Studying Bitcoin privacy attacks and their Impact on Bitcoin-based Identity Methods

Simin Ghesmati[1,2], Walid Fdhila[1,3], and Edgar Weippl[1,3]

[1] SBA research, Vienna, Austria
[2] Vienna University of technology, Vienna, Austria
[3] University of Vienna, Vienna, Austria
(firstletterfirstname)(lastname)@sba-research.org,

Abstract. The Bitcoin blockchain was the first publicly verifiable, and distributed ledger, where it is possible for everyone to download and check the full history of all data records from the genesis block. These properties lead to the emergence of new types of applications and the redesign of traditional systems that no longer respond to current business needs (e.g., transparency, protection against censorship, decentralization). One particular application is the use of blockchain technology to enable decentralized and self-sovereign identities including new mechanisms for creating, resolving, and revoking them. The public availability of data records has, in turn, paved the way for new kinds of attacks that combine sophisticated heuristics with auxiliary information to compromise users' privacy and deanonymize their identities. In this paper, we review and categorize Bitcoin privacy attacks, investigate their impact on one of the Bitcoin-based identity methods namely did:btcr, and analyze and discuss its privacy properties.

Key words: Decentralized identifier, DID, privacy, BTCR, blockchain, Bitcoin

1 Introduction

Bitcoin blockchain [1] is an immutable tamper-proof distributed ledger, where addresses are used as pseudonyms (hashes of public keys), and eventually associated with amounts of bitcoins that can be redeemed using the corresponding private keys. Besides cyrptocurrencies, blockchain technology has enabled a large number of new applications that range from coordinating and monitoring cross-organizational business processes [2, 3, 4] to designing new methods for distributed identity management [5, 6]. Business process automation, for example, requires that the different actors (e.g., customers, employees, business partners), resources, and services interact with each other in a trusted manner. This trustworthy communication, in turn, requires that entities can establish trusted communication channels, with certitude about the authenticity of the entities they are interacting with. In this regard, identity continues to play a primordial role as an enabler of such trustworthy communications. Identity is a collection of data, which defines the attributes of a subject, e.g., cryptographic

material for establishing communication (public key), verification methods for proving identity ownership, or service endpoints. Traditional systems often relied on isolated, centralized or federated architectures to manage identities. While in an isolated model each third party service/business is itself the identity provider IDP (i.e., responsible for storing and managing identities data), centralized and federated models both delegate identity management to separate IDPs, that work in isolation or federation, respectively. However, recent breaches (e.g., 500 million Facebook accounts, and 700 million LinkedIn accounts leaked[1]) exposed the limits of such systems and called for more decentralized models that give users control over their data. With the advent of blockchain, it became possible to create and resolve decentralized identifiers (DIDs) without having to rely on centralized authorities. This opened the door for a multitude of proposals (DID methods) that enable decentralized creation, resolution, update, and revocation of DIDs. It is noteworthy to point out that these DID methods rely on different blockchain technologies and architectural designs. One of the first proposed DID methods specifically use the Bitcoin blockchain and is called did:btcr [7].

In our previous research [8], we demonstrated how it is possible to combine sophisticated heuristics with auxiliary information (e.g. address tag databases) to correlate Bitcoin addresses with their corresponding real identities, which may put users' privacy at risk. In this paper, we review and categorize privacy attacks on the Bitcoin blockchain, which not only may reveal the links between addresses and real-world identities, but also correlate between different identities. Next, we address Bitcoin privacy attacks' impact on the DID method did:btcr. To this end, we adopted the terminology from RFC 6973 [9]. The contributions of the paper are in two folds: (i) Categorizing Bitcoin privacy attacks, and (ii) Investigation of the privacy issues in did:btcr.
The remainder of the paper is organized as follows: In Section 2, we describe the main concepts, while in Section 3 we introduce the methodology, categorize Bitcoin privacy attacks and explain how they may impact users' privacy. In Section 4, we investigate privacy issues in DiD BTCR method, and in Section 5, we conclude the paper and provide the future work.

2 Background

2.1 Bitcoin

In Bitcoin, transactions consist of input and output addresses. The input refers to the output of one of the previous transactions. A mining fee is often included as part of the transaction to increase its chance of being considered by miners. This explains why the sum of the inputs should always be larger than the sum of the outputs. Additionally, whenever the sum of the inputs plus the fee is larger than the amount that should be spent, a fresh address, namely a change address is created to send the remainder to the sender [10]. Figure 1 illustrates a

[1] https://haveibeenpwned.com/

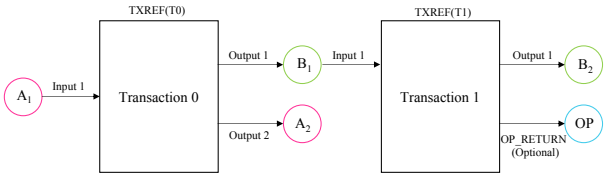

Fig. 1. Bitcoin transactions

simplified form of Bitcoin transactions. In the first transaction, Alice (A_1) sends the bitcoins to Bob (B_1) and gets the remainder back to her change address (A_2). In the following transaction, Bob sends the bitcoins from his address (B_1) to his another address (B_2), while additionally specifying an optional OP_RETURN output. OP_RETURN is an opcode that enables embedding a small amount of data within a transaction.

Bitcoin is a publicly available ledger, and therefore, all the transaction details including sender's and recipient's addresses, the values of transactions, and corresponding timestamps remain visible and can be checked by anyone. Despite the nice properties of blockchain, it in turn, created a niche for attackers to exploit such available data for malicious purposes. Previous and ongoing research has identified several privacy issues that can reveal identities and effectively find the relationships between Bitcoin addresses and the corresponding identities [11, 12, 13, 14].

2.2 Decentralized identifiers (DIDs)

Entities, including users and organizations, utilize global unique identifiers for a variety of use cases such as telephone numbers, ID numbers or URLs. These identifiers are often issued and managed by central authorities. Previous data breaches, however, diminished trust in such centralized architecture and called for decentralized management of identities, where users become their own identity providers. As a result, blockchain-based decentralized identifiers [15] have been proposed, which rely on blockchain and additional cryptographic techniques to prove identifiers' ownership without having to rely on a trusted entity.

A **decentralized identifier (DID)** is a string that includes three main parts: the scheme, the DID method, and the DID method identifier, which should be unique within the DID method. The syntax according to the W3C recommendation [2] is as follows.
$Scheme : DIDmethod : DID\_method\_identifier$
DIDs are usually associated with **DID documents**; i.e., documents that contain information about the verification methods (e.g. cryptographic public keys) and the service endpoints required to interact with the DID subjects. The DID subject is the entity that is identified by the DID, and can be a person, an object or an organization. In addition to the underlying infrastructure (e.g., Bitcoin,

[2] https://www.w3.org/TR/2021/CRD-did-core-20210609/

Ethereum), a **DID method** defines how DIDs are created, resolved, updated, and revoked.
While DIDs in conjunction with DID documents enable creating trustworthy communications (how to communicate with identity owners), **verifiable credentials (VCs)** represent information and claims about identity owners (e.g., name, age, diplomas) [16]. These credentials can be issued by different issuers (e.g., university, employer), and can be cryptographically verified by any third party without having to contact the corresponding issuers.

2.3 BTCR

The BTCR method [7] uses the Bitcoin blockchain to manage DIDs. In did:btcr, DIDs are created using the transaction references $TXRef$, only known once transactions are confirmed. The following is an example of a did:btcr (adopted from [7]), where did is the scheme part, btcr is the DID method part, and xyv2-xzpq-q9wa-p7t is the identifier which is the transaction reference. Transaction reference follows BIP 0136, which encodes transactions positions (including the chain, block height, and transaction index) in the Bitcoin blockchain:
$did : btcr : xyv2 - xzpq - q9wa - p7t$
As aforementioned, creating a DID using did:btcr is achieved by simply creating a Bitcoin transaction. This DID creation transaction may or not refer to a URL that holds a DID document using the OP_RETURN construct. The latter may be stored on a separate storage, e.g., third party server (at the time of writing, IPFS was not supported). In case, the first transaction does not specify an OP_RETURN, a DID document by default is created from the transaction itself. Next operations on the DID (e.g. update transactions) must, however, specify OP_RETURN, otherwise, the DID is considered revoked [17]. An update operation for example, consists of updating the did document and creating new transaction that consumes all previous UTXOs, and that embeds the new link to the updated DID document in the OP_RETURN.

Again, a DID document contains cryptographic material and methods for establishing communication with the DID controller. A verifiable credential issuer (e.g., a university) can then publish their DID, and use it to sign credentials (e.g. diplomas). A verifier (e.g., employer) can check the authenticity of the VC, by resolving the DID that issued the VC, and verifying that it was not revoked using the Bitcoin blockchain. Therefore, the verifier does not have to communicate with the issuer for checking the validity of a given VC, which helps avoid linkability.

3 Bitcoin privacy attacks

3.1 Research method

This section describes the methodology used for collecting and selecting relevant literature, which follows four main steps; (i) research questions identification (cf.

Section 1), (ii) literature search, (iii) literature selection, and (iv) data extraction. **Literature Search.** Collecting relevant literature was carried out through triangulation of a variety of search methods such as manual search and citation search. Scientific databases such as DBLP, IEEE xplore, ACM, usenix and Springer as well as top conferences in the fields of Distributed ledger technology and decentralized identity were searched. **Search Query.** The queries that were employed for searching relevant literature items include and combine the following keywords: "Bitcoin", "blockchain", "distributed ledger technology", "DLT", "privacy", "attack(s)", "anonymity", "deanonymization", "correlation" and "linkability". Only papers from 2009 to 2021 were considered. **Literature Selection.** The search resulted in 479 papers, from which unrelated papers were dropped based on titles and abstracts. Another filtering round based on fast screening of remaining papers resulted in 14 papers that focus on privacy attacks in Bitcoin blockchain. Table 1 lists the venues that were identified ordered by their h5-index and h5-median.

A number of the selected studies have identified privacy attacks, which may reveal links between identities and the Bitcoin addresses. In the following, we categorize and explain the possible attacks that have been applied in the selected papers (Table 2). Based on the paper purposes we categorized the selected papers in five categories including privacy challenges, classification, illicit activities (tracking Bitcoin usage in dark web, ransomware and ponzi schemes), link pseudonyms to IPs, and pattern detection (to find specific patterns related to users behavior in trading systems and remuneration pattern). Some of the papers proposed attacks not specific to Bitcoin. In this paper, we only consider analyzing privacy attacks in the Bitcoin blockchain as we only address Bitcoin privacy attacks in BTCR. Additionally, we employ the four main categories of privacy attacks as identified in [18]; (i) heuristics, (ii) side channel attacks, (iii) flow analysis, and (iv) auxiliary information , which will be explained in next sections.

	Publication	h5-index	h5-median	Publisher
1	ACM Symposium on Computer and Communications Security	88	140	ACM
2	IEEE Transactions on Information Forensics and Security	86	118	IEEE
3	USENIX Security Symposium	80	129	USENIX
4	IEEE Symposium on Security and Privacy	74	142	IEEE
5	Network and Distributed System Security Symposium (NDSS)	71	111	NDSS
6	International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT)	61	89	SPRINGER
7	Computers & Security	59	90	ELSEVIER
8	IEEE Transactions on Dependable and Secure Computing	54	77	IEEE
9	International Cryptology Conference (CRYPTO)	52	87	SPRINGER
10	International Conference on Financial Cryptography and Data Security	46	74	SPRINGER
11	International Conference on The Theory and Application of Cryptology and Information Security (ASIACRYPT)	42	61	SPRINGER
12	Security and Communication Networks	40	51	Wiley
13	Theory of Cryptography	38	58	SPRINGER
14	ACM on Asia Conference on Computer and Communications Security	37	55	ACM
15	Proceedings on Privacy Enhancing Technologies	35	55	
16	IEEE European Symposium on Security and Privacy	34	74	IEEE
17	Designs, Codes and Cryptography	34	50	SPRINGER
18	European Conference on Research in Computer Security	34	43	SPRINGER
19	IEEE Security & Privacy	31	53	IEEE
20	Journal of Information Security and Applications	31	40	ELSEVIER

Table 1. Computer security and cryptography top publications

Category	Paper	Year Publication	Purpose	Blockchain
Privacy challenges	[19]	2018 IEEE S&P	Access privacy challenges	BTC, ZEC
Classification	[20]	2014 FC	User classification	BTC
	[21]	2020 USENIX	Analysis tool	BTC, BCH, BSV, LTC, and ZEC
Illicit activites	[22]	2018 Computer & Security	Tracking ransomware	
	[23]	2018 IEEE S&P	Tracking ransomware	BTC
	[24]	2019 NDSS	Crypto in dark web	BTC
	[25]	2020 Asia CCS	MMM ponzi detection	BTC
Link Pseudonyms to IPs	[26]	2014 FC	Link Pseudonyms to IPs	BTC
	[27]	2014 CCS	Link Pseudonyms to IPS	BTC
	[28]	2017 FC	Clustering heuristics+network layer info	BTC
	[11]	2019 EuroS&P	Link Pseudonyms to IPs	BTC, ZEC, XMR, Dash
Pattern detection	[12]	2017 EuroS&P	Remuneration detection	BTC
	[13]	2019 CCS	Tracing trading transactions	BTC
	[14]	2019 USENIX	Tracing trading transactions	ETH, BTC, LTC, BCH, Doge, Dash, ETC, ZEC

Table 2. Selected papers

3.2 Bitcoin blockchain heuristics

Table 3 summarizes heuristics that were applied to the Bitcoin protocol to identify relationships between addresses (common input ownership, change address detection, address reuse, single input single output, and specific patterns). One of the heuristics (Cluster growth) prevents false positives [21, 10].

Multi/common input ownership. The heuristic assumes that the inputs of a transaction are controlled by the same entity and associates all the inputs to one entity. Since the input of a transaction can only be redeemed by providing its signature, it is unlikely that different users join to create a transaction [18]. Figure 2 illustrates the heuristic, where it is assumed that all the addresses (A_1, A_2, A_3) are controlled by one entity (Alice). To prevent false positives, CoinJoin transactions are excluded in the analysis [21]. CoinJoin [29] is one of the most prominent mixing techniques that has been adopted in practice. In mixing techniques, users mix their unspent transaction outputs (UTXOs) with the other users' UTXOs to obfuscate the relationships between the inputs and outputs. In CoinJoin. the users jointly create and sign a transaction to obfuscate the common input ownership heuristic. CoinJoin transactions should be created in the form of the equal-size output to prevent linking the input and output addresses which makes them distinguishable in the blockchain.

	Multi-input	Change address	Address-reuse	Single in-single out	Cluster growth	Patterns
[20]	✓	✓				
[19]						
[21]	✓(excluding CoinJoin)	✓		✓		
[22]	✓	✓				
[23]	✓(excluding CoinJoin)					
[24]	✓(excluding CoinJoin)	✓			✓	
[25]						
[26]						
[27]						
[28]	✓	✓			✓	
[11]						
[12]						✓Remuneration profile
[13]	✓					
[14]	✓		✓			✓Common relationship

Table 3. Bitcoin blockchain heuristics

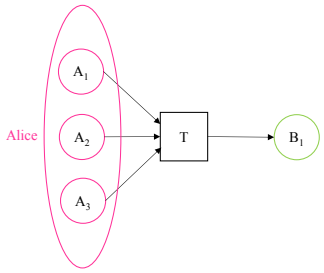

Fig. 2. Multi/common input ownership heuristic

Change address. The heuristic assumes that the change address of a transaction is controlled by the owner of the inputs [10]. The following is a list of common heuristics that are employed to identify change addresses.

- *Fresh address:* A fresh address output can be a change address if the other address appeared before in the blockchain [10].
- *Script types:* The only output with a similar script, if all the inputs have similar scripts (e.g., Pay-to-PubkeyHash (P2PKH), Pay-to-Script-Hash(P2SH)) can be a change address [30].
- *Same input and output:* An input address that is also an output address of a transaction can be a change address [30].
- *Optimal change:* An output that has a smaller amount than all the inputs can be a change address [30].
- *Round numbers:* The non-round number output value can be a change address [30, 31], since the payment amount is typically a round number.
- *Wallet fingerprinting:* Wallets create transactions in a different manner, which can be used to reveal change addresses [31] (e.g. the change output index, locktime behavior match [30])
- *Peeling chain:* In the peeling chain transactions (transactions where a single address with large amounts pay small amounts to other addresses), the output that continues the peeling can be a change address [30].

Address reuse. Whenever the same address is reused, it relates the current transaction to all the transactions that the address previously appeared in. This results in a possible correlation between all transactions enabled with the same address[32]. There is also forced address reuse where the attacker pays a small amount of bitcoin to the used address of the target and follow the address in the blockchain to find other UTXOs belonging to the user if the target combines this UTXO to her other UTXOs in the following transactions [31].
Single input single output. The transaction with only one input and one output is considered as self-payment and the input and the output addresses can be associated with one entity. Indeed, in most cases, the payment transactions consist of multiple inputs and outputs [21].
Cluster growth. Clusters normally grow in small steps, and if applying a heuristic creates a large cluster, it would be as a result of false positives [28].
Specific patterns. New heuristics based on the patterns extracted from users

and transaction behaviors can be employed. For instance, [12] found remuneration patterns based on the analysis of their ground truth. In [14], they found the common relationship between the addresses in the trading services, where receiving the coins from the same address or sending the coins to the same address can indicate a common social relationship.

3.3 Side channel attacks

The correlation of the information such as time, amount, network information, or the user's behavior in the forked blockchains may be used to reveal users or transaction behaviors, thereby compromising their privacy. Table 4 summarizes such side channel attacks, which we explain in the following.

Time correlation. The attacker can correlate the time that a transaction is confirmed (considering appropriate thresholds) with the time that a user interacted with other services. In the table we provided the research [13, 14] that used this attack to find the transactions in the trading services and correlate them with the blockchain data to find the related transactions.

Amount correlation. The attacker can correlate the amount that has been transferred in blockchain with the amount that has been paid (either by fiat or other crypto currencies) in other services where the latter can be publicly seen via websites or application programming interfaces (APIs). In [13, 14], the public trades amounts available in trading services were used to find the corresponding transactions on the blockchain. The attacker can also obtain exchange rates of the fiat currency (if it is paid by fiat currencies) for the date and the time when the transaction is confirmed, and look it up in this interval.

Network layer information. The propagation of transactions between nodes can reveal the data in the network layer. The research [27, 26, 28, 11] indicated the possibility of linking the IP addresses of the nodes to the transactions. To this end, they connected to the Bitcoin nodes and listen to the network to find the original node that is the first who propagated the transaction. It is also mentioned that the access pattern can be used to relate the user to a cryptocurrency address. For instance, visiting a web page with a donation address and then performing a transaction and checking the confirmation in a block explorer can provide an access pattern to link the IP address to that transaction [19].

Cashing out on forks. Cross-chain clustering can create a single chain clustering based on the information obtained from the forked chain cluster. This attack links the addresses in one chain based on the activity of those addresses in the forked chain [21]. Researchers [21] combined the Bitcoin and Bitcoin cash clusters and found that the privacy of almost 5% of the Bitcoin transactions is in danger based on their cash-out behaviors in the Bitcoin Cash.

3.4 Flow analysis

The attacker is able to trace the flow of the money by transaction graph, user graphs, and taint analysis. Table 4 lists the publications that applied the graphs

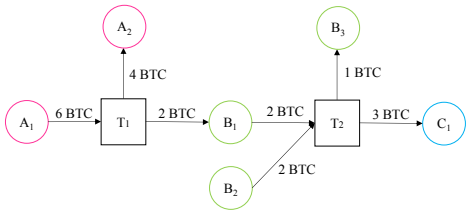

Fig. 3. Transaction graph, adopted from [33]

for their analysis.

Transaction graph. In the transaction graph, the addresses are nodes and the transactions are edges, and the attacker can find predecessors and successors by this graph [20]. Figure 3 illustrates a sample transaction graph where Alice holds 6 BTC, and sends 2 BTC from her address A_1 to Bob B_1 via transaction T_1, as she has 6 BTC in her address, she gets back 4 BTC in her change address A_2. Bob then sends 3 BTC to Carol via transaction T_2 using 2 BTC which he has previously received from the output of T_1 and 2 BTC from the output of another transaction. As can be seen, T_2 has two outputs by which Bob gets 1 BTC as his change (B_3) and pays 3 BTC to Carol.

Taint analysis. This analysis tracks the flow of the money from an address to another [10]. It is defined as the percentage of the balance of the output address that comes from an input address [18].

User graph. In the user graph, users are nodes and the transactions are edges which creates the clusters [20] (e.g by using the heuristics), this graph can find the relationship between different users in the blockchain.

	Time correlation	Amount correlation	Network layer		Cashing out on forks	TX graph/ User graph	Taint analysis
			Map IP to pseudonyms	*Access pattern/ user behavior pattern*			
[20]						✓	
[19]			✓	✓			
[21]					✓ (Combining BCH&BTC)	✓	
[22]						✓	
[23]		✓				✓	
[24]						✓	✓
[25]							
[26]			✓				
[27]			✓				
[28]			✓			✓	
[11]			✓				
[12]		✓ (BTC in $)					
[13]	✓	✓				✓	
[14]	✓	✓					

Table 4. Side channel attacks and flow analysis

3.5 Auxiliary information

The attacker can tag the addresses using several ways including searching on the Internet, interacting with the target, using service APIs, etc. The aforemen-

tioned heuristics, side-channel attacks, and flow analysis find the relationship between the addresses, therefore, if the attacker tag an address, he is able to tag other addresses related to this address. The attacker can not only tag the addresses but also in some cases, can obtain information about the locations, emails, usernames, and etc. Table 5 indicates the resources which have been used in the selected papers to tag the addresses. Some entities publish their addresses in forums, social networks, and websites. As can be seen in table 5, Bitcointalk, Reddit, Twitter are well-known resources to find Bitcoin addresses [13, 20, 22]. Addresses published on the Websites, and addresses which can be queried in the search engines can identify the information about addresses. Services' APIs also provide some additional information that can be related to the addresses (e.g. the information from trading services, such as Localbitcoins, Changelly, Shapeshift) [13, 14, 20]. Some attackers interact with services to obtain the addresses belonging to a specific service [23], it is also called mystery shopper payment [31] where the attacker pays a small amount and follows the address associated with the service in the blockchain. They are non-commercial and commercial databases that provide the address tags based on the ground truth, they found. Walletexplorer, Chainalysis, blockchain.info, and some of the researchers who published their address tags are examples of such databases that were used to tag the addresses [14, 23, 25]. In table 5 the resources that the previous research utilized to tag the addresses are provided.

	Forums	Websites	Search engines	Social networks	Service APIs	Interacting	Address tags DB	others
[20]	✓BitcoinTalk, Bitcoin-OTC	✓Casascius physical coins	✓Google	✓Reddit	✓Mt.Gox		✓blockchain.info	
[19]								
[21]								
[22]		✓BleepingComputer, MalwareTips, 2-spyware	✓Google, Yahoo	✓Reddit				✓†
[23]	✓BleepingComputer±±	✓ID ransomware				✓**	✓Chainalysis	✓Synthetic addr ††
[24]			✓Ahmia, FreshOnions, Google				✓Walletexplorer,	
[25]	✓BitcoinTalk *						✓Walletexplorer, blockchain.info	
[26]								
[27]								
[28]								
[11]								
[12]								
[13]	✓BitcoinTalk	✓Localbitcoins		✓Twitter	✓Localbitcoins ✓Changelly, Shapeshift		✓Walletexplorer, ✓Walletexplorer, researchers data,	
[14]								

±± Ransom addresses in Bleeping computer forum.
† Ransomware knowledge base, YouTube videos, reports from Counter Threat Units (CTU), Incident Responses (IR), and Security Operations Centers (SOC).
†† By running ransomware binaries.
* Extracting Ponzi addresses, profile information, age, gender, location, ...
** Paying a small amount to ransom addresses.

Table 5. Auxiliary information resources

4 BTCR privacy issues and possible countermeasures

In this section, we investigate the privacy of the method did:btcr based on the adopted criteria from RFC 6973 [9] including surveillance, misattribution, correlation, identification, secondary use, and disclosure.

4.1 Surveillance

Any kind of observation and monitoring of the users is considered as surveillance, whether the users are aware of the surveillance or not, it can influence the privacy of the user [9]. In the previous section, we showed the possibility of monitoring users and linking the real-world identities to the Bitcoin addresses which tends to compromise users' activities and their economic situations. The surveillance of DID in the Bitcoin blockchain can be investigated in different aspects. The auxiliary information can be obtained through the interactions with services using DIDs. The service is, therefore, able to follow the user's activities and money flow in the blockchain using Bitcoin privacy attacks. For instance, a payment service where a user authenticates to the device using a DID and then pays using another Bitcoin address that belongs to her, associates the DID to that Bitcoin address. Furthermore, the privacy concerns that a user should take into account when using an immutable blockchain for creating DIDs have a significant role. A user who is aware of such problems can employ privacy-preserving techniques to protect herself against such privacy attacks. A previous research [34, 35] indicated a misconception in the privacy of the Bitcoin blockchain, which can result in serious problems for applications that use blockchain technology. Using Tor services [15], mixing the UTXO before using it for DID BTCR [8] to unlink the relationship between the BTCR UTXO and other UTXOs belonging to the user, and to prevent combining the revoked DID BTCR with other UTXOs in the future to spend the amount associated with the UTXO can be used as possible countermeasures to surveillance of the DID BTCR.

4.2 Misattribution

Misattriubation is considered whenever a user's data or communications are attributed to another, which can consequently affect the user's reputation [9]. Some of the indistinguishable mixing techniques such as PayJoin [36] can relate the users' UTXOs to someone else, using the common input ownership heuristic [37]. PayJoin [36] is one of the successors of the CoinJoin technique, where a user creates a CoinJoin transaction by the recipient of the transaction. The recipient adds her coins as an input of the transaction which consequently increases the payment amount. Therefore, this technique does not require an equal-size output and it is indistinguishable in the blockchain. This would cause privacy problems for the users who are not aware of this issue when using PayJoin as a privacy technique or interacting with the service that implemented PayJoin (e.g., merchants, exchange). Therefore, using the Bitcoin blockchain for DIDs in

did:btcr can put the users at the risk of such privacy misattribution. Providing information for the users to inform them from the possible misattribution by using specific mixing techniques such as PayJoin for the UTXOs that are used in BTCR can to some extent prevent this privacy problem.

4.3 Correlation

Correlation is considered as the combination of different information, which relate to one user [9]. We discuss the correlation in three different aspects including DIDs and DID documents correlation, time correlation, and network correlation. (i) Using the same DID or DID document for interacting with different services can help to trace and correlate user activities [5, 15, 38]. Furthermore, using the same public keys in different DID documents can reveal the link between the corresponding DIDs, e.g., interactions with different services using the same DID while showing different VCs. Inversely, if different DIDs are used for each service while using the same DiD document, then those services can associate those multiple DIDs to the same user. Pairwise-unique DIDs that are issued on a per-relationship basis which can not be correlated to each other or single-use identifier that is discarded once it is exchanged can be used to mitigate this issue [39]. Another issue is that the DID document contains methods for verification of the DID and the attributes including "also known as" and "controller" [15]. Using "also known as", it is possible to specify another identifier belonging to the same user. This can be useful for businesses that use multiple DIDs for their services but should be avoided if not required. Using "controller", another entity can be specified, which is then allowed to change the DID document or to authenticate. This may reveal a relationship between the subject and the controller DiD if they are different. (ii) Considering the network layer correlation, the IP address of the entity can compromise the relationship of common controls, where an attacker can identify the link between different DIDs based on the IP address of the clients [39]. Additionally, using traffic analysis by checking the access history to the DID documents, may help correlate IP addresses to the DID documents. Using TOR or proxy can provide additional privacy [15] in this regard. (iii) Time correlation by employing the same service endpoints can be used to find the relationship of common controls [39]. For instance, timing analysis can be used to correlate users' activities whenever a user uses the same service endpoint in the DID documents. Sharing the service endpoints between a variety of DIDs that are controlled by the different entities [15] can be considered as a possible countermeasure.

4.4 Identification

Identification is considered as relating the information to a specific user to derive her identity [9]. Storing any type of personally identifiable information (PII) in the blockchain, even encrypted or hashed, has the potential to put the users' privacy at risk, as they may be broken and be publicly accessible [5, 7, 15, 38].

Despite DID revocation support, the immutability property prevents deleting the logs of existing BTCR DIDs. Therefore, if the Bitcoin address associated to a DID is later spent with some other inputs without using mixing techniques (will also be considered as revoked), it can link the address used for DID to other addresses owned by the user, based on the common input ownership heuristic. Moreover, if a transaction in the BTCR (when it is revoked) contains a change address, it can be linked to the owner of the inputs. Thus, it is suggested to create the transactions without a change address. Not only Blockchain analysis can identify real-world identities and relate them to DIDs, but also metadata tracing in the DID documents can provide information in the identification of the entities. The visibility of the DID document can leak the metadata about the attributes [6] and provide information about the service endpoints. In BTCR, the attacker can query the Bitcoin blockchain to identify all transactions with OP_RETURN that specify a link to a DID document, thus enabling access to metadata and associated service endpoints. To prevent any privacy leak, URLs to the service endpoints should not include any personal information (e.g. usernames). Usually, the DID documents are stored on servers. If the DID document is stored in the third-party server, the latter may identify the real DiD owner. If the DiD document is stored on a user own server, it becomes possible to correlate the user IP address with the DID document. In this case IPFS (The InterPlanetary File System) [3] can be used as a countermeasure.

4.5 Secondary use

Secondary use is considered as collecting the information about a user without her consent and using it for different purposes other than which the information was collected [9]. We investigate secondary use in did:btcr in three aspects. (i) Read/resolve makes it possible to trace the DID use if it is accessed by third-party services (e.g., universal DID resolver, a naive implementation of Simplified Payment Verification (SPV) clients [40], checking the DID on block explorers), in this case, the attacker can find the resolution pattern. To prevent third party services from collecting information about users, the latter may employ their own Bitcoin full nodes. (ii) The verifier is able to trace the transaction flow, check the history of the UTXOs (e.g. user activities), and if they are spent (accidentally or for changing the ownership, or revocation) monitor next transactions' flow. The verifier can also see all the amounts associated with the address. (iii) a DID real identity can be compromised if used in services that require information about them or their activities (e.g. social networks).

4.6 Disclosure

Disclosure is considered as exposure of information about a user which violates the confidentiality of the shared data [9]. All the privacy attacks that were mentioned in the previous sections can be applied to the addresses that are used as

[3] https://ipfs.io/

DIDs in did:btcr. The users who are not familiar with the privacy issues in the Bitcoin blockchain may encounter some serious problem if their DIDs' addresses link to their other addresses in the blockchain. This tends to lose privacy in their economic activities for the services that they are authenticated by DIDs. To create the first DID in BTCR, the user should provide an address, where she can buy from an exchange. The latter has access to information related to the owner (email address, etc) or in some cases the real identity of the owner when KYC (know your customer) is applied. The user can use mixing techniques [8] beforehand to obfuscate the relationship between the UTXO used in BTCR and the other UTXOs beloging to her. The BTCR updates are required to include the OP_RETURN field; therefore, the users can not utilize current mixing techniques to provide better privacy for their associated addresses. This makes the BTCR updates traceable in the Bitcoin blockchain. Thus, every update in BTCR not only reveals the public key of the previous DID but also indicates the update or changing the access control.

5 Conclusion

In this paper, we presented a review of Bitcoin privacy attacks, which we categorized into four main categories. Then, we investigated and analyzed six possible privacy threats to the DID method did:btcr. In particular, we showed how data analysis of Bitcoin public records, in combination with auxiliary information can be exploited using sophisticated heuristics, to reveal or correlate transactions, identities, or addresses of users. This information, in turn, may be used by malicious actors and cybercriminals to conduct, for example, extortion or ransomware attacks. This study has demonstrated that although BTCR provides some advantages such as protection against censorship, integrity, access and a degree of decentralization, it still lacks methods to deal with the privacy issues identified in this paper. Future research will consist on elaborating and developing new methods, or using existing privacy-enhancing techniques (e.g., mixing techniques, zero-knowledge proofs) to address the aforementioned privacy issues.

Acknowledgments. This research is based upon work partially supported by (1) SBA Research (SBA-K1); SBA Research is a COMET Center within the COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG. (2) the FFG ICT of the Future project 874019 dIdentity & dApps. (3) the FFG Basisprogramm Kleinprojekt 39019756 Decentralised Marketplace for Digital Identity.

References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review (2008) 21260

2. López-Pintado, O., García-Bañuelos, L., Dumas, M., Weber, I., Ponomarev, A.: CATERPILLAR: A business process execution engine on the ethereum blockchain. CoRR **abs/1808.03517** (2018)
3. Ladleif, J., Weber, I., Weske, M.: External data monitoring using oracles in blockchain-based process execution. In Asatiani, A., García, J.M., Helander, N., Jiménez-Ramírez, A., Koschmider, A., Mendling, J., Meroni, G., Reijers, H.A., eds.: Business Process Management: Blockchain and Robotic Process Automation Forum, Cham, Springer International Publishing (2020) 67–81
4. Prybila, C., Schulte, S., Hochreiner, C., Weber, I.: Runtime verification for business processes utilizing the bitcoin blockchain. Future Generation Computer Systems **107** (2020) 816–831
5. Lesavre, L., Varin, P., Mell, P., Davidson, M., Shook, J.: A taxonomic approach to understanding emerging blockchain identity management systems. arXiv preprint arXiv:1908.00929 (2019)
6. Dunphy, P., Petitcolas, F.A.: A first look at identity management schemes on the blockchain. IEEE Security & Privacy **16**(4) (2018) 20–29
7. Allen, C., Hamilton Duffy, K., Grant, R., Pape, D.: Btcr did method. https://w3c-ccg.github.io/didm-btcr/ (2019)
8. Ghesmati, S., Fdhila, W., Weippl, E.: Bitcoin privacy - a survey on mixing techniques. Cryptology ePrint Archive, Report 2021/629 (2021) `https://eprint.iacr.org/2021/629`.
9. Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., Smith, R.: Privacy considerations for internet protocols. Internet Architecture Board (2013)
10. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 conference on Internet measurement conference. (2013) 127–140
11. Biryukov, A., Tikhomirov, S.: Deanonymization and linkability of cryptocurrency transactions based on network analysis. In: 2019 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE (2019) 172–184
12. English, S.M., Nezhadian, E.: Conditions of full disclosure: The blockchain remuneration model. In: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE (2017) 64–67
13. Sabry, F., Labda, W., Erbad, A., Al Jawaheri, H., Malluhi, Q.: Anonymity and privacy in bitcoin escrow trades. In: Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society. (2019) 211–220
14. Yousaf, H., Kappos, G., Meiklejohn, S.: Tracing transactions across cryptocurrency ledgers. In: 28th {USENIX} Security Symposium ({USENIX} Security 19). (2019) 837–850
15. Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M., Holt, J.: Decentralized identifiers (dids) v1. 0. Draft Community Group Report (2021)
16. Sporny, M., Noble, G., Longley, D., Burnett, D., Zundel, B.: Verifiable credentials data model (2019)
17. Wiki: Op_return. https://en.bitcoin.it/wiki/OP_RETURN (2020)
18. Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W.: Mixcoin: Anonymity for bitcoin with accountable mixes. In: International Conference on Financial Cryptography and Data Security, Springer (2014) 486–504
19. Henry, R., Herzberg, A., Kate, A.: Blockchain access privacy: Challenges and directions. IEEE Security & Privacy **16**(4) (2018) 38–45

20. Spagnuolo, M., Maggi, F., Zanero, S.: Bitiodine: Extracting intelligence from the bitcoin network. In: International conference on financial cryptography and data security, Springer (2014) 457–468
21. Kalodner, H., Möser, M., Lee, K., Goldfeder, S., Plattner, M., Chator, A., Narayanan, A.: Blocksci: Design and applications of a blockchain analysis platform. In: 29th {USENIX} Security Symposium). (2020) 2721–2738
22. Conti, M., Gangwal, A., Ruj, S.: On the economic significance of ransomware campaigns: A bitcoin transactions perspective. Computers & Security **79** (2018) 162–189
23. Huang, D.Y., Aliapoulios, M.M., Li, V.G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A.C., McCoy, D.: Tracking ransomware end-to-end. In: 2018 IEEE Symposium on Security and Privacy (SP), IEEE (2018) 618–631
24. Lee, S., Yoon, C., Kang, H., Kim, Y., Kim, Y., Han, D., Son, S., Shin, S.: Cybercriminal minds: An investigative study of cryptocurrency abuses in the dark web. In: NDSS. (2019)
25. Boshmaf, Y., Elvitigala, C., Al Jawaheri, H., Wijesekera, P., Al Sabah, M.: Investigating mmm ponzi scheme on bitcoin. In: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. (2020) 519–530
26. Koshy, P., Koshy, D., McDaniel, P.: An analysis of anonymity in bitcoin using p2p network traffic. In: International Conference on Financial Cryptography and Data Security, Springer (2014) 469–485
27. Biryukov, A., Khovratovich, D., Pustogarov, I.: Deanonymisation of clients in bitcoin p2p network. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. (2014) 15–29
28. Neudecker, T., Hartenstein, H.: Could network information facilitate address clustering in bitcoin? In: International conference on financial cryptography and data security, Springer (2017) 155–169
29. Maxwell, G.: Coinjoin: Bitcoin privacy for the real world. https:// bitcointalk. org/ index. php (2013)
30. Kalodner, H.: Privacy. https:// citp.github.io/ BlockSci/ reference/ heuristics/ change.html (Last accessed 23 July 2020)
31. Wiki: Privacy. https:// en.bitcoin.it/ wiki/ Privacy (Last accessed 23 July 2020)
32. Wiki: Address reuse. https://en.bitcoin.it/wiki/Address_reuse (2021)
33. Möser, M., Böhme, R., Breuker, D.: An inquiry into money laundering tools in the bitcoin ecosystem. In: 2013 APWG eCrime researchers summit, Ieee (2013) 1–14
34. Mai, A., Pfeffer, K., Gusenbauer, M., Weippl, E., Krombholz, K.: User mental models of cryptocurrency systems—-a grounded theory approach. (2020)
35. Krombholz, K., Judmayer, A., Gusenbauer, M., Weippl, E.: The other side of the coin: User experiences with bitcoin security and privacy. In: International conference on financial cryptography and data security, Springer (2016) 555–580
36. Gibson, A.: Payjoin. https:// joinmarket.me /blog /blog /payjoin/ (2018)
37. Ghesmati, S., Kern, A., Judmayer, A., Stifter, N., Weippl, E.: Unnecessary input heuristics and payjoin transactions. In: International Conference on Human-Computer Interaction, Springer (2021) 416–424
38. (W3C), C.C.G.: A primer for decentralized identifiers. https://w3c-ccg.github.io/did-primer/ (2020)
39. Andrieu, J., Appelcline, S., Lohkamp, J., Reed, D., Sabadello, M., Terbu, O., Guy, A.: Did method rubric v1.0. https://w3c.github.io/did-rubric/privacy (2021)
40. Wiki: Simplified payment verification. https://en.bitcoinwiki.org/wiki/ Simplified_Payment_Verification (2019)