The Evolution of Privacy in the Blockchain: a Historical Survey

Sergio Marciante[0000-0001-8380-2962] and Álvaro Herrero[0000-0002-2444-5384]

Grupo de Inteligencia Computacional Aplicada (GICAP), Departamento de Ingeniería Informática, Escuela Politécnica Superior, Universidad de Burgos, Av. Cantabria s/n, 09006, Burgos, Spain.
smm1010@alu.ubu.es, ahcosio@ubu.es

Abstract. In order to store information in a decentralized context and without the presence of a guarantor authority, it is necessary to replicate the information on multiple nodes. This is the underlying idea of the blockchain, that is generating increasing interest nowadays as one of the most-promising disruptive technologies. However, the ledger is accessible to all participants and if adequate precautions are not taken, this may lead to serious privacy issues. Present paper retraces the history of blockchain with particular attention to the evolution of privacy and anonymity concerns, starting from bitcoin. Furthermore, this work presents the most popular solutions to ensure privacy in the blockchain, as well as the main cryptocurrencies that have been proposed after bitcoin to overcome this problem. A critical survey is presented classifying the approaches in mixing protocols and knowledge limitation protocols. Open challenges and future directions of research in this field are proposed.

Keywords: blockchain, ledger, distributed ledger technology, bitcoin, cryptocurrencies, privacy, anonymity, survey.

1 Introduction

In recent years there has been an increasing interest on a new technology that promises to revolutionize the world: the blockchain. This is the first time that a secure and immutable storage of information, comprising the transfer of an asset without the help of an authority as a guarantor, is a reality. As it is widely known, blockchain is a completely decentralized technology that has allowed the creation of cryptocurrencies. These digital coins are being designed to function as a medium of exchange that use advanced cryptographic functions to protect the financial transactions occurred between users/entities that use them [1]. Fueled by the growing market prices of cryptocurrencies, such as bitcoin, blockchains are attracting a lot of interest both in the academia and industry sectors.

The processing of distributed transactions has become the norm for business planning, in which each organization is administered by a single entity or only by a few partners [2]. Blockchain can be considered as a particular type of distributed databases

that stores information in data structures called blocks and that only allows the "append" operation, that is only the insertion of new blocks, leaving the previously entered data unchanged [3]. The term blockchain derives from this data structure used, in fact the transactions are grouped into blocks, with a timestamp and a hash of the previous block, using the MerkleTree method [3]. All transactions (exchange of assets) are stored in a distributed ledger and the technology that is used to store permanently transactions in each node of the network is called Distributed Ledger Technology (DLT) [4]. Attention is now being paid to differentiate blockchain from the more general DLT [4, 5], but this discussion is out of the scope of the present paper. According to acknowledged definitions, a distributed ledger is a database on different nodes, where each one of them replicates and saves an identical copy of the ledger while updating itself by sharing a set of protocols with the other nodes. So the blockchain is a distributed ledger, but not all distributed ledgers are blockchains [5].

A blockchain is said to be permissionless or public if it is open to anyone who wants to participate. As a result, any node that accepts the shared rules can access the network without any authorization. Any user has privileges over the other ones, nobody can control, modify or delete the information that is stored, and nobody can alter the protocol that determines the operation of this technology. A blockchain is said to be permissioned or private if there is a central authority that decides who can participate. In addition to deciding who is authorized to join the network, the central authority can define the rules for participation, as well as the roles and authorizations within the network.

Although the blockchain concept was conceived in 1991 [6], it was not until 2009 that bitcoin arrived. It was the first case of a cryptocurrency that have had notoriety and mass diffusion. As any other cryptocurrency, bitcoin uses a peer-to-peer (p2p) type network in which nodes are potentially located all over the world. These nodes execute collectively a shared program that performs all the functions required to permanently store in the ledger the financial transactions requested by the participating users.

Unlike traditional electronic payment systems, cryptocurrencies do not require trusted third-party organizations, such as a financial institution, to store transactions between users. As the blockchain is replicated by all the nodes of the network, being mutually suspicious, the information contained can be considered as public [7–9]. Although it relies on strong cryptographic mechanisms, the fact that the shared ledger contains the history of all the transactions that took place in a given blockchain implies a serious privacy problem. Sensitive user's information is always exposed, making it vulnerable, as anyone within the network can analyze the shared ledger and look for the target data.

On the other hand, through extensive research, it has been shown that blockchain technology is useful not only for cryptocurrencies. However, the fact that everything is transparent in a public blockchain prevents its direct use in various sectors where privacy is crucial, such as health or documents' among others. Differentiating from previous surveys on security mechanisms of the blockchain [10], the present research is focused on privacy.

As previously stated, privacy is a serious concern regarding blockchain. As a result, some solutions have been proposed so far to deal with this issue. Progress has already

been made which has led to the development of a range of technologies that try to ensure anonymity and privacy in blockchain. Present paper contains a panoramic survey of such solutions from a historical perspective. The remaining sections of the paper are organized as follows: Section 2 analyses the case of bitcoin, while Section 3 describes the main techniques that try to preserve privacy and guarantee anonymity. Finally, obtained conclusions and open challenges are explained in Section 4.

2 Bitcoin as a Case Study

In 2008, a character (under the pseudonym of "Satoshi Nakamoto") introduced the first decentralized cryptocurrency to reach mass circulation: bitcoin. There has been an increasing interest on it and at present time there are more than 18 million bitcoins [12].

The real novelty introduced in bitcoin was to make the ledger store all transactions cryptographically secure and to eliminate the problem of double spending (see below). Before bitcoin, attempts had been made to create a fully decentralized digital currency (e.g. DigiCash by David Chaum [13] and BitGold by Nick Szabo [14, 15]), but vulnerabilities were easily found and made transactions unsecure.

Bitcoin is decentralized, pseudo-anonymous, not supported by any government or other legal entity [16], which is based on a set of technologies already known for some time, but which have been put together in a completely original way. Each technology fits together with the others to form a system to exchange value and permanent storage of information without a central authority that guarantees its operation. The responsibility for the proper functioning of the system is shifted to the blockchain protocol. The network nodes communicate with each other using the bitcoin protocol through a permissionless peer-to-peer (P2P) network (ie accessible to any computer that wants to run the open source bitcoin software) [17].

In order to make a transaction, users need to create two different cryptographic keys, one public and one private, which allow them to demonstrate ownership of coins in the bitcoin network. These keys give the possibility to spend the money they have by signing transactions to a new owner. Possession of the private key, from which the public key can be derived, is the only prerequisite for spending bitcoins. Elliptic curve cryptography (ECC) is used to generate public and private key pairs [18]. Cryptography is used only to identify the user and ownership of the money, but the transactions are visible to anyone and can be viewed using a blockchain explorer [3, 19].

Security Mechanisms in Bitcoin

In order to successfully add a new block to the blockchain, miners (computers that maintain the system) must solve a cryptographic puzzle of variable difficulty named Proof of Work (PoW). This computationally difficult but easily verifiable method is used to protect from attacks of various types (DoS - Denial of Service, Sybil, etc.), as it requires complex computational work. Bitcoin uses a system that derives from Adam Back hashcash [3], which was designed to limit the sending of spam emails.

It is essential that a user can spend the possessed cryptoassets only once. A "Double Spending Attack" occurs when a user manages to spend the same set of coins at the

same time in two or more different transactions. Although the bitcoin payment verification scheme is designed to prevent such problem, it takes some time to verify a transaction. Previous research [20] has shown that it is ineffective when a transaction must be verified quickly. In the first minutes of propagating transactions to all nodes, the same funds can be used twice. This same paper pointed out for a way to detect the double transaction.

The main bitcoin vulnerabilities described in the literature are: the problem of double spending on fast payments [20], the vulnerabilities related to always ensuring at least 51% of the computing power, the security in the custody of the private key, loss of privacy in transactions, and criminals that can take advantage of pseudo-anonymity for their activities [10]. Present paper focuses on the loss of privacy in transactions, which is discussed in the following section.

3 Loss of Privacy in Transactions

All blockchains, based on the same rules as bitcoin, allow users to benefit from an arbitrary number of aliases (or addresses) to move funds. However, the complete history of all transactions is written in the blockchain ledger, that is public and is replicated on each node. It is not an easy task to analyze the data contained in the ledger, but with an adequate software (e.g. BitIodine [21]) they can produce a large number of relevant information about participating entities.

All protocols derived directly from bitcoin are known as "pseudo-anonymous" because all transactions are public and fully traced but they do not contain a direct reference to the identity of the person sending and receiving.

Since it is easy to recover the origin, destination and amount of each transaction, connecting an address to the identity of the owner is enough to completely eliminate the anonymity. In fact, after the birth of bitcoin academic research [22–24] has been carried out to show various weaknesses related to privacy in its protocols and similar ones. Trying to remain anonymous in transactions with bitcoins and similar cryptocurrencies, it is common and usual to generate a new address every time you need to receive new funds, in order to guarantee a certain level of non-connectability and anonymity. As previously explained above, this not enough. Research has stimulated the development of a range of technologies that aim to reinforce privacy and improve anonymity in blockchain technology. Part of this research aims to improve privacy in bitcoin, while others use a new blockchain that integrates new technologies.

In any case, there is a need to preserve information regarding all transactions within a ledger shared by all nodes. The approaches used to avoid the disclosure of confidential information present in each copy of the blockchain are essentially of two types: mixing protocols (see subsection 3.1) and knowledge limitation protocols (see subsection 3.2).

3.1 Mixing Protocols for Bitcoin

Mixing protocols have been developed to combine the transactions of different users, making almost impossible to trace all the amounts sent. In most cases, all the funds of

different users are brought together to a single aggregation point and then divided and mixed into smaller parts. Hence the name "mixer".

This section focuses on the protocols that can be used in blockchains similar to bitcoin. These protocols offered by online suppliers (e.g. https://cryptalker.com/best-bitcoin-tumbler/) divide the funds into many smaller parts in order to convey them to a completely new address, thus breaking the connection with the old address of the same user. However, the mixers are separate structures from the blockchain entrusted to private entities that know the addresses of the initial owners and the final addresses. Therefore, these entities could resell the information in their possession. In any case, the presence of the supplier, which represents a third party in which to place trust, introduces a mechanism to avoid the decentralized nature of the blockchain. The most relevant mixing protocols are described below.

Coinjoin

In the academic field, a lot of research has been carried out with the aim of obfuscating the links between the addresses present in the blockchain, being CoinJoin [25] one of the first approaches. In this protocol, multiple users combine their transactions into one larger transaction, mixing and negotiating currency simultaneously, in one step. However, it is necessary a set of additional mixing rules that can change the incoming and outgoing amounts, so anyone who wants to attack the system cannot derive individual transactions [26].

CoinShuffle

A protocol that decisively improves the CoinJoin-based approach and that allows for a better degree of anonymity is called CoinShuffle [27]. This protocol does not require third parties (reliable, responsible or untrusted) and is fully compatible with the current bitcoin system and all derivative ones. Furthermore, it only introduces a small communication overhead for its users, completely avoiding the additional anonymization costs and minimizing the general calculation and communication costs, even when the number of participants in CoinShuffle is high (around 50).

This latter protocol has undergone further evolutions over time: (i) P2P Mixing and Unlinkable Bitcoin Transactions [28], (ii) ValueShuffle: Mixing Confidential Transactions for Comprehensive Transaction Privacy in bitcoin [11], (iii) SecureCoin: A Robust Secure and Efficient Protocol for Anonymous Bitcoin Ecosystem [29], (iv) TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub [30].

3.2 The Knowledge Limitation Protocols

When it is possible to design a completely new blockchain, more efficient and safer technologies which can make very difficult to trace the actual users of the blockchains can be introduced. In this context, since most of the research on privacy has been developed connected to cryptocurrencies, research on anonymity in the blockchain is based on the analysis of the different technologies introduced for cryptocurrencies. Therefore, although this work intends to treat privacy in the blockchain in a generic way, and regardless of financial use, this section focuses on the various technologies developed for the privacy of the so-called Altcoins, which represent cryptocurrencies other than bitcoin.

Zerocoin

The first new project of a protocol aimed at improving privacy is Zerocoin [31], an extension of the bitcoin protocol designed to improve anonymity in transactions using zero-knowledge tests that allow confirming the validity of encrypted transactions. This protocol was used for the implementation of a new cryptocurrency, Zcoin (XZC) [32]. It is claimed that this new property, the zero-knowledge test, could allow the creation and design of blockchains in many other areas besides that of cryptocurrencies. However, the Zerocoin protocol has some limitations. From the system point of view, it is necessary to create a soft fork in bitcoin to take into account the changes to the protocol. From the protocol point of view, the calculated zero-knowledge test generates large cryptographic signatures that weigh down the blockchain. In addition, other problems were evaluated in subsequent research which were solved with the following protocol: Zerocash.

Zerocash

The Zerocash protocol [33] takes advantage of recent advances in the area of zero-knowledge testing. In particular, it uses zk-SNARK technology (zero-knowledge Succinct Non-interactive ARguments of Knowledge) [34] and, compared to the previous ZeroCoin protocol, it introduces several updates, such as the 97.7% reduction in the size of the transactions that transfer currency and 98.6% reduction in verification time.

Furthermore, it allows anonymous transactions with variable amounts and direct payments to a fixed address without any interaction with the end user, improving both functionality, as it also hides the source address and not only the destination address, as well as efficiency, less space for each transaction and less processing time.

Zcash (ZEC)

The first currency to use the zk-SNARK system with the aim of providing a certain degree of privacy to the end user is called Zcash and was launched on October 2016 [35]. This was developed by the same Zerocoin protocol development team (ZECC - Zerocoin Electric Coin Firm) and allows users to verify a transaction without having to expose their public key and, consequently, be identified. Transactions do not reveal information on the origin, destination and amount of payments, they are also concise and easy to verify, but setting the initial parameters is a complicated process that will ultimately release two keys: the "test key" and the "verification key".

Zcash is one of the few cryptocurrencies supported by highly valued academic research from a security perspective (e.g. [31, 33]). In fact, the technology used by Zcash offers strong guarantees about anonymity security. But despite the theoretical privacy guarantees, the designers' choice to not request that all transactions have to take place in protected mode allows, in part, traceability.

There are two types of addresses available in Zcash: Z-address (private address) and T-address (transparent address). Z-addresses are based on zk-SNARK and provide privacy protection, while T-addresses are similar to those of bitcoin [36].

In addition, it is required that all new generation coins must go through a z-address before they can be spent, thus ensuring that all coins have been shielded at least once.

However, if examine the Zcash ledger you notice that the vast majority of transactions are public, use t-addresses, the so-called transparent transactions. Until August 2018, transactions that had used z-addresses were only around 15% of the total and, in

addition, these protected transactions involved only 3.6% of the total monetary supply. In fact, the majority of Zcash users do not use Z-type addresses [37].

Since most of transactions in Zcash take place using type T addresses, they reveal the addresses of both senders and recipients and the amount sent, thus limiting mixing with other addresses to a very small set compared to all transactions and, consequently, reduce considerably the set of anonymous addresses, where is possible to develop heuristic algorithms based on usage models. Through experimental data, it has been deduced that is possible to trace some users who have had a behavior, in transactions, similar to the initial hypotheses envisaged by the researchers also due to the lack of a native protocol that hides the IP address of the end user.

However, despite the final considerations, the zk-SNARK system proved to be mathematically correct and every data is always deduced from other considerations that come from transparent transactions [38].

Horizen (ZEN)

Zcash has contributed to numerous forks that have risen to different cryptocurrencies which use the same system (zk-SNARK) to avoid exposing their public key and, therefore, guaranteeing the anonymity of users. The youngest cryptocurrency is Horizen (formerly ZenCash) which is a fork of Zclassic, itself a fork of Zcash. Horizen exclude one of the most controversial points about Zcash: the founder's tax.

All cryptocurrencies that use PoW reward the computer (miner) who has found the solution to a puzzle, according to a predefined scheme, with the creation of new money. In the case of Zcash about 20% of all the rewards for miners are sent to the address of the company that developed and maintains this cryptocurrency. This percentage is called "Founders' Reward" [37] or " Founder's tax ".

Monero (XMR)

In 2012 it was released the first cryptocurrency to implement Cryptonote technology [39], called Bytecoin. Monero was created in April 2014 as a fork of Bytecoin [40], focusing on privacy and fungibility. Ir order to do that, it creates a tarnished public ledger, in whose stored transactions it is difficult to establish the origin, destination, and amount. To guarantee privacy, anonymity, and fungibility, Monero uses different technologies that complement each other with acceptable results [41, 42].

In fact, Monero is constantly evolving. The protocol has undergone and continues to have numerous hard forks which improve it in terms of privacy and which make PoW difficult to be implemented in an Application Specific Integrated Circuit (ASIC). In particular, the way in which transactions are chosen to be part of the "Mixin" (the minimum number of transactions to be mixed [43]) has been improved and there has been a further improvement when all transactions have been made private by default .

To guarantee privacy and anonymity Monero tries to meet two criteria: untraceability (for every incoming transaction all possible senders are equally likely) and unlinkability (for two outgoing transactions it is impossible to prove that they are sent to the same person) [39]. Untraceability concerns the protection of the sender and is achieved by using the ring signature. Unlinkability concerns the protection of the receiver and is ensured using stealth addresses. Both untraceability and unlinkability are included in the CryptoNote 2.0 [39] protocol as a system target.

In 1991, Chaum and Van Heyst introduced a new class of signature schemes known as group signatures [44]. They require a trusted entity (group manager), which groups a subset of users. The group manager provides each member of the group with a pair of keys (one private and the other public) so as to allow any member of the group to sign messages anonymously. This group signature proposal allowed the formalization of the model used in Monero: the ring signatures. Ring signatures allow Monero to specify a set of possible signatories without revealing which member actually produced the signature, without resorting to an almighty group manager. The model works without any centralized coordination and there is no predefined group of users. Any user can choose any set of possible signatories, including himself, and sign messages using his private key and the others' public key, without obtaining their approval or assistance [45].

To ensure unlinkability in Monero, all transactions use a single disposable temporary address to avoid recording the recipient's wallet address on the blockchain. These temporary addresses are also called "stealth addresses" and serve to ensure that two transactions remain unconnectable; it is not possible to demonstrate that they are destined for the same entity. Even if a recipient publishes its address to receive funds from many senders, each sender's wallet will generate a single stealth address that will be stored in the ledger. Hence, the real address will never be referenced directly in a transaction, as stealth addresses do not provide any information about the recipient. Each stealth address is generated from a public address when creating a new transaction.

Despite all these Monero technologies, it is possible to perform statistical analyses on the blockchain based on the amounts sent, which could allow an intelligent opponent to group and use them for further investigation. In order to hide the transaction amounts, the Ring Confidential Transactions (RingCT) [47] technology has been implemented in Monero. It keeps this sensitive information private, allowing the sender to demonstrate that it has enough resources for the transaction to be carried out without detecting the value of tele amount. This is possible thanks to cryptographic commitments and range proofs. In accordance with Monero policy of enforcing privacy by default, RingCT has become mandatory for all Monero transactions after September 2017.

Kovri

As an IP address uniquely identifies the host connected to a computer network, the possibility of being able to link a transaction to an IP address could frustrate all the technology that has been exposed so far. Any node that receives the transaction may be able to identify the physical location of the sender. With other privacy features it makes it difficult to link transactions to data stored in the blockchain, but it can be seen that that multiple transactions come from the same IP address and connect them.

Kovri is a Monero feature created to protect the sender of a transaction by hiding its IP address and physical location. This routing technology is designed to obscure transmission sources that extends the Invisible Internet Project technology [48]. Kovri will soon be included in subsequent versions of Monero and therefore used in all transactions as part of Monero's privacy policy by default. In addition, the Monero community is developing this lightweight security-focused software with a general open source implementation and common APIs, so that it can also be used for other applications.

4 Conclusions

The present paper analyzes the evolution of blockchain focusing on privacy and anonymity. Particular attention has been paid to the storage mechanisms and cryptocurrencies. The main technologies aimed at maintaining privacy and anonymity while using a distributed ledger have been discussed and compared. Most of the previous research on privacy has been developed with reference to cryptocurrencies. However, scant attention has been devoted so far to anonymity in the blockchain.

It is worth mentioning that cryptocurrencies, even if little known, have tried to solve the problem of privacy and anonymity with new technologies. These solutions try to solve not only the privacy problem but also that of energy consumption to maintain the system (e.g. Dash [49]).

When analyzing academic research on the vulnerabilities of Zcash and Monero, it can be seen that researchers are now focusing on the weakest elements of these cryptocurrencies. Changes have been proposed in zk-SNARK technology to increase its efficiency without questioning the quality of the protocol. When trying to attack the Monero cryptocurrency, it is never done by directly attacking the group of technologies examined before (ring signatures, stealth addresses, RingCT). This is probably because researchers do not believe that the weakest link in the system lies within these technologies. In Zcash the vulnerabilities were mainly researched in the massive use by users of addresses and transactions not obfuscated by the zk-SNARK protocol, while in Monero the searches to identify users are now more focused on tracing IP addresses.

All systems always have a weaker link that does not depend on a single technology, but on all the technologies that compose them. This has also been well understood by the Monero development group which, for this reason, is slowly introducing new technologies that can maintain anonymity at every level of communication and memorization. In fact, since some research evidence has shown that the weakest link is represented by tracking users through their IP addresses, the Monero development team has responded by starting to develop Kovri technology.

Finally, it can be concluded that the problems still open are linked to a continuous improvement of the existing protocols and in finding new synergies of the various protocols in a single system without creating weak points in the border points. Even for future use in mobile devices, the optimization of the various protocols is also very important to improve the overall system performance and reducing the propagation time and the size of the blocks, while security is still guaranteed.

References

1. Yuan, Y., Wang, F.: Blockchain and Cryptocurrencies: Model, Techniques, and Applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 48, 1421–1428 (2018). https://doi.org/10.1109/TSMC.2018.2854904.
2. Minsky, N.: Decentralized Governance of Distributed Systems via Interaction Control. In: Lecture Notes in Computer Science. pp. 374–400. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29414-3_20.

3. Antonopoulos, A.: Mastering Bitcoin: Programming the Open Blockchain (2ed.). O'Reilly Media, Inc. (2017).
4. Chowdhury, M., Colman, A., Kabir, A., Han, J., Sarda, P.: Blockchain Versus Database: A Critical Analysis. In: 12th IEEE International Conference On Big Data Science And Engineering. pp. 1348–1353. IEEE, New York, NY, USA (2018). https://doi.org/10.1109/TrustCom/BigDataSE.2018.00186.
5. Lange, M., Leiter, C., Alt, R.: Defining and Delimitating Distributed Ledger Technology: Results of a Structured Literature Analysis. In: Di Ciccio, C. (ed.) BPM 2019. pp. 43–54. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30429-4_4.
6. Haber, S., Stornetta, W.S.: How to time-stamp a digital document. Journal of Cryptology. 3, 99–111 (1991). https://doi.org/10.1007/BF00196791.
7. Bleumer, G.: Chaum Blind Signature Scheme. In: van Tilborg, H.C.A. (ed.) Encyclopedia of Cryptography and Security. pp. 74–75. Springer US, Boston, MA (2005). https://doi.org/10.1007/0-387-23483-7_57.
8. Camenisch, J., Hohenberger, S., Lysyanskaya, A.: Compact E-Cash. In: Cramer, R. (ed.) Advances in Cryptology – EUROCRYPT 2005. pp. 302–321. Springer Berlin Heidelberg, Berlin, Heidelberg (2005). https://doi.org/10.1007/11426639_18.
9. Sander, T., Ta-Shma, A.: Auditable, Anonymous Electronic Cash Extended Abstract. In: Advances in Cryptology — CRYPTO' 99. pp. 555–572. Springer Berlin Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_35.
10. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A Survey on the Security of Blockchain Systems. Future Generation Computer Systems. (2017). https://doi.org/10.1016/j.future.2017.08.020.
11. Ruffing, T., Moreno-Sanchez, P.: ValueShuffle: Mixing Confidential Transactions for Comprehensive Transaction Privacy in Bitcoin. In: Financial Cryptography and Data Security. pp. 133–154 (2017). https://doi.org/10.1007/978-3-319-70278-0_8.
12. Stimolo, S.: Stimolo, S. 2019. 18 million mined bitcoins in total. Only 3 million remain, https://en.cryptonomist.ch/2019/10/19/18-million-mined-bitcoins-in-total/, last accessed 2020/02/20.
13. Chaum, D.: Blind Signatures for Untraceable Payments. In: Chaum, D., Rivest, R.L., and Sherman, A.T. (eds.) Advances in Cryptology. pp. 199–203. Springer US, Boston, MA (1983).
14. Szabo, N.: Bit gold, http://unenumerated.blogspot.com/2005/12/bit-gold.html, last accessed 2020/02/20.
15. Tschorsch, F., Scheuermann, B.: Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys Tutorials. 18, 2084–2123 (2016).
16. Grinberg, R.: Bitcoin: An Innovative Alternative Digital Currency. Hastings Science & Technology Law Journal. 4, (2011).
17. Pilkington, M.: Blockchain Technology: Principles and Applications. Edward Elgar (2016). https://doi.org/10.4337/9781784717766.00019.

18. Bos, J.W., Halderman, J.A., Heninger, N., Moore, J., Naehrig, M., Wustrow, E.: Elliptic curve cryptography in practice. In: International Conference on Financial Cryptography and Data Security. pp. 157–175. Springer (2014). https://doi.org/10.1007/978-3-662-45472-5_11.
19. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Manubot (2019).
20. Karame, G., Androulaki, E., Capkun, S.: Double-spending fast payments in Bitcoin. In: Proceedings of the ACM Conference on Computer and Communications Security. pp. 906–917 (2012). https://doi.org/10.1145/2382196.2382292.
21. Spagnuolo, M., Maggi, F., Zanero, S.: BitIodine: Extracting Intelligence from the Bitcoin Network. In: Financial Cryptography and Data Security. pp. 457–468. Springer Berlin Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_29.
22. Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better—how to make bitcoin a better currency. In: International conference on financial cryptography and data security. pp. 399–414. Springer (2012). https://doi.org/10.1007/978-3-642-32946-3_29.
23. Halpin, H., Piekarska, M.: Introduction to Security and Privacy on the Blockchain. In: 2017 EuroS&PW. pp. 1–3. , Paris (2017). https://doi.org/10.1109/EuroSPW.2017.43.
24. Karame, G., Androulaki, E., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating User Privacy in Bitcoin. In: International Conference on Financial Cryptography and Data Security. pp. 34–51. Springer Berlin Heidelberg, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39884-1_4.
25. Maxwell, G.: CoinJoin: Bitcoin privacy for the real world, https://bitcointalk.org/index.php?topic=279249, last accessed 2020/02/22.
26. Maurer, F., Neudecker, T., Florian, M.: Anonymous CoinJoin Transactions with Arbitrary Values. In: Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 522–529. IEEE, Sydney, NSW, Australia (2017). https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.280.
27. Ruffing, T., Moreno-Sanchez, P., Kate, A.: CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In: European Symposium on Research in Computer Security. Springer (2014). https://doi.org/10.1007/978-3-319-11212-1_20.
28. Ruffing, T., Moreno-Sanchez, P., Kate, A.: P2P Mixing and Unlinkable Bitcoin Transactions. In: Network and Distributed System Security Symposium (NDSS) (2017). https://doi.org/10.14722/ndss.2017.23415.
29. Ibrahim, M.: SecureCoin: A Robust Secure and Efficient Protocol for Anonymous Bitcoin Ecosystem. International Journal of Network Security. 19, 295–312 (2017). https://doi.org/10.6633/IJNS.201703.19(2).14.
30. Heilman, E., AlShenibr, L., Baldimtsi, F., Scafuro, A., Goldberg, S.: TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub. In: The Network and Distributed System Security Symposium (NDSS) (2017). https://doi.org/10.14722/ndss.2017.23086.
31. Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In: Proceedings - IEEE Symposium on Security and Privacy. pp. 397–411 (2013). https://doi.org/10.1109/SP.2013.34.

32. Poramin, I.: ZCoin - Academic papers, https://zcoin.io/tech/, last accessed 2020/02/20.
33. Ben-sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized Anonymous Payments from Bitcoin. In: IEEE Symposium on Security and Privacy. pp. 459–474. IEEE (2014). https://doi.org/10.1109/SP.2014.36.
34. Groth, J.: Short Pairing-Based Non-interactive Zero-Knowledge Arguments. In: ASIACRYPT 2010. pp. 321–340. Springer Berlin Heidelberg (2010). https://doi.org/10.1007/978-3-642-17373-8_19.
35. Electric Coin Company: Zcash - Network Information, https://z.cash/upgrade/, last accessed 2020/02/06.
36. Electric Coin Company: Zcash - How It Works, https://z.cash/technology, last accessed 2020/01/10.
37. Hopwood, D., Bowe, S., Hornby, T., Wilcox, N.: Zcash protocol specification. GitHub: San Francisco, CA, USA. (2016).
38. Kappos, G., Yousaf, H., Maller, M., Meiklejohn, S.: An Empirical Analysis of Anonymity in Zcash. In: 27th USENIX Security Symposium. USENIX Association, Baltimore, MD, USA (2018).
39. Van Saberhagen, N.: CryptoNote v 2.0. cryptonote. 1, (2013).
40. Alonso, K.M., koe: Zero to Monero: First Edition, https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf, (2018).
41. Alonso, K.M., Herrera-Joancomartí, J.: Monero - Privacy in the Blockchain. IACR Cryptology ePrint Archive. 2018, 535 (2018).
42. SerHack: Mastering Monero Book, https://github.com/monerobook/monerobook, last accessed 2020/05/08.
43. Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Shashvat, S., Hogan Kyle, Hennessey, Miller, A., Narayanan, A., Christin, N.: An Empirical Analysis of Traceability in the Monero Blockchain. Proceedings on Privacy Enhancing Technologies. 2018, 143–163 (2018). https://doi.org/10.1515/popets-2018-0025.
44. Chaum, D., Van Heyst, E.: Group signatures. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 257–265. Springer (1991).
45. Rivest, R., Shamir, A., Tauman, Y.: How to Leak a Secret. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 552–565. Springer (2001). https://doi.org/10.1007/3-540-45682-1_32.
47. Noether, S., Mackenzie, A., Lab, T.: Ring Confidential Transactions. Ledger. 1, 1–18 (2016). https://doi.org/10.5195/LEDGER.2016.34.
48. Astolfi, F., Kroese, J., Van Oorschot, J.: I2P-The Invisible Internet Project. Leiden University Web Technology Report. (2015).
49. Marley, N.: Dash whitepaper (23 Aug 2018), https://github.com/dashpay/dash/wiki/Whitepaper, last accessed 2020/02/20.