

Article

Blockchain-Based Supply Chain for Postage Stamps

Yury Yanovich^{1, 2, 3, *}, Igor Shiyarov⁴, Timur Myaldzin^{4, 5}, Ivan Prokhorov^{1, 5}, Darya Korepanova^{1, 6} and Sergey Vorobyov^{1, 6}

¹ Software Department, Bitfury, 1016 BP, Amsterdam, The Netherlands; ivan.prokhorov@bitfury.com (I.P.); korepanova.darya@gmail.com (D.K.); sergey-vorobyov@mail.ru (S.V.)

² Center for Computational and Data-Intensive Science and Engineering, Skolkovo Institute of Science and Technology (Skoltech), 121205, Moscow, Russia

³ Laboratory of Data Mining and Predictive Modeling, Institute for Information Transmission Problems (IITP RAS), 127051, Moscow, Russia

⁴ Strategy Office, Russian Post, 131000, Moscow, Russia; igor.shiyarov@russianpost.ru (I.S.); timur.myaldzin@russianpost.ru (T.M.)

⁵ Department of Geography of World Economy, Faculty of Geography, Lomonosov Moscow State University, 119991, Moscow, Russia

⁶ Faculty of Computer Science, Higher School of Economics, 125319, Moscow, Russia

* Correspondence: yury.yanovich@bitfury.com; Tel.: +7-919-770-9649

Received: 18 September 2018; **Accepted:** 11 November 2018; **Published:** 15 November 2018

Abstract: Counterfeit and unaccounted postage stamps used on mailings cost postal administrations a significant amount of money each year. Corporate and individual clients become victim to stamp fraud and incur losses when security teams investigate such mailings. The blockchain technology is supposed to be a solution to make postage stamps market transparent and to guarantee invariability of stamps volume produced and used. The blockchain-based supply chain for postage stamps is introduced in the article.

Keywords: blockchain; supply chain; digital token

1. Introduction

Modern production and service companies generally represent different-scale network structures the nodes performing specific functions. Such structures are frameworks for high-tech value chains (for example, in the space or healthcare industries) or operations at a macroregional or even global level (Internet, international transport and mail). At the same time a distributed organization is associated with additional risks resulting from instability of material, financial and information flows. Supply Chain Management (SCM)—a set of approaches used to integrate suppliers, manufacturers and elements of the sales and distribution infrastructure to select the most efficient supply system, reduce total system costs and satisfy customer service requirements—is studying the problem [1].

Blockchain is a powerful tool for mitigating instability of various flows within network structures. It was first implemented in the Bitcoin cryptocurrency [2] and subsequently found applications in many other areas (state registers, SCM, biomedicine, finance, etc. [3–9]). Regarding SCM blockchain allows to formalize relationships between supply chain members mathematically, securing the required level of privacy.

The blockchain-based supply chain for postage stamps is considered in the article. Authors consider Russian Post as a reference organization. However, the possible application is not limited to a single entity as other post services are also interested with such systems and one could use the prototype for their needs [10]. The rest of the paper is organized as follows:

- The types of indicia and problems of their circulation are listed in Section 2.
- An overview of the blockchain technology is provided in Section 3.
- A general description of the proposed blockchain solution is introduced in Section 4.
- Pitfalls and possible directions for improvement are provided in Section 5.

2. Russian Post Indicia and Associated Risks

Russian Post (hereafter referred to as the Company) accepts mailings with the following indicia (Figure 1):

- meter stamps
- postage stamps
- printed postage impressions for envelopes and postcards (Printed postage impressions are not considered in this article because of the significant dominance of meter stamps and postage stamps in Russia).

2.1. Franking

Franking machines are primarily used by corporate clients processing mail in bulk. Franking machines of different capacity imprint indicium (meter stamp) and greatly speeding up the process of mail processing. Despite the fact that an official franking machine is not designed to print indicia with a face value exceeding the advance paid to the Company for future delivery services, a number of fraudulent schemes with postage meters have been revealed. In fraudulent schemes a franking machine owner is able to send mail for free imprinting false and not cash-backed meter stamps.



Figure 1. Russian post indicium types. Top left: modern meter stamp; top right: out of date meter stamp; bottom left: postage stamps; bottom right: printed postage impression.

In recent years the Company has made significant progress in combating the misuse of franking machines. All the franking machines in Russia are now integrated into a single IT accounting system and meter stamps are strengthened with new protection features.

Now each meter stamp contains a unique QR-code that contains information about mailing, franking machine and its digital signature. Using QR-codes significantly increases the processing speed.

2.2. Stamps

Unlike meter stamps, postage stamps are manually stuck on a mailing. Therefore, the range of their users is limited to individuals and small corporate clients. The cases of using stamps for bulk mailings (from 5000 units) are rare. However, the large size of Russian postage stamps market creates opportunities for fraudulent actors. The most popular schemes that affect the Company's revenue are:

- counterfeit postage stamps
- technically authentic postage stamps bypassing accounting systems.

Both cases, as well as less common in Russia stamps re-use can be considered as a violation of the order and rules of the supply chain "producer → distributor → the Company (sale of stamps) → sender → the Company (delivery) → receiver" where the amount of stamps and its face value cannot not be changed through the chain. Stamp fraud is not rare and revenue protection actions are complicated by the following factors.

Firstly, the Company does not have a monopoly over the Russian postage stamps market. No-name legal entities and individual entrepreneurs are the Company's competitors in corporate procurement. Unlike the production and distribution the sale

of stamps is demonopolized and informal market is flourishing. In fact such alternative suppliers are main source of counterfeit and unaccounted stamps.

Secondly, mail processing speed at postal offices and sorting centers is high and time required for a single stamp verification makes it difficult to perform control procedures without missing processing deadlines.

Thirdly, stamps exist “out of time” and the period of their use is not limited (except for particular issues or stamps with face value in non-denominated rubles), which makes it much more difficult and sometimes useless to reconcile the face value of purchased stamps with the total tariff of accepted mail from a client.

Fourthly, both individuals and corporate customers can use mailboxes bypassing the procedure of mail acceptance. Verification task in this case is transferred to the processing and delivery stages, where a high speed of operations makes it difficult to notice a suspicious stamp and carefully check it. It is important to note that the Company is not the only party losing from counterfeit postage.

A sender is also at risk: purchasing counterfeit stamps will incur a loss when mailings are detained and investigated by a postal security team.

The aforementioned drawbacks of stamps circulation are typical for many postal administrations.

The proposed solution might become a worldwide practice.

3. Blockchain

The blockchain is a distributed database using state machine replication with the following features:

- atomic changes to the database (transactions) are grouped into blocks
- integrity and tamper-resistance of the transaction log are assured by hash links among blocks.

Blockchain is jointly maintained by a number of parties (maintainers) with the security assumptions postulating that a certain fraction of these parties may be non-responsive or compromised at any moment during blockchain operation (i.e., Byzantine fault tolerance [11]).

The key points of the blockchain technology are [3, 12, 13]:

- Linked timestamping [14]: blockchain nature makes it possible to provide a universally verifiable proof of existence or absence of certain data or a state transition in the blockchain database.
- Blockchain uses a consensus algorithm [15, 16], which guarantees that non-compromised database copies have the same views at the database state.
- Applied cryptography routines (e.g., public-key digital signatures [17, 18]) are used to decentralize authentication and authorization of transactions occurring within the network. Transactions are created externally by the blockchain nodes. It limits the consequences of a node discredit.

We will refer to nodes having read access to the entire blockchain as full nodes, which in turn are subdivided into validator nodes (nodes that can add blocks to

the blockchain) and auditing nodes (nodes that have read-only access). Software transferring blockchain data to full nodes is referred to as client software.

Blockchain could mitigate lack of trust by implementing cryptographic accountability and auditability tools [12, 13]:

- As transactions are cryptographically authorized by logical originators of such transactions, blockchain eliminates the risks associated with the single point of failure posed by centralized authorization systems.
- Client-side data validation prevents man-in-the-middle attacks.
- The universality of cryptographic proofs provided to clients allows to securely transfer them to third parties (e.g., for tax accounting or as evidence in legal action).

Blockchains could be categorized by the level of access to the blockchain data [12, 13]:

- In public permissionless blockchains data is public. The consensus algorithm is censorship-resistant (e.g., proof of work used in Bitcoin) which ensures that maintainers are free to enter and leave the system. Write access to the blockchain is public, too. Maintainers accountability in permissionless blockchains is economically secured by prohibitively high cost of attacks in proof-of-work consensus.
- Private blockchains have a well-defined and restricted list of entities with read and write access to the blockchain (e.g., a group of banks, the regulator and law enforcement in a hypothetical banking blockchain). End users of services codified in the blockchain (i.e., bank clients in the example above) do not have any access to the blockchain data.
- Public permissioned blockchains restrict write access to the blockchain data similarly to private blockchains, but are designed to be universally auditable. These blockchains grant read broad access to end users.

The proposed solution is organized as a private blockchain with linked timestamping. The blockchain should be private to keep the Company's monopoly on the primary market. Timestamping in a private blockchain is the most common way to guarantee history invariableness and, therefore, protection of clients' rights. It could be implemented in Exonum (exonum.com), an extensible open-source framework for creating blockchain applications.

Exonum employs service-oriented architecture (SOA, [19]) and architecturally consists of three parts: services, clients, and middleware.

- Services as the most extensible part of the framework, encapsulates business logic of blockchain applications. An Exonum-powered blockchain may have a number of services; the same service can be deployed in various blockchains (possibly with prior configuration). Services have a degree of autonomy and each service performs logically complete and only necessary operations for a particular task. Services interface enables reuse and composability. In blockchain terms, services implement endpoints for processing transactions (cf. POST and PUT requests for HTTP REST services), as well as for read requests (cf. GET endpoints for HTTP REST services) that retrieve persistent information from the blockchain state (for the definition of blockchain state, see below).

- (Lightweight) clients have typical functionality of clients in SOA. They are originators of most transactions and read requests in the system and are correspondingly provided with cryptographic key management utilities and with tools to generate transactions and verify (also cryptographically) responses to read requests.
- Middleware reduces complexity of the system from the point of view of service developers and provides:
 - ordering and atomicity of transactions
 - interoperability among services and clients
 - replication of services among nodes in the network which is designed for service fault-tolerance and auditability by auditing nodes
 - management of service lifecycle (e.g., service deployment)
 - data persistence
 - access control
 - assistance with generating responses to read requests, etc.

4. Blockchain Architecture

We propose a blockchain-based solution for postage stamps circulation and accountancy. The blockchain will keep reliable records of all purchases (on both primary and secondary market) and mail acceptance and stamp cancellation procedures in order to guarantee the use of only officially purchased stamps. At the same time, the Company does not intend to abolish the secondary market leaving the opportunity to resell valid stamps, for example when there is no need for them anymore.

We introduce a digital asset—crypto token Stamp—which follows the physical stamp circulation in the proposed supply chain system. Operations of stamps emission, sale/re-sale and cancellation (when mail is accepted) are accompanied by corresponding transactions with Stamp token in the blockchain network.

4.1. Participants

Below are listed participants of the blockchain ecosystem:

- (Transactions) validators: the computing centres of Russian Post that perform the functions of blockchain validators [14]. The initial list of their public keys is written in the blockchain's genesis block and can subsequently be changed by the consensus of the validators. A high-performance computer with high-speed and reliable Internet access, as well as a private key from the list of validators, are required for their work. Validators check compliance of transactions entering the network with formal blockchain rules; compose blocks from the correct transactions, and participate in the consensus on adding new blocks to the blockchain
- (Token) issuers: Issuers need a computer with Internet access and a private key from the public key listed in the list of the blockchain maintainers to work. The list of privileged public keys is managed by validators. The status of issuer should be assigned to the Company as the only official seller of stamps at the primary market.

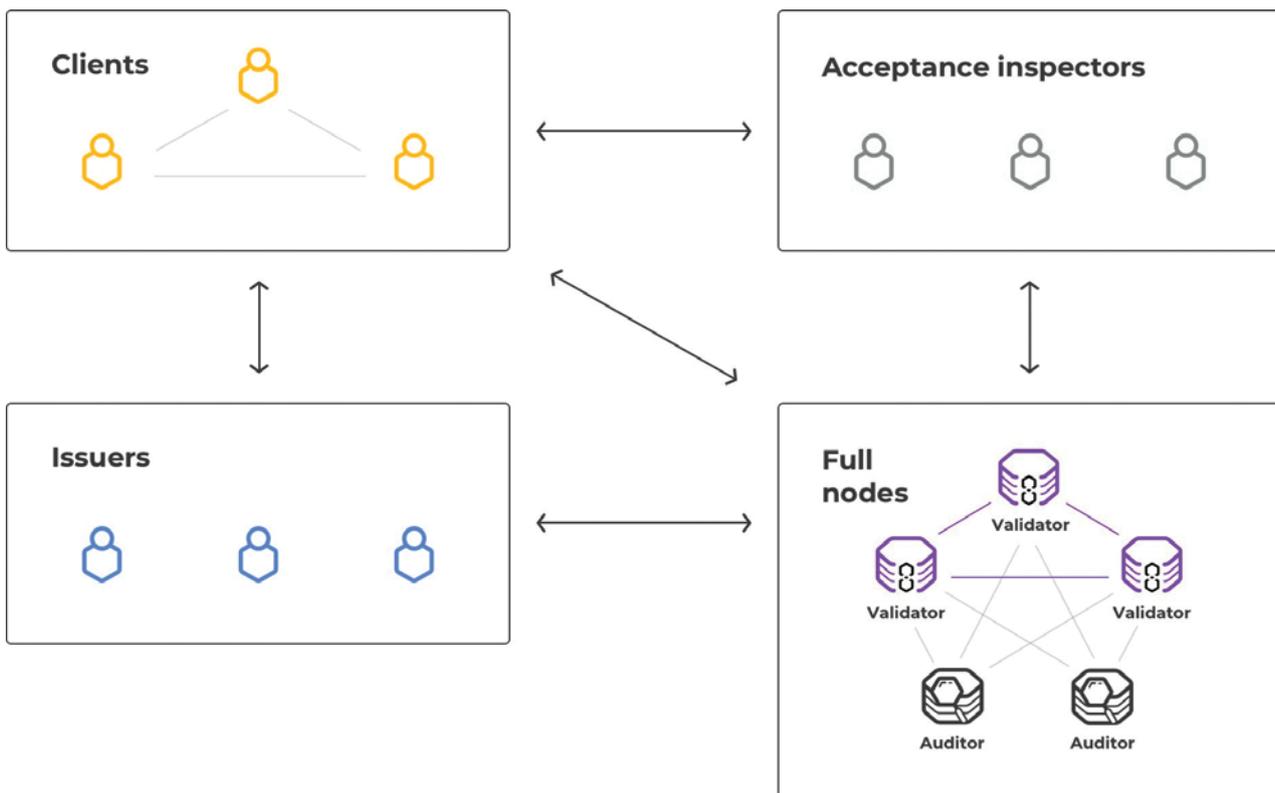
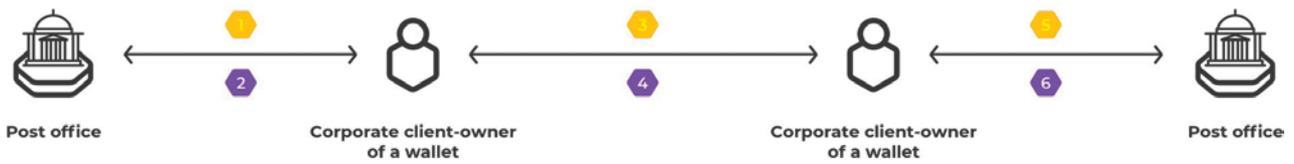


Figure 2. Blockchain network structure.

- (Postal) acceptance inspectors: the Company’s employees responsible for mail acceptance procedures and stamp (both physical and token) cancellation. They need a computer with Internet access and a private key corresponding to the public key from the list of receivers recorded in the blockchain to work.
- Clients: all legal entities participating in the stamps market according to the rules established for corporate clients. They need a smartphone or computer with Internet access to work. Each client is associated with one or several public keys and can receive tokens from the Company or another client that purchased tokens from the Company. Using its private key(s) it can transfer tokens to other participants and create transactions for the provision of postal services.
- Auditors: authorized Company’s representatives and other organizations that hold private keys from the public ones and are included in the list of auditors. They need a computer with an Internet connection to work. Auditors guarantee the correctness of the system performance.

Validators and auditors are the only parties with read access to the whole blockchain. Other users get cryptographic proof of the presence and position of the known transactions in the blockchain [12, 13, 20].

The interaction between participants is represented in Figure 2.



Transaction

- A corporate client purchases stamps from the Company.
- Transfer of stamp from one corporate client to another (secondary market)
- Acceptance of mail with stamps and cancellation

Record of transaction in blockchain

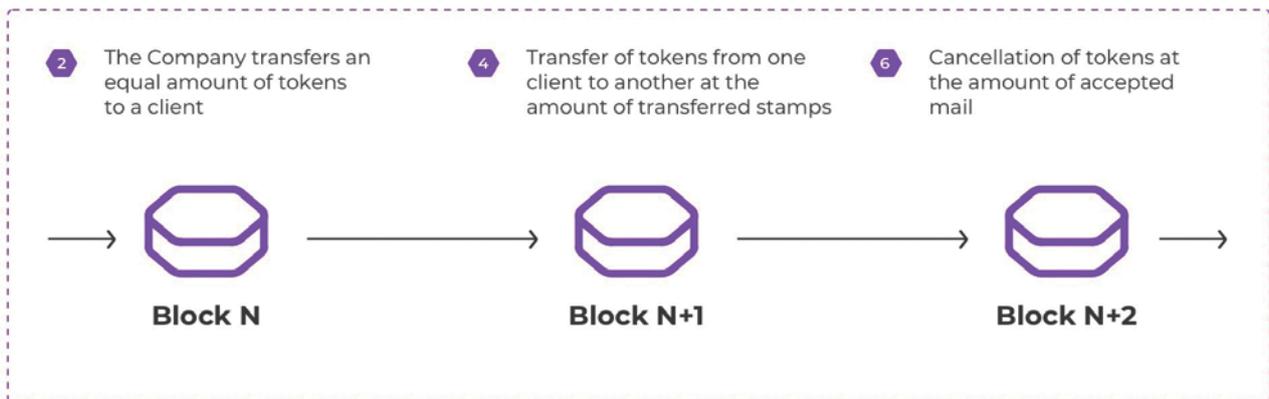


Figure 3. Blockchain-based solution for postage stamps circulation.

4.2. Transactions

The following types of transactions are provided in the blockchain:

- Stamp token emission.
- Tokens transfer. It is possible to launch the platform on a basis of anonymous scheme using evidence with zero disclosure similar to the mechanism of ZCash cryptocurrency [21] instead of a Bitcoin’s pseudo-anonymous scheme [22–29]. It will increase the level of customer privacy.
- Mail preparation: reservation of tokens in amount of mailings to be sent.
- Token cancellation and mail acceptance with stamps cancellation: In order to make the system flexible and efficient we add reverse transactions for token emission, mail preparation and stamps cancellation. Reverse transactions should have limited time to be performed and should be signed by the privileged issuers and acceptance inspectors correspondingly.

4.3. Token Emission and Circulation

Stamp token follows physical stamp circulation in the proposed supply chain system, so the only way to issue tokens is to let physical stamps into circulation. The two emission situations are:

- Purchase of new stamps from the Company
- Declaration of uncanceled stamps, acquired prior to blockchain platform launch. Token transfer transactions would be free of charge.

4.4. Workflow

Postage stamps circulation in the proposed system is represented in Figure 3 and consists of the following steps:

- 1–2. A corporate client purchases stamps from the Company off-chain. Simultaneously, the Company transfers an equal amount of tokens to a client via blockchain.
- 3–4. One corporate client can transfer stamps to another corporate client, i.e., make a deal on a secondary market. He should also make a blockchain token transfer transaction at the same amount of stamps.
- 5–6. A corporate client can send mailings for stamps. From blockchain point of view, the client has to generate mail preparation transaction which declares the mailing parameters and freezes tokens, if mail acceptance inspector can process the operation, he sends transaction which finalizes mailing procedure and burns the client's frozen tokens.

4.5. Demo Code

The demo code is available on <https://github.com/korepkorep/russian-post>.

5. Pitfalls and Future Work

5.1. Denial-of-Service Attack with Transactions

As token transfer transactions would be free of charge, the denial-of-service (DoS) attack with a massive set of transfer transactions may take place. An attack may fill a pull of unconfirmed transactions and slightly increase latency between transaction appearance and its inclusion into a block. The dynamic fractional reserves could be proposed to prevent such a spam [30]. The block capacity is limited similar to bandwidth of Internet channel. However, blocks are expected to be underutilized as modern private blockchains have a high transaction per second rate (see [31] and <https://github.com/exonum/exonum-doc/blob/master/src/get-started/what-is-exonum.md#performance>).

With the fractional reserve model the blockchain will automatically adjust the reserve ratio for the network in case of congestion. The blockchain will set target utilization that leaves enough block space for transaction peaks. Any time peaks are sustained the blockchain reduces the maximum bandwidth-per-share. When a peak is over and there is excess capacity the blockchain can slowly increase the bandwidth-per-share.

5.2. Pseudoanonymity vs Anonymity

All history of tokens owning and transferring (addresses and transactions) is available for blockchain maintainers. But real-world owners of addresses could be unknown in general. Such a system is pseudo-anonymous [22,28]. However, some addresses can be grouped by their ownership using behavior patterns or publicly available information

from off-chain sources. To make the system entirely anonymous, we are going to include ring signatures [32] or zero-knowledge proofs [21].

6. Conclusions

The blockchain-based solution for indicia (stamps) accountancy was proposed in the paper. It prevents usage of invalid and counterfeit stamps and inspires trust among participants in the secondary market. The solution keeps clients pseudoanonymous and guarantees confidentiality of operations.

Author Contributions: Conceptualization, Y.Y., I.S., T.M. and I.P.; Methodology, Y.Y., T.M. and I.P.; Software, D.K. and S.V., Writing—Original Draft Preparation, Y.Y. and T.M., Writing—Review and Editing, I.S., I.P., D.K. and S.V., Project Administration, Y.Y. and I.S.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Simchi-Levi, D.; Simchi-Levi, E.; Kaminsky, P. *Designing and Managing the Supply Chain: Concepts, Strategies, and Case Studies*; McGraw-Hill: New York, NY, USA; Irwin: Huntersville, NC, USA, 2003; p. 354.
2. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 14 November 2018).
3. Swan, M. Summary for Policymakers. In *Climate Change 2013—The Physical Science Basis*; Intergovernmental Panel on Climate Change; Cambridge University Press: Cambridge, UK, 2015; pp. 1–30.
4. Pilkington, M. Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK, 2016; pp. 225–253.
5. Kim, H. M.; Laskowski, M. Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance. *SSRN Electron. J.* 2016, 25, 18–27. [[CrossRef](#)]
6. Korpela, K.; Hallikas, J.; Dahlberg, T. Digital Supply Chain Transformation toward Blockchain Integration. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, Waikoloa, HI, USA, 4–7 January 2017; pp. 4182–4191.
7. Kuo, T. T.; Kim, H. E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* 2017, 24, 1211–1220. [[CrossRef](#)] [[PubMed](#)]
8. Angraal, S.; Krumholz, H. M.; Schulz, W. L. Blockchain Technology. *Circ. Cardiovasc. Qual. Outcomes*, 2017, 10, 5665–5690. [[CrossRef](#)] [[PubMed](#)]
9. Mamoshina, P.; Ojomoko, L.; Yanovich, Y.; Ostrovski, A.; Botezatu, A.; Prikhodko, P.; Izumchenko, E.; Aliper, A.; Romantsov, K.; Zhebrak, A.; et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget*, 2018, 9, 5665–5690. [[CrossRef](#)] [[PubMed](#)]
10. U.S. Postal Service OIG. Blockchain Technology: Possibilities for the U.S. Postal Service RARC Report. 2016. Available online: <https://www.oversight.gov/report/usps/blockchain-technology-possibilities-us-postal-service> (accessed on 14 November 2018).
11. Lamport, L.; Smith, P. M. Byzantine clock synchronization. *ACM SIGOPS Oper. Syst. Rev.* 1986, 20, 10–16. [[CrossRef](#)]
12. Bitfury Group; Garzik, J. *Public Versus Private Blockchains, Part 1: Permissioned Blockchains*; Bitfury: Washington, DC, USA, 2015; pp. 1–23.

13. Bitfury Group; Garzik, J. *Public Versus Private Blockchains, Part 2: Permissionless Blockchains*; Bitfury: Washington, DC, USA, 2015; pp. 1–20.
14. Bitfury Group. *On Blockchain Auditability*; Bitfury: Washington, DC, USA, 2016; pp. 1–40.
15. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* 1982, 4, 382–401. [CrossRef]
16. Breiting, C.; Gipp, B. VirtualPatent—Enabling the Traceability of Ideas Shared Online using Decentralized Trusted Timestamping. In Proceedings of the 15th International Symposium of Information Science, Seattle, WA, USA, 7–9 November 2017; pp. 89–95.
17. Dwork, C.; Lynch, N.; Stockmeyer, L. Consensus in the presence of partial synchrony. *J. ACM* 1988, 35, 288–323. [CrossRef]
18. Salomaa, A. *Public-Key Cryptography*; Springer: Berlin, Germany, 1996; p. 275.
19. Erl, T. *Service-Oriented Architecture, Concepts, Technology, and Design*; Prentice Hall: Upper Saddle River, NJ, USA, 2005; p. 792.
20. Bitfury Group. *Digital Assets on Public Blockchains*; Bitfury: Washington, DC, USA, 2016; pp. 1–37.
21. Ben-Sasson, E.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M.; Sasson, E. B.; Chiesa, A.; Garman, C.; et al. Zerocash: Practical Decentralized Anonymous E-Cash from Bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–21 May 2014; pp. 459–474.
22. ShenTu, Q.; Yu, J. Research on Anonymization and De-anonymization in the Bitcoin System. *arXiv*, 2015, arXiv:1510.07782.
23. Reid, F.; Harrigan, M. An Analysis of Anonymity in the Bitcoin System. In *Security and Privacy in Social Networks*; Springer: New York, NY, USA, 2013; pp. 197–223.
24. Ron, D.; Shamir, A. *Quantitative Analysis of the Full Bitcoin Transaction Graph*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 6–24.
25. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet Things J.* 2017, 4, 1250–1258, doi:10.1109/JIOT.2017.2694844. [CrossRef]
26. Bonneau, J.; Narayanan, A.; Miller, A.; Clark, J.; Kroll, J. A.; Felten, E. W. Mixcoin: Anonymity for Bitcoin with Accountable Mixes. In Proceedings of the Financial Cryptography and Data Security, Christ Church, New Zealand, 3 March 2014–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8437, pp. 486–504.
27. Biryukov, A.; Pustogarov, I. Bitcoin over Tor isn't a Good Idea. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 122–134.
28. Yanovich, Y.; Mischenko, P.; Ostrovskiy, A. *Shared Send Untangling in Bitcoin*; Bitfury: Washington, DC, USA, 2016; Volume 2016, pp. 1–25.
29. Ermilov, D.; Panov, M.; Yanovich, Y. Automatic Bitcoin Address Clustering. In Proceedings of the 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, 18–21 December 2017; pp. 461–466.
30. Steemit. *Steem: An Incentivized, Blockchain-Based, Public Content Platform*; Steemit: New York, NY, USA, 2017; pp. 1–32.
31. Androulaki, E.; Manevich, Y.; Muralidharan, S.; Murthy, C.; Nguyen, B.; Sethi, M.; Singh, G.; Smith, K.; Sorniotti, A.; Stathakopoulou, C.; et al. Hyperledger fabric. In Proceedings of the Thirteenth EuroSys Conference (EuroSys '18), Porto, Portugal, 23–26 April 2018; ACM Press: New York, New York, USA, 2018; pp. 1–15.
32. Noether, S.; Mackenzie, A.; The Monero Research Lab. Ring Confidential Transactions. *Ledger*, 2016, 1, 1–18. [CrossRef]

Full text <https://www.mdpi.com/2227-9709/5/4/42/htm>



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).