Title: Blockchain technology: edit or not?

MSc Research Project
Programme Name: Financial Technology

Tatyana Gricenko

Student ID: X19233027

School of Computing
National College of Ireland

Supervisor : Noel Cosgrave

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Tatyana Gricenko		
Student ID:	X19233027		
Programme:	Financial Technology	**Year:**	2020
Module:	MSc Research Project		
Lecturer:	Noel Cosgrave		
Submission Due Date:	28/09/2020		
Project Title:	Blockchain Technology: edit or not?		
Word Count: 5944	**Page Count: 16**		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: 28/09/2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	v
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	v
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	v

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	

Table of Contents

Abstract

Experts agree that blockchain will help businesses to unlock value and has a potential to disrupt the financial services and other industries. However, it’s just a few companies are ready to transfer their whole database on the blockchain ecosystem. Blockchain technology is also a popular topic to discuss in legislators’ circles. Unfortunately, the interested parties noted that there is not enough governance around the new technological solutions. Blockchain is one of the technologies that requires new governance and legal framework to be compliant with law in the new digital world. At the moment it is not very clear what is required from all the stakeholders to be compliant with the regulatory requirements. Immutable blockchain is append-only system. The techniques to allow deletion or modification of the blockchain while at the same time keep it secure and resilient to attacks and fraud will be very helpful to the users. The inventors of redactable blockchain believe that the “undo function” is needed help in the special circumstances. Since the conflict revolving around the irreversibility of blockchains, it may significantly affect their adoption to vast application areas. Resolving this issue will be benefit all interested parties. This work aims at analysing the capability of the blockchain to be edited. It was identified from the research findings that editing blockchain can only be allowed special situations when all required evidence is provided, and institutions in the financial sector and manufacturing would prefer this type of blockchain.

1 Introduction

Blockchain is the type of decentralised Distributed Ledger Technology. Blockchain can be private or public. Similar to intranet and internet in 1990, permission is needed to join the network for private blockchain, no permission needed to join public blockchain. In public blockchains users do not know each other personally and are the equal owners of the blockchain. Public blockchains are decentralized, there is no senior administrator in this system.

All blockchains are the chains that contain the blocks, linked to each other and depend on the previous one. In this system all the records are kept safely in the chain chronologically. Special protocol (algorithm) controls the work of the system (Figure 1).

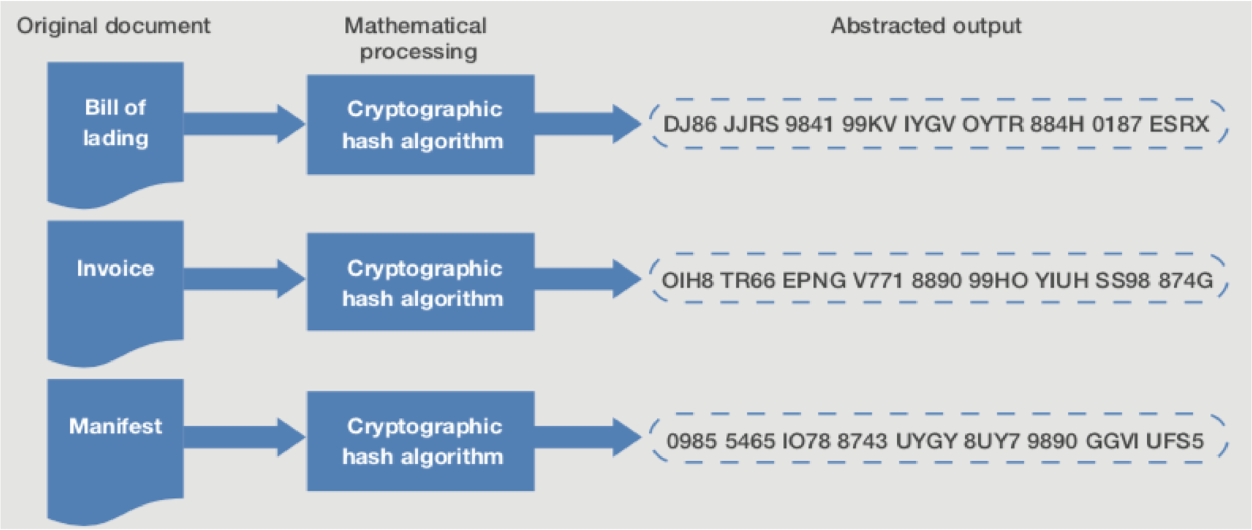
Original document
Mathematical processing
Abstracted output
Bill of lading
Cryptographic hash algorithm
DJ86 JJRS 9841 99KV IYGV OYTR 884H 0187 ESRX
Invoice
Cryptographic hash algorithm
OIH8 TR66 EPNG V771 8890 99HO YIUH SS98 874G
Manifest
Cryptographic hash algorithm
0985 5465 IO78 8743 UYGY 8UY7 9890 GGVI UFS5

Figure 1: Cryptographic hash algorithm (World Economic Forum, 2019)

Every participant can have a copy of a ledger, question and inspect the protocol. Confidentiality of the data is guaranteed by distribution and cryptographic algorithm. The entered text of any size generates immutable output so-called hash of fixed length (Hewett et al., 2019).

As it was mentioned earlier, blockchain is decentralised system. But there are many examples of the centralized institutions. A stock exchange or courts enables relations based on trust among participants unknown to each other, but they should acknowledge their power. Can decentralized network be trustworthy the same way? The blockchains systems can be successfully managed, like in the case of Ethereum Foundation in 2016, directed support and “hard fork” saved the funds of Decentralized Autonomous Organization (DAO) participants (Bhargavan et al., 2016).

In special circumstances, privileged nodes could be appointed to decide to rewrite the history and if transactions can be changed afterwards. “Hard fork” is a protocol modification that turns formerly unacceptable transactions and blocks into acceptable. The process was not simple, before the “hard fork” decision was made, a few options were offered and carefully discussed, every node in the network had a chance to express their opinion (Button, 2019).

Soon after Nakamoto’s whitepaper was out, Bitcoin was accessible for public at the open source in 2009. Blockchain offered the solution to digital trust by keeping vital data in the public domain without the permit to edit it. After the financial crisis in 2008, the trust of consumers in banking was gone, Bitcoin's idea of decentralized financial transactions looked very attractive (Aitsam et al., 2020). Blockchain creators wanted all participants to be able safely exchange resources online without the intermediaries. However, while blockchain indications of a technology is frequently linked to Bitcoin among other cryptocurrencies, there are other expansion of blockchain applications.

In this paper, the introduction offered a summary of the topic of blockchain technology. The literature review, justification of study and the demonstration of the research questions are in the next chapter. The explanation of the methodology and limitations of the research, analysis and findings from the research and literature review are combined in the next chapter. Finally, suggestions for further research are in the final chapter of this paper.

2 Literature Review

2.1 Irreversibility of the blockchain and the illegal content

Matzutt et al. (2018) expressed the concerns about the illegal content in the blockchain. Random content can be secretly and permanently added, shared to the blockchain nodes, the participants can be held liable for the ownership of the content. The illegal content could be on the Bitcoin blockchains, acquired with financial transactions, even this is not the initial purpose of this type of blockchains.

Some blockchains, like SeemIt are set up to distribute content. The participants of Bitcoin blockchain can become victims of the illegal content without their knowledge. It is impossible to give a notice to take down unwanted content to the administrators. Due to the irreversibility of blockchain the content cannot be removed or deleted by the mediators (Schellekens, 2019).

2.2 Irreversibility of the blockchain and the “Right to erase”

The “right to be forgotten” entails permanent deletion of private data on requesting and from the points they have been distributed. The impact of including the “right to be forgotten” on modern businesses is enormous, while its incorporation into the forthcoming technological developments design is presently arguable (Politou et al., 2018).

Even though some researchers would argue that anonymizing private data that inhabits within blockchains, supposed to be encrypted with public and private keys and the hashed data is pseudonymous rather than anonymous. The compliance of the blockchain with the General Data Protection Regulation solely via the utilization of public-key cryptography and hash values cannot be assured (Schwerin, 2018).

Eberhardt et al. (2017) suggested that the personal data could be stored off-chain. This method regulates blockchain system architecture, help scalability issues, reduce data storage. However, the researchers have been critiqued by Dorri et al. (2019) for reducing the security of blockchains by introducing additional attack vectors by removing hash indicators and turning anonymous hash data into pseudonymous. At the same time, these techniques are introducing additional delays and complexities.

2.3 Technological solutions to modify blockchain

Luu et al. (2016) have been experimented with the irreversibility of smart contracts. The blockchain transaction is different to distributed applications, which can be at the time of bugs detection, smart contacts staying in the blockchain are immutable and irreversible. Precisely, the moment the code of contactors is moved to the network of the blockchain, it is impossible to patch bugs or change their functionalities. Also, smart contracts cannot be deleted from the blockchain at the time their utilization is ending. Instead, they are a portion of the blockchain past record and possibly preserved by several nodes. Indeed, similar while creators have advanced thoughts about the way of disabling manually, by putting in ad-hoc code automatically or in the contracts, by calling self-destructive functions (Bartoletti et al., 2017).

The immutability of smart contracts makes reference just to their real code rather than to their condition that is majorly set from their functions and variables, within the Ethereum network, as the state of variables within contracts is stored eternally. Additionally, the functions within the "code of contracts" are irreversible the moment they are positioned in the blockchain. Notably, decentralized applications exploit such immutability to keep data consistently, and some time to confirm ownership and provenance, such as writing a document's hash on the blockchain so they can check the integrity and existence of the document (Bhargavan et al., 2016).

Nevertheless, due to their smart contracts' immutable nature, there has been the identification of their correctness as being a crucial factor for their safe and suitable behaviour. Moreover, contrary to their analogue matching parts, the immutability of smart contracts does not permit traditional contract law tools for alteration and termination, to become successfully applicable to the smart contracts (Derler et al., 2019).

Some researchers support having fresh standards set to undo and alter smart contracts to make sure that the usual tools attain their initial objectives when they are applicable to the blockchain technology. A cryptocurrency system referred to as "mini-blockchain" has been presented by Matzutt et al. (2020) as a pruning choice to blockchain applications. Here significantly reduced synchronisation time and saved 255 GiB of storage was achieved. This method suits, when there is no necessity for a complete blockchain by disconnecting transactions, and hence, it enables transactions to be cast-off after a secure time length has passed. Even though blockchain pruning satisfies privacy and scalability requirements, it has been claimed that it does so at the security's expense since even when there is the maintenance of the old block headers, shortening the history of blockchains yields to reduced security (Finck, 2018). Moreover, pruning has as well been critiqued for its less stable enforceability since there is no assurance that nodes will elect to keep the complete chain. Nevertheless, it has been predicted that pruning might suit private blockchain context in which the working situation is more effortlessly adjusted and controlled (Palm, 2017). The idea of pruning in private chains is logical, but the application cannot be used in notary services or smart contracts (Aitsam et al., 2020).

Krawczyk and Rabin (2000) offered the initial technical suggestion, that challenged the immutability of the blockchain by introducing chameleon hash, a fundamental cryptographic function, which enables approvals. Morever, Ateniese et al. (2017) partnered with Accenture global consulting company to improved the method. They presented the technique, where chameleon hash collision has to be maintained private as the trapdoor can be taken from one collision, was proposed a better design to any collision number. Using the trap key knowledge, it is possible to obtain collisions efficiently, and hence, substitute the block’s content. Thus, knowing the key, any blockchain’s redaction is possible, encompassing modification, insertion, and deletion of any block. The suggested system also leaves “mark” to demonstrate when any blocks have been changed, keeping blockchain transparent and auditable (Ateniese et al., 2017). Derler et al. (2020) extended the method to be able to make modifications on a transaction level, instead of block level. Their works presented systematised in fine – grained modifications and sanitizable signatures.

Furthermore, the other technical resolution for deleting data kept within blockchains without “hard forks” is suggested by Puddu (2017), where a mutable blockchain, which can allow modification and deletion of the content in the blockchain. The recommended design controls the traditional blockchain's consensus mechanisms to vote on alternative forms of the blockchain history. In this case, it does so by introducing mutable transactions that represent the transaction sets, which have a variety of possible types of transactions. Within a transaction set, only a single transaction is marked as active, whereas the rest are fundamentally inactive substitutes. Notably, all alterations are done using transactions of a specific kind. Validators perform meta-transactions, which are given out by smart contracts or users and their verification (Puddu et al., 2017).

Criticizing the situations, permitting bad actor within a public blockchain not to encompass a transformation for his or her transaction, Deuber, Magri, and Thyagarajan (2019) offered a redactable blockchain, which is independent of the immense cryptographic tools and is appropriate for the special situations. In this regard, its procedure uses voting based consensus uses “proof of work” and is limited by an agreement that has the asks and limitations for the editing. In this case, any user can recommend the edit operation. However, this process is done only if the blockchain policy approves it. Additionally, the protocol provides liability for the edit activities, as any kind of editing within the blockchain can be verified openly. Even if the “proof-of-concept” application of the recommended procedure only presents a minute overhead with the authentication of the chain in comparison with the immutable one, the suggested public blockchain functions on the presumption that most of the miners within the network are authentic, and they perform realistically whenever they vote to reject or take the edit commands (Deuber et al., 2019).

Improving previous works, Marsalek and Zefferer (2019) proposed algorithms for an editable blockchain that facilitates alteration, incorporating reductions of unspent output of transactions in blockchain. The suggestion accomplishment proves the suggested resolution's security and demonstrates positive impacts on functioning. The resolution is based on a consensus, which controls whether or not the suggested corrections are applied. Data associated to practical alterations is kept in a supplementary blockchain. Using this data, the blockchain can be effectively authenticated, the information in this blockchain can be changed later (Marsalek et al., 2019).

A “memory-flexible blockchain model” custom-made toward Internet of Things network is presented by Dorri et al. (2019), where model enables users to compress, modify, or entirely delete the transactions from the blockchain while preserving the consistency of the transactions. Notably, this process is realized by computing the block’s hash above the hashes of its established transactions and not of their substances, thereby allowing a transaction to be taken out from a block without impacting the hash steadiness authorizations. Dorri et al. (2019) noted precisely, for every transaction kept within a blockchain, there is the calculation of specific value as the employed “secret keeping hash” known only by the party that generates the transaction. Moreover, to delete a kept transaction, the operator needs to confirm he or she has formerly created the matter by comprising in the eliminate transaction the hashes used to produce the secret of the transaction to be taken out and the encoded formula of the hashed secret by means of the public key (Dorri et al., 2019).

Kuhn (2018) revealed a data structure, an algorithm, and a block matrix, which allow the secure removal of illogical records while ensuring the preservation of hash-based integrity guarantee that the remaining blocks stay unaltered. Nevertheless, the resolution has been only concentrated on “permissioned blockchains” to make sure their compliance with the “right to be forgotten” erasing requirements and their transaction integrity.

Aitsam et al. (2020) presented the analysis of different methods to help minimise the illegal insertion. The researchers compared editable blockchain with other methods to delete the unwanted content and noted that the filtering quality of editable blockchain was good, usability was not guaranteed, network burden was high, this type of blockchain was difficult to deploy.

3 Justification of the Study

Professionals noted that in parallel with the financial services, blockchains could eventually transform several significant industries, ranging from Internet of Things to healthcare (Marsalek et al., 2019).

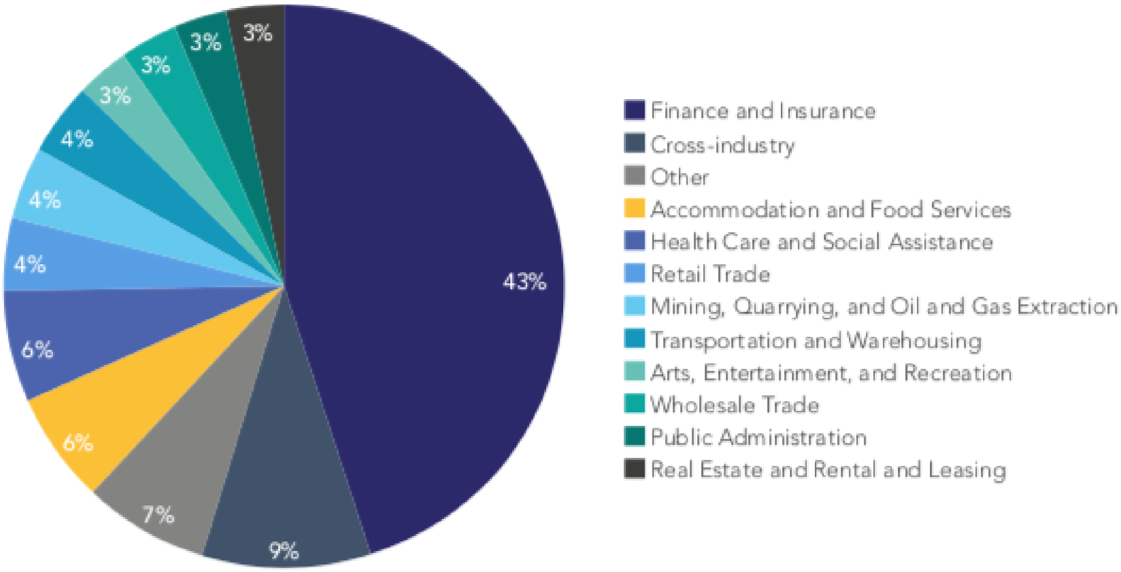

Figure 2: Live Networks by sectors (Cambridge Centre of alternative finance, 2019)

The Figure 2 created by Cambridge Centre for Alternative Finance research and represents data from 25 countries of 67 existent functioning blockchain systems. Finance and Insurance industries dominated by forty three percent (Rauchs et al., 2019). Blockchain use cases could unlock value for businesses and set up fresh bases for social and economic schemes. While most of the applications of blockchain are likely are still coming up, the forthcoming impact and direction of the blockchain technology cannot be predicted.

Irreversibility of blockchain verifies that the transaction data, in the blockchain, is tamper-proof, which means that they cannot be changed or erased. A data configuration of records is in a tree, where the leaf nodes have the hash of a distinctive data confirmation and all the other nodes of the tree include the hash of the two nodes below them. The Merkle root can then be used to authenticate reliability of the data records and variations if any of the data records comprised into the tree alteration (Puddu et al., 2017).

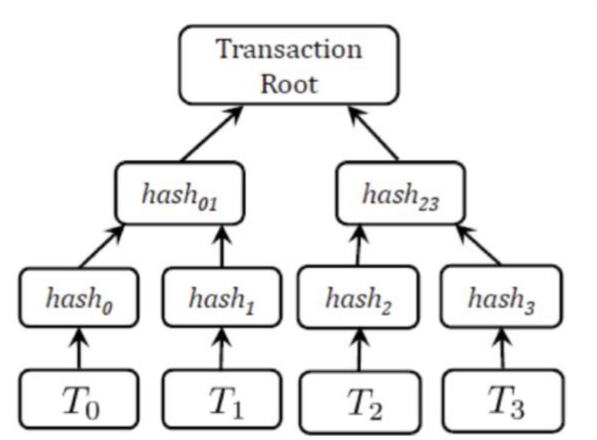

Figure 3, Merkle tree (Puddu et al., 2017)

Irreversibility of blockchain comes from the way it is and verified as a result of the cryptographically connected blocks that are linked together with the preceding block's hash value. The inconvenience of the data accumulated in blockchain cannot be changed can only be added. The benefits of the blockchain immutability feature are obvious: when data saved in the blockchain, the employing the blockchain in security-critical truthfulness of the data is safeguarded forever. Blockchain is valued for audit logs, financial transactions, and data that need protection and integrity (Marsalek et al., 2019).

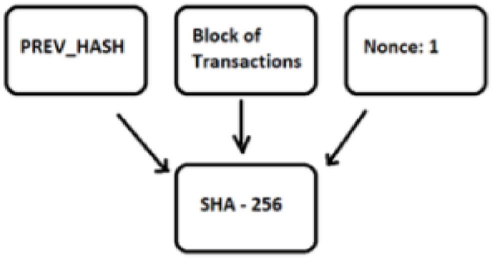

Figure 4, Proof of Work (Atsam, M., et al. 2020)

Aitsam et al. (2020) noted that there are other elements contributing to blockchain’s irreversibility. SHA 256 algorithm is used to validate Proof of Work (PoW) in Bitcoin blockchain. Consensus algorithm helps in the decision-making process of Distributed Ledger Technology. The approval of all the nodes is needed to add the new block. PoW requires nodes to put their nonce and Prev_Hash into the block and solve a puzzle, the first problem solver is given a privilege to add a new block. To get the best hash value, computer performs from 10 to 21 calculations. The computational power is used by miners to find the most suitable nonce, a random number, they use only once. When the value is found the nodes notifies other miners and they stop mining and need to validate the block. If the authorisation is successful, participants are working on the value of the next block. In Bitcoin blockchain Proof of Stake (PoS) shows how many coins each participant owns. The owners of the coins will dominate the network. To speed decision-making process up, the delegates can be nominated to validate the blocks. With Delegated Proof of Stake (DPoS) the network participants have more authority and privileges (Aitsam et al., 2020).

Particularly within permissioned blockchains' context where, there is a limited number of nodes, interfering with blockchain data is not supposed to be considered as being not possible to change, as there is constantly a likelihood of most of the dominant organizations to vote for their kind of certainty and to change the ledger consequently. A lengthy chain of the blocks causes the profound history of blockchains to become immutable because of the high costs involved for changing the blocks' hash-based veracity, guaranteeing immutability within private blockchains is stronger and less costly so long as most of the validating nodes follow the rules (Finck, 2018).

"Hard fork" cannot be used as a solution often because of the complexity. Therefore, it is widely held that modifying transaction data within the public blockchains not possible.

4 Research Gap

Blockchain technology is a comparatively new field of study primarily examined by computer and finance scholars. There are very few academic studies analysing blockchain technology from the consumers' perspective. Substantial research is currently being performed to design and develop techniques that are aimed at allowing deletion or modification of the blockchain, while at the same time it should be transparent, auditable, and secure (Politou et al., 2019). This research paper analyses if the blockchain can be modified.

5 Research Questions

This paper has four main objectives. The literature examined to make sure the readers understand the concept of redactable blockchain, why redaction is needed, and modification methods identified. All positive and negative feedback reviewed. The findings from literature review and the results from the questioner will help to the knowledge of immutable and redactable blockchains among interested parties. The suggestions will be assembled together from the analysis of literature review and questioner on the possible actions interested parties could do to prepare for the wider adoption of the blockchain technology. The objectives of this research paper transform into three research questions:

Are blockchain enthusiasts aware of redactable blockchain technology? Originally blockchain was created as append only system and the irreversibility guaranteed the trust and assurance about security and resilience to fraud. The literature review showed high level of knowledge and understanding of redactable blockchain type among academic researchers this can be measured by the number of academic works related to the question. The answers to questioner will be analysed and compared. Statistical test will answer about the entire population.

Is there preference in redactable blockchain technology type in particular industry sector? Due to the differences some industries could have more situations when corrections are needed and the irreversibility could be not the strengths, but weakness of the technology.

Finally, is there difference in knowledge, effectiveness, suitability, compliance, security and resilience to fraud understanding between immutable and redactable blockchain in entire population of blockchain enthusiasts?

Analysis and results of the quantitative web survey and statistical tests will be discussed later to explain these questions further.

6 Research Methodology

The utilization of data in form of statistics that offers descriptions and analysing data reduces the effort and time that the researcher would have devoted to describing his or her findings. One weakness is the research objectivity, which means that the researcher is just an observer. With such kind of respondent and researcher relationship, it is hard to obtain in-depth research. The limitation could be that the researcher will not understand individuals or the group working with him or her, and hence, will fail to appreciate them (Eyisi, 2016).

This research was limited to six thousand words and twelve weeks. Statistical data was used as an instrument for the research to reduce time. The data and the numbers were gathered and analysed. The particular order was followed in this research. First of all, the data was gathered for the analysis. The questionnaire complemented and confirmed the discoveries from the literature review. Quantitate results, generated by R Studio were summarized in the tables. The charts were transferred to Configuration Manual from the web survey to visualise the data in form of pie and bar charts and compared with the findings from literature review. The evaluations and analysis helped with conclusions and discussions.

7 Design specification and implementation

In this regard, the questioner was designed. The link to online survey shared with a hundred and fifty professionals. The participation in the web survey was confirmed by blockchain enthusiasts in writing. The questioner was open for four weeks and was closed after this period. The questionnaire had twenty questions, which were related to trust and editability of the blockchain.

Fundamentally, the participants could either point out that they agree, disagree, or did not have a clear answer for each particular question asked. The respondents were from the authors of this research paper LinkedIn connections. It was explained to the participants that no personal data will be collected during the research. This helped more active participation. The respondents showed their interest in the topic by answering during their free time from work. It was following up e-mail reminder sent to twenty percent of the respondents. After the second reminder, the answers were received straight away. The third reminder was not needed, and the time was saved.

The answers were downloaded from web survey and analysed in R Studio statistical package. The findings showed the awareness of the topic. More than sixty seven percent (hundred and one respondent) randomly selected professionals from different industries found time to contribute by sharing their opinions. The last question asking to add more to the topic of redactable blockchain was answered by more than a half of the respondents.

8 Evaluation and Analysis

The first four questions in the questioner were asked about the respondents (Figures 5,6,7,8, Configuration Manual). The majority of the respondents were from 18 to 45 age group. Technology and financial services industries dominated. Education corresponded with authors professional circle, only a few were with school education. Ten years professional experience was the most prevailing answer.

The categorical values were generated in R Studio and are summarised in the Table 1 and included in the Appendix on page 24. To establish correlation between the age, type of industry, work experience and the knowledge of the blockchain enthusiasts about the immutable and redactable blockchains p-values, using Pierson's Chi Square and Cramer's V coefficient were calculated using R Studio statistical package. As in all cases p-values are greater than 0.05, two variables are dependent. Values of all Cramer's V coefficients are greater than 0.25, indicating strong correlation. The results are summarised in the Table 1.

Table 1: Correlation between variables

Independent Variables	**Immutable**		**Redactable**	
	Pearson's Chi Square (p-value)	**Cramer's V coefficient**	**Pearson's Chi Square (p-value)**	**Cramer's V coefficient**
Age Group	0.2467	0.2569	0.2143	0.2649
Type of Industry	0.0553	0.422	0.104	0.3961
Experience	0.7208	0.2642	0.7188	0.2646

In question five only twenty two percent of the respondents agree that irreversibility needed to trust the technology. This resonates with literature review findings about fraud, illegal content, GDPR incompliance presented in the immutable blockchain. Twenty-nine per cent gave neutral answer. Nearly fifty percent of the respondents disagreed, indicates that respondents find the irreversibility cannot guarantee technology trustworthiness (Figure 9).

Answering question six (Figure 10), the respondents noted that in financial services and manufacturing industries redactable blockchain type would be preferred. The results generated with R Studio and summarized in the Table 2.

Table 2: Preference of blockchain

Industries	Neutral	Immutable	Redactable
Technology, media and telecommunications	6%	86%	8%
Financial services	3%	22%	75%
Manufacturing	9%	25%	66%
Retail, wholesale, logistics and distribution	14%	70%	16%
Industrial products and construction	15%	71%	14%
Automotive	10%	70%	20%
Life science and health care	5%	55%	40%
Government and public services	3%	90%	7%

Questions seven, eight and nine tested the awareness of the redactable capability of blockchain (Figures 11,12,13). Nearly half of the respondents demonstrated their awareness. Second popular answer showed that they accept this capability only under full accountability. More than a half of the respondents shared their knowledge of redaction methods. The most popular method was chameleon hash, the method originally created for private blockchains, but can be used with public blockchains.

For example, Rajasekhar et al. (2018) implemented chameleon hash in practice. They showed how to redact blockchain by using Bitcoin blockchain example. The chameleon hash technique was improved, sharing the secret by non-linear way. Florian et al. (2019) used Bitcoin public blockchain to demonstrate the method that permits to delete data from the local nodes, functionally preserving local deletion. Ashritha et al. (2019) introduced a second trapdoor key. Here, the change does not occur without consensus of the block original originator and the block data is certified by the digital signatures. Understanding the limitation of all the current suggestions, that offer to "build-new-chain approach for redactions", without amalgamation with present structures like Ethereum and Bitcoin, Reparo was suggested by another group of researchers. This method represents a publicly verifiable layer on top of any blockchain to implement reparations (Thyagarajan et al. 2020).

The answer to question ten and eleven (Figures 14,15) corresponded with the findings from the literature review, for example, Politou et al. (2019) noted that industry and academia will welcome the resolution of the conflict around the immutability of the blockchain. It may considerably affect the adoption of blockchains, it is important to resolve this issue. Unavoidably, many advocates of the blockchain and the crypto campaigners have considered the "right to be erasure" as being a barrier for blockchain technology expansion to full applications area. In this regard, the World Economic has issued a recommendations how data can be achieved (European Commission, 2018). In a similar way, the Organization for Economic Co-operation and Development has started to investigate the risks and benefits of the blockchain for societies and economies, while the United Nations is progressively accepting the blockchain technology (Politou et al., 2019). At the same time, the European Commission, with the

European Parliament's support, launched the “European Union Blockchain Observatory and Forum” intending to inspire citizens, industry, and governments to gain from the blockchain prospects (Lyons et al., 2018). However, there are fans of the sophisticated cryptographic methods to assure personal privacy within the decentralized blockchain architectures. Notably, research works have been performed to illustrate how the requirements of the “right to erasure” can be satisfied for the private and public blockchains (Martin-Bariteau, 2018).

To answer question twelve, the respondents will trust only High/Supreme Court to edit blockchain on a case by case basis, only in the special circumstances. The respondents showed that they would not trust the government, accounting firms or Artificial Intelligence to perform the modifications (Figure 16). This could be researched further.

Originally blockchain was attractive because it was irreversible. More than a half of the respondents to answering question thirteen, noted that redactable blockchain is more risky than immutable (Figure 17). Irreversibility is essential to the safety of the blockchain, as it prohibits change the data in the blockchain, and hence, it allows a single, internationally acknowledged behaviour among participants. Precisely, irreversibility serves to support the likelihood of decentralized trust in intrinsically thrustless contacts (Ølnes et al., 2018).

The answer to question fourteen corresponds with the findings from the literature review, for example, Finck (2018), who noted that while it is not possible to rollback, delete, or update transactions the moment they are recorded within a blockchain, some people would present a contrary argument. Given that irreversibility is a developing, and not fundamental to blockchain’s data structure feature, an agent with an adequate computing power amount could alter it. (Figure 18) demonstrates that the idea of a blockchain is not correctable system, is not right and confusing.

Answering question fifteen, nearly forty-eight percent of respondents agreed that editable blockchain could be another type of permissioned blockchain that will evolve from the original decentralized and permissionless version like in the case of Quorum (Figure 19). This question was asked to check the reaction of the respondents to the idea of the centralisation in the enterprise blockchains. Time will prove if editable blockchains are future of finance and will evolve to be compatible with law, be secure and resilient to financial fraud and human error. The permissionless enterprise blockchains could be investigated further in another research paper.

The last five questions were asked to understand the entire population of blockchain enthusiasts. Figures (20, 21, 22, 23, 24). All p-values of Shapiro Wilk test show that p values were less than 0.05, the differences did not follow the normal distribution. Hence, the non-parametric alternative of t-test was chosen in this case.

Table 3: Criteria for two blockchain types

	Immutable	**Redactable**	**Immutable**	**Redactable**
Variables	**mean**	**mean**	**standard deviation**	**standard deviation**
Knowledge	6.77	5.51	2.17	2.09
Effectiveness	6.43	7.81	2.23	2.38
Suitability	5.77	8.48	2.00	2.19
Compliance	1.77	8.48	1.31	2.37
Security	9.05	6.77	1.72	1.56
Resilience to fraud	9.05	6.77	1.72	1.56

Wilcoxon signed rank test with continuity correction was carried out in R Studio. The symmetry of the differences between the two paired groups validated by boxplots and displayed approximately symmetrical distribution. In this case the medians instead of means were compared. The findings were summarised in Table 4. The results showed a significant difference between immutable and redactable blockchains p-values less than 0.001 for all the five criteria: knowledge, effectiveness, suitability, compliance, security and resilience to fraud.

Table 4: Criteria for two blockchain types

	Immutable	**Redactable**		
Variables	**median**	**median**	**Is statistically different**	**Wilcoxon sign rank test**
Knowledge	7	6	Yes (95%)	p-value < 2.2e-16 or <0.001
Effectiveness	7	8	Yes (95%)	p-value = 9.386e-06 or <0.001
Suitability	6	10	Yes (95%)	p-value = 3.323e-14 or <0.001
Compliance	1	10	Yes (95%)	p-value < 2.2e-16 or <0.001
Security	10	7	Yes (95%)	p-value < 2.2e-16 or <0.001
Resilience to fraud	10	7	Yes (95%)	p-value < 2.2e-16 or <0.001

9 Discussions and Conclusions

If we examine the “right to be forgotten” from a developer viewpoint, the first response is to consider how we could adequately delete the data. It is impossible to do if blockchain is irreversible. Solicitors examine the actual effect of the situation on individuals or business. They examine how this looks from the law point of view, but developers looks at technical erasure. If a solicitor thinks about the “right to be forgotten,” there is no guarantee that he or she has the same “right to be forgotten” developer studied in college. The same is with a developer. This is a huge problem with immutable blockchain (Wirth et al., 2018). The answers to the last question, were the respondents were asked to add extra to the topic of editable blockchain illustrated the above. The developers and lawyers need to work together to make sure that the technology is resilient to different types of attacks and fraud. The absolute irreversibility of blockchain technology cannot guarantee security or prevent incidents analogous to DAO “hard fork” case.

Wirth et al. (2018) noted that the disagreement exists over the blockchain protocols’ immutability and has been offered significant prominence in the recent times due to the General Data Protection Regulation adoption, and most significantly, due to the “right to be forgotten” that assumes the retrospective deletion of private data on request and from locations they have been stored. Moreover, for the blockchain supporters and cryptocurrency activists, even just questioning the blockchain’s irreversibility nature is equivalent to conflict, and hence, they consider the right to erasure as a barrier to the extensive blockchain technology adoption. Privacy supporters look upon the irreversibility of the blockchain as a danger to privacy rights and data protection (Ølnes et al., 2018). Nevertheless, for the business users, restricted irreversibility in permissioned blockchain systems, considering particular conditions, can bring in the correct balance between keeping the main components of a blockchain and adjusting it for the practical needs. In such a viewpoint, the new advances in bringing in reversibility are appealing to both the enterprises and regulators (Politou et al., 2019).

Recently, Israeli Blockchain company Kirobo, created “undo function”, a solution to correct the human error to cancel cryptocurrency transaction if the funds were sent to the wrong address (Peng, 2020).

In the financial services industry, the utilization of the digital currencies in different countries, which are based on the blockchain technology, is quickly increasing since several large banks have now declared blockchain ventures to set up novel businesses as well continually invest and engage in the blockchain technology. Notably, while the blockchain is among the upcoming trends, five to ten years is needed to witness this technology in practice. Despite the slow integration of the blockchain in the real-life applications, the incompatibility of the blockchain with privacy rights and data protection, blockchain enthusiasts are very interested in the technology. This work proved that the reversibility is needed in special circumstances and should be investigated on a case by case basis. In this regard, and toward researching techniques and methods to accomplish blockchain protocols’ compliance with the “right to be forgotten”, to help victims of fraud and illegal content, cryptographic methods that conditionally changing blockchain’s core feature of irreversibility have been presented. For this research paper the editable blockchain would be preferable in financial services and manufacturing industries.

10 Future work

This research triggered the topics that could be investigated further. First of all, it is worth to examine security, financial and operational risks that are not presented in the immutable blockchain and will be present with the redaction capability.

Secondly, further investigation is required to find out redactable blockchain preferences by conducting structural interviews with professionals from financial services and manufacturing industries that are currently using live blockchain networks to get more insights about specific situations where the redactable blockchain could be preferred. The results could be compared between two industries and with recent academic and industry publications.

Finally, this research showed that Big 4 accounting firms, artificial intelligence and government cannot be trusted to redact the blockchain. It understood that reduction can happened in special circumstances in the High court. It is worth to examine the opinion of judges and model possible scenarios how this could be done using the technical methods suggested in this research.

References

Aitsam, M., & Chantaraskul, S. (2020). Blockchain technology, technical challenges and countermeasures for illegal data insertion. *Engineering Journal*, *24*(1), 65–72. doi: 10.4186/ej.2020.24.1.65

Ashritha, K., Sindhu, M., & Lakshmy, K. V. (2019). Redactable Blockchain using Enhanced Chameleon Hash Function. *2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019*, 323–328. doi: 10.1109/ICACCS.2019.8728524

Ateniese, G., Magri, B., Venturi, D., & Andrade, E. R. (2017). Redactable Blockchain - Or - Rewriting History in Bitcoin and Friends. *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017*, 111–126. doi: 10.1109/EuroSP.2017.37

Bartoletti, M., & Pompianu, L. (2017). An Empirical analysis of smart contracts: Platforms, applications, and design patterns. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10323 LNCS*, 494–509. doi: 10.1007/978-3-319-70278-0_31

Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., Kulatova, N., Rastogi, A., Sibut-Pinote, T., Swamy, N., & Zanella-Béguelin, S. (2016). Formal verification of smart contracts: Short paper. *PLAS 2016 - Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, Co-Located with CCS 2016*, 91–96. doi: 10.1145/2993600.2993611

Button, C. D. (2019). The forking phenomenon and the future of cryptocurrency in the law. *Review of Intellectual Property Law*, *1*(19), 1–36. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/johnmars19&div=4&id=&page=

Derler, D., Samelin, K., & Slamanig, D. (2020). *Bringing Order to Chaos: The Case of Collision-Resistant Chameleon-Hashes*. doi: 10.1007/978-3-030-45374-9_16

Derler, D., Samelin, K., Slamanig, D., & Striecks, C. (2019). *Fine-Grained and Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based*. *February*. doi: 10.14722/ndss.2019.23066

Deuber, D., Magri, B., & Thyagarajan, S. A. K. (2019). Redactable blockchain in the permissionless setting. *Proceedings - IEEE Symposium on Security and Privacy*, *2019-May*, 124–138. doi: 10.1109/SP.2019.00039

Dorri, A., Kanhere, S. S., & Jurdak, R. (2019). MOF-BC: A memory optimized and flexible blockchain for large scale networks. *Future Generation Computer Systems*, *92*, 357–373. doi: 10.1016/j.future.2018.10.002

Eberhardt, J., & Tai, S. (2017). On or Off the Blockchain? Insights on Off-Chaining Computation and Data. *Insights on Off-Chaining Computation and Data. In: De Paoli F., Schulte S., Broch Johnsen E. (Eds) Service-Oriented and Cloud Computing. ESOCC 2017. Lecture Notes in Computer Science, vol 10465*(September). doi: 10.1007/978-3-319-67262-5_1

European Commission. (2018). *European countries join Blockchain Partnership | Shaping Europe's digital future*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

Eyisi, D. (2016). The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education Curriculum. *Journal of Education and Practice*, *7*(15), 91–100. Retrieved from www.iiste.org

Finck, M. (2018). Blockchains and the General Data Protection Regulation. In Blockchain Regulation and Governance in Europe (Issue July). doi: 10.1017/9781108609708.004

Hewett, N., Lehmacher, W., & Wang, Y. (2019). Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction. *World Economic Forum*, *March*, 26.

Krawczyk, H. & Rabin T. (2000). Chameleon signatures. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2000*. San Diego, CA: The Internet Society

Kuhn, D. R. (2018). *A Data Structure for Integrity Protection with Erasure Capability IEEE IT Professional View project Security for the internet of things View project*. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/05/31/data-structure-for-integrity-protection-with-erasure-capability/draft/documents/data-structure-for-integrity-with-erasure-draft.pdf

Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. *Proceedings of the ACM Conference on Computer and Communications Security*, *24-28-Octo*, 254–269. doi: 10.1145/2976749.2978309

Lyons, T., Courcelas, L., & Timsit, K. (2018). *Blockchain and the GDPR : a thematic report prepared by the European Union Blockchain Observatory and Forum*. 4–31. Retrieved from https://www.eublockchainforum.eu/sites/default/files/reports/workshop_3_report_-

_government_services2fdigital_id.pdf

Marsalek, A., & Zefferer, T. (2019). A correctable public blockchain. *Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE 2019*, 554–561. doi: 10.1109/TrustCom/BigDataSE.2019.00080

Martin-Bariteau, F. (2018). Blockchain and the European Union General Data Protection Regulation: The CNIL's Perspective. *SSRN Electronic Journal*, 1–12. doi: 10.2139/ssrn.3275783

Matzutt, R., Henze, M., Ziegeldorf, J. H., Hiller, J., & Wehrle, K. (2018). Thwarting unwanted blockchain content insertion. *Proceedings - 2018 IEEE International Conference on Cloud Engineering, IC2E 2018*, 364–370. doi: 10.1109/IC2E.2018.00070

Matzutt, R., Kalde, B., Pennekamp, J., Drichel, A., Henze, M., & Wehrle, K. (2020). *How to Securely Prune Bitcoin's Blockchain*. Retrieved from http://arxiv.org/abs/2004.06911

Ølnes, S., & Jansen, A. (2018, May 30). Blockchain technology as infrastructure in public sector -An analytical framework. *ACM International Conference Proceeding Series*. doi: 10.1145/3209281.3209293

Palm, E. (2017). *Implications and Impact of Blockchain Transaction Pruning*. 75. Retrieved from http://www.diva-portal.org/smash/get/diva2:1130492/FULLTEXT01.pdf.

Peng, T. (2020). *An Israeli Blockchain Startup Claims It's Invented an 'Undo' Button for BTC Transactions*. Coin Telegraph. Retrieved from https://cointelegraph.com/news/israeli-blockchain-startup-offers-undo-button-for-bitcoin-transactions

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), 1–20. doi: 10.1093/cybsec/tyy001

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain Mutability: Challenges and Proposed Solutions. *IEEE Transactions on Emerging Topics in Computing*, 1–13. doi: 10.1109/TETC.2019.2949510

Puddu, I., Zurich, E., Dmitrienko, A., & Capkun, S. (2017). *μchain: How to Forget without Hard Forks*. Retrieved from https://eprint.iacr.org/2017/106.pdf

Rajasekhar, K., HarshiniYalavarthy, S., Mullapudi, S., & Gowtham, M. (2018). Redactable blockchain and it’s implementation in bitcoin. *International Journal of Engineering & Technology*, *7*(1.1), 401. doi: 10.14419/ijet.v7i1.1.9861

Rauchs, M., Blandin, A., Bear, K., & Mckeon, S. (2019). *2 Nd Global Enterprise Blockchain*. Retrieved from https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-enterprise-blockchain-benchmarking-study/

Schellekens, M. (2019). Does regulation of illegal content need reconsideration in light of blockchains? *International Journal of Law and Information Technology*, *27*(3), 292–305. doi: 10.1093/ijlit/eaz009

Schwerin, S. (2018). Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study. *The Journal of the British Blockchain Association*, *1*(1), 1–77. doi: 10.31585/jbba-1-1-(4)2018

Thyagarajan, S. A. K., Bhat, A., Magri, B., Tschudi, D., & Kate, A. (2020). *Reparo: Publicly Verifiable Layer to Repair Blockchains*. Retrieved from http://arxiv.org/abs/2001.00486

Wirth, C., & Kolain, M. (2018). Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data. *In Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET)*, 6. doi: 10.18420/blockchain2018_03

Appendix

Table 5 : Independent Variables

	Immutable			Redactable		
Age	**Expert**	**Novice**	**Total**	**Expert**	**Novice**	**Total**
<18	3	0	3	1	2	3
18 to 25	14	8	22	3	5	8
26 to 35	24	3	27	13	9	22
36 to 45	19	8	27	18	9	27
46 to 50	9	5	14	13	14	27
>50	5	3	8	4	10	14
Total	**74**	**27**	**101**	**52**	**49**	**101**
Work experience in years:						
1	2	0	2	1	1	2
2	4	1	5	3	2	5
3	7	1	8	6	2	8
4	4	3	7	4	3	7
5	4	1	5	3	2	5
6	3	1	4	2	2	4
7	1	0	1	1	0	1
8	2	3	5	2	3	5
9	1	0	1	0	1	1
10	2	0	2	2	0	2
>10	44	17	61	28	33	61
Total	**74**	**27**	**101**	**52**	**49**	**101**
Industries:						
Automotive	2	5	7	1	6	7
Education	1	0	1	0	1	1
Financial services	17	2	19	11	8	19
Government and public services	1	1	2	0	2	2
Industrial products and construction	1	2	3	1	2	3
Law	8	3	11	4	7	11
Life sciences and health care	5	5	10	4	6	10
Manufacturing	6	2	8	5	3	8
Retail, wholesale, logistics, and distribution	7	2	9	3	6	9
Student	2	0	2	1	1	2
Technology, media and telecommunications	24	5	29	21	8	29
Total	**74**	**27**	**101**	**51**	**50**	**101**

Table 6: Literature research technical approaches and related topics

Publication	Year	Technical methods					Other					
			Chameleon Hash	µchain	Off /side chaining	Secret Keeping Hash	Mini - blockchain	GDPR	Human error	Illegal content	Smart Contracts	Redactable bitcoin blockchain
Krawczyk & Rabin		2000	x			x						
Bhargavan et al.		2016										
Luu et al.		2016					x					
Ateniese et al.		2017	x						x	x		
Bartoletti & Pompianu		2017								x	x	
Puddu et al.		2017		x	x							
Eberhardt & Tai		2017			x							
Finck		2018						x				
Ølnes & Jansen		2018						x				
Kuhn		2018										
Palm et al.		2018					x					
Rajasekhar et al.		2018	x									x
Schwerin		2018						x				
Ashritha et al.		2019	x									x
Deuber et al.		2019				x						
Dorri et al.		2019			x			x				
Florian et al.		2019							x			
Schellekens		2019								x		
Politou et al.	2018	2019	x					x				
Marsalek & Zefferer		2019	x	x	x							
Aitsam et al.		2020	x							x		
Derler et al.	2019	2020	x									x
Matzut et al.	2018	2020					x			x		
Thyagarajan et al.		2020	x					x		x		x