The Bisq DAO: On the Privacy Cost of Participation

Liam Hickey*[1] and Martin Harrigan†[1]

[1]Department of Computing, Institute of Technology, Carlow, Republic of Ireland

Abstract

The Bisq DAO is a core component of Bisq, a decentralized cryptocurrency exchange. The purpose of the Bisq DAO is to decentralize the governance and finance functions of the exchange. However, by interacting with the Bisq DAO, participants necessarily publish data to the Bitcoin blockchain and broadcast additional data to the Bisq peer-to-peer network. We examine the privacy cost to participants in sharing this data. Specifically, we use a novel address clustering heuristic to construct the one-to-many mappings from participants to addresses on the Bitcoin blockchain and augment the address clusters with data stored within the Bisq peer-to-peer network. We show that this technique aggregates activity performed by each participant: trading, voting, transfers, etc. We identify instances where participants are operating under multiple aliases, some of which are real-world names. We identify the dominant transactors and their role in a two-sided market. We conclude with suggestions to better protect the privacy of participants in the future.

1 Introduction

Bitcoin and its altcoin brethren, with the notable exception of "privacy coins", seek decentralization first and privacy second [10]. The synergistic pairing of blockchain analysis service providers with regulated cryptocurrency exchanges has exploited this. The former perform blockchain-wide analyses for high coverage but low individual identification. The latter enforce identity checkpoints for high individual identification but low coverage. Their pairing, combining aggregation with identification, is an example of a well-known privacy-risk [20].

Bisq is a decentralized cryptocurrency exchange that does not enforce identity checkpoints but relies on the Bitcoin blockchain and its own peer-to-peer

*Email: liamhickeyire@gmail.com
†Email: martinharrigan@gmail.com

network to operate; thereby falling under the purview of blockchain analysis service providers rather than regulators. In this paper we analyse the Bisq DAO, the component of Bisq responsible for decentralizing its governance and finance functions, from a privacy perspective. We contend that there is a privacy cost to participating in the Bisq DAO and its extent may be unexpected by participants.

Specifically, our analysis applies *address clustering* with a Bisq DAO-specific heuristic. Address clustering is a cornerstone of blockchain analysis. It employs heuristics to partition the set of addresses observed on a blockchain into *address clusters* that are likely controlled by the same participant. When combined with *address tagging*, or associating real-world identities with addresses, and graph analysis, it is an effective means of analysing blockchain activity at both the micro- and macro-levels, see, e.g., [16, 11]. The Bisq DAO relies on a colored-coin issued on the Bitcoin blockchain known as the BSQ token and is subject to this form of analysis. We utilise the properties of BSQ token transactions in the creation of a Bisq DAO-specific address clustering heuristic.

This paper reviews related work (Sect. 2); introduces Bisq, the Bisq DAO and our Bisq DAO-specific address clustering heuristic (Sect. 3); details our analysis and results (Sect. 4); and concludes with suggestions to defeat the heuristic in the future (Sect. 5).

2 Related Work

We categorise related work into four areas: address clustering, token analysis, transaction analysis and decentralized exchanges.

Address clustering is a fundamental building block upon which many high-level blockchain analyses can be performed, see, e.g. [16, 14, 9, 7, 8, 15, 11, 12]. Recently, specialized approaches for sharing address tags [5], crowd-sourcing the classification of transactions [25] and developing address clustering heuristics for the Ethereum blockchain [23] have extended this line of research.

We use address clustering to track the BSQ token, a colored-coin issued on the Bitcoin blockchain by the Bisq project. Tokens are a form of "digital voucher" that provide access to a service or asset while providing revenue or funding to token-based business models [22]. There are several network analyses of ERC20 tokens on the Ethereum blockchain that analyse their age, economic value, activity volume, etc. [21, 24].

Additionally, specialized heuristics have proved successful in tracing transactions in "privacy coin" blockchains. For example, heuristics have been used to link public addresses on either side of Zcash shielded transactions [19] and to identify the true transaction inputs in Monero RingCTs (Ring Confidential Transactions) [17].

Decentralized exchanges enable traders to exchange cryptocurrencies and/or fiat currencies without having to trust a centralized entity to act as an intermediary for the exchange or as a custodian for the currencies. However, decentralized exchanges vary widely in terms of technology, trustlessness and

security [13]. Bisq is an example of a decentralized exchange. It goes to great lengths to decentralize all aspects of its operation. The Bisq DAO is an attempt to decentralize its governance and finance functions.

Decentralized exchanges are a focus of the DeFi, or *Decentralized Finance*, community. The DeFi movement encompasses several projects that aim to extend the decentralized nature of cryptocurrencies to other areas of modern finance. These projects typically take the form of DApps, or *Decentralized Apps*, that operate using smart contracts. There are several decentralized exchange DApps within the DeFi movement, such as Uniswap[1], Kyber[2] and Bancor.[3] These decentralized exchange DApps facilitate the exchange of ERC20 tokens using methods such as community powered liquidity pools or order book based protocols. While these decentralized exchanges differ somewhat in terms of functionality, the Uniswap whitepapers serve as an effective outline of how liquidity pool based exchanges operate on the Ethereum blockchain [2, 3].

We use common terminology from graph theory through-out the paper. Please refer to [6] or a similar reference for definitions.

3 Bisq, The Bisq DAO and Address Clustering

The following is a simplified description of Bisq and the Bisq DAO; see [1] for a more thorough treatment. Bisq, formerly known as Bitsquare, is a decentralized exchange that enables traders to exchange bitcoins for altcoins and fiat currencies without enforcing identity checkpoints. Bisq nodes connect to a peer-to-peer network over Tor to create an order book, coordinate trades and resolve disputes. Trades require security deposits that are held using Bitcoin multi-signature transactions to deter fraud. At the time of writing, traders have completed over 60 000 trades using Bisq.

3.1 The Bisq DAO

There are two types of participant in the Bisq ecosystem: those who use Bisq solely as a decentralized trading platform and those who take part in the development, operation and governance of Bisq. The Bisq DAO, or Bisq *decentralized autonomous organisation*, is the vehicle through which the latter group manages the governance and finance functions of Bisq in a decentralized fashion [4]. Participants in the Bisq DAO can make and vote upon proposals relating to Bisq using a stake based voting system, with voting taking place in approximately monthly cycles known as DAO cycles. The DAO cycle times are determined by block heights on the Bitcoin blockchain. The former group may also participate in the Bisq DAO to a lesser extent by acquiring and burning BSQ tokens in lieu of trading fees.

[1] `https://uniswap.org`
[2] `https://kyber.network`
[3] `https://www.bancor.network`

3.2 The BSQ Colored-Coin

The Bisq DAO operates by tracking and interpreting the issuance and actions of a token or colored-coin issued on the Bitcoin blockchain (BSQ). Participants of the Bisq DAO must first hold some BSQ in order to make and vote upon proposals. There is a two-sided market for BSQ. On the supply side, BSQ can be acquired in several ways. BSQ was minted and distributed in a genesis transaction on 15th April 2019. Additionally, new BSQ is minted and distributed in DAO cycles to contributors using the proposal and stake based voting system. BSQ can also be traded between parties in much the same way as non-colored bitcoin using transfer transactions. On the demand side, traders using Bisq can opt to pay trade fees at a reduced rate by acquiring and burning BSQ, thereby increasing the demand for BSQ and rewarding contributors indirectly. In this way, BSQ is used to financially reward contributors as well as manage the operations of the Bisq DAO itself.

Every action on the Bisq DAO, such as a proposal or vote, takes the form of a BSQ transaction. There are twelve transaction types:

1. **Trade fee** transactions pay Bisq trade fees at a reduced rate using BSQ. The reduced rate incentivises users trading on Bisq to pay using BSQ rather than bitcoin, thereby creating a demand for BSQ.

2. **Transfer** transactions transfer BSQ between addresses in much the same way as non-colored bitcoin.

3. **Compensation request** transactions request BSQ compensation for contributions to the Bisq project. Users supply non-colored Bitcoin that will be converted into BSQ should the request be accepted by vote.

4. **Reimbursement request** transactions are functionally similar to compensation requests. They reimburse users for out-of-pocket expenses relating to Bisq or compensate users for failed trades.

5. **Proposal** transactions make proposals that are neither compensation nor reimbursement requests. The acceptance of these proposals is determined by vote.

6. **Blind vote** transactions vote on open requests and proposals during the blind vote stage of a DAO cycle.

7. **Vote reveal** transactions publish unblinded votes during the vote reveal stage of a DAO cycle.

8. **Lockup** transactions lock BSQ for a specified duration. They are often used as a bond for a specified role in Bisq such as a trade mediator or arbitrator.

9. **Unlock** transactions unlock previously locked BSQ.

Table 1: The twelve valid BSQ transaction types, their counts and whether or not they are self-tranfers.

	Count	Self-Transfer?
Trade Fee	27 285	✓
Transfer	2095	✗
Compensation Request	269	✓
Blind Vote	239	✓
Vote Reveal	236	✓
Proposal	87	✓
Lockup	39	✓
Asset Listing Fee	22	✓
Proof of Burn	22	✓
Unlock	11	✓
Reimbursement Request	5	✓
Genesis	1	✗

10. **Asset listing fee** transactions list new tradeable assets on Bisq, such as a new altcoin.

11. **Proof of burn** transactions destroy BSQ. They do not have a specific use case but can be used as a form of reputation by proving that an individual burned BSQ.

12. The **Genesis** transaction was the initial transaction that minted and distributed the initial quantity of BSQ.

3.3 The Self-Transfer Issue & the Address Clustering Heuristic

Due to the Bisq DAO's reliance on the BSQ token, a significant amount of DAO related activity is published to the Bitcoin blockchain. Bisq attempts to limit the extent to which any activity can be linked to users by generating new address(es) for each transaction. However, Bisq-DAO specific information can aid in this regard. While Bisq generates new address(es) for each BSQ transaction, the majority of these transactions are actually self-transfers, i.e., the same participant owns all of the addresses associated with all of the transaction inputs and outputs. In the list of twelve transaction types above, all but the transfer transactions and the genesis transaction are self-transfers. This points to our Bisq DAO-specific address clustering heuristic: for each self-transfer BSQ transaction, the addresses referenced by all of its transaction inputs and all of its transaction outputs belong to the same participant; for each BSQ transfer transaction, the addresses referenced by all of its transaction inputs and all but the first of its transaction outputs belong to the same participant. Only the

address referenced by the first transaction output in a BSQ transfer transaction belongs to the recipient rather than the sender. The self-transfer issue allows the addresses referenced at either side of these transactions to be clustered. The prevalence of self-transfer transactions compounds this issue as only the BSQ genesis transaction and transfer transactions are not necessarily self-transfers.

We have specified a heuristic by which the addresses associated with BSQ transactions can be clustered. This is a heuristic because it is possible for a participant to manually construct a BSQ transaction that violates these assumptions. However, it is not supported by the Bisq software, e.g., the only way to transfer BSQ is to create a BSQ transfer transaction. We implemented this heuristic; the analysis and results are detailed in the next section.

In this paper we analyse all 30 313 BSQ transactions as of Bitcoin block height 627 911 after the completion of Bisq DAO Cycle 12 on 27th April 2020. Table 1 shows the distribution of the BSQ transaction types, excluding two irregular transactions. We note that 90% of the transactions burn BSQ for trade fees and 93% are self-transfers: participants burn BSQ and/or signal an action to the Bisq DAO (submitting proposals, voting, locking BSQ, etc.), but the remaining BSQ and underlying bitcoin are returned to the same participant.

4 Analysis and Results

The transaction inputs and outputs of the 30 313 BSQ transactions reference 109 719 distinct addresses.[4] The address clustering heuristic produces 1027 address clusters. That is, it partitions the 109 719 addresses into 1027 subsets such that all addresses in the same subset are likely controlled by the same participant. Generally, it is difficult to assess the validity of an address clustering due to the unavailability of a ground truth [18]. However, the Bisq DAO offers the following partial solution. We assign a *role* to each address cluster:

1. If an address cluster contains at least one address referenced by a transaction output of a BSQ proposal transaction, we assign it the *proposer* role.

2. If an address cluster is not a proposer but it contains at least one address referenced by a transaction output of the BSQ genesis transaction, we assign it the *generator* role.

3. If an address cluster is neither a proposer nor a generator, we assign it the *user* role.

4.1 Address Tagging

There are 775 users, 178 generators and 74 proposers. The roles are significant because we can assign *tags*, or links to pseudonyms and real-world identities, to

[4] Our number differs from that shown on the BSQ Block Explorer (`https://explorer.bisq.network`) since our number includes addresses not carrying BSQ-colored bitcoins.

all of the proposers using data stored by the Bisq DAO for the BSQ compensation, reimbursement and proposal transactions. Furthermore, we can assign tags to many of the generators using GitHub account usernames associated with transaction outputs of the BSQ genesis transaction.

Prior to the launch of the Bisq DAO and the BSQ colored-coin, the Bisq community performed the operations of the Bisq DAO and managed the issuance and circulation of prototypical BSQ colored-coins manually and centrally. During this bootstrapping phase, the Bisq community tracked voting and stakes using a spreadsheet.[5] Additionally, contributors creating compensation requests at this time stated the BSQ address to which compensation should be directed in the request's associated GitHub issue. Using the addresses found in both the spreadsheet and within the issues found on GitHub, we created a pre-launch BSQ tag database.

The Bisq DAO was launched on the 15th April 2019. BSQ holders were given the opportunity to specify the address they wished to use in the BSQ genesis transaction. They could take one of three actions: retain their pre-launch address; publicly announce a new address or change their address privately by notifying the individual(s) who constructed the genesis transaction. For each of these cases, we can create a mapping from pre-launch addresses to post-launch addresses, thus creating a post-launch tag database for addresses referenced by the BSQ genesis transaction. Creating a mapping for the first two cases is trivial as addresses are publicly stated on GitHub.[6] However, we were also able to ascertain post-launch addresses for those who chose to change their addresses privately. We found that the ordering of the transaction outputs of the BSQ genesis transaction matched the ordering of the entries in the spreadsheet.

Together, we can assign tags to 96 distinct address clusters. We stress that assigning tags to individual addresses is trivial; the information is publicly available and released by the proposers and generators. However, we are assigning tags to entire address clusters generated using our Bisq DAO-specific heuristic and all of their constituent activity, e.g., trading, voting, transfers, etc.

Returning to the question of validity, we inspected the tags assigned to each address cluster. Out of the 96 tagged address clusters, we identified four with conflicting tags: four address clusters were assigned multiple tags that, ignoring obvious capitalization and spelling errors, were not the same. This could be an indication of false positives generated by our address clustering heuristic. However, on further inspection, we observe that one case contains three different pseudonyms who submitted three different BSQ compensation proposal transactions for overlapping translation contributions. In the other three cases we observe real-world names combined with pseudonyms. We don't believe these are false positives but evidence of participants operating under multiple aliases. The privacy risk is stark.

Additionally, there are nine shared tags: several address clusters were assigned tags that were identical to tags assigned to other address clusters. These

[5] `https://long.af/kcaift`

[6] `https://github.com/bisq-network/compensation/issues/260`
`https://github.com/bisq-network/compensation/issues/263`

are false negatives generated by our address clustering heuristic. They may be due to participants managing multiple Bisq nodes with distinct BSQ wallets or migrating between BSQ wallets using BSQ transfer transactions. We use the shared tags to reduce the number of address clusters to 1015 and the number of tagged clusters to 84. In the context of address clustering, a false negative is less serious than a false positive: assuming that two address clusters may be controlled by two separate participants when in fact they are controlled by one is a lack of information whereas assuming that one address cluster is controlled by one participant when in fact it is controlled by more than one is incorrect information.

4.2 The Address Cluster Graph

Once we have generated the address clusters, we can perform higher-level analyses of activity within the Bisq DAO. We can construct an *address cluster graph* where each vertex corresponds to an address cluster or Bisq DAO participant and each edge corresponds to a set of BSQ transfer transactions where the source and target vertices represent the sender and recipient of the transactions, respectively. Figure 1 is a visualization of the largest connected component of the address cluster graph where the total value of the transactions associated with each edge exceeds 3000 BSQ. This is an arbitrary value chosen to produce a graph whose size is suitable for this paper; an interactive graph visualization system is required to navigate the entire graph.

The color of each vertex represents the role of the corresponding address cluster: red vertices are proposers; blue vertices are generators and white vertices are users. The size of each vertex is proportional to the total amount of BSQ sent to the addresses in the corresponding address cluster. We note that all of the red vertices and three out of the eight blue vertices can be linked with pseudonyms, GitHub account names, and/or real-world names. The address cluster graph represents a financial network where the vertices represent Bisq DAO participants, many of which are identifiable, and the edges represent financial relationships. This is a privacy risk since it implies the applicability of a multitude of financial network analysis techniques.

4.3 The Two-Sided BSQ Market

All BSQ originates with contributors of the Bisq project in either the transaction outputs of the BSQ genesis transaction or the issuance transaction outputs of the accepted BSQ compensation and reimbursement request transactions. Once minted, BSQ can be transferred between any number of participants until it is eventually burnt, primarily by traders for trading fees. We can use the address cluster graph to classify the BSQ transfer transactions based on the roles of the sender (the source address cluster) and the recipient (the target address cluster). The breakdown for the 2095 BSQ transfer transactions (see Table 1) is 971 transfers from proposers and generators to users, 621 transfers from users to users, 350 transfers from proposers and generators to proposers and generators,

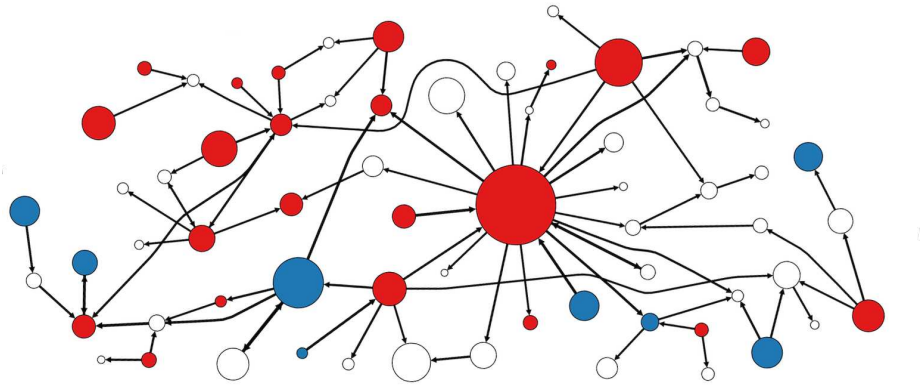

Figure 1: A graphical summary of the significant flows of BSQ between address clusters (Bisq DAO participants). Vertex color indicates role (red for proposers, blue for generators, and white for users) while vertex size indicates transaction volume; see the text for the full details.

and 153 transfers from users to proposers and generators. Although there are far fewer proposers and generators than users, the proposers and generators are involved in 70% of all BSQ transfer transactions.

A similar situation presents itself in Bitcoin: large centralized services such as exchanges, mining pools, gambling services and darknet markets generate 'super-clusters' in the address clustering of the Bitcoin blockchain [9]. Even though they are few in number when compared with the total number of Bitcoin users, they have high degree centrality in their corresponding address cluster graph and are involved in a significant number of Bitcoin transactions [14]. Because of this they are a focus of regulators and blockchain analysis service providers. Within Bisq, the proposers and generators could attract a similar focus: they are involved in a significant number of BSQ transfer transactions, they play a central role in the network and, in many cases, they are easily identifiable.

4.4 The Dominant BSQ Transactors

At the time of our analysis, the Bisq DAO had minted 4 529 424.22 BSQ, the participants had burnt 681 210.40 BSQ, primarily for trade fees, and 3 848 213.82 BSQ remained in circulation. It is an easy task to identify the address clusters that have transacted the most BSQ. Out of the top ten BSQ transactors, five can be linked with GitHub account names and real-world names. The individuals are providing their names when submitting BSQ compensation and reimbursement proposal transactions. Our address clustering heuristic is linking this information with the entirety of their Bisq DAO activity including their transaction volume and balances.

4.5 Impact Within the Bitcoin Blockchain

Thus far, we have assessed the Bisq DAO and BSQ token in isolation. However, all BSQ transaction data is published to the Bitcoin blockchain. The set of BSQ transactions is, by definition, a subset of the set of Bitcoin transactions. We can assess the impact of the Bisq DAO on address clusterings of the entire Bitcoin blockchain.

The address clusters generated by our heuristic are equally valid when viewed through the lens of the larger Bitcoin blockchain. By extension, the observations stemming from the use of this heuristic are equally applicable. Since the results of the Bisq DAO-specific clustering heuristic can be extended to the Bitcoin blockchain, a comparison between our heuristic and conventional blockchain clustering heuristics can be made.

Initially, we intended to merge the results of both clustering heuristics to refine the resultant address clusters. However, we found that when the address clusters generated by both heuristics were merged, they produced large clusters with many false positives. We believe this is due to CoinJoin transactions involving bitcoin that was later colored as BSQ.

5 Conclusion

We demonstrated the privacy cost in participating in the Bisq DAO. Specifically, we showed that participants may be revealing more information than they intend, especially when submitting BSQ compensation and reimbursement proposal transactions. Even though Bisq generates new address(es) for every BSQ transaction, 93% of these transactions are self-transfers, i.e., all of the transaction inputs and outputs belong to the same participant. This points to a Bisq DAO-specific address clustering heuristic. We implemented this heuristic and applied it to all BSQ transactions to date. The heuristic proves effective in aggregating all activity performed by each participant such as trades, votes, proposals, etc. We can attach pseudonyms, GitHub account names and real-world names to many of the central participants. This has important implications for user privacy. Although not examined in this paper, it has further implications for the Bisq DAO voting system and address clustering in the broader Bitcoin blockchain.

A number of approaches can be taken to defeat this heuristic. The heuristic relies on BSQ self-transfer transactions being easily identifiable. The Bisq software could trigger false positives or false negatives in this heuristic by introducing ambiguity into the distinction between self-transfers and non-self-transfers. Other than the BSQ genesis transaction, transfer transactions are the only BSQ transactions that are not entirely self-transfers. As a result, transfer transactions have the effect of separating clusters generated by our heuristic. Disguising transfer transactions so that they cannot be distinguished from self-transfer transactions would trigger false positives in the heuristic, invalidating generated clusters. For example, a participant could create a BSQ trade fee transaction

to transfer BSQ where the "change" was directed to the recipient and a small amount of BSQ was burnt to satisfy the requirement of a BSQ trade fee transaction. While this solution defeats the heuristic as it stands, there are other ways in which BSQ transaction types can be deduced. Every trade fee transaction is linked to the multi-signature transaction of a Bisq trade. Consequently, any trade fee transaction that isn't linked to a Bisq trade could be identified as a disguised transfer transaction and treated as such.

Additionally, transfer transactions can be used to trigger false negatives in our heuristic, thereby diminishing the heuristic's effectiveness. Triggering a false negative requires the use of 'dummy' transfer transactions after each self-transfer transaction. This transfer transaction sends BSQ from the change address used in the last self-transfer to a new address owned by the same user. This gives the appearnce of BSQ being sent between parties, thus reducing the size of the address clusters generated by our heuristic. While dummy transfer transactions reduce the effectiveness of the heuristic, they also create transactions that aren't otherwise needed, increasing the cost for users. Of course, functionality to create dummy transactions and a best-practices guide could be included in the Bisq software and documentation and only used to improve privacy as required.

The Bisq DAO is an innovative approach to decentralizing the governance and finance functions of a decentralized exchange. However, when viewed through the prism of blockchain analysis and address clustering, it appears vulnerable. Participants of the Bisq DAO, including traders, will expect certain limits on what is known about them and on what others can find out. Blockchain analysis could unsettle this expectation and have a 'chilling effect' on adoption.

6 Acknowledgements

The authors are grateful to the members of the Bisq community and the anonymous reviewers that provided feedback on earlier versions of this paper.

References

[1] Bisq network documentation. `https://docs.bisq.network`.

[2] Uniswap whitepaper.

[3] H. Adams, N. Zinsmeister, and D. Robinson. Uniswap v2 core, 03 2020.

[4] C. Beams and M. Karrer. Phase zero: A plan for bootstrapping the Bisq DAO. `https://docs.bisq.network/dao/phase-zero.html`.

[5] Y. Boshmaf, H. A. Jawaheri, and M. A. Sabah. BlockTag: Design and applications of a tagging system for blockchain analysis. In *IFIP International Conference on ICT Systems Securit and Privacy Protection*, pages 299–313. Springer, 2019.

[6] R. Diestel. *Graph Theory*. Springer Graduate Texts in Mathematics. Springer, 2017.

[7] D. Ermilov, M. Panov, and Y. Yanovich. Automatic Bitcoin address clustering. In *The IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 461–466, 2017.

[8] E. Filtz, A. Polleres, R. Karl, and B. Haslhofer. Evolution of the Bitcoin address graph: An exploratory longitudinal study. In *The International Data Science Conference (iDSC)*, pages 77–82. Springer, 2017.

[9] M. Harrigan and C. Fretter. The unreasonable effectiveness of address clustering. In *The IEEE International Conference on Advanced and Trusted Computing (ATC)*, pages 368–373. IEEE Computer Society, 2016.

[10] J. Harvey and I. Branco-Illodo. Why cryptocurrencies want privacy: A review of political motivations and branding expressed in "privacy coin" whitepapers. *Journal of Political Marketing*, pages 1–30, 2019.

[11] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, K. McRoberts, E. Bursztein, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy. Tracking ransomware end-to-end. In *The IEEE Symposium on Security and Privacy*, pages 618–631. IEEE, 2018.

[12] M. Jourdan, S. Blandin, L. Wynter, and P. Deshpande. Characterizing entities in the Bitcoin blockchain. In *The International Workshop on Blockchain and Sharing Economy Applications (BlockSEA'18) at the IEEE International Conference on Data Mining (ICDM)*. IEEE, 2018.

[13] L. X. Lin. Deconstructing decentralized exchanges, 2019.

[14] M. Lischke and B. Fabian. Analyzing the Bitcoin network: The first four years. *Future Internet*, 8(1), 2016.

[15] D. D. F. Maesa, A. Marino, and L. Ricci. Data-driven analysis of bitcoin properties: Exploiting the users graph. *International Journal of Data Science and Analytics*, pages 63–80, 2018.

[16] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. A fistful of bitcoins: Characterizing payments among men with no names. *Communications of the ACM (CACM)*, 59(4):86–93, 2016.

[17] M. Mser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin. An empirical analysis of traceability in the Monero blockchain. In *Proceedings on Privacy Enhancing Technologies*, pages 143–163, 2018.

[18] J. Nick. Data-driven de-anonymization in Bitcoin. Master's thesis, ETH Zürich, 2015.

[19] J. Quesnelle. On the linkability of Zcash transactions. `https://arxiv.org/abs/1712.01210`, 2017.

[20] D. J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 2006.

[21] S. Somin, G. Gordon, and Y. Altshuler. Network analysis of ERC20 tokens trading on Ethereum blockchain. In *The International Conference on Complex Systems (ICCS)*, pages 439–450. Springer, 2018.

[22] P. Tasca. Token-based business models. In T. Lynn, J. G. Mooney, P. Rosati, and M. Cummins, editors, *Disrupting Finance: FinTech and Strategy in the 21st Century*. Palgrave, 2019.

[23] F. Victor. Address clustering heuristics for Ethereum. In *Financial Cryptography and Data Security (FC)*, Lecture Notes in Computer Science (LNCS). Springer, 2020. to appear.

[24] F. Victor and B. K. Lüders. Measuring Ethereum-based ERC20 token networks. In *Financial Cryptography and Data Security (FC)*, Lecture Notes in Computer Science (LNCS), pages 113–129. Springer, 2019.

[25] M. Weber, G. Domeniconi, J. Chen, D. K. I. Weidele, C. Bellei, T. Robinson, and C. E. Leiserson. Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics. In *The Anomaly Detection in Finance Workshop (ADF) at the SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)*, 2019.