



King's Research Portal

DOI:

[10.1109/BRAINS49436.2020.9223286](https://doi.org/10.1109/BRAINS49436.2020.9223286)

Document Version

Peer reviewed version

[Link to publication record in King's Research Portal](#)

Citation for published version (APA):

Platt, M., Pierangeli, F., Livan, G., & Righi, S. (2020). Facilitating the Decentralised Exchange of Cryptocurrencies in an Order-Driven Market. In *2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020* (pp. 30-34). [9223286] (2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020). IEEE. <https://doi.org/10.1109/BRAINS49436.2020.9223286>

Citing this paper

Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

General rights

Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Research Portal

Take down policy

If you believe that this document breaches copyright please contact librarypure@kcl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Facilitating the Decentralised Exchange of Cryptocurrencies in an Order-Driven Market

Moritz Platt
Department of Informatics
King's College London
London, UK
moritz.platt@kcl.ac.uk

Francesco Pierangeli
Department of Political Economy
King's College London
London, UK
francesco.pierangeli@kcl.ac.uk

Giacomo Livan
Department of Computer Science
University College London
London, UK
g.livan@ucl.ac.uk

Simone Righi
Department of Computer Science
University College London
London, UK
s.righi@ucl.ac.uk

Abstract—This article discusses a protocol to facilitate decentralised exchanges on an order-driven market through a consortium of market services operators. We discuss whether this hybrid protocol combining a centralised initiation phase with a decentralised execution phase outperforms fully centralised exchanges with regards to efficiency and security. Here, a fully efficient and fully secure protocol is defined as one where traders incur no trading costs or opportunity costs and counterparty risk is absent. We devise a protocol addressing the main downsides in the decentralised exchange process that uses a facilitating distributed ledger, maintains an order book and monitors the order status in real-time to provide accurate exchange rate information and performance scoring of participants. We show how performance ratings can lower opportunity costs and how a rolling benchmark rate of verifiable trades can be used to establish a trustworthy exchange rate between cryptocurrencies. The formal validation of the proposed technical mechanisms is the subject of future work.

Index Terms—Cryptocurrencies, Atomic Swap, Cross-Chain Trading, Hashed Time-Locked Contracts (HTLC), Exchange Rates, Order Books, Order-Driven Markets, Quality Scoring

I. Introduction

With the introduction of the Peer-to-Peer Electronic Cash System ‘Bitcoin’ [1] and the subsequent creation of many so-called Altcoins utilising similar principles, the problem of exchanging cryptocurrencies has emerged. Such exchanges are fundamental for the long-term development of a diverse and robust cryptocurrency ecosystem [2], [3]. To facilitate the full degree of economic activities in such a heterogeneous environment, exchanges between fiat currencies and cryptocurrencies as well as exchanges amongst cryptocurrencies are necessary. ‘CoinBene’, the largest cryptocurrency exchange [4], saw a top

trading volume of approximately \$1.5 B over a 24 hour period in November 2019 [4]. This illustrates the potential size of the cryptocurrency exchange market.

A. Exchange Paradigms

Commercial providers offering cryptocurrency exchange capabilities on the market today act as centralised exchanges (CEXs). They provide market-making capabilities by serving the public’s demand to trade with immediacy by standing ready to buy currency from participants who wish to sell and selling to participants who wish to buy [5]. Immediacy is provided by holding sufficiently large quantities of all cryptocurrencies for which exchanges are supported. This model is well understood in academia and industry since it is based on the same principles as foreign exchange spot trading where trading firms act as market makers.

The concept of decentralised exchanges (DEXs), however, is less well defined. Fundamentally, any exchange of different cryptocurrencies can be implemented as a peer-to-peer transaction in which one participant (the initiator) transfers a previously agreed amount of one cryptocurrency to another participant who in turn transfers a previously agreed amount of a different cryptocurrency back to the initiator. The goal of this paradigm is to eliminate the negative effects that arise from the involvement of a third party (cf. section I-B) through their disintermediation. DEXs leave *critical functions*, such as transaction signing, to the individual actors [6].

B. Risks and Benefits of Different Exchange Paradigms

Since CEXs require participants to settle their obligations first, participants are exposed to counterparty risk: the risk of funds being lost on the provider side. The recent past has provided several examples of the loss of assets in the exchange process, either due to theft or exchanges shutting down [7], [8]. Exchanges with high transaction volumes were found to be more likely to experience a breach leading to theft, while smaller exchanges were found to have a higher

This research has been partially carried out within the project ‘Incentives and Governance Model for Decentralized Exchanges Operating in the Crypto-Asset Ecosystem’ and was supported through the 1st Internal Fund Call for Project Proposals on Distributed Ledger Technologies by the University College London Centre for Blockchain Technologies. We are also grateful for financial support from the UK EPSRC VOLT Project, grant number EP/P031811/1.

risk of shutting down prematurely [9]. Furthermore, the fact that considerable bid-ask spreads are observed for centralised exchanges [10] shows that such centralised models are accompanied by significant trading costs. Centralised providers also had restricted access to their offerings in the past [11]. The advantages of the centralised paradigm are faster processing of trades by holding a reserve of cryptocurrencies on the exchange side, the possibility of dealing in fiat currencies and the availability of more complex trading products.

Table I
Exchange Paradigms

Aspect	CEX	DEX
Risk of misappropriation of funds in transit	High	None
Exclusion of participants	Feasible	Unfeasible
Direct trading costs	Prevalent	None
Trading partner discovery	Trivial	Complex
Exchange rate transparency	Transparent	Opaque
Opportunity costs due to tied capital	Low	High

Decentralised exchange processes in their purest form—not involving any third party at any point of the process—overcome most of the risks that are observed in centralised exchanges. They do come with unique downsides though. Participants must follow suitable protocols to allow for recovering funds from an uncooperative counterparty (cf. section I-C) to reliably eliminate counterparty risk. This is essential since in decentralised exchange scenarios, trades may be established on an ad hoc basis between distrusting and potentially pseudonymous actors, making it challenging to rely on law enforcement and the legal system to recoup losses. In addition to these serious downsides, due to their nature, DEXs lack rate discovery mechanisms and require manual matching of the buy and sell sides. Furthermore, DEXs that are based on protocols that lock collateral (either via timing constraints or through the collateralisation of external vaults) can incur opportunity costs for the participants in cases where trades that were previously agreed upon fall through. Table I highlights which paradigm is beneficial to traders based on the discussed aspects.

C. Related Work

The Ethereum community has created the Ethereum Improvement Proposal (ERC) 20 [12] that is widely recognised as de facto standard for tokens on the Ethereum network and asserts enabling decentralised exchanges as one of its main objectives. While only low exchange volumes between different ERC-20 based tokens have been observed in actuality [13], a great deal of attention has been paid to the problem of exchanging different types of assets backed by one chain. Atomic cross chain swaps, i.e., exchanges of assets on *different* chains with transactionality, however, are still a nascent field of research. The prevalent paradigm underlying atomic cross chain swaps are ‘Hashed Time-Locked Contracts’ (HTLC), allowing for off-chain contract negotiations. This paradigm is believed to have emerged on the Bitcoin blockchain [14] and was subsequently implemented on various blockchains [15], [16] and formally studied [14], [17].

While alternative approaches using multi-signature transactions [18] or the collateralisation of independent vaults [19] have been proposed to improve the speed or costs of swaps, HTLCs remain the prevailing approach [20]. Most relevant cryptocurrencies in use today can be connected through HTLCs [21].

In addition to these contributions in the technological field, significant findings in the architecture and design of DEX have been made. Lin [22] analysed different implementations of DEX with varying compositions of central components and decentralised protocols. She defines discovery mechanisms as a distinctive characteristic of an exchange architecture and differentiates between on-chain and off-chain order books, showing how on-chain order books provide censorship resistant, trustless matching while off-chain order books provide better performance and lower cost. Fully decentralised exchanges maintaining no central components were criticised for being vulnerable to arbitrage through the exploitation of timing issues related to on-chain, smart contract-mediated trades [23]. Several exchange protocols support off-chain order books. Among those are ‘0x’ [24] where ‘relayers host and maintain an off-chain order book in exchange for transaction fees’, ‘Swap’ [25], that introduces ‘indexers’ as off-chain services that aggregate and match peers based on their intent to trade and ‘IDEX’ [26], an exchange that approaches off-chain order books by maintaining a centralised trading engine. These protocols all operate on the Ethereum blockchain.

D. Motivation

This article outlines the ongoing work of validating the hypothesis that a protocol that allows for initialising decentralised exchanges via a consortium of market services operators on a supporting distributed ledger system improves exchange processes. Ultimately, we aim to examine whether the protocol proposed outperforms traditional exchanges with regards to efficiency—as measured by trading costs and opportunity costs—and security—as measured by counterparty risk. This paper approaches this question by describing a prototypical protocol.

II. Methods

A. Environment

The environment within which the protocol operates shown in figure 1 consists of a supporting DLT network γ that is shared by the the market services operators $O_{1..n}$ and the exchange participants (i.e. I, II) as well as other blockchains maintaining the supported cryptocurrencies (i.e. α and β).

Participants of the protocol operate nodes on γ that serve the purpose of exchanging messages with an instance of O during exchange rate discovery (cf. section II-B1) and order matching (cf. section II-B2). In contrast to ephemeral address-based identities that are common on public permissionless blockchains, participant nodes on γ are associated with durable identities, meaning they are unique and will not change over time. This property makes the node identity a suitable identifier for an evolving performance score as this score will be based on multiple trades over a longer period of time. Participant nodes will persist information about orders they are planning to engage in internally in order to keep track of obligations.

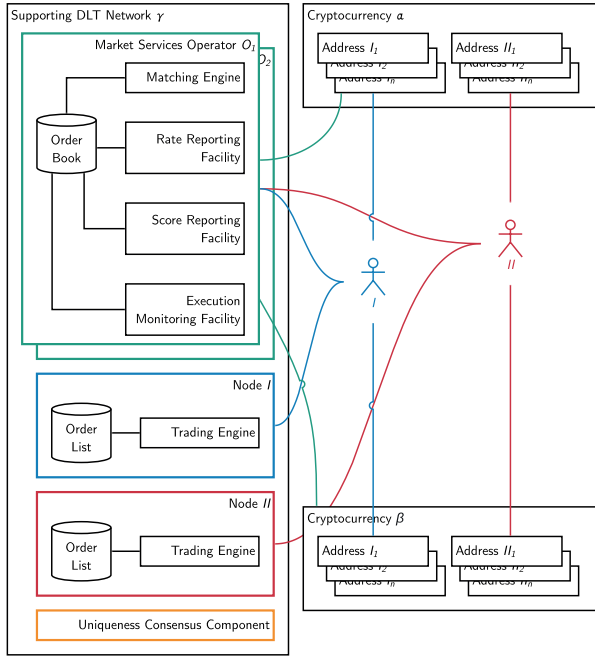


Figure 1. The participants I and II interact with the source and target cryptocurrencies α and β while the Market Services Operators O_1 and O_2 provide supporting capabilities.

Each instance of O exposes a multitude of services. The matching engine provides a public API on γ to query for available trades. This trade information is extracted from the order book that is private to O . O maintains the order book via the matching engine by updating the state of trades once they are executed. The rate reporting facility is also operated by O and will produce a trustworthy exchange rate based on order book data (cf. section II-B4). The score reporting facility will equally access the order book, providing a different view on the data contained. The execution monitoring facility periodically connects with the supported public blockchains α and β to evaluate whether any of the trades established earlier have come to fruition, in which case the execution monitoring facility will update the order book with this information. α and β represent the source and target blockchains. I and II maintain addresses on both as these hold the currencies they aim to exchange. Both I and II can maintain an arbitrary number of addresses on each blockchain in order to preserve their privacy.

Operation of Market Service Nodes: Order book data held by O is replicated via a point-to-point protocol and evolved via the unspent transaction output (UTXO) model, ensuring a coherent view of rates and scores throughout the network of market service operators. Using a Byzantine fault tolerant [27] consensus protocol between market service operators allows the system to recover from a subset of dishonest market service operators.

B. Protocol

The proposed protocol is a multi-stage decentralised/centralised hybrid protocol that facilitates HTLC-based exchanges. The protocol can be applied to any scenario where there is a pair of actors $\{I, II\}$ that wish to exchange cryptocurrencies held on two blockchains, α and β , that support HTLCs with

compatible hash functions (cf. section I-C) through a facilitating DLT system γ . γ acts as an environment offering a *matching engine*, a *rate reporting facility*, a *score reporting facility* and an *execution monitoring facility*, all backed by a centrally stored order book, in an effort to alleviate the downsides of pure DEXs.

The protocol encompasses the following steps:

1) *Exchange Rate Discovery:* The figure 2 shows the optional first step of the protocol. In this step, participants can query a price-reporting facility deployed in γ for the exchange rate between two given currencies.

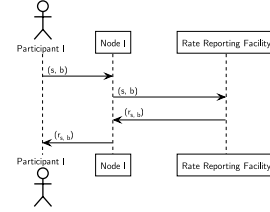


Figure 2. $Participant_I$ discovers rate $r_{s,b}$ for selling s in exchange for b by querying the *RateReportingFacility* via *Node_I*, which is deployed on the DLT system γ .

This facility can be used by both parties of an exchange to determine a fair exchange rate. The rate obtained is informational, but constitutes actionable information for those participants who wish to execute a trade at a market price, similar to the way centralised exchanges would offer a fixed rate to their clients.

2) *Order Matching:* The environment in which this protocol operates constitutes an order-driven market, which is defined as a market in which heterogeneous agents trade via a central order-matching mechanism [28]. Central order matching is provided by a matching engine deployed in γ .

a) *Sell Side:* To encode an order for exchanging a defined amount of one cryptocurrency for another, any account holder on γ can post an order message to the matching engine (cf. figure 3). Some technological prerequisites have to be met to enable γ to process these requests in a performant and privacy-preserving manner.

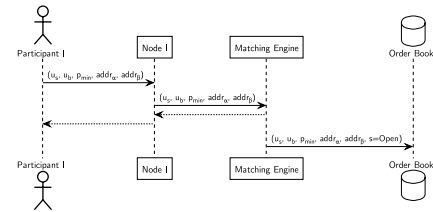


Figure 3. $Participant_I$ posts an order for selling u_s units of s for u_b units of b using the matching engine. $Participant_I$ demands a minimum performance rating of p_{min} from potential counterparties. The order book will reflect the status s of the order as *Open*.

The order posted using the matching engine includes the parameters relevant to the trade (units offered, u_s , and units sought, u_b) and the technical parameters necessary for performing the trade via an HTLC (success address, $addr_\beta$; failure address, $addr_\alpha$; and the locking secret hash). Furthermore, $Participant_I$ will include a minimal performance rating p_{min}

in the order. This value is used as a threshold to exclude participants whose past performance was below expectations (cf. section II-B4). The matching engine will store the order in the order book with a status of *Open*.

b) *Buy Side*: Potential buyers can query the matching engine for orders that are of interest to them. As shown in figure 4, the matching engine will filter the order book by the cryptocurrency pair defined by the querying party, taking into account their performance rating.

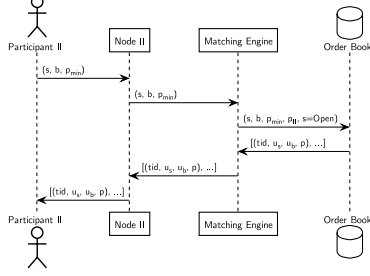


Figure 4. *Participant_{II}* indicates to the matching engine that they are willing to buy units of b in exchange for s as well as the minimum performance rating p_{min} they expect the counterparty to have. The matching engine subsequently queries the order book for all orders with status s of *Open* that match both the performance rating requirement p_{min} of the buyer and their rating P_{II} . The matching engine then returns appropriate orders with their IDs tid along with the actual performance rating of the seller p .

Subsequently, some aspects of all orders they qualify for based on their personal performance rating are made available to them. These aspects are the units offered (u_s) and the units sought (u_b). No other data about the order are provided before a buyer expresses their intention to enter in a trade.

3) *Exchange*: Once a buyer expresses their intention to engage in a particular trade—as referenced by its offer ID—this trade will no longer be visible to other potential buyers in the order book of the matching engine and the details of the trade will be made available to the buyer. The buyer also needs to communicate their success address (where they seek to receive funds) and failure address (where they can be refunded) to the seller (cf. figure 5).

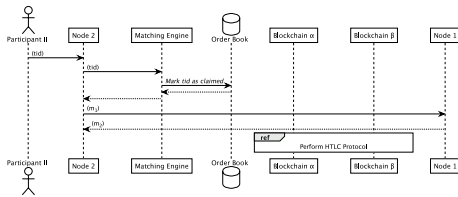


Figure 5. *Participant_{II}* instructs their node on γ to claim a trade as referenced by its id tid . The matching engine removes the trade from the list of available trades. Subsequently the user nodes exchange the necessary information to invoke the HTLC protocol in α and β (m_1, m_2).

Participant_I and *Participant_{II}* then engage in an exchange by following the respective HTLC protocol connecting blockchains α and β . While there are subtle differences between the implementations of HTLCs on different chains, in essence, an HTLC protocol will allow a participant to lock the requested amount of assets for a predefined duration. If within that duration,

a counterparty can present cryptographic proof of payment of the expected exchange amount to the expected exchange address, the locked funds will automatically be transferred to the counterparty's stated target address [29]. This process is based on a bilateral HTLC and does not require any involvement of γ , thus maintaining the atomicity of the exchange.

4) *Execution Monitoring*: The system proposed alleviates the downsides of centralised exchanges (cf. table I) by offering key data in two dimensions: a trustworthy exchange rate and a performance rating. A trustworthy exchange rate is defined as a rolling benchmark rate calculated as a result of actual trades. *Actual* trades are trades that were verified to have happened. A participant's performance rating is computed using the total volume of their successfully fulfilled obligations t_s in relation to the total volume of their failed trades (t_f), i.e. $P = t_s - t_f$. Variations in this score could cap P at a defined threshold to prevent leaking the total trade volumes to third parties or weigh more recent transactions higher.

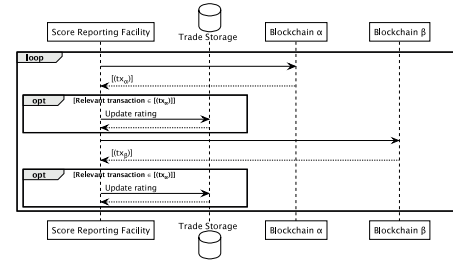


Figure 6. A market operator node observes the blockchains α and γ , feeding relevant transactions (tx_α, tx_β) back to the internal score reporting facility.

Measuring exchange rates and performance ratings require the monitoring of actual exchanges. Therefore, the execution monitoring system will monitor all supported blockchains (i.e. α , β , etc.) on an ongoing basis (cf. figure 6). Since transactions on these blockchains are public, it is feasible to observe all transfers, identifying the trades that were established in an earlier step (cf. section II-B2a). Once a transfer is observed, the performance rating of the participant will be updated. Subsequently, the rolling exchange rate will take the trade into account.

III. Results and Discussion

A. Context of the Protocol

Using native HTLC technology of the underlying blockchains, the protocol exhibits high latency since it requires transactions to be settled on-chain. The cost incurred for participating in the protocol is dependent on the operational costs relayed from market service providers. Should no direct costs be charged, then the total cost of participation is limited to gas costs and opportunity costs for tied capital. Opportunity costs for tied capital are expected to be lower for this protocol when compared to a protocol that does not employ performance monitoring. The protocol provides privacy by keeping the order book exclusive to operators of market service nodes. In contrast to on-ledger order books, here, the public cannot inspect the order book directly. The protocol offers high interoperability as it allows to connect arbitrary blockchains that support HTLC.

B. Security Analysis

While using bilateral HTLC precludes the protocol from being vulnerable to participant assets being stolen, other attacks are conceivable: Market services operator nodes are intended to be operated by a consortium of honest actors. A majority of honest actors is necessary to maintain a system that reports correct scores for participants. Should this majority not exist, then dishonest market services operator nodes can collude and report arbitrary ratings for participants. They could also form a cabal with preferred users, redistributing lucrative trades to them. Furthermore, dishonest market services operators could slow down the protocol by delaying messages to a point where it would become unattractive to participants.

IV. Conclusion

This paper discusses our ongoing work exploring decentralised exchange initiation via a supporting DLT system. We propose a protocol and message format for exchanging the trade information and technical attributes necessary for establishing HTLC-based exchanges between potentially distrusting actors. Framing the decentralised exchange space as an order-driven market, we show how this protocol can ease trading partner discovery, thus lowering the friction during the preliminary phase of a trade. We show how performance scoring can lower opportunity costs by reducing the risk of trades falling through. We show how a rolling benchmark rate of verifiable trades can establish a trustworthy exchange rate between cryptocurrencies. This approach bears similarities to existing protocols that utilise off-chain order books with the difference that it can operate cross-chain and that it introduces the concept of a consortium of market services operators. While the protocol is effective under the assumption of the honesty of a majority of market services operators, we show that it is vulnerable to attacks from dishonest operators that collude with other network participants.

Given these findings, future work should focus on further decentralising the protocol, using techniques like zero-knowledge proofs, to make exchange rate and reliability score discovery independent of a central actor or centralised consortium.

References

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <http://www.bitcoin.org/bitcoin.pdf> (Accessed 2014-04-17).
- [2] N. Gandal and H. Halaburda, "Competition in the Cryptocurrency Market," Working Papers 14-17, 2014. [Online]. Available: <https://econpapers.repec.org/RePEc:net:wpaper:1417>
- [3] J. Franke, W. K. Härdle, and C. M. Hafner, *Financial Econometrics of Cryptocurrencies*. Cham: Springer International Publishing, 2019, pp. 545–568.
- [4] CoinMarketCap. (2019, Nov.) Top 100 Cryptocurrency Exchanges by Trade Volume. [Online]. Available: <https://coinmarketcap.com/exchanges/coinbene/> (Accessed 2019-11-01).
- [5] R. A. Schwartz and L. Peng, *Market Makers*. Boston, MA: Springer US, 2013, pp. 487–489.
- [6] N. Sexer. (2018, Jan.) State of Decentralized Exchanges, 2018. [Online]. Available: <https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79> (Accessed 2019-11-02).
- [7] F. Bolici and S. D. Rosa, "Mt.Gox Is Dead, Long Live Bitcoin!" in *Empowering Organizations*, T. Torre, A. M. Braccini, and R. Spinelli, Eds. Cham: Springer International Publishing, 2016, pp. 285–296.
- [8] U. Chohan, "The Problems of Cryptocurrency Thefts and Exchange Shutdowns," *SSRN Electronic Journal*, 2018.
- [9] T. Moore and N. Christin, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 25–33.
- [10] N. Bundi and M. Wildi, "Bitcoin and market-(in)efficiency: a systematic time series approach," *Digital Finance*, Mar 2019.
- [11] J. Wilmoth. (2018, Oct.) Decentralized[?] Ethereum Exchange IDEX Waves Goodbye to New York Traders. [Online]. Available: <https://www.ccn.com/decentralized-ethereum-exchange-index-waves-goodbye-to-new-york-traders/> (Accessed 2019-11-09).
- [12] F. Vogelsteller and V. Buterin, "ERC-20 Token Standard," EIP 20, Nov. 2015. [Online]. Available: <https://eips.ethereum.org/EIPS/eip-20> (Accessed 2019-11-04).
- [13] F. Victor and B. K. Lüders, "Measuring Ethereum-Based ERC20 Token Networks," in *Financial Cryptography and Data Security*, I. Goldberg and T. Moore, Eds. Cham: Springer International Publishing, 2019, pp. 113–129.
- [14] M. Herlihy, "Atomic Cross-Chain Swaps," in *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*, ser. PODC '18. New York, NY, USA: ACM, 2018, pp. 245–254.
- [15] S. Bowe and D. Hopwood, "Hashed Time-Locked Contract transactions," BIP 199, Mar. 2017. [Online]. Available: <https://github.com/bitcoin/bips/blob/master/bip-0199.mediawiki> (Accessed 2019-09-29).
- [16] M. Black and T. L. and, "Hashed Time-Locked Contracts," Liquidity Team, EIP 1630, Nov. 2018. [Online]. Available: <https://github.com/matthewjblack/EIPs/blob/EIP-1630/EIPS/eip-1630.md> (Accessed 2019-10-02).
- [17] M. Herlihy, B. Liskov, and L. Shrira, "Cross-Chain Deals and Adversarial Commerce," *Proc. VLDB Endow.*, vol. 13, no. 2, p. 100–113, Oct. 2019.
- [18] J.-Y. Zie, J.-C. Deneuville, J. Briffaut, and B. Nguyen, "Extending Atomic Cross-Chain Swaps," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, C. Pérez-Solà, G. Navarro-Arribas, A. Biryukov, and J. Garcia-Alfaro, Eds. Cham: Springer International Publishing, 2019, pp. 219–229.
- [19] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais, and W. J. Knottenbelt, "XCLAIM: Trustless, Interoperable Cryptocurrency-Backed Assets," Cryptology ePrint Archive, Report 2018/643, 2018. [Online]. Available: <https://eprint.iacr.org/2018/643>
- [20] M. H. Miraz and D. C. Donald, "Atomic Cross-Chain Swaps: Development, Trajectory and Potential of Non-Monetary Digital Token Swap Facilities," *Annals of Emerging Technologies in Computing*, vol. 3, no. 1, pp. 42–50, Jan. 2019.
- [21] T. Griffith. (2019, Jun.) Atomic Swap Readiness. [Online]. Available: <https://swapready.net/> (Accessed 2019-11-09).
- [22] L. X. Lin, "Deconstructing Decentralized Exchanges," *Stanford Journal of Blockchain Law & Policy*, pp. 58–77, 1 2019, <https://stanford-jblp.pubpub.org/pub/deconstructing-dex>. [Online]. Available: <https://stanford-jblp.pubpub.org/pub/deconstructing-dex>
- [23] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges," 2019.
- [24] W. Warren and A. Bandeali, "0x: An open protocol for decentralized exchange on the Ethereum blockchain," Tech. Rep., 2017. [Online]. Available: https://github.com/0xProject/whitepaper/blob/master/0x_white_paper.pdf (Accessed 2019-11-04).
- [25] M. Oved and D. Mosites, "Swap: A Peer-to-Peer Protocol for Trading Ethereum Tokens," Tech. Rep., 2017. [Online]. Available: <https://swap.tech/whitepaper/> (Accessed 2020-06-01).
- [26] "IDEX: A Real-Time and High-Throughput Ethereum Smart Contract Exchange," Tech. Rep., 2019. [Online]. Available: <https://index.market/static/IDEX-Whitepaper-V0.7.6.pdf> (Accessed 2020-03-11).
- [27] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.
- [28] C. Chiarella and G. Iori, "A simulation analysis of the microstructure of double auction markets," *Quantitative Finance*, vol. 2, no. 5, pp. 346–353, 2002.
- [29] L. Deng, H. Chen, J. Zeng, and L.-J. Zhang, "Research on Cross-Chain Technology Based on Sidechain and Hash-Locking," in *Edge Computing – EDGE 2018*, S. Liu, B. Tekinerdogan, M. Aoyama, and L.-J. Zhang, Eds. Cham: Springer International Publishing, 2018, pp. 144–151.