BITFURY
Exonum

Blockchain-Based Solution to Prevent Postage Stamps Fraud

Darya Korepanova, Stanislav Kruglik, Yash Madhwal, Timur Myaldzin, Ivan Prokhorov, Igor Shiyanov, Sergey Vorobyov and Yury Yanovich

Abstract

Counterfeit stamps cause considerable financial damage to the states and companies. The blockchain-based supply chain management system for their market is proposed in the article. It can make stamps circulation transparent and guarantee invariability of stamps volume produced and used. The technical description and performance tests of the proposed system are provided.

1. INTRODUCTION

A blockchain is a powerful tool which increases trust in network structures through applied cryptography and transaction history immutability. It was first implemented in the Bitcoin cryptocurrency [1] and subsequently found applications in many other areas (state registers, supply chain management task (SCM), biomedicine, etc. [2, 3, 4, 5, 6, 7, 8, 9, 10]). SCM blockchain allows formalizing relationships between supply chain members mathematically, securing the required level of privacy.

The blockchain-based supply chain for postage stamps is considered in the paper. It was shown that postal stamp circulation could be considered as SCM [11] and illegal changes in it cause considerable financial damage to the states and companies [12, 13, 14] The proposed research is a continuation of the previous study [15]. We provide detailed technical, solution description and performance tests in the present one. Authors consider Russian Post (hereafter referred to as the Company) as a reference organization but it must be mentioned that the proposed solution can be generalized to other indicia. The rest of the paper is organized as follows. The indicia and its circulation issues are listed in Section 2. A technical description of the proposed blockchain solution is introduced in Section 3. Experimental design and results are provided in Section 4. The obtained results are discussed in Section 5. The paper is concluded in the Conclusion section.

2. RUSSIAN POST INDICIA AND ASSOCIATED RISKS

The company accepts mailings with the following indicia: meter stamps, postage stamps and printed postage impressions for envelopes and postcards. We limited our research to the first two types only due to the limited spread of the last type in Russia.

2.1. Meter stamps and franking machines

Franking machines are primarily used by corporate clients processing mail in bulk. Franking machines of different capacity imprint indicium (meter stamp) and significantly speeding up the process of mail processing. Even though 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, many fraudulent schemes with postage meters have been revealed. In fraudulent schemes, a franking machine owner can send mail for free by imprinting false and not cash-backed meter stamps.

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 mail. 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 or technically authenticating postage stamps bypassing accounting systems. Both cases, as well as less frequent in Russia stamps re-use can be considered as a violation of the order and rules of the postal stamps supply chain. These actions are not rare, and the following factors complicate revenue protection actions.

First, the Company does not have a monopoly over the Russian postage stamps market. Unlike the production and distribution, the sale of stamps is demonopolized and informal market is flourishing. Alternative suppliers are the primary source of counterfeit and unaccounted stamps.

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

Third, the period of stamps use is not limited (except for particular issues or stamps with a 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 standard mail from a client.

Fourth, 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 incur a loss when mailings are detained and investigated by a postal security team.

The drawbacks mentioned above of stamps circulation are typical for many postal administrations. The proposed solution might become a worldwide practice.

3. PROPOSED SOLUTION

Blockchains could be categorized by the level of access to the blockchain data [16, 17] and the proposed solution is organized as a private permissioned blockchain with linked timestamping. The blockchain for stamps circulation should be private to keep the Company's monopoly on the primary market, and it could be permissioned to increase the user's privacy. Timestamping in a private blockchain is the most common way to guarantee history invariableness and, therefore, protection of clients' rights. We implemented the system on an extensible open-source framework for creating blockchain applications called Exonum [18].

To perform experiments, we created Exonum based digital cryptocurrency that circulates in the same manner as the real physical stamp in the investigated supply chain model. In more detail, we associate with each physical stamp the cryptocurrency entity or simply crypto token. As in typical cryptocurrency, each token can be emitted, sold and retailed. In addition to these operations, each token can be cancelled that corresponds to the case then appropriate physical stamp was used in mail sending. The proposed blockchain system keep a reliable record of the whole circulation of tokens to guarantee that each physical stamp was used only once and secondary users can trust that physical stamp is valid. It is the private blockchain system in which only validators and auditors have read access to the whole blockchain. Below we determine existing participants in our system and other technical details about transactions and workflow.

3.1. Participants

In our system, we determine five different types of users with different rights and functionality.

- **Validators**: maintain the whole blockchain network. They check the correctness of transactions entering the network, form a new block and participate in the consensus algorithm. Their initial public keys are stored in blockchain genesis block and can be later changed through validator's consensus.
- **Token issuers**: entities that can emit new tokens. System maintainers choose their private keys and managed by validators.
- **Acceptance inspector**: entities that can cancel the token after physical stamp of the corresponding real-life stamp.
- **Clients**: users of blockchain network, they are associated with one or several public keys and can participate in token's lifecycle. By utilizing their private keys, they can transfer tokens to other clients.
- **Auditors**: external users who can check the correctness of consensus protocol in the whole blockchain network.

All participants can monitor the current status of known tokens in the blockchain and their proof of correctness. Only validators and auditors have read access to the whole network.

3.2. System structure

The whole deployed system can be divided into four parts presented below

- **Wallet:** users data to be stored in the blockchain according to the business logic of the application

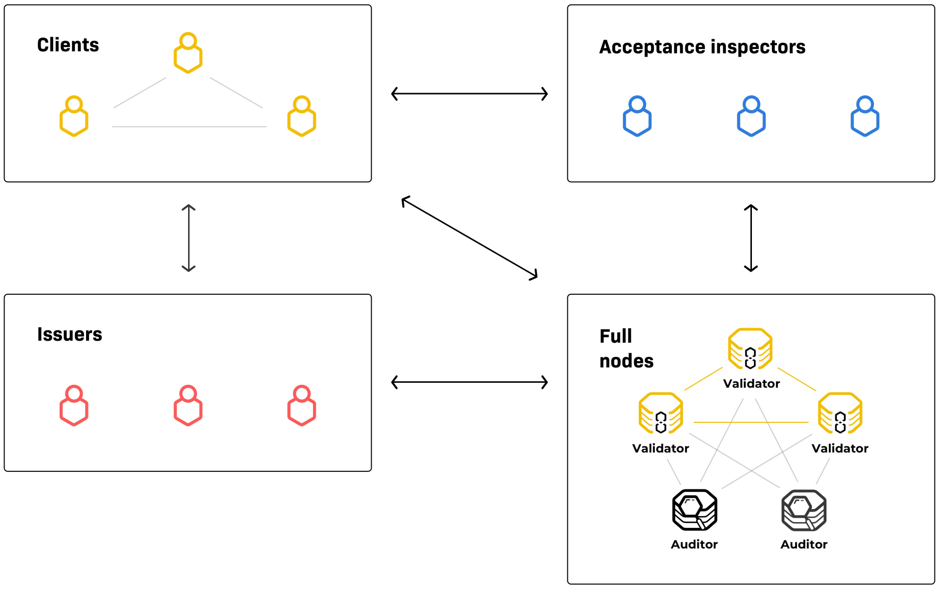

Figure 1: Blockchain network structure

- **Schema:** a structured view of the key-value storage, the architecture of the on-chain database
- **Transactions:** kind of messages whose perform atomic actions on the blockchain state
- **API (application programming interface):** a set of clearly defined methods of communication among users and blockchain nodes.

Below we will determine their structure before that let us determine the typical workflow for each type of system users. The client workflow looks as follows: a client creates Wallet by adding initial funds, after that Wallet and necessary information (holder, history, etc.) is written into the Schema. To send or spend tokens, which are in the clients wallet, the holder deploys transactions, changing his wallet balance. These types of transactions are free of charge. All changes are reflected in the Schema. As the blockchain contains all the required information, the client may check for correctness of the interaction via API. These actions are presented in Figure 2. Token issuers, as well as acceptance inspectors, can change the total amount of tokens in the system by changing the balance in users' wallets through the corresponding transaction. Validators check the correctness of transactions and group them in blocks while auditors check the correctness of these actions.

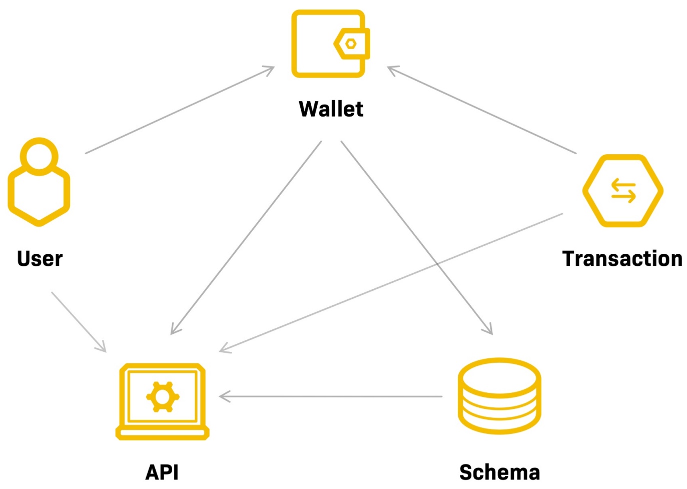

Figure 2: Typical client workflow

3.2.1. Wallets

The wallet corresponds to the place that stores each user's token balance. In systems it represents as a structure that contains five fields: `pub_key`, name, balance, `history_len`, `history_hash`. The first field of the wallet is a public key of the holder. The holder can change the state of the wallet via transactions, as described above. The second and third fields of the structure mean name and balance of the wallet. Initial wallet balance is 100 stamps, and it may be changed. `history_len` and `history_hash` describe how many operations a wallet holder made.

3.2.2. Schema

The schema represents the architecture of the internal on-chain database. In it, we differentiate two different views of storage. The first one, Snapshot, is used in reading requests and corresponds to an immutable view of the storage, the second one, Fork, is used in the transaction process and correspond to a mutable view of storage where the changes can be easily rolled back. Current storage view is declared as a generic wrapper. It must be mentioned that Snapshot provides random access to every piece of data inside the database and to isolate the wallets map into a separate entity we have to add a unique prefix to it.

3.2.3. Transactions

We differentiate six types of transactions that correspond to the possible actions in the investigated system and present them below

- **Transfer transaction** corresponds to the standard procedure of token transfer from one to another wallet. It has four fields. The first one is from. This field contains the sender's public key. The second one is to. This field contains the recipient's public key. The third one is the amount. It contains information "How many funds we are going to transfer". The last one is the seed. This field is special, because we need it, to avoid repetition of the same transactions.

- **Issue transaction** corresponds to token emission operation made by the issuer. It has four fields. The first one is `pub_key`. This field contains the public key of the wallet holder, whose wallet balance should be increased. The second one is the issuer_key. This field contains the public key of the issuer. The third one is the amount. It contains information "How many funds we are going to issue". The last one is the seed. This field is special, because we need it, to avoid repetition of the same transactions.

- **Create wallet transaction** corresponds to the appearance of a new client in the system. It has two fields. The first one is `pub_key`. This field contains the public key of the wallet creator. The second one is name. This field contains the name of the wallet.

- **Mail preparation transaction** corresponds to the reservation of tokens in the amount that needs to send necessary physical mails. It has four fields. The first one is meta. It contains information about stamping. For example, "I would like to stamp 3000 tokens". The second one is `pub_key`. It contains information about the entity public key. The third one is the amount. This field is about the number of tokens that should be stamped. The last field is the seed field.

- **Mail acceptance transaction** corresponds to the accept/reject Mail Preparation transaction by the inspector It has five fields. The first one is `pub_key`. It contains information about inspector public key. The second one is `sender_key`. It contains information about person public key who wants to stamp tokens. The third one is the amount. This field is about the number of tokens that should be stamped. The fourth one is accept. This field is about the inspector's decision (Accept or reject). The last field is the seed field.

- **Cancellation transaction** corresponds physical stamp cancellation by inspector. This kind of transaction needs three fields. The first one is `pub_key`. This field contains the public key of the inspector. The second one is `sender_key`. This field contains the public key of the transaction creator. The last one is `tx_hash`. This field contains the hash of transaction that should be cancelled.

3.2.4. API

To organize end-user interaction with the investigated system, we implemented the node API. With this aim we declare an empty struct that includes a set of methods which consist of information about the connection to the blockchain node instance as well as blockchain instance itself, that needs to implement read requests.

4. EXPERIMENTS

We performed experiments in a single data center (DC) and used twenty-one virtual machines (16 validators, 4 clients, 1 auditor). Each validator was running on a separate virtual machine with 3.75 GiB RAM, 2 Core Intel Xeon Platinum CPUs running @3.4GHz, and the blockchain database was stored on an elastic block store (EBS) drive connected to each instance. Nodes used Exonum version 0.9. All virtual machines were in one availability zone within one Amazon Web Services region (EU-central-1). The demo code is available on https://github.com/korepkorep/russian-post.

4.1. Blockchain Design

In all experiments the following consensus parameters were used: block capacity of 2000 transactions, propose timeout of 0 seconds and signature size of 64 bytes.

Four generators send different types of transactions to all validators during the experiments with a constant flow. The flow is chosen to be a bit bigger than the blockchain tps. Each validator check transaction signature before its addition into the pool of unconfirmed transaction. The given scenario could be considered as a real-life high-load mode.

4.2. Performance Tests

We measured transactions per second (`TPS`, the bigger, the better) for the different total amount of validators. The results were averaged over 100 000 transactions processing for each case. The mean value and standard deviation were of interest.

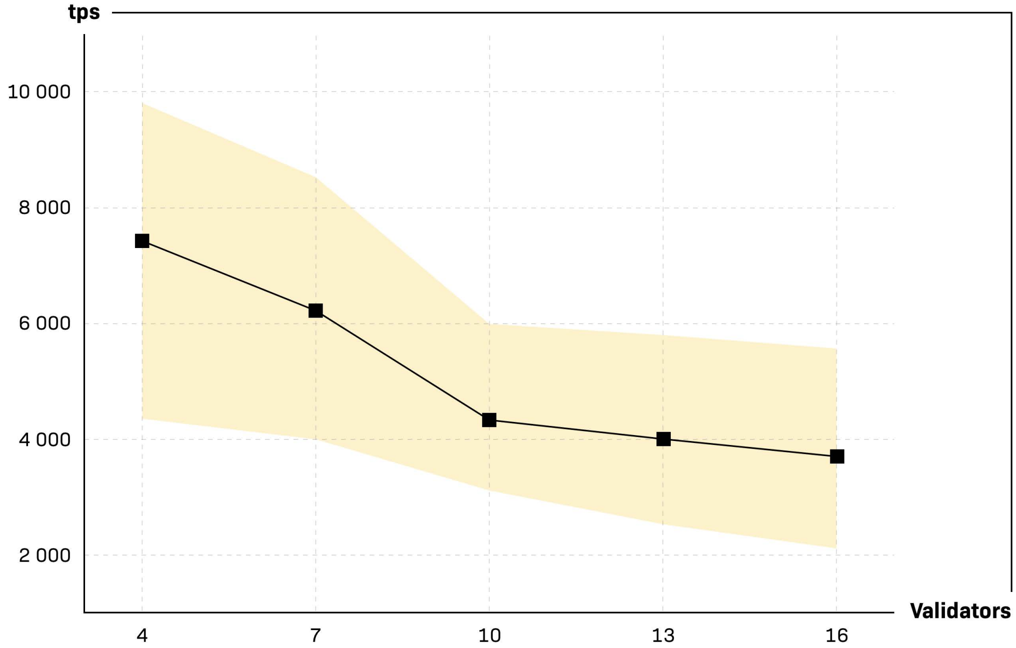

Figure 3: **TPS** as a function of validators number

Note. Almost all the blocks were filled with transactions in our experiments, so one can estimate block acceptance time in seconds as 2000/`TPS`.

4.2.1. Different Validators Number

The number of consensus messages over network grows as a square of validators number in Exonum. It decreases blockchain performance. We considered different number of validators to estimate this effect. `TPS` experimental results are in Figure 3.

Exonum shows more than 5000 `TPS` with block faster than each 0.5 seconds on average. This amount decreases with the validators number increase from 7100 `TPS` to 3700 `TPS`.

4.2.2. Fail-Stop Validators

The simplest model of validators failures is fail-stop. We choose it to demonstrate how does improper nodes behaviour slow consensus down. The total number of validators was 16 and from 0 to 5 were stopped (up to 1/3, which is the maximum allowed the number of fail parties as Exonum uses Byzantine fault-tolerant algorithm [19, 20, 21]). `TPS` as functions of working validators fraction are in Figures 4 correspondingly.

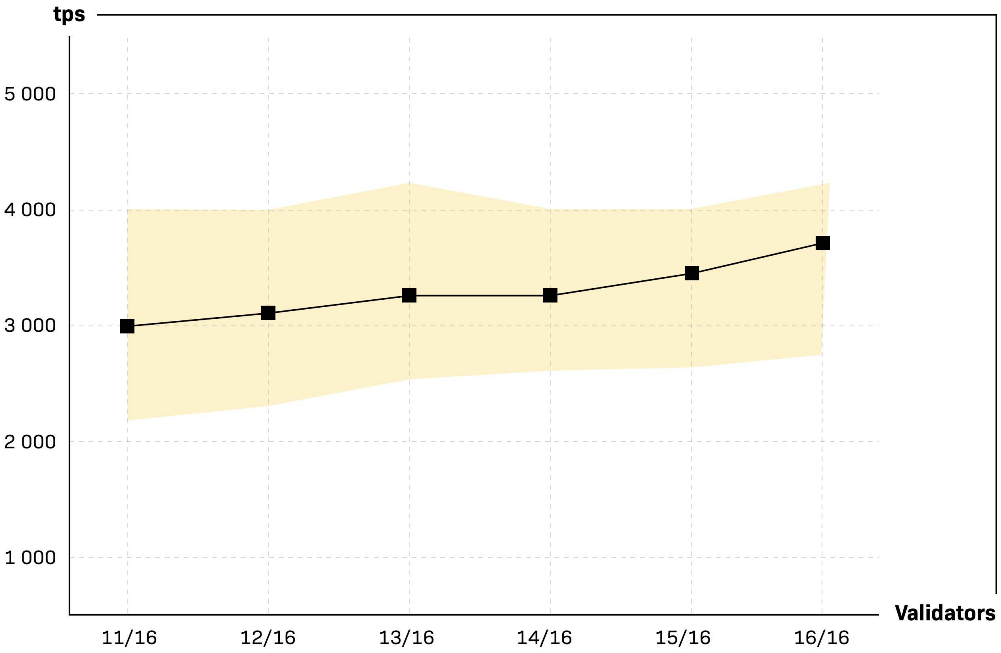

Figure 4: **TPS** as a function of working validators fraction

Exonum shows more than 3000 TPS for the cryptocurrency for maximum allowed number of the fail stop validators with the total number of validators equals to 16. This amount decreases with a working validators fraction decrease up to 20% maximum value. The number of fail-stop validators increase TPS variance.

5. DISCUSSION

5.1. Results of performance tests

The proposed system has a throughput of around 5000 TPS which is enough to handle with around 400 million Russian Post mailings per year [22] Since a single transaction can contain information about bulk mailings. Also, fail-stops validators test shows that in the real-life system with the limited number of validators can effectively deal with improper validators behaviour including offline during scheduled maintenance as the decreased capacity still meet system requirements.

5.2. *Denial-of-Service Attack with Transactions*

Because in the proposed system the token transfer transaction is free of charge the malefactors can generate a massive set of transfer transactions to make the denial-of-service attack. One of the possible approach to handle with it is dynamic fractional reserves in which we limit block capacity similarly as the Internet [23]. In it, we automatically adjust the reserve ratio for the network in case of congestion. Namely, the system automatically set target utilization that leaves enough block space for transaction peaks. Any time peaks are sustained the blockchain reduces the maximum bandwidth-per-share and when a peak is over it slowly increases this parameter.

5.3. *Pseudoanonymity vs Anonymity*

The proposed system is pseudo-anonymous [24, 25], namely, all history of tokens owning and transferring is available for blockchain maintainers although real-world token owners can be unknown in general even though we can group them using publicly available external information and behavior patterns [26, 27, 28]. In future work, to make the system entirely anonymous, we can include ring signatures [29] or zero-knowledge proofs [30].

6. CONCLUSIONS

The blockchain-based solution for postage stamps accountancy is considered in the paper. Its technical description, implementation and performance tests are proposed. The solution prevents usage of invalid and counterfeit stamps and inspires trust among participants in the secondary market. The performance tests show that the proposed solution meets the subject area of real-life throughput requirements.

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *www.bitcoin.org*, pp. 1–9, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] M. Swan, “Summary for Policymakers,” in *Climate Change 2013 - The Physical Science Basis*, Intergovernmental Panel on Climate Change, Ed. Cambridge: Cambridge University Press, 2015, pp. 1–30.

[3] M. Pilkington, “Blockchain Technology: Principles and Applications,” in *Research Handbook on Digital Transformations*. Springer, 2016, pp. 225 – 253.

[4] H. M. Kim and M. Laskowski, “Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance,” *SSRN Electronic Journal*, vol. 25, no. 1, pp. 18–27, 8 2016. [Online]. Available: http://www.ssrn.com/abstract=2828369

[5] K. Korpela, J. Hallikas, and T. Dahlberg, “Digital Supply Chain Transformation toward Blockchain Integration,” in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 1 2017, pp. 4182–4191.

[6] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 11 2017.

[7] S. Angraal, H. M. Krumholz, and W. L. Schulz, “Blockchain Technology,” *Circulation: Cardiovascular Quality and Outcomes*, vol. 10, no. 9, pp. 5665–5690, 9 2017.

[8] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak, I. O. Ogu, and A. Zhavoronkov, “Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare,” *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, 1 2018. [Online]. Available: http://www.oncotarget.com/fulltext/22345

[9] M. Kouhizadeh and J. Sarkis, “Blockchain Practices, Potentials, and Perspectives in Greening Supply Chains,” *Sustainability*, vol. 10, no. 10, p. 3652, 10 2018. [Online]. Available: http://www.mdpi.com/2071-1050/10/10/3652

[10] N. Alzahrani and N. Bulusu, “Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain,” in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock’18*. New York, New York, USA: ACM Press, 2018, pp. 30–35.

[11] D. Simchi-Levi, E. Simchi-Levi, and P. Kaminsky, *Designing and Managing the Supply Chain: concepts, strategies, and case studies*. McGraw-Hill/Irwin, 2003.

[12] J. Winter, “Counterfeit Stamps Giving Postal Service a Lickin,” 2010. [Online]. Available: https://www.foxnews.com/us/counterfeit-stamps-giving-postal-service-a-lickin

[13] R. Gratton, “Counterfeit stamps cost Canada Post millions a year, expert says,” *CBC*, 2013. [Online]. Available: https://www.cbc.ca/news/canada/montreal/counterfeit-stamps-cost-canada-post-millions-a-year-expert-says-1.1375040

[14] D. Kryukov and A. Papandina, “Fake for billions,” *Rbc.ru*, 2016. [Online]. Available: https://www.rbc.ru/newspaper/2016/10/05/57f37aae9a794771a6e42728

[15] Y. Yanovich, I. Shiyanov, T. Myaldzin, I. Prokhorov, D. Korepanova, and S. Vorobyov, “Blockchain-Based Supply Chain for Postage Stamps,” *Informatics*, vol. 5, no. 4, p. 42, 11 2018.

[16] Bitfury Group and J. Garzik, “Public versus Private Blockchains. Part 1: Permissioned Blockchains,” *bitfury.com*, pp. 1–23, 2015. [Online]. Available: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf

[17] ——, “Public versus Private Blockchains Part 2: Permissionless Blockchains,” *bitfury.com*, pp. 1–20, 2015. [Online]. Available: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt2-1.pdf

[18] Y. Yanovich, I. Ivashchenko, A. Ostrovsky, A. Shevchenko, and A. Sidorov, “Exonum: Byzantine fault tolerant protocol for blockchains,” *bitfury.com*, pp. 1–36, 2018.

[19] C. Dwork, N. Lynch, and L. Stockmeyer, “Consensus in the presence of partial synchrony,” *Journal of the ACM*, vol. 35, no. 2, pp. 288–323, 4 1988. [Online]. Available: http://portal.acm.org/citation.cfm?doid=42282.42283

[20] N. Lynch, *Distributed Algorithms*. Morgan Kaufmann Publishers, 1996.

[21] J. Dollimore, T. Kindberg, and G. Coulouris, “Distributed Systems: Concepts and Design,” p. 944, 2005.

[22] Russian Post, "Russian Post Revenue in 2017 increased by 8.1% to 178.1 billion rubles (russian)," 2018. [Online]. Available: https://www.pochta.ru/news-list/item/2329582471

[23] Steemit, "Steem: An incentivized, blockchain-based, public content platform." *Steem.io*, pp. 1–32, 2017. [Online]. Available: https://steem.io/SteemWhitePaper.pdf

[24] Q. ShenTu and J. Yu, "Research on Anonymization and De-anonymization in the Bitcoin System," *arXiv*, pp. 1–14, 2015. [Online]. Available: http://arxiv.org/abs/1510.07782

[25] Y. Yanovich, P. Mischenko, and A. Ostrovskiy, "Shared Send Untangling in Bitcoin," *bitfury.com*, vol. 2016, pp. 1–25, 2016.

[26] A. Biryukov and I. Pustogarov, "Bitcoin over Tor isn't a Good Idea," in *2015 IEEE Symposium on Security and Privacy*. IEEE, 5 2015, pp. 122–134. [Online]. Available: http://ieeexplore.ieee.org/document/7163022/

[27] D. Ermilov, M. Panov, and Y. Yanovich, "Automatic Bitcoin Address Clustering," in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 12 2017, pp. 461–466. [Online]. Available: http://ieeexplore.ieee.org/document/8260674/

[28] S. S. Chawathe, "Clustering Blockchain Data." Springer, Cham, 2019, pp. 43–72.

[29] S. Noether, A. Mackenzie, and T. M. Research Lab, "Ring Confidential Transactions," *Ledger*, vol. 1, no. 0, pp. 1–18, 12 2016. [Online]. Available: http://ledger.pitt.edu/ojs/index.php/ledger/article/view/34

[30] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Practical Decentralized Anonymous E-Cash from Bitcoin," in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. IEEE, 5 2014, pp. 459–474.