VIRTUALIS INDICIUM

BY *VIRTUALIS*

OOI SHU HE | KOH ZHI YUEN | JENNY LOW CHING YEE | LAI YEE HERN

TABLE OF CONTENTS

1) INTRODUCTION

1.1) ABOUT BLOCKCHAIN TECHNOLOGY

In this era of information, technology blooms like flowers after winter, making great advancement every day. Many day to day processes, even as simplest as managing financial resource or organisation assets has become more and more complex and challenging due to the increase in demand from consumers. However, security and privacy have become more of a concern than ever in correlation with such development. As the digitalization of most of the human operation goes, such operations have become more vulnerable to cyber-attacks and exploits over time. Blockchain technology, a new database technology that could essentially change the computing paradigm of a programmer has been introduced. This technology is now commonly used to manage important data world widely due to its highly secured and good privacy nature. Bitcoin, a type of cryptocurrency, which is also a good example of the application of blockchain, has been generally accept and widely used in many European countries today. Bitcoin transaction has become so normal that its implementation can be found in Walmart. Asian counties have started to follow this trend, with more and more generalisation and implementation of blockchain application in the recent year.

Blockchain technology can be confusing at first, but no doubt it is an interesting technology to understand. Blockchain is a relatively new concept and rapidly growing industry. Similar data structures have existed long before the popular bitcoin cryptocurrency was conceived, however, principal theories of blockchain architectures used today were first outlined and defined in the original bitcoin white paper written and published by Satoshi Nakamoto in 2008. (Blockchain Technologies, 2016)

So, what is blockchain? Just like the name of this technology, blockchain is like a series of block being chained together in a distributed manner. Information transfer between block owners are done by digital signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the information. A sender can verify the signatures to verify the chain of the ownership. Diagram 1 below provides a better visual representation of blockchain concept.

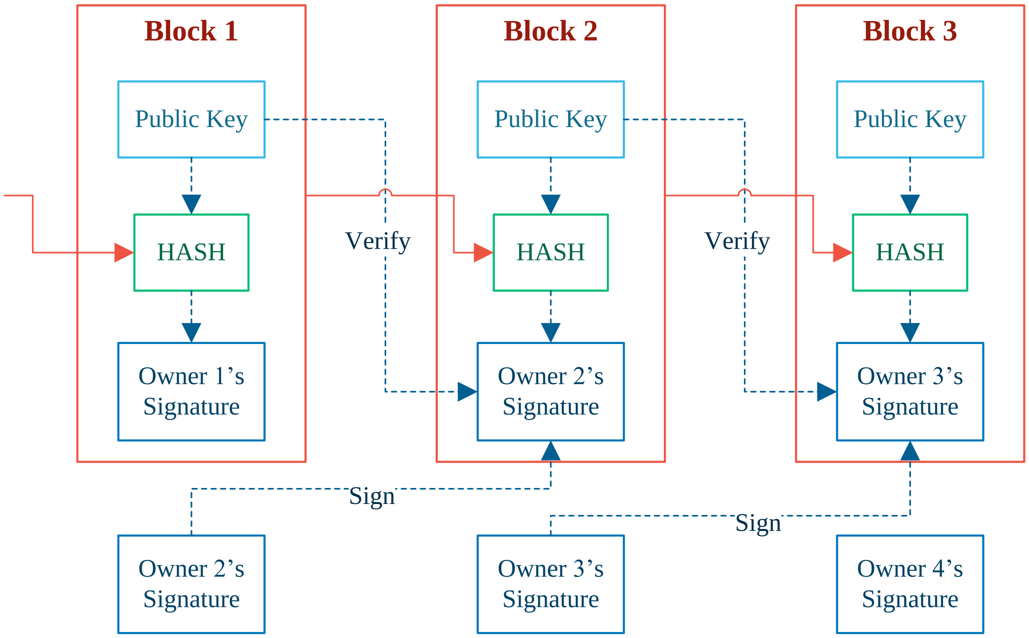


Diagram 1: Blockchain Technology (Nakamoto, 2008)

Blockchain has better privacy and it is more reliable compare to the old transaction system which trusted third parties is involved. When third parties are involved, it also open up a new possibly channel of information leakage. Blockchain has been specifically designed to overcome such matters. In blockchain technology, the transaction is solely between the sender and the receiver, plus it is further verified by computing algorithm programmatically. Diagram 2 and 3 shows the difference between how the old system and blockchain works.

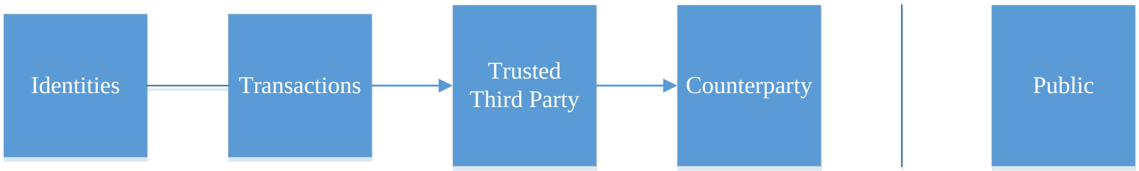


Diagram 2: Old system transaction (Nakamoto, 2008)

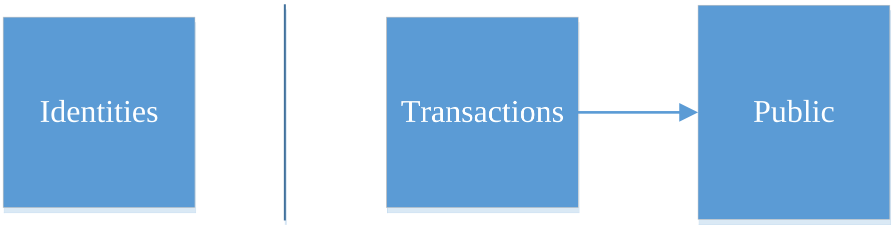


Diagram 3: Blockchain transaction (Nakamoto, 2008)

Let us say goodbye to the legacy centralised database and progress towards the age of blockchain.

1.2) AIM

1.2.1) REVOLUTION IN INFORMATION TRANSFERRING

Virtualis Indicium strives to introduce a new means of information transferring, engineering a highly-secured channel that could drastically reduce the risk of data leakage, eventually granting a higher level of information protection against cyber-attack. Besides, it also aims to safeguard crucial corporate data, particularly electronic mails and attached documents through the creation of a safer and well-secured environment for data accessing within an organisation.

1.3) PROBLEM STATEMENT

In this advanced world of technology, messages or attachments between one and another party is not restricted to mail or faxes, as it can be easily send between parties now by using electronic mail (e-mail) or any cloud-based file transferring applications such as Dropbox, Google Drive or One Drive, all three known to be the few popular applications in this age. However, even with the technologies applied in these software, the security level and convenience of these software are not met or suitable for industry level's companies to allow file sharing between staffs, managerial level staffs and high level authorities. *Virtualis Indicium* strives to revolutionise the current way of corporate data and information sharing within an organisation. The three major key points that the application tackles on are stated as below:

- Vulnerability towards cyber-attack
- Data leakage due to human error, violation or negation of IT policy and unethical behaviour of information accessing.
- The presence of third parties in information sharing and its potential threats.

1.4) OBJECTIVE

(i) To develop a new electronic mailing system with the integrated usage of blockchain API and VPN.

(ii) Allows the management within a group of users possess a better control over the internal data flow, reducing the risk of data leakage.

(iii) Enhance the protection level of corporate data by eliminating the presence of third parties (external servers) through the usage of blockchain architecture.

1.5) CASE STUDY & LITERATURE REVIEW

The team had done several case studies regarding the three problem statements stated above. Allow the following content to enlighten you. In the near years, several cases have proved that most file-sharing applications have the records or past events of company's information leakage, hacking invasion and intrusion of privacy.

This case studies are just merely an extract of the problem of the current era is facing. If you may notice, theses case studies all covers the topics of security breach, information stealing and intrusion of privacy. These have been taken into discussion and documentation as it shows the extended and dangerous impact of data leakage. It shows that a highly-secured government email account ranging to a personal private email server can be hacked and data can be steal or retrieve from it. It also shows that most internet based file-sharing applications such as Dropbox, it is not reliable for data transferring and distribution as it has a risk of getting user's important information into the hands of unauthorized entities.

1.5.1) CYBER-ATTACK

Cyber-attack, which also known as Computer Network Attack (CNA) is an attack which carried out by a hacker which socially and politically through the internet to damage or destroy a computer network or a system. Most of the time, cyber-attacks use malicious code to modify the computer logic and data. The result of this attacks can cause critical damage to the user which is information and identity theft. Some of the examples of cyber-attack are identity theft, fraud, malware, phishing, spamming, spoofing and many others.

Most of the victim that being targeted by the cyber-attack are individual organisation and individuals to obtain technical and sensitive information, which is also for vandalism or monetary gain purpose.

There are some methods used in typical cyber attack

- Espionage: First, the hacker creates the malware
- Intrusion: the hacker send the malware to the target and initial infection of target
- Evolution / Internal spread: Once the user receives the malware, it will seizure of system administrator authority
- Attack: Once it successfully seizure all the system administrator authority, it will start to access to important document storage servers

The team had done a comprehensive review on several notable examples of cyber-attack that listed as below:

Elimination of traces of activity: After all those steps are done, the users had to suffer serious information leakage. The following are examples of cyber-attack happens all over the world.

i) RedHack's vs. Turkey Case Study

For example, the case of the hacktivist group Redhack leaking a set of emails allegedly belonging to Minister of Energy and Natural Resources Berat Albayrak, son-in-law of President Recep Tayyip Erdogan in Turkey. This provokes Turkey to block off access to cloud storage services including Dropbox, Microsoft's OneDrive, and code hosting service GitHub. (How hacktivist group RedHack gamed Turkey's censorship regime, 2016)

ii) *The Podesta Emails*

On 7th of October 2016, WikiLeaks began leaking the personal emails of Clinton campaign chairman John Podesta. Cybersecurity experts report that Fancy Bear, a group of Russian-linked hackers, had indeed infiltrated Podesta's Gmail account. However, the biggest impact of the Podesta Emails' leaks is towards Hilary Clinton, one of the candidates for the U.S.A Presidential Election 2016. It generates a string of troublesome stories for the Democratic nominee. (The Podesta Emails, 2016)

Besides the Podesta emails, WikiLeaks also exposed emails and files such as Yemen Files, TISA and Hillary Clinton Email Archive which will be further elaborated below.

iii) *Hillary Clinton Email Archive #1*

On March 16, 2016, WikiLeaks launched a searchable archive for over 30 thousand emails and email attachments sent and received from Hillary Clinton's "home brew" email server while she was Secretary of State. She was relying on the server for all her electronic correspondences, both work-related and personal which was soon leaked to the public. (Hillary Clinton emails - what's it all about?, 2016) (Hillary Clinton Email Archive, 2016)

From the case studies above, most of the problems are originated from or based on e-mails. However, there are also cases involving popular file-transfer applications such as Dropbox.

iv) *Hillary Clinton Email Archive #2*

According to (Dropbox data breach: 68 million user account details leaked, 2016), four years after a data breach at cloud storage service Dropbox, details of more than 68 million user accounts have reportedly been leaked. However, in a selection of files obtained through sources in the database trading community and breach notification service Leakbase, Motherboard found around 5GB of files containing details on 68,680,741 accounts, which includes email addresses and hashed (and salted) passwords for Dropbox users. Security researcher Troy Hunter also verified the data dump.

v) Australian Red Cross Blood Service Security Breach

A backup file containing information including names, addresses and emails on 550,000 blood donors was leaked as a result of human error, according to Australian Red Cross Blood Service chief executive, Shelly Park.

The backstory of the massive security breach happened because a file containing donor information which is located on a development website was left unsecured by a contracted third party whom developed and maintain their website. (550,000 Red Cross blood donor records leaked due to "human error", 2016)

vi) Sailor details

According to ITPRO, on 23rd of November in 2016, details of more than 130 thousand current and former sailors have reportedly been leaked by a laptop used by an HP Enterprise Services employee. The leaked information includes names and sensitive information like social security numbers. (Hackers steal 130,000 sailors' details in US Navy breach, 2016)

vii) Sony

On November 25, 2014, a month before Christmas, a group of hacker calling themselves the Guardian of Peace which also known as GOP leave the Sony network crippled for a few days by hacking their way into Sony Picture. The GOP posted the valuable insider information including their unreleased films to the internet. The leaked also included approximately 4000 past and present employees' personal information to the internet and revealed curious practices at Sony. (A Breakdown and Analysis of the December, 2014 Sony Hack, 2014)

viii) BeautifulPeople.com

According to ITPRO, less than a year after the Ashley Madison debacle, the data from BeautifulPeople.com has been leaked on the internet. The leaked information included sensitive personal information of the user as well as private message. Furthermore, some sensitive information like body type, mobile phone number are being sold online. Some of the information which already been encrypted were also been stolen. (BeautifulPeople.com hacked and personal details leaked, 2016)

ix) Japan Travel Agencies

According to Japan's major travel agency which also known as JTB, a total of 793 million users' data had been leaked to the hackers. The leaked information included names, address, email address and passport numbers. (Japan's largest travel agency fears data leak impacts 8 million users, 2016)

x) Friend Finder Network

As many years past, Friend Finder Network was hack for a second time. The hacker leaked the information of 339 millions accounts from the website and include over 15 millions "deleted" accounts that haven't purged from the databases. (These were the biggest hacks, leaks and data breaches of 2016, 2016)

1.5.2) DATA LEAKAGE

1.5.2.1) Common causes of Data Leakage

To further understand the topic and challenge of increasingly distributed and mobile businesses face in protecting sensitive information, the team has did a research and gather results from surveys conducted by Cisco. Conducted in 10 countries selected based on their differences in social and business cultures, they discovered that despite the differences, employees around the world are engaging in risky behaviors that put corporate and personal data at risk.

Employee behaviors related to the topic are:

i) Unauthorized application use

When a staff is accessing unauthorized applications such as personal email, instant messaging or online backing on business networks, they can place sensitive corporate data and employee's personal information at risk as these applications are often unmonitored and do not use corporate security standards.

ii) Unauthorized network access

Although there is IT security policies that employees had to follow when they are using corporate computers, employees often bypassed IT settings to download music, shop online or visit unauthorized websites. When a staff is accessing unauthorized network access, the staffs increases the chance of placing confidential details of the company online. Websites that are either compromised or deliberately malicious, present the risk of a user's computer being infected with malware such as a keylogger with introduce the risk of data theft.

iii) Misuse of login system

The login system is known as one of the oldest and simplest means of computer security. However, this simple yet robust functionality has been abused and misused by users. Based on statistic, at least one in three employees said they leave their computers logged on and unlocked when they are away from their desk. This is does not just provide a way for potential intrusion, but invites the attacker inside.

According to another group of statistics:

• 28 percent of employees in China store login and password information for personal financial accounts on their work devices.

• 18 percent of employees share passwords with co-workers, and that rate jumps to 25 percent in China, India, and Italy.

• 10 percent of employees in India, the United Kingdom, and Italy keep written notes of login information and passwords on their desk at work, leaving sensitive data accessible if the machine is stolen even if the computer is logged off.

• 5 percent of employees in the United Kingdom and France leave passwords to personal and financial accounts printed on their desks at work, so their information can be stolen with any other computer even if their work computer is safeguarded. (CISCO, 2014)

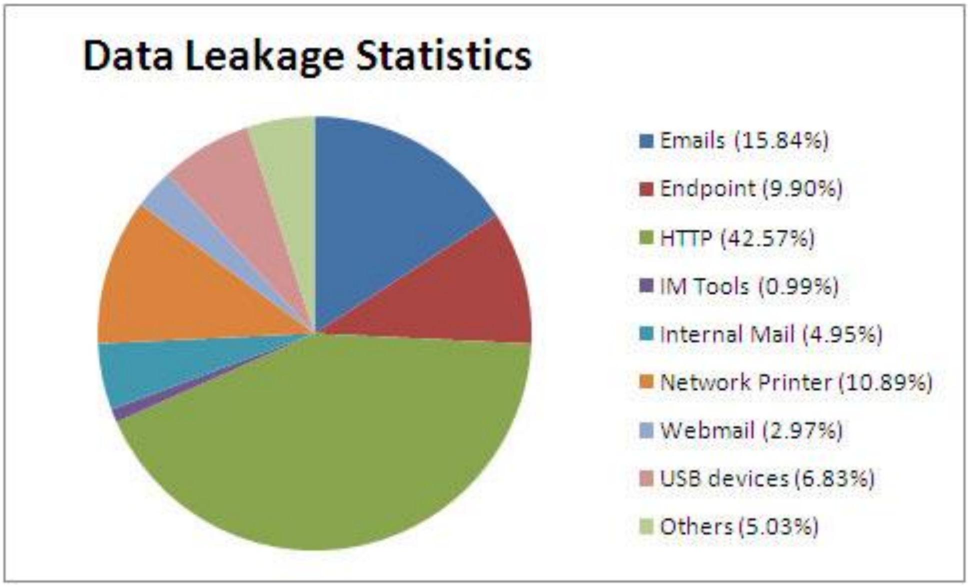
This does not just invite the intruder to control the applications in the invaded computer but also increase the potential of information leaked.

1.5.2.2) Data Leakage Statistics

In order to implement the correct protective measures, investigation has been done on this research paper which explains the type of data leaked based on publicly disclosed Data Leakage:

- Confidential Information – 15%
- Intellectual Property – 4%
- Customer Data – 73%
- Health Records – 8%

When it comes to file transferring, there are many ways to do it and it had all been proven to be a victim of data leakage shown in Graph 1.



Graph 1: Data Leakage Statistics (SurveilStar Employee Monitor, 2008)

Transferring data through HTTP is widely known to the public as insecure as malware and phishing applications may be hidden and prompt users to enter their respective details. Next, email, internet mail and webmail are proven to be easily hacked and leaked by the case studies above. Even with a physical file transferring medium such as a USB drive or pen drive, data leakage is not avoidable as well.

1.5.2.3) Impact/Consequences of Data Leakage

i) Legal Liability

Individuals and corporations that are the victims of an organisation data theft may sue the respective organisation for damages. Inclusive of the legal costs, if the court rules in favour in the prosecution, the business will be accountable for the damages done. This has a high potential to put the company out of business. For example, ChoicePoint Inc had over 160,000 consumer records compromised. It has been estimated that over 800 cases of identity theft resulted from this loss.

ii) Disturbance of Company's Productivity

Following the leakage or complete loss of sensitive data, the company will take up time and money to re-gather and store the respective data deleted or stolen into the system or database again. In addition, if an intellectual property is stolen, time will be needed to go into redesign/redevelopment of the respective property. What this brings is disruptive elements to the company as the original routine, plan, or schedule of the company has been altered to suit the replacement of the information lost.

iii) Business Reputation

As you may have noticed, when a company encounters the problem of a data leakage, news of it will be published online and in various magazines and papers. This damage of business reputation is difficult to measure. However, effects such as decline in sales, rejection of usage of products, legal issues and lowered of organisation's image should be expected. (Gordon, 2007)

This shows the one of the problems that the team has clearly identified and wish to solve with the usage of *Virtualis Indicium.*

1.6) PRESENCE OF THIRD-PARTY APPLICATIONS

With the application of *Virtualis Indicium*, the presence of a third-party applications between files transactions will be eliminated. Based on the elaborations made above, we may conclude that using an e-mail/file transferring application creates problems such as leakage of company's information, intrusion of hackers and email's conversation's privacy issue.

With the usage of a third-party application as a middleman between file transfers, these third-party applications may collect, use and distribute the customer's information without their knowledge.

According to this article from (Yahoo Tech, 2015), scammers are using Google Drive as the perfect tools to abuse the trust of customers in Google to steal their personal information. Scammers used emails designed to fool users into visiting a counterfeit website hosted on Google's own servers. A hidden script on the Google Drive page will then captured their information, then redirecting the users to a genuine document to avoid suspicion. In summary, this is another problem created with the usage of a third-party application between files transfers.

The team believes that with the presence of a third-party application between files transactions, the risk of information being stored in a centralized place and stolen will be heightened. Below are the examples of case happens around the world.

2) FUNCTIONALITY OF APPLICATION

Virtualis Indicium (VI) aims to revolutionise the means of information sharing and transferring. In order to do so, the applications will create a channel for such purpose with the integration of blockchain concept and Virtual Private Network (VPN). The information transferring channel is identical to electronic mailing service in its modal. Documents such as images, pdf files could be attached to the mail like common email. However, the usage of blockchain concept and VPN distinguishes with from ordinary email and further enhance its security and privacy.

2.1) BLOCKCHAIN: DECENTRALISED CONSENSUS, SMART CONTRACTS, TRUSTED COMPUTING

One of the concerns of using public or external email servers are the presence of third parties. Such presence could potentially increase the system vulnerability against cyber-attack and various CNAs. Moreover, human errors or unethical behaviours of information handling from the employees of third party companies could possibly lead to mass corporate data and classified files leakage. Shall any of this situation happens, it can severely damage the financial interest, credibility and reputation of an organisation.

However, this issue could be resolved with the usage of blockchain concept. How? One of the essential elements behind the blockchain concept are smart contracts and smart property. The basic idea behind this element is that a transaction's contractual governance between two or more parties can be verified programmatically via the blockchain, instead of via a central arbitrator, rule maker or gatekeeper. If two parties can agree between themselves, there is no need to depend on a central authority (Mougayar, 2015). This key element allows the elimination of third parties in information transferring. Information that internally transferred within an organisation should always remain within it. Relying on third parties mail servers to store such internal information is just like storing valuable belongings in a public warehouse, where it is being safeguard by someone else who is unsure about its importance and could potentially exploit it. The third parties would never know the consequences of leaking such piece of valuable information, especially in this era of Information. To name an example, Podesta case which the information leaked from Gmail server.

By eliminating such situation, an organisation can possess a better control over their internal data flow. With many communication channel booming over the year, email however remains as the de facto way of sending official documents in many organisation, companies, or even government agencies and political parties. Official documents are often finalised and contains valuable data such as strategic decision, marking and business plan or classified data that could essentially harm the interest of the organisation shall any leakage happens. An email that contains important data should directly goes from the sender to its recipient without going through an external party. Through the concept of blockchain, the validity of such data transaction will be verified by all member devices among the network. However, the contents of it is only known and accessible by the two direct peers (and also the administrative layer, which will be covered later on). Such implementation could prevent information hijacking by a business competitors by any means.

2.2) VIRTUAL PRIVATE NETWORK (VPN): PRIVATE BLOCKCHAIN & ADMINISTRATION

With the benefits of blockchain stated above, *Virtualis Indicium* will bring in VPN to its arsenal, further expanding its' potential. This concept took inspiration from an identical product available today - VPNCoin. The concept of *Virtualis Indicium* allows a database to be shared without the presence of a third party central authority. To note an example, if several staffs in different department wants to maintain a joint information sharing medium for convenience and benefits, what will be needed is:

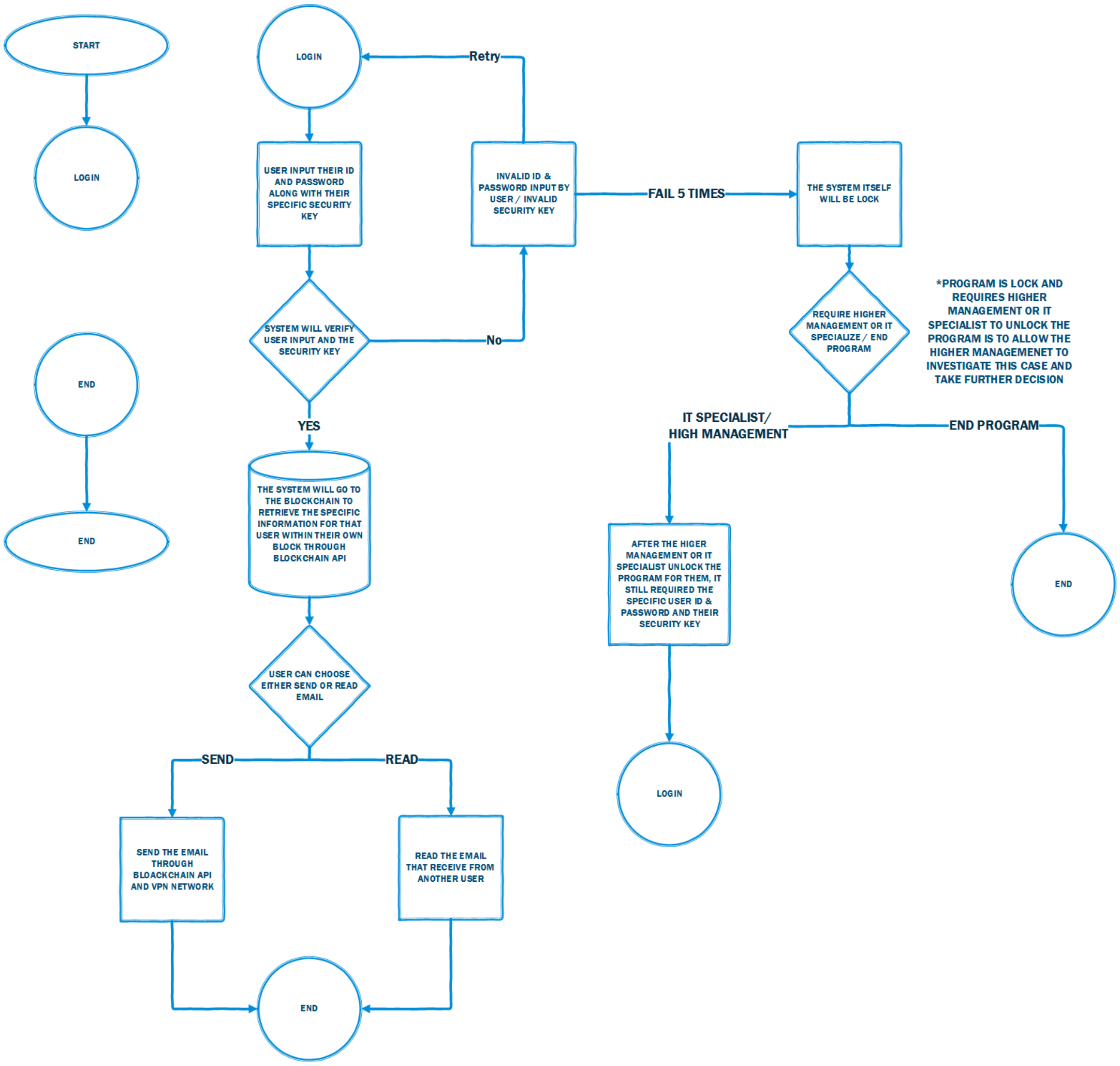
- A peer-to-peer network that allows data transactions to be created by any party and propagated quickly to all connected nodes.
- A way to identify conflicts between transactions and resolve them automatically.
- A synchronisation technology that ensures all peers converge on an identical copy of the database.
- A method for tagging different pieces of information as belonging to different participants, and enforcing this form of data ownership without a central authority.
- A paradigm for expressing restrictions on which operations are permitted, e.g. to prevent one company from inflating the directory with fictitious entries.

As you may see, this list cannot be simply supported by today's off-the-shelf databases. Current peer-to-peer replication technology is clumsy and has a complex approach to conflict resolution. Those databases that do support row-based security still require a central authority to enforce it. Furthermore, standard database-level restrictions like unique keys and check constraints cannot protect a database against malicious modifications. It just so happens that blockchain supports and provides them.

Additionally, by integrating blockchain into VPN, *VI* also add an extra flavour to the application – Administration. Since *VI* is targeting group of users, there will always be a "administrative layer" within the group. They could be the leader, the management etc. This administrative layer plays the role of monitoring, supervisory, and administration. Even though *VI* strives to eliminate the presence of third party central authority, the existence of internal central authority is compulsory and they should be granted a certain degree of control over their group and the information transfer. The "owner" of this VPN has control over devices within the VPN domain. They can adjust the accessibility of each devices based on real life position of the device owners, monitoring information shared and transferred within the network and take further decision shall any unexpected issues arise. Moreover, VPN also enabled a higher level of protection on this network. Integration of blockchain and VPN also opens many potential features that could be introduced in the future.

2.3) SYSTEM DESIGN

2.3.1) FLOWCHART


START
LOGIN
END
END
LOGIN
USER INPUT THEIR ID AND PASSWORD ALONG WITH THEIR SPECIFIC SECURITY KEY
SYSTEM WILL VERIFY USER INPUT AND THE SECURITY KEY
No
INVALID ID & PASSWORD INPUT BY USER / INVALID SECURITY KEY
Retry
YES
THE SYSTEM WILL GO TO THE BLOCKCHAIN TO RETRIEVE THE SPECIFIC INFORMATION FOR THAT USER WITHIN THEIR OWN BLOCK THROUGH BLOCKCHAIN API
USER CAN CHOOSE EITHER SEND OR READ EMAIL
SEND
READ
SEND THE EMAIL THROUGH BLOACKCHAIN API AND VPN NETWORK
READ THE EMAIL THAT RECEIVE FROM ANOTHER USER
END
FAIL 5 TIMES
THE SYSTEM ITSELF WILL BE LOCK
REQUIRE HIGHER MANAGEMENT OR IT SPECIALIZE / END PROGRAM
*PROGRAM IS LOCK AND REQUIRES HIGHER MANAGEMENT OR IT SPECIALIST TO UNLOCK THE PROGRAM IS TO ALLOW THE HIGHER MANAGEMENET TO INVESTIGATE THIS CASE AND TAKE FURTHER DECISION
IT SPECIALIST/ HIGH MANAGEMENT
END PROGRAM
AFTER THE HIGER MANAGEMENT OR IT SPECIALIST UNLOCK THE PROGRAM FOR THEM, IT STILL REQUIRED THE SPECIFIC USER ID & PASSWORD AND THEIR SECURITY KEY
LOGIN
END

3) TECHNICAL DESCRIPTION

3.1) SOFTWARE REQUIREMENT

i. Netbeans IDE (Java)

ii. Blockchain API

iii. Packet Tracer (Cisco NetAcad)

3.2) HARDWARE REQUIREMENT

i. Functional Computer

ii. Server machine (alternatively online server hosting service, virtual machine server)

4) USERS' BACKGROUND

4.1) TARGET USERS

Virtualis Indicium target group of users who required a platform for information sharing such as colleagues within a same department or company, students in a same class groups, intakes or even faculty, as well as departments in government sectors. The information will be shared among the group members in a form of email. Documents such as images and pdf files can be attached to the mail and send to the recipient by the senders.

The following are some examples of the group of users that *Virtualis Indicium* can greatly benefits:

i) Companies, office groups and organisation

In small offices or organisations, the transaction of data between managers and staff should remain in the company at all time. The corporate data of a company is private yet undisputedly important to the company. Business competitors could make analytical review on hijacked corporate data and formulate new plan that could deal financial harm in response.

Furthermore, the business and marketing plans of a company is a secret that shall remain only among the direct associated decision maker to prevent leakage of information to infiltrators and spies from competing company. If the plans is not secured, the company may face failure in their upcoming products or business modules.

Strategies planning for a company to run their business is extremely essential. However, this information is vulnerable without a secured channel of information sharing and transferring. Rival companies that obtained such information could exploit it or even use it as their own. This happens frequently between the competition of business among companies.

ii) University

In universities, crucial details such as exam questions, results or even docket numbers always being transfer between lecturers and university administration. The students often should not know such information before the official publish of their results. However, university information sharing channel is often fragile and ended up being a "test field" for students, especially in IT-specialised university. They will attempt to disrupt and exploit the system, eventually obtaining this information that they are not support to know. Thus, by using *Virtualis Indicium* among the lecturer group, the information will be better secured.

Besides, checking and submission of assignment can be done through this platform between lecturers and students. The content of the assignment is protected if the files are transferred in through *Virtualis Indicium*. The idea will be remains only between the two parties of the file transfer, which is the lecturer ant student. Thus, reducing the likeliness of idea hijacking and plagiarism.

iii) Government

Highly classified files that relates to national security and political information is the top secret in any nation's government. The information should not be known by outsiders through any means of security measurements. However, many countries still put their national secrets and classified data at risk by relying on third party servers and systems. *Virtualis Indicium* strives to eliminate this needs to increase the security level of such information.

Moreover, information sharing and electronic mailing within government agencies are significantly more important compare to universities and companies. The information flow in-between each department, especially in military and political sectors should always be classified and no leakage shall be allowed. A simple data breach in the national information system could lead to severe outcomes that could even harm the national security and the well-being of its citizens.

4.2) BENEFIT TO USERS

i) A channel of electronic mailing through a highly-secured and well-designed applications. Able to communicate crucial information within a group without concerns.

ii) Peer-to-Peer and Virtual Private Network architecture as security measurement to further safeguard the information flow and prevent data leakage. Eliminating the risk and threats that relying on third party servers could bring.

iii) A more effective and efficient way of information sharing through a specifically designed application.

iv) Administrative layer within a group can have better view and control over the internal data and information flow.

v) Privacy of the group and its members are secured through the usage of VPN and blockchain.

5) FUTURE & POTENTIAL DEVELOPMENTS

5.1) GLOBAL SCALE: ERA OF V-MAIL

Currently *Virtualis Indicium* is focusing on the information transferring and sharing within an organisation or group. In the future, *VI* will be expanded to a larger scale which can cover a bigger company with complex organisational structures, or even to the extent of cross-organisational information trading. *VI* has the potential to be developed into global scale. By then, VI will completely remove the means of central authority, both externally and internally, creating a peer-to-peer means of information transferring. It can eventually replace the conventional way of electronic mailing, generalising the benefits of blockchain and VPN to everyone in this particular day to day operation. Creating a new era of "V-Mail".

5.2) DISTRIBUTION MODE

Currently, the mail that is send through *Virtualis Indicium* will only remains within the application and user's specific block to prevent data leakage through unethical way of information sharing among group members or incompliances of IT policy. However, a "distribution mode" setting has been scheduled for *Virtualis Indicium* in the future. This setting allows the sender to select whether this mail is distributable or non-distributable. In another words, whether that particular mail can be download or forward to the other users. On top of that, *VI* also intends to include printer devices and printing selection into this setting. This features can greatly enhance the user-friendliness of the application, increasing the productivity of the *VI* users.

5.3) SECURITY LEVEL CLEARANCE IN LOGIN

Level of security clearance is another scheduled additional feature that will be introduced to *Virtualis Indicium*. In order to further reduce the risk of data leakage through unethical behaviour of information accessing, or violation of IT policy by a group member, the team has decided to design a level-based login system and implement it in stage. The application requires two credentials to login, the MAC address of the device and a unique key generated based on MAC address during program setup. By doing this, the information within each application (or block, under the blockchain concept) can only accessed exclusively by the owner of the device. Thus, in order for a culprit to hijack or exploit the information, apart from obtaining the unique key, they need to physically access the exact same device of the victim, which is very unlikely to happen. In addition, MAC address has been selected as credentials as usually there are no way to spoof a MAC address, which make its more secured compare to IP address. These level of security can be applied on middle level group members or employees as sometime they played parts in high level decision-making and might receive important corporate data from their superior. For higher level employees who required a more extensive security measurements, another real-time generated codes are required on top of the two existing credentials. Whenever the high level staffs wish to login to their application, they are required to obtain another code generated by an extension of *VI* which only valid for three to seven minutes. Shall hardware integration allows, biometric authentication device can also be included into the system, achieving a even higher level of security measurement. Such security level clearance-based login system could ultimately increase the system resistance against privacy invasive or unethical behaviour of colleagues or other members.

6) CONCLUSION

To put it in a conclusion, the current method of information sharing and transferring possess many potential threats and risk that often left unnoticed or neglected. After going through an in-depth case studies and researches over cyber-attack and data breaching, Team *Virtualis* intends to resolve such issues with the introduction of *Virtualis Indicium*, an information transferring application which will initially focus on electronic mailing with attached documents feature. *Virtualis Indicium* eliminate the presence of third party in information sharing, creating a peer-to-peer means of information transferring. VI will begin its long crusade against cyber-attack, data breaching and leakage through the integration of blockchain concept and VPN technology, creating a well-secured channel of electronic mailing and information transferring. With this, *Virtualis Indicium* and Team *Virtualis* wish to revolutionise the conventional way of information sharing and transferring, safeguarding the interest and generalising the benefits of such technology breakthrough to everyone. *Virtualis Indicium*, the virtualisation of information, a new era of information sharing.

REFERENCE

550,000 Red Cross blood donor records leaked due to "human error" (2016) IT PRO.

A Breakdown and Analysis of the December, 2014 Sony Hack (2014) Risk Based Security.

BeautifulPeople.com hacked and personal details leaked (2016) IT PRO.

Blockchain Technologies, 2016. *Blockchain Technology Explained.* [Online]
Available at: http://www.blockchaintechnologies.com/blockchain-definition
[Accessed 1 November 2016].

CISCO, 2014. *Data Leakage Worldwide: Common Risks and Mistakes Employees Make.* [Online]
Available at: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html
[Accessed 27 October 2016].

Dropbox data breach: 68 million user account details leaked (2016) James Rogers.

Emerging Tech, 2015. *Understanding the blockchain.* [Online]
Available at: https://www.oreilly.com/ideas/understanding-the-blockchain
[Accessed 27 October 2016].

Gordon, P., 2007. *Data Leakage – Threats and Mitigation,* s.l.: SANS Institute .

Hackers steal 130,000 sailors' details in US Navy breach (2016) IT PRO.

Hillary Clinton Email Archive (2016) WikiLeaks.

Hillary Clinton emails - what's it all about? (2016) Anthony Zurcher.

How hacktivist group RedHack gamed Turkey's censorship regime (2016) Efe Kerem Sozeri.

Huge Cyber-attack Takes Nearly One Million Germans Offline (2016) Jack Loughran.

Investopedia, n.d. *Blockchain.* [Online]
Available at: http://www.investopedia.com/terms/b/blockchain.asp
[Accessed 26 October 2016].

Japan's largest travel agency fears data leak impacts 8 million users (2016) Charlie Osborne.

Mole, B., 2016. *From Bitcoin to puke-tracking: Walmart uses blockchains to monitor food,* Washington: Beth Mole.

Mougayar, W., 2015. *Understanding the Blockchain.* [Online]
Available at: https://www.oreilly.com/ideas/understanding-the-blockchain
[Accessed 2 November 2016].

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* [Online]
Available at: https://bitcoin.org/bitcoin.pdf
[Accessed 5 November 2016].

SurveilStar Employee Monitor, 2008. *Prevent Data Leakage and Protect Your Business Data.* [Online]
Available at: http://www.surveilstar.com/prevent-data-leakage.html
[Accessed 28 October 2016].

Technopedia, n.d. *Cyber Attack.* [Online]
Available at: https://www.techopedia.com/definition/24748/cyberattack
[Accessed 1 November 2016].

The Podesta Emails (2016) WikiLeaks.

These were the biggest hacks, leaks and data breaches of 2016 (2016) Zack Whittaker.

Yahoo Tech, 2015. *Scammers Are Using Google Drive to Steal Your Logins – Here's How to Stay Safe.* [Online]
Available at: https://www.yahoo.com/tech/scammers-are-using-google-drive-to-steal-your-125186285634.html
[Accessed 28 October 2016].