CRecMent

Blockchain-based Criminal Record Management

Blockchain as a process execution infrastructure

May 2022

Ottavianelli Edoardo

ottavianelli.1756005@studenti.uniroma1.it

Piermartini Matteo

piermartini.1802597@studenti.uniroma1.it

Polifemo Aurora

polifemo.1802485@studenti.uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

Contents

1 Customer segments and early adopters **2**

2 Problem statement **3**

3 Existing alternatives **6**

3.1 Analysis 6

3.2 Alternatives 6

3.2.1 Canada 6

3.2.2 European Union 7

3.2.3 China 8

4 Solution **10**

5 Unfair advantage **12**

6 Unique Value proposition **13**

7 High-Level concept **14**

8 Key Metrics **15**

9 Cost Structure **16**

10 Revenue Streams **18**

11 Business Model Canvas **19**

12 Conclusion **20**

1 Customer segments and early adopters

There are more than 10.7 million people incarcerated on earth, of which over 2 million just in the United States [1] [2]. Beyond the high number of inmates, the criminal records for major as well as for minor crimes, are growing from year to year, so the information kept by them should be traced and secured properly. For what we know now, governments are trying the best they can to guarantee it. We would like to provide a better solution to fulfill this gap using the power of the Blockchain as a means to ensure some fundamental aspects. We have to acknowledge the fact that there exist prisons managed by private corporations under government concession, but those are a minimum share of all the prisons around the world, so our target is the public sector since it is more profitable. We shall not forget that this is a critical customer type, so we need to provide reliable integration between all the parties involved (such as the Police Department and public officials, government organizations, ministers, Judicial Offices etc.)

Given that the Blockchain is not corruptible, a key feature of our solution is data integrity; so our early adopters could be governments having problems with corruption and that want to raise the population's trust. Other possible early adopters could be countries which security has become an important point of view for a correct management of the nation.

2 Problem statement

There are different problems that the governments have to handle when dealing with the maintenance and usability of criminal records. Especially in the US the number of people that are locked up in prison is very high, we can count more than 2.3 Million inmates, it follows that this high number makes the maintenance of all their data a big issue.

Nowadays the majority of the governments in the high-developed countries use digital processes to keep population data, however there are still small parts that involve analog data transfers. Moreover, there are developing countries in which these processes are not so advanced.

The traditional process of moving paper documents from one office to another takes a lot of time and effort, thus it increases the overall time needed to complete an entire juridical process. Even if they don't use paper-based communication, a single email that must be sent from an office to another could be time consuming.

For example, for the Italian government it takes at least three business days to deliver your personal criminal records documentation from where it is kept to your home[3].

Databases are the main systems used to store data, therefore they are also the major technology used to keep important information about criminals. These collections of data, if used in a wrong manner, may suffer from some vulnerabilities that allow to an external attacker to damage the integrity and validity of the data, or to obtain some information without any permissions. There had been some important attacks over the years which had as target the databases of major government organization. For example, as reported by different newspapers, there was a ransomware attack on

a British company called "Dacoll" which handles confidential data belonging to the British police [4]. This company manages access to Police Nation Computers (PNC) through a "NDI" technology which allows remote access to police nation computers. This service is used by 90% of UK agents for various business purposes. Through this attack, the attackers stole information from these computers/databases and then demanded compensation from the British government. However, the compensation was not paid and the data was published on the attacker's website.

These problems are mainly caused by vulnerabilities related to databases, such as their bad management and bad maintenance, nevertheless they could be even caused by vulnerabilities of the services they make use of (as in the previous example from the "NDI" service).

Data integrity is an important security feature that needs to be implemented especially when dealing with sensible information, such as the ones contained in criminal records. With data integrity we mean the accuracy and consistency of the data over its entire life-cycle.

This characteristic needs to be dealt with by prisons and police departments. The number of data corruptions and tampering is high and it increases with time. People, so as criminal organizations, are becoming more capable in using the Web and the new technologies in their favor.

It's not just a problem that comes from the outside world. We know that for money anybody would do anything, so there are Correction Officers that could be bribed to change the data of some felons, or even delete all of it, from within the system itself without even trying to hack inside it.

To summarize, the three main problems stated are all time and money consuming for the reasons specified above. For the first problem, the consumers need a better

process to handle juridical information, instead for the other two they should leave behind traditional technologies to avoid the related security issues.

3 Existing alternatives

3.1 Analysis

Governments nowadays rely on several companies able to build services intended to manage criminal records, however due to the sensitivity of these information it seems that nobody disclosed technical details about this topic.

It's easy to guess that many companies build these type of infrastructures in the "traditional" manner (centralized databases and web servers), considering that it's the main way to keep data, but few of them provide a reliable decentralized system, due to its newness and complexity. And it appears that there are even fewer companies concerning our same matter. Given that these do not focus on criminal records or cyber law, and that it's not so simple and convenient for them to enter this kind of market, we can see ourselves in a more privileged position.

3.2 Alternatives

Since our customers are governments, we focus our analysis on them. Even if they currently have their own systems to handle these kind of problems, the vast majority of them have similarities. We will present some of them.

3.2.1 Canada

The Canadian Police Information Centre (CPIC) is a centralized database (managed by the Royal Canadian Mounted Police) storing information for the Canadian Police. It's the main service delivering information regarding crimes to over 80,000 law enforcement officers across Canada [5]. In order to access some data, these have to

be requested, but a person can access only its personal data, or other people's data with their permission.

Another useful tool that Canadian officers use is the Police Information Retrieval System (PIRS). This indexing system is used by RCMP to store, read and update information on individuals being involved (also in the past) in criminal investigations. According to the RCMP, PIRS contains limited information linked to investigations and criminal records, in addition to specifics of an event in a brief description. As we can read from an old article on the website of the OPCC: "Unlike CPIC, which essentially contains factual information (e.g., charges and convictions), PIRS may also contain information provided by witnesses, victims and other associated subjects that can be highly subjective, as well as the names of the witnesses, victims, and acquaintances of the accused individual. PIRS also differs from CPIC in that it contains information on occurrences and incidents that never resulted in charges." [6].

3.2.2 European Union

In April 2012, the European Criminal Records Information System (ECRIS) was established. Its goal is to improve the exchange of criminal records throughout the EU. It's a decentralized system that allows for the request-based sharing of criminal records kept in national databases. The system works successfully because each Member State keeps track of all convictions against its citizens, even those in neighboring Member States.

When a third-country national (TCN) is convicted, however, the record is only kept in the convicting Member State, and there is no way of knowing if anyone else has it. Sending 'blanket' inquiries to all Member States is the only way to find out.

Only 10% of all requests made through ECRIS concern TCN, indicating that this system is burdensome and discouraging.

A solution to this problem was adopted in 2016, the idea was to improve ECRIS by using a search mechanism that finds out if some other EU state has information on a TCN subject. In addition to this, in 2017, there was a proposal to make the ECRIS system centralized, instead of decentralized. Although the entire criminal records would still have to be retrieved through the present ECRIS, the centralized system would contain information to identify a person and the convicting Member State. [7].

3.2.3 China

In 2018, in China the "Hangzhou Court" became the first court in the world to use evidence stored in a Blockchain-based platform. Over time, a large proportion of Chinese courts started using these third-party platforms to keep reliable evidence in appellate courts.

On June 2018, a court of appeal was activated in Hangzhou court. A website owner was charged to have used an article with copyright without the author's consensus. After discovering the illegal use of his article, the author has decided to keep the evidence in order to have something to present in court. The mechanism used to save this evidence was the following: the author took the URL of the web page and sent it to the third-party platform created to storage the evidences. The web service that received the URL of the page used a plug-in to take a screenshot of the web page and to generate the log of the all operations done by the creator of the page. After the generation of the evidence, the web service has calculated the evidence's hash value and has uploaded it to two Blockchain ("Factom" and "Bitcoin"). In this

way all the evidence was used during the prosecution of the crime.

By using this method the court needed to examine the admissibility of evidence through some aspects: the qualification of the third party platform, the credibility of the tools used to capture the web page information, and the integrity of the storage of evidence in the Blockchain.[8]

4 Solution

Our core change will be the infrastructure where the data is held, switching from a traditional client-server to a decentralized architecture. The Blockchain is a system in which the data is not stored in a central data storage system, such as in databases, but multiple nodes have their local view of the data. It might seem that these views could have some incongruousness, since there is not a centralized element that puts them in sync, making the system appear unreliable. However this problem is solved by the Consensus algorithm: the valid view of the system will be the one shared by the majority of nodes.

By using this practice the system will achieve many benefits that are meant to solve the problems listed in the previous section.

Our solution is aimed to simplify the processes and the data sharing involved in the criminal-records related activities. Since there are a lot of parties involved (government organizations, courts, individuals, police stations, airports, etc.), we don't want to add an additional layer of complexity that would make the management catastrophic.

The solution we are proposing will simplify the heavy/analog processes making it conceivable to automate different elements (wherever possible) and to reduce the time required to share information: there would be no need to use emails, paper documents, hand signatures and certificates in the offices. This change will also decrease the error rate due to human mistakes.

In order to achieve this goal the key is to provide a simple but effective user interface that can be used from different devices. In this way it would be easier for individuals to handle the infrastructure, even for those that are not so experienced with the digital world. In general, it is known that people are lazy and even a little

change in their daily working routine could make them lose their productivity; so we will provide also a quick course to help the public administration to recover their productivity in the quickest way possible.

There are two big problems with the traditional process currently still used: the handling of data security and data integrity.

As already explained in Chapter 2, databases have vulnerabilities, so if used in a wrong way by an application (e.g. input not sanitized and directly used to build queries) they could cause serious damages, e.g. they could be exploited through SQL injections, making an attacker read, delete or update some criminal records.

For obvious reasons, given that systems underneath criminal records are crucial we cannot deny that they are already built with security in mind, so it is clearly a little bit harder (but not impossible) to tamper with the data they contain from the external. Nevertheless, they still use databases to keep that data and as said above these have some flaws, so using a Blockchain based infrastructure removes those issues. But what if the threat comes from within? An administrator could have (as not) the permission to delete data from the system, with the Blockchain infrastructure that modification cannot be made unnoticed, considering that each block in the chain contains its own hash and the hash of the previous block, so if one of these gets modified the hash wouldn't match anymore. [1]

We will work with governments and so each of them will adjust considering their own laws with respect to data, privacy and information security of their citizens. From this follows that our solution will have a common base infrastructure that can be easily adapted in different scenarios so as to overcome the rigidity of the data policies of the various countries.

[1] CRAB: Blockchain Based Criminal Record Management System [9]

5 Unfair advantage

Our product is designed to be an alternative way to storage critical data. It has some advantages with respect to our competitors especially for the use of the Blockchain. As we already said, along with this infrastructure comes a data exchange and management that is more secure and controlled than the ones proposed by our competitors. The centralized systems used by our contenders is susceptible to attacks from the external world, the system is flawed and has vulnerabilities, just for the fact of being a database. Our architecture is more secure, it is decentralized and every movement is traced, so even a slightly change from the normal behavior could raise an alarm. However, the Blockchain is still a topic that is not so known by everyone, so people could be skeptical to buy our product beforehand, but once they understand how everything works, the solution we are presenting is a better choice than the ones with traditional infrastructures. The benefits that our consumers will get from adopting our product are not only functional, considering the problems it would solve regarding security and usability, but because of the implementation of a simple user interface, they will become more productive and quick while working.

6 Unique Value proposition

For governments who need data security and speed, our blockchain based infrastructure helps maintain criminal records.

This is our unique value proposition, we tried to produce a catchy and useful sentence. The aim of it is to provide a fast understanding of what we do and what problem we want to solve for potential costumers. This is a well known template used in the marketing field, it's presented by Geoff Moore in one of his book back in 1991, called *Crossing the Chasm* [10]; its basic format is: "For [target customer] who [needs or wants X], our [product/service] is [category of industry] that [benefits]".

It is simple but still effective because it touches both the fears and the needs of our customers: data security and speed. Our clients need security in digital processes and at the same time they need to avoid time consuming analog tasks. The quote also exhibits the core product we are selling, a blockchain based infrastructure. In a few words we are able to reflect the idea behind the product the customers will buy, basically, we are stating the object of the problem: criminal records.

The sentence is more a phrase that states what differentiates us from the market, rather than a slogan.

7 High-Level concept

We have created a short and concise slogan that explains how our technology works:

Criminal records, get 'em fast and secure.

This slogan briefly explains the advantages of using the blockchain instead of the databases currently used.

The goal of our product is to improve security in the management of criminal records, preventing an attacker from changing the status of some sensitive data through any type of attack or through vulnerabilities in databases. The Blockchain prevents these types of attacks through a system based on encrypted transactions and data, therefore more difficult to attack by any type of attacker.

Another additional goal is to increase the speed of data retrieval with respect to the systems used nowadays. For example, the Italian system takes several days to recover and transmit data of a criminal record after it has been requested by an individual. Once more, through the use of an advanced tool, such as Blockchain, we can drastically increase the speed of the data exchange between establishments, therefore avoid wasting too much time on the delivery of a criminal report.

To sum up, the Blockchain technology allows us to build an effective, secure and fast product that can be used by prisons that need faster and more secure management of sensitive data.

8 Key Metrics

The implementation of CRecMent is innovative: Blockchain is becoming little by little part of our reality, our product will be state-of-the-art, it is going alongside with progress. The metrics we use to measure the success of our company are:

- **Number of security breaches**: By comparing the breaches that were made using the old infrastructure and our new one, we can evaluate if our system is really as secure as we thought it to be. We can measure it by simple finding how many blocks were modified without permission in the Blockchain.
- **Satisfaction from the usage of our product**: we measure not only how satisfied our customers and consumers are with our product, but we are gonna consult even the individuals that had to deal with our clients.
- **Speed of retrieving data**: We can evaluate the speed with which the different facilities that implemented our product were able to retrieve the data that comes from a criminal record based in another facility.
- **ROI metric**: The Return On Investment statistic is a calculation that compares our profits to our costs. This indicator can be calculated by removing the cost of investment (infrastructure costs, etc.) from the current value of investment and dividing the result by the cost of investment.

9 Cost Structure

Due to the nature of the customers we will make specific adjustments for each government, however we plan to build a common core architecture for all the projects. Considering that to achieve the stipulated goals, these types of project require a large workforce, for a start we thought to recruit thirty software people (junior and senior developers, project manager, sysadmins, cryptographers, QA testers) and a team of cyber law experts.

The product will be deployed on the machines of the customer, so the hardware cost won't be at our expenses. In order to help the development process and to build faster, reliable and quality software we need to use development tools like test servers, IDE, bug/issue tracker and video communications app licenses. Fortunately, we can use some open source projects to save part of the budget.

It's likely that there are going to be private companies trying to enter the same market, becoming our competitors; in order to not lose our sector supremacy we plan to have a Research & Development section in the near future. We will also provide maintenance for the first year, then we will negotiate it with our customers, so this cost will deeply depend on the agreement reached in the contract.

In the figure below (*Figure 1*) the histogram chart describing how the cost structure will change during the years is shown. In the first year we will have to spend our total budget on workforce and development assets. The development assets cost will decrease after the second year because once we bought the servers and workstations the only remaining costs are licenses. The cost of maintenance and R&D instead will slowly increase, even if in the future these costs will return as earnings.

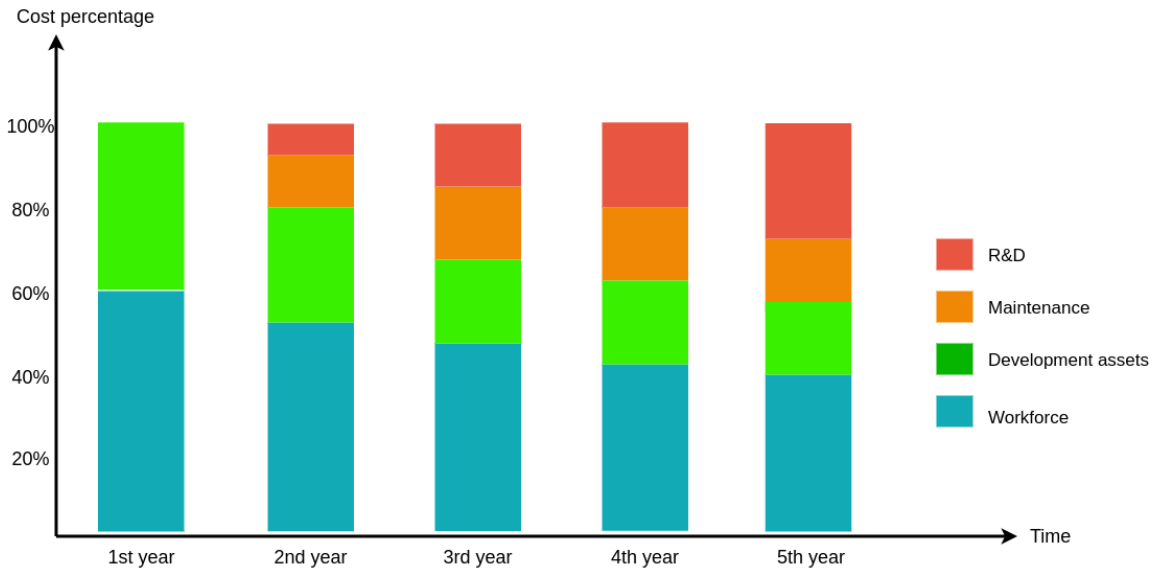

Figure 1: The cost of the structure over the years

10 Revenue Streams

Funds are a fundamental component of a company and as for every new start-up we need to have a source of income. Regarding our project, the sources can be the following:

- **Contract signature fee:** Customers could be an important source of revenue. In fact, they are the ones paying for contracts that guarantee a safe and efficient service. There can be different types of contracts, from annual to several consecutive years. Since we are talking about a service that handles important data it is very likely that a customer will sign this contract for several consecutive years. This will allow us to have guaranteed revenues for a long time.

- **Investors:** There could be some investors that would want to invest on our idea. We could find a private investor that believes in our purpose and invests capital in order to develop the system with even more innovative technologies. The investment is made by buying shares of the enterprise.

- **Maintenance revenue:** An additional source of income could be through system maintenance. The maintenance does not have additional costs for the first year of our service's agreement, instead for the following years the customers will have to pay for those if they want to carry out maintenance.

11 Business Model Canvas

1. Problem

- Data Integrity
- Process speed
- Information Security

Existing Alternatives

Traditional data storage systems aka databases

4. Solution

Blockchain-based infrastructures can provide by default data integrity and security, since it's digital at all the process speed will increase

8. Key Metrics

- Number of Security Breaches
- Satisfaction from the usage of our product
- Speed of data retrieval
- Return of Investment

3. Value Propositions

For governments who need data security and speed, our blockchain based infrastructure helps maintain criminal records.

High-Level Concept

Criminal records, get 'em fast and secure.

9. Unfair Advantage

- Blockchain-based infrastructure
- Data integrity and security by design

5. Channels

- Public competition announcements
- Social networks

2. Customer Segments

- Governments

Early Adopters

Governments having problems with corruption and that want to raise the population's trust.

7. Cost Structure

- Workforce
- RD
- Development assets
- Maintenance

6. Revenue Streams

- Contract signature fee
- Investors
- Maintenance revenue

12 Conclusion

To summarize all the reasoning we have done above, we want to build a company whose goal is it to make the management and treatment of sensible data, such as criminal records, more secure and reliable. We are selling to governments that will provide our service to other important representative administrations as for instance police departments and penitentiaries. Our attempt is to achieve these purposes by using a state of the art infrastructure known as Blockchain.

In conclusion, we can say that the resolution we are trying to illustrate is innovative and it has a more reliable security than the systems used nowadays.

So based on that, our company could be successful, but we don't think that it will be a success that comes right away, because we have to consider that the argument of Blockchain is not that well-known and this would make it questionable to buy our product. Indubitably, we have to reckon that it's not easy to enter in this kind of market too, so it will also depend on how many competitors will start selling similar solutions and on how we will keep improving our product accordingly.

References

[1] Prison Studies - World prison population list
https://www.prisonstudies.org/sites/default/files/resources/downloads/world_prison_population_list_13th_edition.pdf

[2] Prison Studies - United States prisons stats
https://www.prisonstudies.org/country/united-states-america

[3] Italian criminal records office
https://certificaticasellario.giustizia.it

[4] CyberNews.com - UK police data leaked by cl0p ransomware group
https://cybernews.com/news/uk-police-data-leaked-by-cl0p-ransomware-group/

[5] AllCleared - CPIC: How are criminal records stored?
https://allcleared.com/blog/cpic-criminal-records-stored/

[6] Office of the Privacy Commissioner of Canada - CPIC & PIRS
https://web.archive.org/web/20090408211405/http://www.privcom.gc.ca/information/fr_010813_01_e.asp

[7] European Criminal Records Information System
https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/635554/EPRS_ATA(2019)635554_EN.pdf

[8] China Justice Observer
https://www.chinajusticeobserver.com/a/how-chinese-courts-review-electronic-evidence-stored-on-blockchain

[9] CRAB: Blockchain Based Criminal Record Management System
https://link.springer.com/chapter/10.1007/978-3-030-05345-1_25

[10] Geoffrey A. Moore. Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers. Harper Business Essentials, 1991.
https://en.wikipedia.org/wiki/Crossing_the_Chasm