Virtual Private Blockchains: Security Overlays for Permissioned Blockchains

Samuel Onalo*, Deepak GC†, Eckhard Pfluegel‡
Faculty of SEC, Kingston University
Kingston upon Thames, Surrey, KT1 2EE, United Kingdom
email: *k1450301@kingston.ac.uk, †d.gc@kingston.ac.uk, ‡e.pfluegel@kingston.ac.uk

***Abstract*—Blockchain technology, while maturing, is still lacking features that would be considered indispensable in real-world business applications. In particular, the lack of transaction confidentiality in a public blockchain is a challenging problem. A possible solution might be the concept of a private blockchain. However, maintaining such permissioned blockchains requires resources, depends on a central authority and contradicts the original philosophy of pioneering blockchain systems such as Bitcoin. In this paper, the concept of a *Virtual Private Blockchain* (VPBC) is proposed as a mechanism to create a blockchain architecture with properties akin to those of a private blockchain, however leveraging existing public blockchain functionality. A VPBC can be set up between individuals or organisations, does not require any significant administrative maintenance, inherits all the functionality from the public blockchain, and achieves anonymity and transaction confidentiality with respect to any public blockchain node who does not belong to the VPBC. Building on this theoretical concept, it is then shown how the cryptographic technique of secret sharing can be used in order to implement a simple VPBC architecture. A proof-of-concept architecture has been created and early experiments indicate that the creation of VPBCs for potential real-world application scenarios might be feasible.**

Index Terms*—*Public Blockchain; Private Blockchain; Permissioned Blockchain; Blockchain Confidentiality; Security Overlays; Virtual Private Networks; Secret Sharing.

I. Introduction

According to recent research, the adoption of Blockchain technology is steadily increasing, and major business organisations are currently investigating how to benefit from features such as immutability and public verifiability of data, decentralised architecture and (pseudo) anonymity of transactional data. As blockchain technology is gradually maturing, the quest for suitable applications is shaping the future of decentralised, networked functionality providing data integrity services and innovations in the fields of big data, cloud computing and cryptography. However, current blockchain technologies are not always able to address all specific security requirements for individual, specialist applications. For example, a public blockchain application would not be able to provide the required confidentiality to allow independent financial institutions to share sensitive data securely and anonymously.

A possible solution to this problem is the concept of a private blockchain. This is a restricted-access network, where permission has to be granted to prospective participants for transactional and administrative participation in network activities. Typically, cryptocurrencies are built on public blockchains, in which anyone can elect to join and participate. By contrast, private blockchains are targeted towards businesses and institutions who want the benefits of blockchain technology (e.g., distributed ledger consensus and immutability) but want to limit the scope of the facility, to in-house entities and trusted partners. However, maintaining such a private blockchain requires resources. Also, it contradicts the original intention of the pioneering Bitcoin technology, aiming to not rely on a central body.

The fundamental research question addressed in this paper is whether there are alternatives to the concept of a private blockchain architecture. A focus is on innovative security architectures, the application of suitable cryptographic techniques, and their use within the blockchain architecture. Furthermore, an assessment of the benefits arising from the real-world use cases of this architecture is of importance.

In this paper, the following contributions are made. First, the novel concept of a *Virtual Private Blockchain* (VPBC) is shaped, implemented and initially evaluated. A VPBC is a mechanism to create a blockchain architecture with properties akin to those of a private blockchain, however leveraging existing public blockchain functionality. Second, we show how to use the cryptographic technique of secret sharing in order to implement a simple VPBC. Finally, we devise a proof-of-concept architecture and first experiments indicate that there appear to be no major obstacles in adopting VPBCs in future real-world application scenarios.

To our knowledge, both the conceptual ideas of this paper as well as the application of secret sharing in an architecture across several blockchain systems are novel and have not been proposed in this form, in the literature to date.

This paper is organised as follows: In Section II, concepts and techniques for securing blockchain functionality are presented. Section III contains the description of the VPBC architecture, while in Section IV, an implementation and evaluation is reported. Section V relates the results of this paper to the literature, and the paper concludes in Section VI.

II. Blockchain Security

In this section, we review the basic security aspects of the blockchain. We will start with briefly recalling security concepts and techniques currently in use for achieving existing security goals in publicly available blockchain systems, with a focus on confidentiality. This will be followed by more

 ISBN: 978-1-61208-818-1

advanced techniques improving specific dependability and security aspects of the blockchain suggested in the recent literature as conceptual contributions or used in prototype solutions.

A. Cryptographic Techniques for Blockchain Security Features

A number of cryptographic techniques are in place in mainstream blockchain applications in order to fulfil basic security requirements.

Cryptographic hash functions are used in order to ensure the integrity of the public ledger, a global record of Blockchain transactions. Based on a suitable, efficient data structure (the hash tree), even minor changes in large amounts of data can be detected and repaired if necessary. Furthermore, the principle of mining which is a digital protocol, mimicking the creation of scarce resources, implements necessary work for creating new, validated blocks by performing a pre-image attack on given hash digest values. Validation can be carried out efficiently by re-computing the digest.

The authenticity of digital messages and data is usually demonstrated or verified using digital signatures. It allows for the effective origin and message integrity as well as non-repudiation of communication between two parties. In a Blockchain, participants can sign transactions with their private keys. In Bitcoin, the concept of a wallet is implemented, controlling the spending power of a user based on a private and public key pair. Cryptocurrency transactions are not completely anonymous in nature, however, the true identities of transactors are hidden and are not provided as part of the accessible data stored on the public blockchain. The transactions are considered to be pseudonymous as the only form of identity any node on the network possesses is the wallet identity which effectively is the public key of the wallet that is owned by the node.

B. Establishing Transaction Confidentiality

More recently, a number of Blockchain systems have started addressing the lack of confidentiality for transactional information, through a variety of mechanisms. We shall present two approaches, provided by the prominent Blockchain systems Hyperledger Fabric and Multichain. These are also, the systems we have used for our first experiments towards a novel security solution, as described later on in this paper.

1) HyperLedger Fabric Channels : Hyperledger is an open-source ecosystem of blockchain services run and maintained by IBM which has developed a means of providing confidentiality by the use of a private communication "subnet". The principle is to implement so-called *Channels* [1] between two or more specific network members. A complex infrastructure of cryptographic protocols and a range of security services including confidential inter-channel communication and transactions are available. While this provides a sophisticated and powerful infrastructure for achieving the desired confidentiality on the Blockchain, it requires expertise and resources in order to deploy, configure, and manage a HyperLedger Fabric Blockchain within one or potentially several organisations.

2) Multichain Stream Confidentiality : The Multichain Blockchain system acknowledges the confidentiality loss of any raw data stored on a public ledger and proposes to address this by using a combination of symmetric and asymmetric cryptography. Any data intended to be submitted to the system is encrypted before being stored and timestamped on the chain. The password for reading the encrypted data is only made available to a subset of blockchain participants, leaving others unable to read it.

The method makes use of three blockchain streams [2], whose purposes are as follows:

- A first stream is used by participants to distribute their public Rivest, Shamir and Adleman (RSA) keys.
- A second stream is used to publish large pieces of data, bulk-encrypted using the Advanced Encryption Standard (AES) algorithm.
- A third stream provides data access. For each authorised participant, a stream entry is created which stores a security credential encrypted with the participant's public key.

While this architecture appears secure and efficient, it requires the availability of a Public Key Infrastructure (PKI) expert for effective management.

C. Advanced Blockchain Dependability and Security

In this section, the specialist topic area of using advanced cryptographic techniques for improving blockchain security is explored. This will help in illustrating the novelty of our approach in terms of how we achieve anonymity and confidentiality, using the cryptographic technique of secret sharing.

The main overall challenges for the blockchain are scalability and privacy. The first challenge is a serious reason why currently, most blockchain systems do not qualify as mainstream payment systems. They do not have enough processing power to process enough transactions per second. The second challenge – as already explored earlier – is problematic for both businesses and individuals: transactions are stored on a public database (the public ledger), which does not allow confidentiality.

Recently, the cryptographic technique of secret sharing and more generally threshold cryptography have been suggested in order to improve scalability and security aspects of blockchain security. This emerging area has so far only been explored in a small number of papers [3]–[6].

In [3] [6], the authors address the scalability of blockchain transactions by reducing the storage requirements for the public ledger, using an information dispersal scheme. A significant reduction in storage cost is achieved and furthermore, the integrity of transaction data can be improved. As an additional outcome, a reduction in energy cost due to block validation (bitcoin mining) is also achieved. Their scheme mainly focuses on reliability and redundancy, but not on security although there would be scope to do so. The key technique required for security enhancements is secret sharing, which can be seen

 ISBN: 978-1-61208-818-1

as a variation of the information dispersal employed by the previous authors.

The paper [4] pursues this research avenue further by using a space-efficient secret sharing scheme. It differs from the previous work by not relying on encryption but solely on creating secret shares of a transaction block, and store them on different nodes altogether. This reduces storage requirements and communication costs. It also achieves confidentiality, although a rigorous security analysis is not undertaken and appears difficult due to the potential security weaknesses of the underline secret sharing scheme.

The paper [5] addresses the lack of a more sophisticated internal controls against fraud in Bitcoin. A new cryptographic threshold-signature scheme for Elliptic Curve based digital signatures is introduced. Wallets that create transactions using this signature algorithm are called threshold wallets. The major advantage of this scheme is the fact that the private key used to create the digital signature of the transaction is not required as an entire quantity, but is stored as shares in a distributed fashion. This achieves joint control of Bitcoins and extends the build-in multi-signature feature of Bitcoin, by addressing the problem of "hot storage". Two applications of the new threshold scheme are presented in the form of use cases: for businesses, to eliminate the problem with single-point of failure and for individuals, a two-factor secure Bitcoin wallet. The authors suggest that using this algorithm could be key to overcoming some of Bitcoin's biggest challenges, preventing organisations or individuals from using the system to conduct business transactions.

III. Virtual Private Blockchains

In this section, the main contribution of this paper is presented. Inspired by previous work on secure overlay architectures (see further in Section V), a blockchain architecture achieving security goals typically benefited by Private Blockchains is devised. An emphasis is on ensuring confidentiality and anonymity of sensitive transaction information that would be disclosed to all other users if it was contained in the public ledger of a traditional blockchain. These security goals are achieved by leveraging the existing Public Blockchain functionality through a suitable mechanism. The resulting Virtual Private Blockchain architecture resembles that of a traditional virtual private network, which explains the terminology "Virtual" following the original concept introduced for Online Social Networks in [7].

A. VPBC Characteristics

A VPBC has a number of interesting and appealing characteristics, both in terms of functionality and security properties.

- The term "virtual" is justified as a VPBC utilises existing Blockchain functionality and is by nature a Blockchain itself. In particular, a VPBC inherits any built-in, internal Blockchain security mechanisms.
- A VPBC is not visible to other Blockchain users that are not part of it, and it is transparent to its users. This achieves both usability and security, which is a desirable characteristic.
- Furthermore, it should be possible for users to be part of multiple VPBCs, and the impact of a VPBC on the overall Blockchain performance should not be noticeable.

Any specific VPBC implementation would have to ensure that these characteristics hold, that the precise mechanisms of inner workings would be hidden to the user, and that they do not adversely affect usability (and user experience).

We interpret the individual public blockchains as black boxes, operating in a transparent manner, with the sole purpose being the validation of transactions followed by storing them in the public ledger. The overall impact of the individual blockchains' mining process and types of consensus algorithm (proof-of-work, proof-of-stake) on the VPBC are not investigated more in detail in this paper, although this would be an interesting piece of future work.

B. Basic Idea

In order to implement a VPBC, one needs to substitute confidential transaction content with pseudo-content or, more specifically, data bits of the originally intended content through information dispersal. The precise choice of this pseudo-content will strongly depend on the particular blockchain application and will need to be carefully analysed prior to setting up the VPBC. Furthermore, a mechanism for reversing the substitution process is needed, so that other members of the VPBC can retrieve the original information. This might require exchanging secret information amongst participants of the VPBC and will have to be achieved using an out-of-bound channel, such as an email or a phone conversation. This is the equivalent of setting up a VPN in a traditional networking architecture, based on a manual configuration of keys for encryption.

The basic idea is simple, and an explanation using the Bitcoin application is straightforward. Assume Alice wants to pay Bob 100 bitcoin but would like to conceal this value to others who have access to the Bitcoin public ledger. Alice could split the amount into two parts, say 100 = 30 + 70, send 30 bitcoin to Bob, convert the remaining 70 bitcoin to a different cryptocurrency and use the corresponding, alternative blockchain architecture to pay Bob. Subject to minor fluctuations, Bob is satisfied, having received the total amount via the two individual systems. The same idea could then be extended to using more than two blockchains, making it more difficult for an eavesdropper to reconstruct the real, original information.

While this method is effective for numerical values, it would be more difficult to apply for symbolic information. For example, if an address such as "Washington, D.C., USA" was to be split into town and country information and included in two different transactions, an attacker could potentially spot the correlation between these transactions. This could help in narrowing down search space or even to identify the used scheme. In the next section, we will present a more sophisticated approach which solves this problem.

 ISBN: 978-1-61208-818-1

C. Secret Sharing Approach

Expanding on the basic approach explained in the previous section, the precise cryptographic scheme that is underlying the VPBC architecture developed in this paper is the technique of *secret sharing*. The idea of secret sharing is to divide given data (the *secret* s) into n parts (the *shares*) in such a way that knowing (at least) m shares allows for reconstructing s. In an *ideal* secret sharing scheme, knowledge of less than m shares will not reveal any information on s. A secret sharing scheme with parameters m and n satisfying the aforementioned properties is also called a (m, n)-threshold scheme. A popular scheme is based on polynomial interpolation, introduced by Shamir [8].

Our VPBC architecture can now be explained as follows. Rather than using the example of Bitcoin, consider a generic public blockchain, and a requested transaction with sensitive transaction information t, requiring protection. Using a suitable ideal (m, n)-threshold secret sharing scheme, t will be shared as n pieces of information (transaction shares) $t_1, \ldots, t_n$, and these will be used for the individual transactions, executed on n independent public blockchains. Note that the resulting shares are random numbers and do not preserve any patterns that might be in the initial secret. The recipient, prior to using the scheme, has been informed about the selected blockchains. As soon as there are new transactions, a subset of m transactions (which in reality are shares of the real transaction) will be collated and the original secret transaction data can be reconstructed.

D. Security

In this section, we discuss the security of our VPBC approach. We showed that a VPBC implementation based on secret sharing is secure against any attacker being limited to accessing less than m blockchains, provided a (m, n)-threshold secret sharing scheme is used. If the secret sharing scheme is an ideal scheme, no information about the original transaction data is revealed by intercepting any of the shares. Furthermore, any collection of at the most $m - 1$ shares still does not yield any information about the original secret, in an information-theoretic sense. The security principle underlying the approach is security through obscurity. Provided that the specific transaction data protected through secret sharing is selected carefully and the resulting transaction shares appear innocuous, the technique could then be seen as a way of hiding information akin to steganography by cover modification.

In order to retrieve the sensitive information, an authorised user has to collate a collection of m transaction shares and apply the reconstruction method of the specific secret sharing scheme. In conclusion, this approach provides confidentiality under the assumption that no more than $m - 1$ blockchains would be attacked.

A number of attacks on the scheme exist, and we describe two approaches which appear the most straightforward.

1) Brute-Force Attack: In order to carry out an attack on the confidentiality of a VPBC transaction, the correct corresponding combination of transaction shares could be identified using brute-force searching across m different blockchains, users and different transactions per user. In addition, the particular secret sharing scheme would have to be known in order to reconstruct the initial transaction from the shares.

In order to gauge the feasibility of the attack, we can gather the following data: currently, there is an estimated number of about over 6900 public blockchains [9] available on the market at the time of this writing, with a tendency of this number to grow in the near future [9] [10]. This yields $n \leq 6900$ and $m \leq n$ for the secret sharing parameters, and futhermore, a number of $\binom{n}{m}$ transaction share combinations that need to be brute-forced. Denote by T the average number of daily transactions in the n participating blockchains. Then, there are $t = \binom{n}{m} T^m$ transaction combinations per day to be considered. The resulting data that needs processing is likely to be huge. For example, there are approximately $T \approx 300,000$ daily Bitcoin transactions [11]. On the other hand, the use of a $(m, 6900)$-secret sharing scheme might not be very feasible, and a balance between the level of provided protection and the computational effort for creating (and reconstructing) shares need to be found. This interesting question is planned to be investigated further by our research.

2) Deanonymisation Attack: Another way to attack this scheme would be to carry out deanonymisation (data-reidentification) techniques in order to identify users, frequently engaging with the same set of blockchains, in order to narrow down the number of required searches. While feasible in principle, it requires installing and monitoring of a maximum number of possible blockchain systems, up to the theoretical number of 6900, c.f. previous section. A criminal organisation or any other group of professional attackers could well cope with the demands of this attack, but it would be unlikely to be feasible for an individual.

On the other hand, any of these attacks resulting in a successful breach of confidentiality could be prevented by adding an out-of-band channel between individual users, for example using email or text message. If one of the transaction shares is transmitted on this channel, a successful attack purely based on processing the blockchain data would not be possible. As eavesdropping on the email message would be relatively easy, a further strengthening of the security using for example Pretty Good Privacy (PGP) or Secure/Multipurpose Internet Mail Extensions (S/MIME) should be implemented. While still possible for attackers with higher privilege (such as governments or technically more advanced cybercriminals), this improved method would be worthwhile, as it achieves a considerable strength of the security with a manageable overhead.

IV. System Simulation

One reason why Blockchain technology is enjoying growing popularity and rapid adoption is the availability of free implementations. The research described in this paper aims to provide a publicly available VPBC system, implemented as an interface for common blockchain implementation such as Multichain or Fabric Ledger, using a range of programming

 ISBN: 978-1-61208-818-1

languages including Java and Python. This interface will allow processing transactions prior to their sending to the individual public blockchain systems. Typically, a cryptographic technique such as secret sharing will be applied in order to implement confidentiality. Efficiency and ease of use will be taken into account.

In order to investigate the feasibility of our proposed VPBC architecture, we simulated a proof-of-concept VPBC based on leveraging two Multichain blockchain systems. The two private Multichain blockchain systems (A and B) were set up on different instances of Ubuntu 12.04 LTS servers, with node A and node B representing cryptocurrency payment and digital value exchange systems (public blockchains). Multichain provides an inter-communication Application Program Interface (API), giving access to the blockchain background application. This API was used by a separate process, implementing our Virtual Private Blockchain, where the desired transaction is generated and executed via a smart contract. We may refer to this as a (virtual) node C. The client process, which can run any of the three Linux systems or a dedicated machine, generates the smart contract, performs the splitting (or more generally, the secret sharing) of the asset and creates the terms of the individual smart contracts by initiating the payment on node A and node B. The transactions on node A and node B are verified by the blockchain, and upon successful execution of both transactions, our system will report a successful conclusion/execution of the virtual transaction.

The commands below show an automated process of asset transfer on the Multichain blockchain using the bash script command and the process builder function in the Java programming language. The first instruction launches the blockchain in the background and then, using the instruction in the second line, one is able to see connected nodes with the necessary permissions to transact with the primary node. With that information, the third and fourth instructions show available assets on all connected nodes. The last two instructions implement the asset transfer and confirm the successful execution of the transaction.

```
processBuilder.command("bash", "-c", "multichaind VPBC
-dameon;
multichain-cli VPBC listtpermissions;
multichain-cli VPBC listassets;
multichain-cli VPBC gettotalbalances;
multichain-cli VPBC sendasset 1...asset1 100;
multichain-cli VPBC gettotalbalances 0;
```

V. Related Work

In this section, a brief literature review on security overlays for social network system architectures and instant messaging protocols is given. A discussion section helps to contrast this previous work with our VPBC framework presented in this paper.

A. Virtual Private Network Overlay Architectures

Several key papers [7], [12]–[16] have introduced and established the idea of improving security features of a network system architecture by creating a higher-level architecture based on a network security protocol bearing similarities to a virtual private network. While preserving the functionality of the original system, additional benefits such as sender and recipient anonymity or message confidentiality can be implemented.

In [7], the authors introduce the notion of a Virtual Private Social Network (VPSN), achieving the goal of implementing the anonymity of user-generated content in an Online Social Network (OSN). Their terminology is motivated by the similarity to a traditional Virtual Private Network (VPN), where users of the VPSN corresponds to network devices in a VPN. An implementation based on encryption and using an out-of-band channel was reported in the follow-up work [7], where the authors describe a Firefox browser plug-in called FaceVPSN.

In [12] and later [13], a different cryptographic technique is used to implement a related goal: the idea is to use steganography to hide posts in a social network by making them "socially indistinguishable" and hence difficult to detect. The need for an out-of-band is also present in this method.

An alternative architecture based on a distributed communication protocol with n channels has been proposed in [15], combining steganography with an (m, n)-threshold secret sharing scheme, applied to the plaintext message, followed by hiding the resulting individual shares in a suitably crafted carrier-medium.

In [16], a secure channel between two OSN Friends using instant social messaging is established based on a different type of distributed steganography. This implements a security control for message content facing an untrusted OSN provider. An Android mobile app prototype implementation is described, using two instant social messaging channels (Twitter and Google+).

The idea of overlay security architectures has also been applied to insecure network protocols. In [17], a secure multichannel protocol for SMS banking is developed. The cryptographic technique of steganography is used in two different information-theoretical models, inspired by the low-entropy and high-entropy approach of [13]. The resulting protocol achieves confidentiality of an SMS-banking transaction against an untrusted GMS service provider. An extended version of the protocol [18] also provides resistance against delay and replay-attacks, using cryptographic nonces.

B. Discussion

Both the idea of security overlay architectures and the cryptographic technique of secret sharing has been the initial inspiration for the work in this paper, in terms of concept and implementation.

To our knowledge, the security overlay presented in this paper is novel and unique in the context of blockchains, and there are some subtle differences compared to the previous works: a VPBC is not serving as a security control against a centralised communication service provider (such as an OSN provider). In fact, the communication setting is decentralised right from the start and remains as such. The VPBC architecture introduces several layers of the same communication

 ISBN: 978-1-61208-818-1

model, due to the use of multiple blockchain implementations. This use of secret sharing is fundamentally different from that in [4] as, in a VPBC, shares are stored on different Blockchain implementations.

A VPBC architecture distributes the single public ledger (containing the transaction data) *vertically* onto the specific, chosen blockchain implementations while keeping the *horizontal* distribution of the public ledger as an entity, copied across all blockchain nodes, and kept in sync. Hence, a VPBC could be classified as a new type of blockchain technology bearing similarities with a Permissioned Blockchain as it is using a public ledger and a closed group of validators (the individual members of the VPBC who have to arrange membership out-of-band) while introducing a new type of ledger distribution – vertically rather than horizontally.

VI. Conclusion

In this paper, a novel Blockchain architecture is introduced by designing a security overlay, spanning across multiple Blockchain implementations. The resulting system is referred to as a Virtual Private Blockchain (VPBC) and can be interpreted as a Permissioned Blockchain with vertical (rather than horizontal) distribution of the public ledger. An evaluation of a prototype VPBC system simulation is reported.

Blockchain technology has been met with scepticism from many parties. Apart from security issues, the apparent lack of current mainstream use cases and applications, potential violations of data protection (such as the General Data Protection Regulation (GDPR)) and other shortcomings, there is also a danger of private organisations misusing data stored in private Blockchains. A VPBC might offer a solution to this problem as there is no central ledger database, offering the opportunity to exploit transaction data by a single entity for commercial purposes.

On the other hand, one drawback of the VPBC architecture is the additional overhead required for sending and validating several transactions, for each transaction on the VPBC although, in practice, this might be compensated for by the resulting security benefits. Furthermore, any VPBC – while offering attractive features in terms of confidentiality and anonymity – can also be subject of misuse. For example, illegal activities such as money laundering would be much easier to implement using a VPBC than other Blockchain architectures. As with any security solution, frequently there are ethical issues attached to its use and misuse, and developers and users alike need to remain mindful of these aspects.

In the same way as nowadays, adopters of cloud computing routinely use multiple clouds and the first multi-cloud systems have been suggested, the idea of a multi-blockchain will become more acceptable over time. Eventually, the idea of a VPBCs might become more mainstream as well. At this current moment in time, it can only be speculated what the precise future holds for the Blockchain, whether it is "virtual" or "real".

References

[1] C. Cachin *et al.*, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, no. 4, 2016.

[2] Multichain, "Stream Confidentiality," 2019, accessed 27/02/2020. [Online]. Available: https://www.multichain.com/developers/stream-confidentiality/

[3] R. K. Raman and L. R. Varshney, "Dynamic Distributed Storage for Blockchains," in *IEEE International Symposium on Information Theory - Proceedings*, 2018.

[4] H. Chen, H.-L. Wu, C.-C. Chang, and L.-S. Chen, "Light repository blockchain system with multisecret sharing for industrial big data," *Security and Communication Networks*, 2019.

[5] S. Goldfeder, J. Bonneau, R. Gennaro, and A. Narayanan, "Escrow protocols for cryptocurrencies: How to buy physical goods using bitcoin," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017.

[6] R. K. Raman and L. R. Varshney, "Distributed storage meets secret sharing on the blockchain," in *2018 Information Theory and Applications Workshop (ITA)*. IEEE, 2018, pp. 1–6.

[7] M. Conti, A. Hasani, and B. Crispo, "Virtual private social networks," 2011.

[8] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[9] J. Wanguba, "How Many Cryptocurrencies Are There In 2020," 2020, accessed 16/09/2020. [Online]. Available: https://e-cryptonews.com/how-many-cryptocurrencies-are-there-in-2020/

[10] Coin Market Cap, "All Cryptocurrencies," 2020, accessed 16/09/2020. [Online]. Available: https://coinmarketcap.com/all/views/all/

[11] Bitcoin.com, "Bitcoin Market Charts," 2020, accessed 16/09/2020. [Online]. Available: https://markets.bitcoin.com/crypto/BTC

[12] F. Beato, M. Kohlweiss, and K. Wouters, "Scramble! Your Social Network Data," in *Privacy Enhancing Technologies*, S. Fischer-Hübner and N. Hopper, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 211–225.

[13] F. Beato, E. De Cristofaro, and K. Rasmussen, *Undetectable Communication: The Online Social Networks Case*, July 2014.

[14] M. Conti, A. Hasani, and B. Crispo, "Virtual Private Social Networks and a Facebook Implementation," vol. 7, no. 3, 2013.

[15] C. Clarke, E. Pfluegel, and D. Tsaptsinos, "Confidential Communication Techniques for Virtual Private Social Networks," *2013 12th International Symposium on Distributed Computing and Applications to Business, Engineering & Science*, vol. 12, pp. 212–216, 2013.

[16] E. Pfluegel, C. Clarke, J. Randulff, D. Tsaptsinos, J. Orwell, and K. E. Khajuria, "A secure channel using social messaging for distributed low-entropy steganography," in *Cybersecurity and Privacy-Bridging the Gap*. River Publishers Series in Communications, 2017.

[17] O. Obinna, E. Pfluegel, C. A. Clarke, and M. J. Tunnicliffe, "A Multi-Channel Steganographic Protocol for Secure SMS Mobile Banking," in *The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017)*. Cambridge: IEEE, Dec. 2017.

[18] O. Obinna, E. Pfluegel, M. J. Tunnicliffe, and C. A. Clarke, "Ensuring Message Freshness in A Multi-Channel SMS Steganographic Banking Protocol," in *International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2018),*. Glasgow: IEEE, June 2018.

 ISBN: 978-1-61208-818-1