Token Standard for Heterogeneous Assets Digitization into Commodity

Vyacheslav Davydov
Moscow Financial University at Government
125993, Moscow, Russia
+7-499-943-9582
novdav2017@yandex.ru

Yash Madhwal
Skolkovo Institute of Science and Technology
121205 Moscow, Russia,
+7-495-280-1481
yash.madhwal@skoltech.ru

Alexander Gazaryan
National Research University Higher School of Economics
125319, Moscow, Russia
+7-495-771-3232
aggazaryan@edu.hse.ru

Yury Yanovich
Bitfury
123100 Moscow, Russia,
+7-495-477-4477
yury.yanovich@bitfury.com

Abstract—The paper describes the transfer of exchange investment mechanisms to the cryptocurrency and tokenized assets market. We propose an architecture of a new token standard, which allows dividing different assets into a commodity. The implementation of the prototype on the Ethereum platform is provided. An example of the token application on the banking system is presented.

Keywords—tokenization; blockchain; smart contract.

I. INTRODUCTION

The rapid development of blockchain technology in recent years has generated many projects for its implementation in various fields. Decentralized exchanges, voting, supply chain, state registries, medicine, the Internet of things, etc. [1], [2], [3], [4], [5], [6], [7], [8], [9] but the financial sector [10], [11], [12], [13] is the first and probably the most popular application area. This paper looks upon the lending market [14], which is part of the financial domain.

The main risks for investors in the peer-to-peer lending market are credit risk and liquidity risk [15], [16]. Various models for calculating and reducing credit risk are proposed [17], [18], [19], [20], [21], [22], including portfolio diversification [23], [24].

Classical diversification reduces credit risk, but each investor creates a unique tool as a result. On the one hand, this enables the investor to get an exclusively suitable instrument for his purposes. However, on the other hand, it is unlikely that such a tool is also appropriate for another investor, thus making it difficult to find a buyer for a unique instrument. Alternatively, one investor provides it in order to give an additional discount to attract customers.

Therefore, it is reasonable to diversify so that all the resulting tools have the same properties. This provides an opportunity not only to reduce the risks of investors but also to create a universal tool with all the properties of a marketable product, i.e. a commodity. This approach diversifies the presence of a secondary market, offsets the typical properties of a universal tool for all investors and allows, with a high level of liquidity, to attract more investors to the commodity, which reduces the level of profitability of the universal investors [25].

In this paper, we design smart contract-based blockchain solution for investment, as well as implement this solution in the Solidity language for the Ethereum platform [26] and show its use for loan portfolios.

II. FINANCIAL MECHANISMS FOR CRYPTO ASSETS

2.1. Initial Coin Offering

The Initial Public Offering (IPO) [27] is a type of public offering in which shares of a company are sold to institutional investors the right to sell it on the exchanges.

The blockchain analogue of the IPO is the Initial Coin Offering (ICO) [28]. To transfer IPO procedure to the crypto world, one replaces the exchange asset (stock) with a digital asset, i.e. a token, which is sold for cryptocurrency through a smart contract [26].

A secondary market for reselling of tokens also exists. After the end of the ICO sale, tokens

are placed on various crypto exchanges [29]. The user balances and transactions are still stored and processed in smart contracts to support decentralization, and the exchange acts as a trustless provider. The approach significantly simplifies the investment procedure but also involves the risk of scam ICO project.

2.2. Transparent Investment

Investing in funds and transferring exchange account management to a fund manager is another way to transfer the classic financial mechanism to crypto assets.

In the case of ideal investment, investor funds are protected at the legislative level. In the case of crypto assets, the movement of funds transferred to management is regulated by smart contracts. So, the history of transactions cannot be forged, and all asset movements are entirely transparent to the investor [30], [31].

This results in the simplification of the financial procedure. The risk of theft of invested funds by the manager is absent, but the cost can be a significant disadvantage as one has to make a large number of transactions on the blockchain. In the case of reliable loaded networks, this can cost significant funds.

2.3. Asset Tokenization

The idea behind this mechanism is to accompany the issuance of a stock asset by issuing a corresponding token. In this case, all methods of regulating crypto assets using smart contracts are transferred to real exchange assets and combined using legislative methods. This solves many problems associated with the use of either of the two approaches.

III. CRYPTO TOKEN STANDARDS

A need for unification of interfaces has raised with the development of tokenization mechanisms. The ERC-20 (Ethereum Request for Comments –20) [32] token standard was developed to provide methods for the balance checking and transferring of the ICOs-like tokens, i.e. it supports the main functions of cryptocurrencies. All ERC-20 tokens (of a given type) are equal and only their amount matters, i.e. they are interchangeable.

We want each token to be a separate entity that has its unique parameters in some applications. The virtual cats from the CryptoKitties project [33] are an example of such objects: every kitty is a personality! The standard for such tokens in the Ethereum network is ERC-721 [34].

ERC-20 and ERC-721 tokens require the deployment of separate contracts per token type. This places a lot of redundant bytecode on the blockchain and limits certain functionality by the nature of separating each contract into its address. ERC-1155 is a standard interface for contracts that manage multiple token types [35].

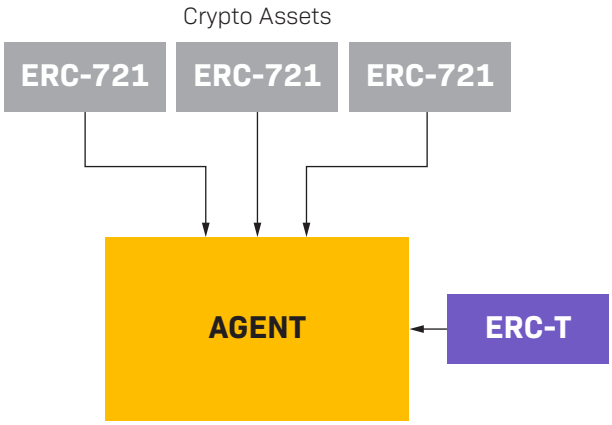

Figure 1. ERC-T creation

IV. PROPOSED TOKEN ARCHITECTURE

This section describes the architecture of the implemented token standard, a description of the tokenization algorithm, and the token's life cycle.

4.1. Notations

- ERC-T is the name of the proposed token standard.
- An agent is some network address that has the right to own crypto assets.

4.2. Approach Description

Suppose some agent owns k tokenized assets of different nature. Once they are united into a single portfolio, this portfolio becomes a unified asset. Each of the source tokens can be interpreted as a crypto asset with variable returns. If they are combined and issuing unit tokens, investors receive the classic advantages of ETF funds–lowering the financial entry threshold and risks diversifying. The contract of the described above token-share is implemented as the ERC-T(okenization) standard for the Ethereum network, which is an add-on to the ERC-20 standard.

4.3. ERC-T Architecture for Ethereum

4.3.1. ERC-T Creation

An agent combines his crypto assets in ERC-T creates a new instance of the ERC-T smart contract. The created smart contract "remembers" its creator.

4.3.2. Transfer of ownership of the merged crypto assets to the created ERC-T contract. Token Issue

In this architecture, the source crypto assets are presented in the form of smart contracts ERC-721. The interface of this standard provides for the transfer of ownership of tokens to third-party agents, including smart contracts. Through this interface, the owner also transfers, at this stage, the ERC-T token is not notified in any way about the acquisition of ownership rights to crypto assets. The key point is that the interface of the ERC-T contract does not provide for the reverse transfer of crypto assets ERC-721. All tokens transferred to ERC-T are assigned to it forever. These crypto-assets provide the unit tokens emitted in the future. Upon completion of the transfer of the combined assets, the agent sends the transaction to his ERC-T with the addresses of the crypto assets transferred to his possession. The transaction sender is validated, and the transmitted crypto assets addresses belong to this contract. If validation passes correctly, tokens are issued, the number of tokens issued is also determined by the owner of the contract when sending the transaction.

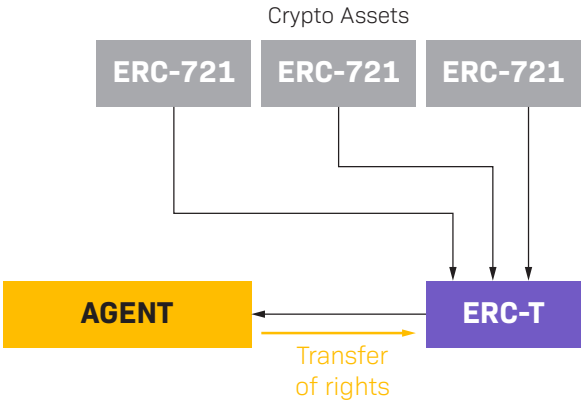

Figure 2. Rights transfer and tokens issuing

4.3.3. Public offering

This stage is similar to the public offering of ERC-20 tokens. Starting from a certain point, a crowd sale is announced, and the ERC-T contract allows you to send it the ETH cryptocurrency, in exchange for which the tokens of the transaction are sold with tokens. ICO ends upon the sale of all tokens, or on the owner's command, unsold tokens are credited to the address of the creator of the smart contract. Sometimes before a public offering comes presale—closed placement. At this stage, the sale is made only to a certain circle of agents who have received permission to purchase from the owner; these agents of this certain circle are known as whitelist accounts. Issuance of permissions is carried out through the corresponding function in the smart contract. ERC-T tokens are purchased through a call to a specific function of the smart contract. From the amount transferred by the investor, the number of tokens accrued is calculated at the rate determined by the owner before the start of the ICO.

4.3.4. Crypto Assets Workflow

Before the transfer of ownership of the token to the ERC-T contract, its life cycle is fully consistent with the ERC-721 standard. Agents can transfer, exchange and sell these tokens. Upon the fact of combining this crypto asset with others through the ERC-T standard, it is forever assigned to an instance of ERC-T, providing the cost of the issued tokens. At the end of the ICO, the ERC-T contract continues to own the combined tokens. Therefore, it receives dividends from these crypto assets. The profit received is distributed among the holders of ERC-T tokens in a ratio equal to the ratio of the balances of the token holders. Otherwise, the ERC-T tokens are no different from the ERC-20 standard and can also be traded on the secondary market.

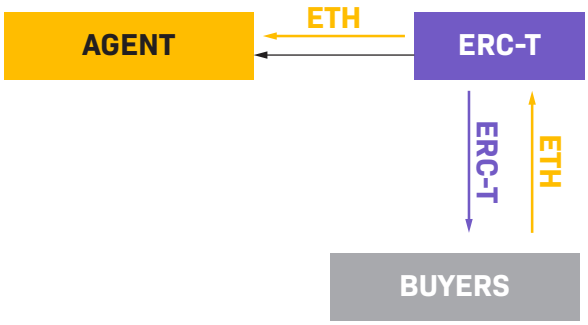

Figure 3. Public offering

V. IMPLEMENTATION DETAILS

ERC-T is practically no different by its interface from the generally accepted standard ERC-20. The Open Zeppelin solidity repository [36] was taken as the basis. We used the Ethereum platform Solidity language version 0.5.0 for the implementation. The prototype is not platform-specific and can be easily transferred to other blockchain frameworks such as EoS, Exonum, Hyperledger [37], [38], [39].

5.1. Main Differences Between ERC-T and ERC-20 Standards

- The constructor is implemented.
- A call-back payable function has been implemented to receive dividends from crypto assets.

- A public array of addresses of agents that are holders of ERC-T tokens has been added.
- The function of sending dividends to token holders in a ratio equal to the balance ratio has been implemented.
- The mint and transfer functions of the ERC-20 interface have been changed.

5.2. Initial Coin Offering for ERC-T

The public offering mechanism is the same as the ERC-20 standard. Presale and Crowdsale contracts for ERC-20 tokens can be transferred to ERC-T with virtually no changes.

5.3. Link to Github Repository

The demo code is available on https://github.com/minority169/ERCX.

VI. BANK LOAN PORTFOLIO TOKENIZATION

In this Section we reduce the loan portfolio workflow to the proposed token circulation. To do so, we introduce an algorithm that takes a loan portfolio as an input and returns the set of ERC-T token packets.

Bank's parameters

- I is the amount in dollars, for which one token of any of the loans will be sold at initial placement;
- D is the percentage of return per annum expected by an investor buying a token packet;
- T is the period in days for which the investor invests during the initial placement in the token packet;
- n is the number of tokens per packet.

At the input of the tokenization algorithm, a loan portfolio of N Bank loans are received. Each loan i, where $1 \le i \le N$ has a set of parameters according to Basel II notations [40]:

- PD_i is the default probability of a loan of i over the term of T;
- LGD_i is the level of losses in the default of a loan i over the term of T;
- E_i is the amount of loan debt i at the time of tokenization;
- D_i is the rate of interest on a loan i over the term of T.

The first part of the algorithm is to split each loan into the tokens with the given outcome value mathematical expectation. The loan interest rate mathematical expectation $E[D_i]$ is calculated by the formula

$$E[D_i] = D_i - (\frac{365}{T} + D_i) \cdot PD_i \cdot LGD_i.$$

Given the input parameters DI, I, T, and the resulting value $E[D_i]$, the size of the p_i token for a loan i is calculated from the formula

$$p_i = \frac{I(1+DI \cdot \frac{T}{365}))}{1 + E[D_i] \cdot \frac{T}{365}))}.$$

The number of tokens z_i into which the loan with the number i is divided is calculated by the formula

$$z_i = \frac{E_i}{p_i}.$$

The second part of the algorithm is to distribute all received tokens into packages of n tokens each. Moreover, each package can contain no more than one token from each tokenized loan, which ensures the achievement of a given level of profitability and risk for the package. For such a distribution, an iterative procedure is used, consisting of two steps. The procedure receives a lot of F tokens, consisting of N elements, as well as the number of tokens in the generated packages $n \le N$.

Let the superscript j denote the iteration number and let all values be an integer. We assume that $N^1 = N$, $F^1 = F$.

Step 1. All tokenized objects of the set F^1 are sorted in descending order of the number of tokens in the object. Let us denote the obtained sequence of the number of tokens in the tokenized objects $Z^1 = [Z_1^j, Z_2^j, \ldots, Z_n^j]$, where the subscript is the serial number of the object and N^j is the number of objects at the step j.

Step 2. Select n, i.e. the highest values of $[Z_1^j, Z_2^j, \ldots, Z_n^j]$, forming a token packet of them. All received blocks are identical and contain one token each of the n objects with the largest number of tokens. Such a formation is possible since $Z_n^j \le Z_j^j$, $1 \le j \le n$. As a result, n new values are formed $Z_j^{j+1} = Z_j^j - Z_n^j$, $1 \le j \le n$. At least one of the values obtained is zero. The combination of the obtained nonzero values, as well as the elements $[Z_{n+1}^j, Z_{n+2}^j, \ldots, Z_{Nj}^j]$ form the sequence F^{j+1}. Thus, the number of objects with a non-zero remainder of tokens after each step decreases by at least 1, which is equivalent to the inequality $N^j < N^{j+1}$. If after the next step of the algorithm the inequality $n < N_j$ is fulfilled, then the resulting set F^{i+j} and the value N^{i+1} go to the input of Step 1. Otherwise, the operation of the algorithm is completed.

Properties of Algorithm:

- It terminates no more than after $N - n$ iterations.
- The number of E tokens that did not fall into any of the packages satisfies the inequality

$E < (n-1)d$, where d is the maximum remainder of tokens in one of the $n-1$ non-tokenized objects after the algorithm is finished.

- The number d cannot be greater than the number $Z^1_{N^1-n}$, i.e. the number of tokens in the object with the number N^1-n in the set Z^1.

VII. CONCLUSION

The solution for financial markets' classical mechanism transferring to the blockchain is proposed in this article. The approach is implemented in Solidity and is based on ERC-20 and ERC-721 token standards and can be used in any Solidity supporting blockchain platform. This idea can also be transferred to several other blockchain frameworks. The algorithm of bank loan portfolio reducing to the proposed token packets is also presented here. It is fast, but does not claim to be optimal. The formalizing and solving the problem in terms of the domain-specific discrete optimization problem can be of interest for further research.

VIII. ACKNOWLEDGMENT

This research received no external funding.

References

[1] M. Swan, Blueprint for a new economy. Cambridge: Cambridge University Press, 2015.

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

[3] Tether, "Tether: Fiat currencies on the Bitcoin blockchain", 2018. [Online]. Available: https://tether.to/wpcontent/uploads/2016/06/TetherWhitePaper.pdf.

[4] R. Osgood, "The Future of Democracy: Blockchain Voting", in COMP116: Information Security. 2016, pp. 1–21. [Online]. Available: http://www.nytimes.com/2016/12/09/us/.

[5] 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.

[6] D. Korepanova, S. Kruglik, Y. Madhwal, T. Myaldzin, I. Prokhorov, I. Shiyanov, S. Vorobyov and Y. Yanovich, "Blockchain-Based Solution to Prevent Postage Stamps Fraud", in 2019 IEEE International Conference on Blockchain and Cryptocurrency(ICBC). IEEE, 2019, pp. 171–175. [Online]. Available: https://ieeexplore.ieee.org/document/8751495/.

[7] N. Kshetri and J. Voas, "Blockchain in Developing Countries", IT Professional, vol. 20, No. 2, pp. 11–14, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8338009/.

[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] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", IEEE Access, vol. 4, pp. 2292–2303, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7467408/.

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

[11] 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.

[12] 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.

[13] I. Eyal, "Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities", Computer, vol. 50, No. 9, pp. 38–49, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8048646/.

[14] R. Henriquez, I. Cohen, N. Bittan and K. Tulbassiyev, "Blockchain and Business Model Innovation: Designing a P2P Mortgage Lending System", SSRN Electronic Journal, pp. 1–37, 4 2019. [Online]. Available: https://www.ssrn.com/abstract=3371850.

[15] P. Giudici, B. Hadji-Misheva and A. Spelta, "Network Based Scoring Models to Improve Credit Risk Management in Peer to Peer Lending Platforms", Frontiers in Artificial Intelligence, vol. 2, pp. 3–5, 2019. [Online]. Available: https://www.frontiersin.org/article/10.3389/frai.2019.00003/full.

[16] A. Gaigalienė and D. Cesnys, "Determinants of Default in Lithuanian Peer-To-Peer Platforms", Management of Organizations: Systematic Research, vol. 80, No. 1, pp. 19–36, 12 2018. [Online]. Available: https://doi.org/10.1515/mosr-2018-0011, https://content.sciendo.com/view/journals/mosr/80/1/article-p19.xml.

[17] X. Ye, L.-a. Dong and D. Ma, "Loan evaluation in P2P lending based on Random Forest optimized by Genetic algorithm with profit score", Electronic Commerce Research and Applications, vol. 32, pp. 23–36, 11 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1567422318300759, https://linkinghub.elsevier.com/retrieve/pii/S1567422318300759.

[18] Y. Yan, Z. Lv and B. Hu, "Building investor trust in the P2P lending platform with a focus on Chinese P2P lending platforms", Electronic Commerce Research, vol. 18, No. 2, pp. 203–224, 6 2018.

[19] Z. Yuan, "Research on Credit Risk Assessment of P2P Network Platform: Based on the Logistic Regression Model of Evidence Weight", Journal of Research in Business, Economics and Management, vol. 10, No. 2, pp. 1874–1881, 2018. [Online]. Available: www.scitecresearch.com/journals/index.php/jrbem.

[20] C. Serrano-Cinca, B. Gutierrez-Nieto and L. Lopez-Palacios, "Determinants of Default in P2P Lending", PLOSONE, vol. 10, No. 10, p. e0139427, 10 2015. [Online]. Available: https://dx.plos.org/10.1371/journal.pone.0139427.

[21] G. Zhou, Y. Zhang and S. Luo, "P2P Network Lending, Loss Given Default and Credit Risks", Sustainability, vol. 10, No. 4, p. 1010, 3 2018. [Online]. Available: http://www.mdpi.com/2071-1050/10/4/1010.

[22] C. Serrano-Cinca and B. Gutierrez-Nieto, "The use of profit scoring as an alternative to credit scoring systems in peer-to-peer (P2P) lending", Decision Support Systems, vol. 89, pp. 113–122, 9 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167923616301063.

[23] H. Zhao, L. Wu, Q. Liu, Y. Ge and E. Chen, "Investment Recommendation in P2P Lending: A Portfolio Perspective with Risk Management", in 2014 IEEE International Conference on Data Mining. IEEE, 12 2014, pp. 1109–1114. [Online]. Available: http://ieeexplore.ieee.org/document/7023455/.

[24] H. Zhao, Q. Liu, G. Wang, Y. Ge and E. Chen, "Portfolio Selections in P2P Lending", in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining-KDD'16. New York, New York, USA: ACM Press, 2016, pp. 2075–2084. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2939672.2939861.

[25] V. Davydov and M. Khalilova, "Business model of creating digital platform for tokenization of assets on financial markets", IOP Conference Series: Materials Science and Engineering, vol. 497, No. 1, pp. 0120691–0120697, 4 2019.

[26] V. Buterin, "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform", Etherum, pp. 1–36, 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[27] G. N. Gregoriou, Initial Public Offerings: An International Perspective. Butterworth-Heinemann, 2006.

[28] C. Catalini and J. Gans, "Initial Coin Offerings and the Value of Crypto Tokens", National Bureau of Economic Research, Cambridge, MA, Tech. Rep., 3 2018. [Online]. Available: http://www.nber.org/papers/w24418.pdf.

[29] G. Fenu, L. Marchesi, M. Marchesi and R. Tonelli, "The ICO phenomenon and its relationships with ethereum smart contract environment", in 2018 IEEE 1st International Workshop on Blockchain Oriented Software Engineering, IWBOSE 2018—Proceedings, vol. 2018—Janua. IEEE, 3 2018, pp. 1–7.

[30] G. W. Peters and E. Panayi, "Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money". Springer, Cham, 2016, pp. 239–278.

[31] Bitfury Group, "On Blockchain Auditability", bitfury.com, pp. 1–40, 2016.

[32] F. Vogelsteller and V. Buterin, "ERC-20 Token Standard", 2015. [Online]. Available: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md.

[33] Dapper Labs, “CryptoKitties”. [Online]. Available: https://www.cryptokitties.co.

[34] “ERC-721”. [Online]. Available: http://erc721.org.

[35] “ERC1155: Multi Token Standard”. [Online]. Available: https://github.com/ethereum/EIPs/issues/1155.

[36] “OpenZeppelin Contracts”. [Online]. Available: https://github.com/OpenZeppelin/openzeppelin-contracts.

[37] I. Grigg, “EOS — An Introduction”, 2017. [Online]. Available: https://eos.io/documents/EOS-An-Introduction.pdf.

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

[39] C. Cachin, “Architecture of the Hyperledger Blockchain Fabric”, IBM Research, vol. July, 2016.

[40] Basel Committee on Banking Supervision, A revised framework on international convergence of capital measurement and capital standards, 6 2004, No. 1. [Online]. Available: https://www.bis.org/publ/bcbs107.htm, http://www.bis.org/publ/bcbs128.pdf.