

Trading Application Based on Blockchain Technology

Jovan Kanevche, Jovan Karamachoski*, Magdalena Puncheva, Ninoslav Marina

Abstract: Blockchain is a growing distributed list of records that are linked using cryptographic hashes. Its robustness, simplicity, immutability and trust are basis for development of interesting innovative business solutions. Considering some use-case scenarios within the financial sector, we developed a Blockchain based trading application placed on the Cosmos network. Cosmos is a decentralized network of independent, scalable, and interoperable Blockchains, creating the foundation for new economy. Our work describes the application functionalities for buying, selling and renting goods. It shows the easiness of trading, while eliminating the third parties and demonstrates the disruptive potential of the Blockchain technologies.

Keywords: application; blockchain; buying; renting; selling; Tendermint; trading

1 INTRODUCTION

The Blockchain technology is a distributed network technology, capable to achieve consensus over the data that circulates in the network. The new data structure implemented in the Blockchain technology offers **high level of redundancy, traceability and liveness of the records**. The Blockchain technology is not one solution to fit all the implementation scenarios, different types are defined to suite the different implementation scenarios. General division of the Blockchain technologies types is in **four groups: public permissionless, public permissioned, private permissionless, private permissioned**. The grouping is done depending on the openness of the data that is circulating in the system (public and private) and the procedures for access restriction and user authentication for access management (permissionless and permissioned). All four types of Blockchain technologies show different characteristics and performance metrics. Depending on the use-cases scenarios, suitable type of Blockchain has to be selected.

There are lot of Blockchain technology currently on the market. Most of them are focused on the financial aspect of the Blockchain technology and the digital currency introduced by the Blockchain technology. Generally the public type of Blockchain has gained the attention from the masses, especially by the introduction of the **Bitcoin** [1], **Litecoin** [2] and **Ethereum** [3]. These Blockchain technologies are covering the majority of the Blockchain market. The success of the Bitcoin and Ethereum attracted many researchers to broaden the use of the Blockchain technologies in other use case scenarios. The main focus of the Bitcoin and Ethereum is the financial aspect but the introduction of Smart contracts [3], made this system suitable to use of the Blockchain technology in many systems beside than financial sector. Some of the most prominent use-cases are logistics, real estate and healthcare.

In this paper we are presenting **novel trading application based on Tendermint Blockchain technology** that allows the users to buy, sell or rent goods, thus eliminate any requirement for third parties or notaries in the trading

process. To the best of our knowledge, this is the first trading application based on Tendermint Blockchain technology that allows cheaper, faster and highly secure transactions on a public Blockchain technology.

2 RELATED WORK

Great number of trading applications based on Blockchain technology are present on the market, but most of them are focused on the process of selling or buying items, but not renting items. Initially the trading applications were developed with idea of exchanging digital assets or services. One of the greatest influence on the development of trading applications based on Blockchain technologies was the collectible game known as CryptoKitties [4, 5]. The CryptoKitties is game of collectible and breedable assets represented as virtual cats, developed on the Ethereum platform. This game created enormous rise of transactions on the Ethereum network and showed the capabilities of the Blockchain technology in the process of trading digital assets.

Another innovative approach, described in [6], is trading of **computational power in a decentralized fashion**, based on Ethereum platform. The proposed framework assumes that spare computational resources can be shared with entities and charged for the service. The agreement between the parties, the terms of use and the settings are managed by Smart contract.

In [7] the authors show the results from the developed proof-of-concept of a marketplace based on Ethereum Blockchain. The solutions offers functionalities of trading digital, but also physical goods. It implements mechanisms for group escrow arbitrage, integration with logistic entity and reputation system.

The importance of the development a marketplace based on a Blockchain technology is presented in [8], where the authors are showing the marketplace developed on the Ethereum Blockchain but also are giving price and taxes comparison for trading on some of the mainstream shopping platforms and the newly developed Blockchain based marketplaces.

Beside the general applications for decentralized marketplaces build on Blockchain technology, where the users can buy or sell assets, there are solutions for renting goods. In [9] the authors are proposing Blockchain based application for house renting, developed on Ethereum platform and integrated with IPFS [10] and Oraclize services [11]. A car leasing system is presented in [12], developed on a private Blockchain in order to make it more cheap for the users.

Most of the solutions presented in the literature are based on the **Ethereum Blockchain technology**, by implementation of Smart contract characteristics. The current version of Ethereum network struggles to cope with the increased number of transactions and makes the trading process expensive and very time consuming. The development of the **trading application based on Tendermint protocol** will significantly improve the speed of transaction finalization and keep the transaction fees very small.

3 TENDERMINT FRAMEWORK BASICS – THE PROTOCOL STRUCTURE AND THE CHARACTERISTICS

The Tendermint framework [13] and the Cosmos Hub [14] offer modular approach in the building of Blockchain applications. The high modularity is key factor for faster and broader adoption due to better adaptation to other technologies. Moreover the IBC (InterBlockchain) protocol developed by the Tendermint community offers flawless integration of different types of Blockchain technologies in one ecosystem. Additionally the Tendermint framework offers layers structure of the Tendermint Blockchain application and a key concept for separation of the consensus mechanisms and the higher layers of the application. This separation makes the application easily adaptable to other Blockchain frameworks.

3.1 Tendermint Framework Structure

According to the Tendermint framework an application is segmented in **three layers** (see Fig. 1): Networking, Tendermint Core (Consensus layer) and ABCI (Application BlockChain Interface) interface. On top of the ABCI interface is the application definition developed in a Cosmos SDK.

The Tendermint networking layer defines the **peer-to-peer gossiping procedures and network formation**. Compared to the traditional point-to-point networking approach, the gossiping procedure in Tendermint networking layer provides more optimal and less redundant message exchange procedures.

On top of the Tendermint network layer is the Tendermint consensus mechanism, which is **Practical Byzantine Fault Tolerant** [15] based consensus mechanisms with significant improvements by implementation of nil vote and vote locking mechanism for simpler consensus achievement. Tendermint consensus mechanisms provides fast consensus cycles and fast transaction validation with high throughput of transactions in

a non-Byzantine environment. The Tendermint's State Machine Replication mechanisms can hold up an attack of up to 1/3 of adversary Byzantine nodes interfering the consensus mechanism.

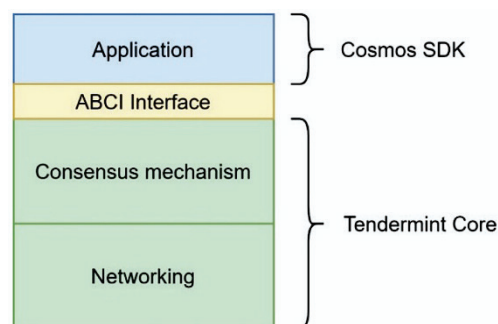


Figure 1 Tendermint layered structure

The ABCI interface is a layer that defines the connection functions between the consensus mechanism and application. It defines the methods handling procedures and translation of the parameters from the consensus mechanism to the appropriate parameters in the application and vice versa. This interface enables the fusion between the Tendermint consensus mechanisms and Ethereum environment defined by the Ethermint community, which results in the development of Ethermint solution. Beside this popular fusion, there is possibility to make any other adaptation of existing Blockchain technology to work on top of the Tendermint consensus mechanism.

3.2 Tendermint Characteristics

Tendermint is lightweight consensus protocol offering high transaction throughput, scalability, fast transaction finalization and implementation of Smart contracts, which makes the Tendermint as one of the most suitable protocols for development of trading application. Moreover it has highly energy efficient property compared to the Bitcoin and Ethereum consensus mechanisms, due to PBFT-based consensus mechanisms which does not require computationally intensive processes in order to conduct the consensus among the users.

In some cases of the trading practice, the transfer of the goods require legal transfer of ownership, approved by a notary or other middleman entities. This approach is additional financial burden to the requester of the service or the buyer. The openness and liveness of the data, the traceability and immutability of the records, and the redundancy provided by the Blockchain technology make the applications build on these platforms to be highly trustable. This characteristic and the implementation of Smart contracts will eliminate the requirement of third party or middleman in the trading processes.

4 BLOCKCHAIN-BASED TRADING APPLICATION

The application covers trading of miscellaneous items, but the most significant impact will be in the trade of

vehicles, real estate and other items where the trade has to be covered with notarized contract. The main purpose of this application is to exploit the strength of the Blockchain technologies and eliminate the involvement of third parties (notaries) in the process of trading goods. The Blockchain technologies are capable of providing publically accessible, provable and traceable transactions, and the implementation of Smart contracts creates automated processes for ownership transfer and can be linked to any institution that requires to update the ownership status.

A Smart contract is self-executable code residing on the Blockchain, identified by an address, callable from other Smart contracts or directly by a user. The Smart contract is capable to swap the ownership of an item and transfer the funds for the item in a single call, and pay small fee for the execution of the Smart contract. That way the trading actions of buying and selling, by use of Smart contract, will be executed in a single call of the Smart contract by providing the buyer’s address, seller’s address and the amount of tokens required for transaction completion. In a case of insufficient funds, the transaction is halted and it will not proceed. The renting process is more complex than the selling and buying procedures, and requires additional functionalities due to temporal transfer of ownership of the items and the way of charging for item usage (per use or time interval).

4.1 Logical Structure

The application cover the trading activities of selling, buying and renting. The current version of the application assumes instant fund transfer for the buying and selling processes. The simple functionality of the transfer functions can be further expanded with fund-locking approach in a situations when this application will be linked to delivery services. The fund-locking approach will lock the money for bought or sold item until the delivery is not confirmed by delivery service (either by physical delivery or transfer the digital good through online services).

The renting use-case has more complex functionalities in order to cover the most cases that appear in a renting scenarios. Figure 2 shows the simplified diagram of interaction between the entities in the renting process.

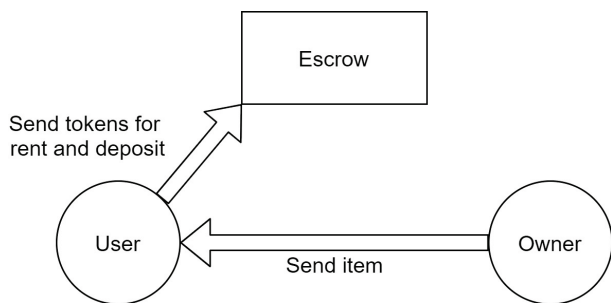


Figure 2 Rent item interaction

The renting process includes Escrow entity which locks the funds for renting until the item is hold by the renter. The renting process starts at the moment when the renter prepays the rent and deposits pre-agreed amount as damage or stilling

deposit. The owner approves the start of the renting and rent period starts. The rent can be charged per time interval or per use, depending on the owner preference which is stated in the advertisement.

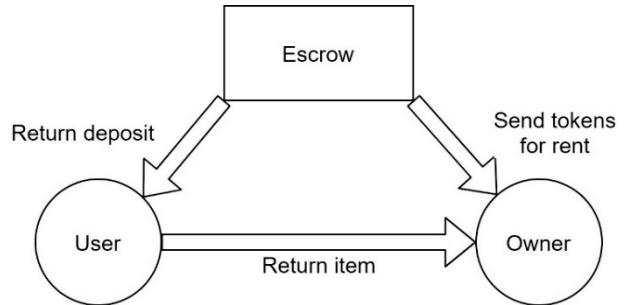


Figure 3 Item return procedure with no damage detected to the item

The rent finishes when the renter sends back the item or the prepaid rent fund is completely spent. Next step is when item owner receives the item and checks for damages. If there are no damages to the item, the damage deposit is sent back to the renter and the rent fund is transferred to the owner wallet (see Fig. 3). If any damage is registered, the rent fund and damage deposit is transferred to the owner wallet, and note for the damage is attached to the item (see Fig. 4). In case when the item is not returned on time, the item is marked as stolen, and rent fund and damage deposit is transferred to the owner (see Fig. 5).

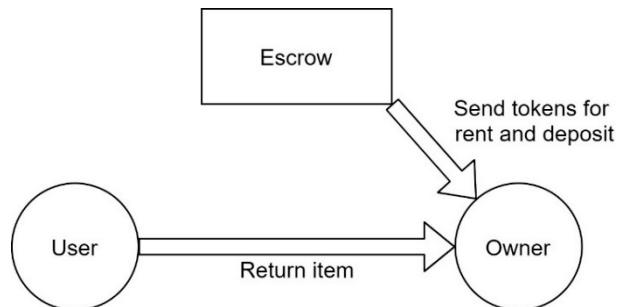


Figure 4 Item return procedure with damage detected to the item

For the time interval rents, there is possibility to charge the rent depending on the length of the rent, so at the moment of item return there will be unspent rent fund that will be returned to the renter, together with the damage deposit if there is not damage to the item.

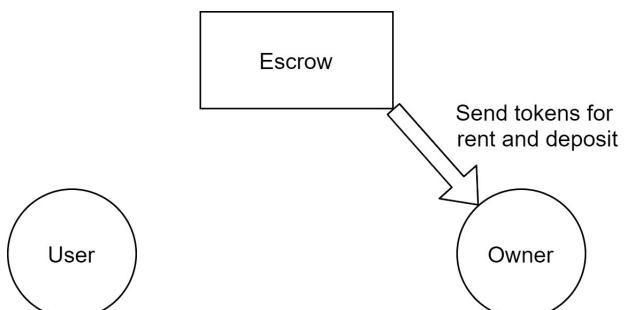


Figure 5 Item return procedure when the item is stolen

Tradefire - Application for Renting, Buying and Selling

Enter you wallet mnemonic to use

Enter mnemonic

Login

Register user

First Name	
Last Name	
Email	
Address	
Telephone	

Submit

Figure 6 Index page of the application

<p>My wallet</p> <hr/> <p>Address</p> <p>cosmos1kvnn749ujfs92z8qnrU0xstbnx0938cpjwmh4</p> <p>Balance</p> <p>1000 token</p>	<p>Create a Listing</p> <p>Rent ▾</p> <table border="1"> <tr> <td>Identifier</td> <td></td> </tr> <tr> <td>Description</td> <td></td> </tr> <tr> <td>Price per hour (example: 10token)</td> <td></td> </tr> <tr> <td>Deposit (example: 10token)</td> <td></td> </tr> <tr> <td>Damages</td> <td></td> </tr> </table> <p>Submit</p>	Identifier		Description		Price per hour (example: 10token)		Deposit (example: 10token)		Damages	
Identifier											
Description											
Price per hour (example: 10token)											
Deposit (example: 10token)											
Damages											

Filter Listings

Rent Item ▾

Search

Available Rents

List is empty

Current Rents

List is empty

Figure 7 Trading page of the application

4.2 Interface Design

The application is divided in two pages where the initial page is the index page, and the second one is the trading page. The first page has two segments: login and sign in section.

On the first page (see Fig. 6) the user can login into the application by use of previously created wallet, more precisely to enter into the wallet the user has to provide the mnemonic of the wallet. If the user has no account, in the sign in section it is possible to create wallet by providing the

personal information and this way the user will be added to the system and create wallet to transfer the funds or manage the items for trading.

The second page, the trading page, has three sections (see Fig. 7). The first section is the user account information section where the user have better insight of the available fund and the wallet address. The second section is the advertisement creation section, where the user can add advertisement for renting, buying or selling an item. A listing creation process will require from the user to add identifier, description and price of the item. In the case of creation listing for a renting item, the owner has to provide damage deposit and any previous damages reported by the owner. The third section is the filtering or search section where the user can find advertisement for renting, buying or selling item. This section has subfields to show available items for trading and past transactions. Also in the case of renting item, there is subfield for current rents.

5 CONCLUSION

The Blockchain technologies will have immense impact on the trading processes in the future. The transparency of the interactions in the Blockchain network increases the trust in this technology. The cryptocurrency mass adoption and the integration of this type of currency with everyday trading processes is inevitable. The traceability and provability of the transactions are also important characteristics that make the Blockchain technology capable to act as notary. The implementation of the Smart contract may further automate the notarization process in the Blockchain system and eliminate the third parties in the trading process. This additionally impacts the decrease of the costs for trading and decrease of transaction fees. This application proves the ability of the Blockchain technology to make the trading processes transparent, secure and cheaper.

Notice

The paper will be presented at MOTSP 2021 – 12th International Conference Management of Technology – Step to Sustainable Production, which will take place in Poreč/Porezeno, Istria (Croatia), on September 8–10, 2021. The paper will not be published anywhere else.

6 REFERENCES

- [1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf> (Accessed: Sep-2019)
- [2] Litecoin. <https://litecoin.org>. (Accessed: Sep-2019)
- [3] Buterin, V., et al. (2014). Ethereum white paper: A next-generation smart contract and decentralized application platform, Ethereum, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
- [4] CryptoKitties collectibles. <https://www.cryptokitties.co/>. (Accessed: 2021)
- [5] Serada, A., Sihvonen, T., & Harviainen, J. T. (2020). CryptoKitties and the new ludic economy: how blockchain introduces value, ownership, and scarcity in digital gaming. *Games and Culture*, p. 1555412019898305. <https://doi.org/10.1177/1555412019898305>
- [6] Nardini, M., Helmer, S., El Ioini, N., & Pahl, C. (2020). A Blockchain-based Decentralized Electronic Marketplace for Computing Resources. *SN Computer Science*, 1(5), 1-24. <https://doi.org/10.1007/s42979-020-00243-7>
- [7] Kabi, O. R. & Franqueira, V. N. (2018). Blockchain-based distributed marketplace. *International Conference on Business Information Systems*, 197-210. https://doi.org/10.1007/978-3-030-04849-5_17
- [8] Ranganthan, V. P., Dantu, R., Paul, A., Mears, P., & Morozov, K. (2018). A decentralized marketplace application on the ethereum blockchain. *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, 90-97. <https://doi.org/10.1109/CIC.2018.00023>
- [9] Qi-Long, C., Rong-Hua, Y., & Fei-Long, L. (2019). A Blockchain-based Housing Rental System. <https://doi.org/10.5220/0008097201840190>
- [10] Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3). *IPFS*, <https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf>.
- [11] Adler, J., Berryhill, R., Veneris, A., Poulos, Z., Veira, N., & Kastania, A. (2018). Astraea: A decentralized blockchain oracle. *2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*, 1145-1152. https://doi.org/10.1109/Cybermatics_2018.2018.00207
- [12] Kwame, O.-B., Xia, Q., Sifah, E. B., Amofa, S., Acheampong, K. N., Gao, J., Chen, R., Xia, H., Gee, J. C., Du, X., et al. (2018). V-chain: a blockchain-based car lease platform. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1317-1325.
- [13] Kwon, J. (2014). Tendermint: Consensus without mining. *Draft v. 0.6, fall, 1(11)*.
- [14] Kwon, J. & Buchman, E. (2018). A Network of Distributed Ledgers. *Cosmos, dated*, 1-41.
- [15] Castro, M., Liskov, B., et al. (1999). Practical byzantine fault tolerance. *OSDI 1999, 99*, 173-186.

Authors' contacts:

Jovan Kanevche, BSc
University of Information Science and Technology "St. Paul the Apostle",
Partizanska bb, 6000 Ohrid, Republic of North Macedonia

Jovan Karamachoski, MSc
(Corresponding author)
University of Information Science and Technology "St. Paul the Apostle",
Partizanska bb, 6000 Ohrid, Republic of North Macedonia
jovan.karamachoski@uist.edu.mk

Magdalena Puncheva, PhD
MIT University,
Bulevar 3-ta Makedonska Brigada,
1126 Skopje, Republic of North Macedonia

Ninoslav Marina, PhD
University of Information Science and Technology "St. Paul the Apostle",
Partizanska bb, 6000 Ohrid, Republic of North Macedonia