Chief Technology Officer at SecuTix, a leading European SaaS ticketing platform, highlighted this issue with a focus on looking at emerging technologies to combat the problems surrounding ticketing fraud; he argues that a serious contender for addressing the issues threatening the industry today is blockchain technology. So long as the ticket is issued as an email, a PDF or a barcode image that can be shared and copied, fraud will remain prevalent. We need to adapt and move to a new type of digital tickets with identity checks and exchange rules in place. Now will be explained how blockchain technology can work in practice for the ticketing industry and how it can play a role in tackling issues related to black market, security, user trust, and the lack of an industry protocol. Blockchain is not the ultimate solution to prevent all fraud, but combined with other technologies we can achieve a simple way to securely transfer tickets, control their resale and severely damage the efforts of ticketing fraudsters. When using blockchain, the initial purchase is exactly the same as it is currently, with total freedom for the ticketing provider. Payment is also the same. User experience and user interface are the same with the only difference coming when the ticket is issued to the client.

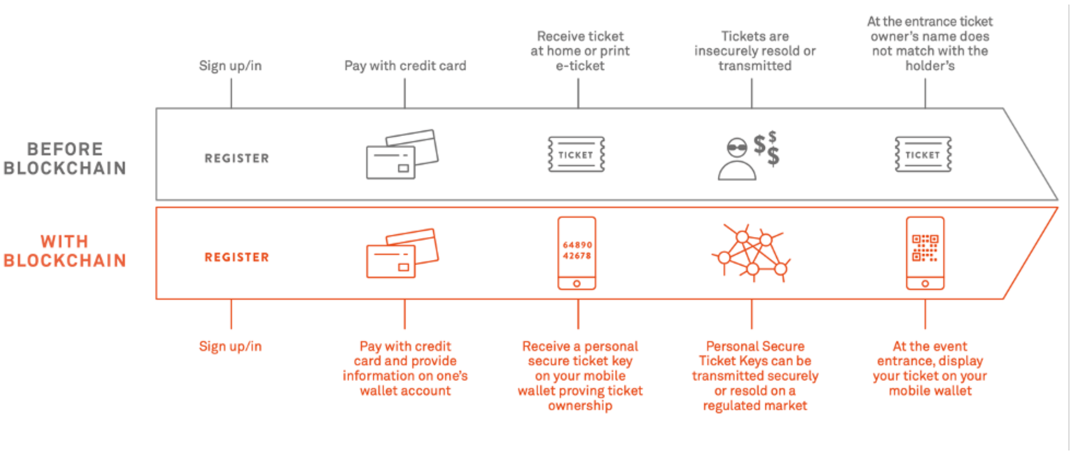

Sign up/in
Pay with credit card
Receive ticket at home or print e-ticket
Tickets are insecurely resold or transmitted
At the entrance ticket owner's name does not match with the holder's
BEFORE BLOCKCHAIN
REGISTER
TICKET
TICKET
WITH BLOCKCHAIN
REGISTER
64890 42678
Sign up/in
Pay with credit card and provide information on one's wallet account
Receive a personal secure ticket key on your mobile wallet proving ticket ownership
Personal Secure Ticket Keys can be transmitted securely or resold on a regulated market
At the event entrance, display your ticket on your mobile wallet

Fig.4 - Secutix before and with Blockchain

7.1.2 e-Wallet

Instead of generating a PDF or a barcode, the client has to register their e-wallet or use their existing one if it's already set up. This is a simple registration process on their smartphone that then binds their phone to an e-wallet of the blockchain. The tickets are then seamlessly transferred to the blockchain. The e-wallet offers easy transfer and resale features, which are all governed securely by the blockchain (smart contract). This is much better than allowing the tickets to circulate printed on paper or as PDF files, beyond the control of the provider. When the customer arrives at the event, instead of showing their piece of paper and its barcode, they use their smartphone and its e-wallet. The smartphone app can then automatically interact with the access control. The majority of customers, especially millennials, are already well versed in using their smartphones for transactions, and this is no different. There's no need to remember a physical ticket, and everyone already carries their smartphone everywhere. Blockchain does not change anything significant for the customer and they are totally unaware that there is an underlying blockchain on the back-end, not contrasting the front-end of the service. But for the organisers, the benefits are great. With blockchain they can identify who holds a ticket, while also providing customers with the confidence that they can buy and resell valid tickets at a fair price.

7.1.3 No Barcodes

This ‘ticket’ is one hundred percent digital. The elimination of the barcode is the key to preventing customers from extracting the ticket out of the blockchain and then bypassing the security rules, auditability and traceability provided by the whole system. Because if you send your barcodes or you put it in your cloud service or share it on social media, you are going to face risk in term of security and your ticket is easily stolen by hackers.

7.1.4 Access Control

The lack of a barcode may cause venue operators concerns about access control. There are two ways to tackle this.

- Blockchain aware access control: the venue can invest in reliable and fast ‘blockchain aware’ access control. These will directly interact with the e-wallet via Bluetooth or NFC (Near Field Communication) and check the validity of the ticket inside the blockchain. The access control software integrates with the blockchain in a uniform and standard way regardless of which system originated the ticket, and regardless of whether the ticket was transferred or resold. The venue can manage this type of access control using either smartphones or tablets.

- Two-step access control: if you already have barcode-based access control software and several dozen existing turnstiles or mobile readers, it does not mean that you have to get rid of them. There can be a ≪two-step access control≫ where the ticket is first extracted from the blockchain and materialized into a standard barcode, allowing use of the existing access control. This extra step can be smoothly added in the physical screening step, using very cheap devices. So you can enjoy all the advantages of blockchain tickets without incurring high setup costs.

7.1.5 The Black Market

In 2015, there was a 55% rise in ticket fraud year-on-year, (City of London Police’s National Fraud Intelligence Bureau and Get Safe Online). Fraud is creating a global loss of trust in the industry. It’s not one or two organisations anymore, it’s a worldwide problem. Bots are the main drivers of fraud for highly sought-after events. Bots disrupt the contact between event organisers and their final customers who are attending the events, thus breaking the relationship between the two, which is a real problem for the industry. Bots will always be present in attempting to take tickets away from real fans, but the industry needs to make it harder for these professional, fraudulent companies to do so. Thanks to the smart contract that is executed when any ticket transfer happens, we can add custom constraints during transfers. For example:

- Set a maximum resale price
- Restrict transfers to a specific time period
- Prevent ticket resale but allow returns
- Comply with current and future government regulations (e.g., tickets could be sold only to an e-wallet containing a passport number).

These constraints will help regulate the market and will obviously reduce the ability of the black market to resell at uncontrolled prices.

7.1.6 Security

Given recent terrorist attacks, security is a top priority for operators of venues of any size, from 80,000 seater stadiums to smaller 2,000 standing venues. Customers expect that organisers will do bag checks on every person, but when tickets get resold and end up in the hands of a different person, this becomes a daunting task. Some venues are installing X-ray scanners or other types of physical screening, similar to airport security, which in turn takes away some of the enjoyment and ease of attending events. Everything that happens in the blockchain is audited and impossible to modify afterwards. Therefore an event organiser will always know, at any time, which e-wallet owns a ticket. This means they can cancel the ticket or get in direct contact with the owner. It allows the application of KYC (Know Your Customer) processes to identify and verify customers. This technology can also be enhanced with secure or trusted e-wallets.

7.1.7 Customer Trust

A big concern for those buying tickets is whether they have paid for a real one or a fake. Customers are being defrauded by fake ticket websites posing as legitimate authorized ticketing agents. This leads to massive disappointment, loss of money, increasing levels of mistrust of the ticketing industry and a downgrade of the brand reputation. Customers are also concerned with being able to resell their ticket safely and securely at a fair price, or to hand it over to a friend if they can't attend. Will the new ticket owner be turned away at the entrance? Blockchain enhances customer trust levels because they can be guaranteed they are buying a valid ticket and it puts a stop to duplicate sales. If they want to switch the ticket to a friend, they can simply click on “send to a friend”, add their identity details, and the data is updated in the blockchain when the recipient receives the tickets.

7.1.8 Lack of Industry Protocol

Unlike many other industries, there is no standard protocol in ticketing. This means we can’t exchange data or track customers beyond the boundaries of a given supplier. The lack of an exchange protocol in the industry facilitates fraud on the secondary market. When a ticket is resold on the secondary market, it no longer belongs to the original buyer whose details the event organisers have. Therefore event organisers do not know exactly who is at their event. This is due to the fact that tickets are issued in a format that cannot be adapted for exchanges on the secondary market. Not only you cannot change the name of the ticket holder, but you cannot control how many times it will change hands. Finally, there are many access control solutions, but each of them has to interface with the chosen ticketing solution. If there were a standard ticketing protocol, all access control solutions would be compatible with all ticketing solutions issuing them. New installations would be quicker and cheaper. Blockchain will create a standard ticketing protocol. The technology acts as a giant database, thereby creating a de facto standard. Every ticketing company and access control provider will have a standardized implementation for existing and new business. All this is backed by intrinsic permissions and data access authorizations built into the blockchain. Therefore an organiser can easily grant any access control provider the authority to verify his tickets. When a ticket holder passes their ticket onto a friend, the smart contract execution will cancel the original ticket and create a new one for the friend. It disappears off their e-wallet and appears in the new ticket holder’s e-wallet. This avoids any confusion at the gate, as the new ticket works with the access control. The following figure illustrate a simplified overview of SecuTix service.

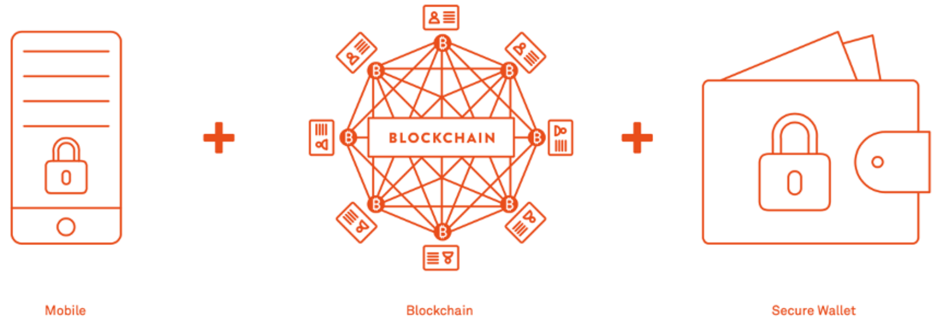


Fig.5 - Secutix, simplified service overview

SecuTix has leveraged the blockchain, merging it with mobile and access control to create a technologically responsive e-ticket that you cannot copy or transmit without following certain guidelines and rules. It allows the organiser to know who will attend and to ensure that tickets are resold at a fair price, hence dictating the rules of secondary market. Blockchain creates a real opportunity for a dramatic change in the way the ticketing industry deals with fraud. It is a powerful tool to mitigate the risk of fraud. We don't pretend blockchain is the last surviving chance for ticketing, as fraudulent professionals will always find a way to react to the technology advances, but it will make things much more complicated for them and actually, in 2021 is the most advanced technology to solve several problems mentioned along this thesis.

7.2 Socios.com

The socios.com is a platform operating on the basis of blockchain technology and smart contracts for the purpose of offering a tokenized voting platform where fans can buy, sell and execute voting or "crowd managers" rights in their sports teams and benefit from extra VIP benefits. Owning Chiliz tokens and exchanging them on Chiliz-powered platforms like Socios.com, fans can acquire voting rights and the ability to participate in decisions and guidance for teams, leagues, game titles and events. It's a solution scalable and flexible enough to work across sports and esports ecosystems. (CHZ socios.com whitepaper)

The issuer of the Chiliz token is HX Entertainment Limited, which one has adopted rigorous KYC procedures to verify the identity of every applicant, and the beneficial owner (where applicable) that has expressed interest in acquiring Chiliz and only those contributors which have successfully identified themselves in the KYC procedure to the Issuer's satisfaction, have been successful in participating in the Chiliz Private Placement. As a technological foundation, blockchain is the de-facto choice to do so in an eloquent manner. To ensure integrity, they run their own permissioned instance of the Ethereum blockchain. This permissioned sidechain is the core of Socios.com. It hosts every team, league, game title or other organisation who connects with the platform, together with each organisation's crowd voting mechanisms run as a semi-autonomous organization on this blockchain. Running their own permissioned sidechain will drastically reduce transaction costs by allowing the use of a Proof of Authority (PoA) consensus algorithm to confirm each new block of the permissioned chain - with each block storing polling/ decision results - instead of necessitating the use of Proof of Work (PoW) consensus. Everything that occurs on the Socios.com platform in terms of Chiliz ERC20 transactions - new accruement of Fan Tokens converted from Chiliz ($CHZ) tokens and Socios.com account balance exchanges as part of the platforms other service features - will be stored in an auditable, permanent manner via public ledger on the main Ethereum blockchain. Chiliz ($CHZ) Tokens will be emitted on the main Ethereum blockchain, while partner-specific Fan Tokens will be emitted on Socios.com permissioned sidechain. This means that on a functional level the Socios.com platform itself serves as the only bridge which enables the exchange of Chiliz tokens and Fan Tokens (and vice versa). The Socios.com platform's public ledgers, which together chronicle a full history of platform-wide transactions, can be audited by anyone.

Ten reasons the Socios.com permissioned sidechain is based on Ethereum (CHZ socios.com whitepaper):

- We believe in the spirit of open-source development, having found inspiration from innovations created by open-source communities for the last 15 years.
- Ethereum provides a complete toolkit for developers to build Apps, Smart Contract and other blockchain based solutions.
- Ethereum and Solidity - its smart contract scripting language is supported by a very well-established and active community.
- Compared to other blockchains that have not delivered on usecase promises, Ethereum is a proven technology running live applications by the thousands.
- Ethereum comes with a Turing complete smart contract scripting language.
- Ethereum is a mature ecosystem where tools like Parity, Truffle or Open Zeppelin continue to push quality and security upwards.
- Ethereum's vast choice of consensus algorithms (including Proof of Authority) allows any chain topology, including permissioned chains.
- Ethereum has much higher performance when deployed on permissioned chains.
- Ethereum is 'future proof' when considering its roadmap (Metropolis and Serenity phases), which paves the way for things like Proof of Stake, Sharding or Plasma chains.
- With communities - including the Enterprise Ethereum Alliance - rallying around the environment, Ethereum benefits from the consensus-confidence of its diversely focused active adopters.

We have seen how SecuTix has incorporated blockchain technology in its service. They used blockchain technology in a powerful way, but they were limited in creating a better service by the scarce knowledge and adoption of this technology by people. Blockchain will definitely be a game changer but it's important that the industry recognizes blockchain does not solve all the problems at a stroke. The problem that still SecuTix and its partners (UEFA, Opera National de Paris, Musee Picasso Paris, etc.) are encountering are related to card payment fraud, ticket transfer that is still possible, fake data, trial & adoption of a new technology.
We have seen also how Socios.com platform allow to buy & engage with football clubs in a transparent and safe way, exploring the platform focusing on the main technical features linked to blockchain technology. Along this section I am going to discuss those specific problems while contributing with proposing a possible solution to fill those gaps.

Chapter 8

A new alternative solution: Tickets as NFT with PoA

- Card payment fraud

  There is still a requirement for a money transfer to purchase the ticket and we are all aware of the possible fraud with card payments. One solution is to bind the blockchain to a cryptocurrency. Technically, such binding is feasible: Ethereum is the best known and there are recent blockchain based applications connecting football clubs and football fans; the best one is Socios.com (explained in section 6.7) platform's blockchain backed, tokenized voting system; capable of driving transparent and democratic crowd decision making processes for teams & entities from any game type or sporting vertical. The Chiliz ($CHZ) token is used by fans to acquire branded Fan Tokens from any team or organization partnered with the Socios.com platform and enact their voting rights as their fan influencers. This company has shown that football clubs & fans are starting to approach the technology with different eyes. If fans embraced this cryptocurrency-based model because they feel engaged in a reliable way, why not selling also match tickets with the same currency or another one strictly similar and specifically targeted for ticketing purpose, avoiding speculation and volatility. If we look at the problem that are limiting worldwide cryptocurrencies adoption is mainly the market volatility, but proceeding with a targeted audience and with a permissioned blockchain running on top of Ethereum, doing ticket transactions with cryptocurrencies the problem of card payment fraud linked to online football match ticketing is no more a problem. To ensure integrity, Socios.com run their own permissioned instance of the Ethereum blockchain. This permissioned sidechain is the core of Socios.com; running their own permissioned sidechain will drastically reduce transaction costs by allowing the use of a Proof of Authority (PoA) consensus algorithm to confirm each new block of the permissioned chain. Other than being a scalable solution, this system also ensure transparency as Socios.com's PoA sidechain is publicly auditable. Hence those features may be combined with tickets sold as NFT ERC-721 and ERC-1155; in this way the ticket is released as smart contract, thus applying all the constraints the issuer club wants to fix and also encouraging fans by providing security and an immutable and non-perishable proof of participation, which one can be seen as a collectible. NFTs can help to overcome the current weaknesses of existing non-blockchain event ticketing systems, such as susceptibility to fraud, lack of control over secondary market transactions and validation of ownership. In conclusion, merging different architecture and technologies such as the ones of SecuTix and Socios.com, and selling tickets as NFTs in such a way to distinguish per importance every seat per each part of the stadium and giving to the event organizer the right to set ticketing rules can be a solution for every football stakeholder.

- Ticket transfer still possible

  Nothing prevents a ticket holder from selling a ticket that's held within a blockchain, but at least with the technology we will know that the transaction has happened. The smart contract may restrict the price paid for resale, but it cannot prevent money changing hands at the same time, such as a cash payment. This problem is quite difficult to be solved because you can not have control over people who are exchanging cash offline, but of course event organiser will be able to identify every ticket transfer given that blockchain technology provide traceability.

- Fake data

  There will still be some 'Donald Ducks' and 'Mickey Mouses' trying to attend events as we can't prevent people from inputting fake data. But this problem does not persist with Proof of Authority consensus algorithm and of course, in the worst scenario, they can be stopped at the gate of the venue.

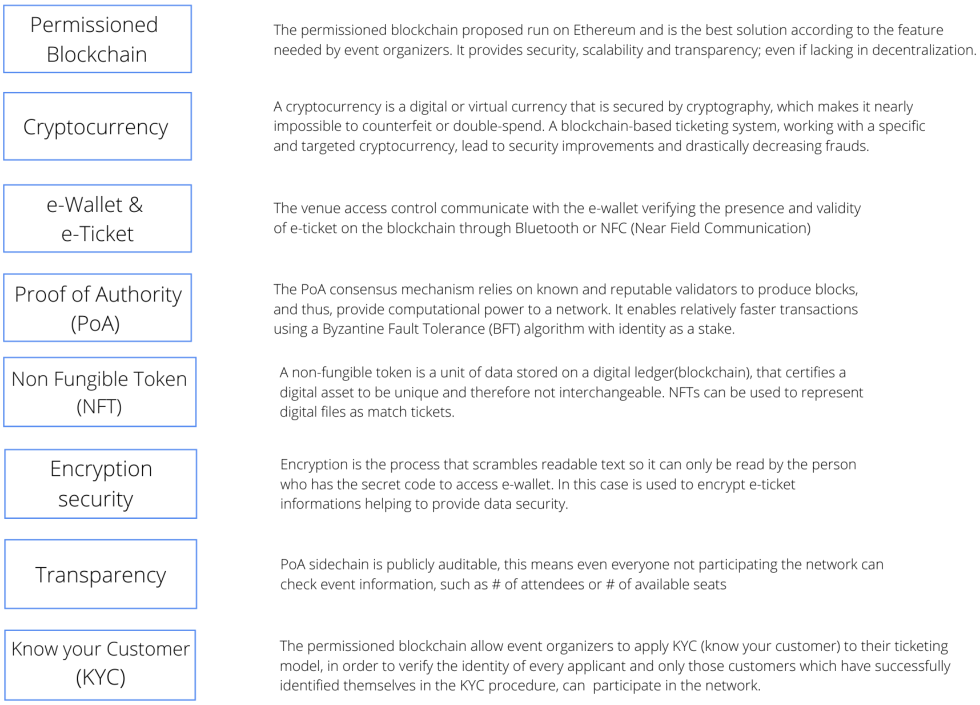
- Trial and adoption of a new technology

  Although blockchain will be part of the solution, this technology is still at its early stages of application. As with any new paradigm, surmounting a number of technology and user adoption challenges will be key to its success but in the meanwhile Socios.com is continuously increasing in number of participating clubs and final users (fans). This means people are starting to embrace this new form of transaction model, regardless any speculation or bubble.

Chapter 9

Conclusion

We have seen that ticketing is not as simple as it can seem. Even associations of a certain caliber as UEFA, leader in the Football sector, are encountering problems related to fraud and security. This thesis has given an overview of the process involved in event ticketing and tried to provide possible solutions in order to fill the system gap. The permissioned blockchain is the key element where to start implementing a working ticketing system, with the integration of a cryptocurrency that together with PoA consensus algorithm combined with the features of Non Fungible Tokens can result in the right choice for football clubs that want to implement their own B2C ticketing system and for Association as UEFA and FIFA. On the first line, the security on both side, organizer and customer, are essential to keep innovating the constantly growing football world that needs to be secured. The awareness and adoption of blockchain technology by people is a key point in order to make this thesis proposal works. In this last figure 5 is explained a resume of the proposed solution to football ticketing system.



Permissioned Blockchain	The permissioned blockchain proposed run on Ethereum and is the best solution according to the feature needed by event organizers. It provides security, scalability and transparency; even if lacking in decentralization.
Cryptocurrency	A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. A blockchain-based ticketing system, working with a specific and targeted cryptocurrency, lead to security improvements and drastically decreasing frauds.
e-Wallet & e-Ticket	The venue access control communicate with the e-wallet verifying the presence and validity of e-ticket on the blockchain through Bluetooth or NFC (Near Field Communication)
Proof of Authority (PoA)	The PoA consensus mechanism relies on known and reputable validators to produce blocks, and thus, provide computational power to a network. It enables relatively faster transactions using a Byzantine Fault Tolerance (BFT) algorithm with identity as a stake.
Non Fungible Token (NFT)	A non-fungible token is a unit of data stored on a digital ledger(blockchain), that certifies a digital asset to be unique and therefore not interchangeable. NFTs can be used to represent digital files as match tickets.
Encryption security	Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code to access e-wallet. In this case is used to encrypt e-ticket informations helping to provide data security.
Transparency	PoA sidechain is publicly auditable, this means even everyone not participating the network can check event information, such as # of attendees or # of available seats
Know your Customer (KYC)	The permissioned blockchain allow event organizers to apply KYC (know your customer) to their ticketing model, in order to verify the identity of every applicant and only those customers which have successfully identified themselves in the KYC procedure, can participate in the network.

Fig.5 - Resume of the contribution of this thesis

9.1 Future Work

The presented system architecture is still abstract. Even if this thesis proposed a solution, researchers should try to implement it, while applying some new technologies to better manage the situation on-site at the event. Future researches may be focused on increasing the overall security level regards identity management, and with the advancement in adoption some parallel studies can be made to improve ticketing system, hence could be addressed the problem of integration of IAM(Identity Access Management) even if right now can't be a concrete solution since the adoption of the technology is at the beginning and our digital identity is not registered on DLT yet.

Chapter 10

References

Qteishat, M. K., Alshibly, H. H., Al-ma'aitah, M. A. (2014). The impact of e-ticketing technique on customer satisfaction: an empirical analysis. JISTEM-Journal of Information Systems and Technology Management, 11(3), 519-532.

Courty, P. (2017). Ticket resale, bots, and the fair price ticketing curse. Retrieved from http://web.uvic.ca/ pcourty/FPT1005.pdf

The Australian Government the Treasury. (2017). Ticket Reselling in Australia. Retrieved from www.itsanhonour.gov.au

Vacca, J. R. (2013). Computer and information security handbook. (J. R. Vacca, Ed.) (2nd ed). Waltham, Mass.: Morgan Kaufmann.

Waterson, M. (2016). Independent Review of Consumer Protection Measures concerning Online Secondary Ticketing Facilities. Retrieved from https://bit.ly/2wLvnrB

Vincent Larchet (2014). Secutix whitepaper

Tackmann, B. (2017). "Secure event tickets on a blockchain." In: Lecture Notes in Computer Science (Vol. 10436 LNCS, pp. 437–444). Springer, Cham.

McMillan, C. (2016). "Secondary ticketing: the problem and possible solutions, explained." Retrieved from https://inews.co.uk/culture/music/secondary-ticketing-problems-solutions/

Mengxuan Liu (2021). A Hybrid Blockchain-Based Event Ticketing System

D Yaga, P Mell (2019). "Blockchain technology overview." National Institute of Standards and Technology

Internet Society (2018). Do Blockchain have anything to offer identity?

Qteishat, M. K., Alshibly, H. H., Al-ma'aitah, M. A. (2014). The impact of e-ticketing technique on customer satisfaction: an empirical analysis. JISTEM-Journal of Information Systems and Technology Management

Chiliz socios.com whitepaper (2018)

Vitalik, B. (2013). Ethereum white paper: a next generation smart contract decentralized application platform.

Larimer, D. (2014). Delegated proof-of-stake (dpos).Bitshare whitepaper,81, 85.

Isaksson, C., Elmgren, G. (2018). A ticket to blockchains.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger.

IBM (2017). Blockchain for Supply Chain.