INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Blockchain-based Smart Contract for Decentralized Marketplace

Syifa Nurgaida Yutia [a,*], Rana Zaini Fathiana [a], Siti Zahrotul Fajriyah [a]

[a] *Faculty of Information Technology, Telkom Institute of Technology Jakarta, Jakarta, 11710, Indonesia*

Corresponding author: [*]syifanurgaida@ittelkom-jkt.ac.id

***Abstract*— The advance of information technology has a growing influence on one of the most popular social trends: online shopping. The rising popularity of online shopping among the general public, as indicated by the growth in the number of online purchasers each year, has prompted business owners to pursue online ventures. The marketplace is intrinsically tied to online buying activity that connects merchants and customers, allowing customers to search for various goods and services from various providers. However, service failures are vulnerable to centralized market systems that emerge frequently. When the company's services to customers fail to satisfy consumer expectations. A breakdown in purchasing and selling essential services, including product delivery and customer support, is referred to as service failure. As a result, not only does this harm confidence, but it may also cause clients to migrate to an alternative marketplace. The marketplace's competitiveness is based on consumer confidence. The decentralized marketplace can address this security concern. A decentralized marketplace is meant to build a system that does not require the confidence of a third party using blockchain technology and smart contracts that can record all transactions clearly and consistently, allowing them to serve as a single point of truth between distrusting entities. The findings largely support the feasibility of Ethereum Smart Contracts to construct a decentralized marketplace. However, there are some places where further study and development are needed.**

***Keywords*— Blockchain; smart contract; decentralized marketplace; ethereum; service of failure.**

Manuscript received 11 Jan. 2022; revised 29 Mar. 2022; accepted 2 May 2022. Date of publication 31 Aug. 2022.

I. INTRODUCTION

A marketplace can be defined as a place where sellers and buyers gather to make transactions [1]. The marketplace is an evolution of e-commerce by allowing buyers to find different types of goods and services offered by different sellers. Thus, the difference between marketplace and e-commerce lies in the intermediary, and the marketplace is an intermediary that connects sellers and buyers. On the other hand, e-commerce does not require intermediaries because sellers sell products directly to buyers on a standalone platform, so there is no need for intermediaries.

Marketplaces have significantly impacted the business world from a firm and consumer perspective [2]. The marketplace is growing rapidly in Indonesia, there are many successful marketplaces such as Tokopedia, Shopee, BukaLapak, OLX, and many other marketplace platforms are some of the media that bring national economic growth. Small and medium businesses, in particular, benefit greatly from a marketplace. Business actors may easily sell their items to the marketplace and just need to supply comprehensive information about the things they offer in the marketplace, such as product information, pricing, and delivery, to participate in the marketplace. Marketplaces serve three primary functions: 1) Connecting sellers and buyers. 2) Facilitating the exchange or transaction of goods, services, information, payment transactions, and shipping regulations. 3) Providing institutional infrastructure as a legal and regulatory framework for all market activities [3]. However, due to the centralized system, the marketplace has various challenges in carrying out its job—the purchasing and selling procedure on a centralized Marketplace. As seen in figure 1, sellers may post product details, change items, and delete things on the marketplace. The customer can then pay for the merchandise and cancel the purchase.

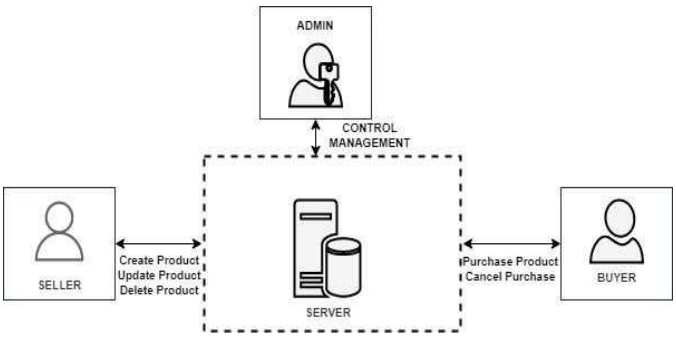

Fig. 1 Centralized Marketplace

As a third party administering the market, the marketplace administrator has complete authority over the database. Complete control over the system leads to a lack of confidence in the marketplace system, a crucial need that directly influences transactions [4]. All electronic buyers and sellers are concerned about the issue of trust and satisfaction [5],[6]. This is critical since it influences consumer trust [7]. There are various disadvantages to a centralized marketplace system that blockchain can address.

TABLE I
CENTRALIZED MARKETPLACE VS DECENTRALIZED MARKETPLACE

No	Issues in a Centralized Marketplace	Using Blockchain to Solve Problems
1	Platform users are concerned about privacy, personal information misuse, and product quality [8],[9].	Blockchain technology allows multiple parties to verify trustworthy identities, ensuring the highest level of security for customer databases and systems.
2	Platform users cannot access personal information, such as purchase ratings and histories.	All past purchase history, reviews, and data may be stored on the blockchain. To put it another way, proof of ownership cannot be altered or lost.
3	In their sole discretion, marketplace companies may ban sellers from using the platform at any time if they believe the seller is causing them harm.	Blockchain technology does not require the existence of a third party to govern the system, no one has power over it, and no unilateral blockage is possible.
4	The seller is responsible for both product registration and sales commission, and this diminishes the profit margin. Thus, the seller raises the price to the consumer to compensate.	There are no delays in processing payments or pending transactions since blockchain transactions are instantaneous and do not go through traditional institutions. Customers may make instant purchases, helping them complete their orders more quickly.

A decentralized marketplace uses blockchain technology to enable direct interaction between merchants and buyers, as seen in figure 2.

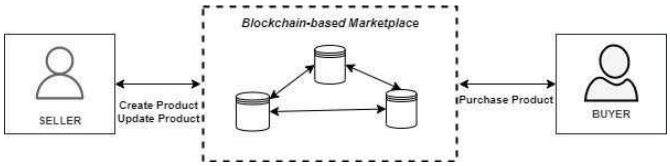

Fig. 2 Decentralized Marketplace

Smart contract technology, which can fully automate services to establish trust, cut costs, and safeguard user data without needing a third party to function as a transaction mediator, is used to carry out each transaction on the platform. When a transaction occurs, the smart contract follows a set of procedures that the seller and buyer have agreed. This transaction data is validated and kept across all of the blockchain network's nodes in a decentralized way. In a decentralized marketplace, the absence of third parties offers a number of benefits to both sellers and customers. Blockchain has been used in the marketplace in previous studies [10]. This paper seeks to finish the smart contract design process by unit testing the smart contracts that have been created, allowing them to provide full smart contract programming for a decentralized marketplace.

II. MATERIALS AND METHOD

A. Blockchain Explained

When Satoshi Nakamoto released Bitcoin in 2008 [11], blockchain use was widespread and well-known. Cryptocurrencies and blockchain have developed as novel methods to aid financial institutions and a variety of other use cases, including supply chains, healthcare, and care systems [12]. One of the purposes of the Blockchain technology that is being developed and established is to diminish or remove the role of intermediaries or third parties, sometimes known as "Middlemen." Blockchain's primary features are decentralization, permanence, anonymity, and testability [13]. Because blockchain is an immutable and transparent distributed ledger, no one can refute the truth. As demonstrated in Figure 3, the data contained in the blockchain is represented as a link (chain) on the block.

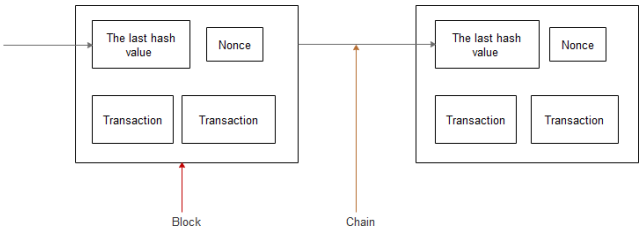

Fig. 3 Relationship between Block and Chain

As shown in the diagram, blockchain is replicated via a peer-to-peer network, the information it contains is extremely difficult to erase, and the points in the system may trust one another [14]. This structure is made up of multiple linked and sequential units. The block is connected because the previous block's hash value is utilized in constructing the next block. Therefore, changing the information will be more difficult since it will have to update the following block [15]. The hash function has two unidirectional properties: the hash value cannot be altered back to its original form and is impact resistant if the two inputs do not have the same hash value [16], as well as the ability to speed up the integrity verification procedure [17]. A consensus algorithm will be used to validate the new block. This is commonly referred to as mining [18]. The new block will be added to the current blockchain after it has been properly validated [19]. There is a link between one block and the one before it.

Blockchain technology has various qualities that make it advantageous. Among these qualities are as follows [20]:

- *Decentralization:* There is no requirement for a third party in a transaction. The consensus algorithm is employed in a distributed network to preserve data consistency.

- *Distributed Database:* Every participant on the blockchain has complete access to the database and its history. Such data or information is not under the control of any party. Without the need for middlemen, each party may directly verify the records of its transaction partners.
- *Persistence:* The transaction validation procedure is quick, and miners will not identify incorrect transactions. Removing transactions that have already occurred on a blockchain is not feasible.
- *Anonymity:* Each user in the blockchain network can communicate with one another using a unique address. The interaction does not reveal each user's genuine identity in this situation.
- *Auditability*: Every transaction relates to the preceding transaction in a blockchain network, and this will make transactions easy to authenticate and look for.

Blockchain technology is a solution that can be utilized to alleviate flaws in the present marketplace system. However, we must first establish whether the usage of blockchain technology is the correct decision; we must first study it to determine which sort of blockchain is appropriate for our situation. Figure 4 depicts a schematic that may be used to determine blockchain use decisions, along with some fundamental rules that must be followed.

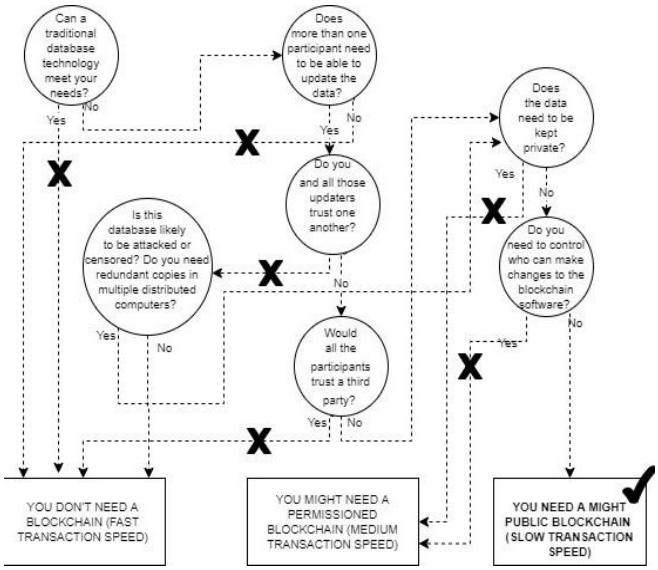

Fig. 4 Decisions are made on what type of blockchain to use [20].

Using the model in Figure 4, we can deduce that the creation of a decentralized market necessitates the use of a permissionless blockchain. According to Cachin and Vukolić [21], the following are some types of blockchain.

- *Permissionless Blockchain:* such as Bitcoin or Ethereum, anybody may be a user or host a node, everyone can "write," and anyone can participate in consensus in deciding the state's validity.
- *Permission Blockchain:* is a blockchain run by a known entity, similar to consortium blockchains, in which consortium members or stakeholders in a specific business context run the Permission Blockchain network. Blockchain permission systems may identify nodes that can manage and change shared data and frequently contain controls over who can issue transactions.
- *A private blockchain is a blockchain permitted by a single entity with* just one trust domain.

B. Smart Contracts

A smart contract is a computer mechanism that digitally facilitates, verifies, and enforces contracts between two or more parties on the blockchain. Because smart contracts are often delivered and backed by the blockchain, they have various distinguishing characteristics. The smart contract program code is first stored and validated on the blockchain to avoid tampering with the contract. Second, smart contract execution is carried out anonymously amongst individual nodes without the trust of centralized administration or third-party coordination. Third, smart contracts function similarly to smart agents in that they store cryptocurrencies or other digital assets and allow them to be transferred when certain criteria are met [22]

Blockchain-enabled smart contracts can broaden Bitcoin's capabilities and the sorts of services that blockchain technology allows. Various potentially inefficient and perhaps unsustainable legal and financial services can be maintained through smart contracts deployed on the blockchain [23]. Smart contracts can help market systems by utilizing blockchain technology. Blockchain technology can access network data, validate it, and disseminate it to all dispersed nodes. A decentralized data operation and preservation platform are achieved by utilizing a peer-to-peer network.

C. Design of a Blockchain-Based System

This section describes the aspects of a blockchain-based system that are distinct from the system as a whole, such as system architecture, the definition of requirements, determining participants, assets, transactions, and access control.

1) System Architecture: The Decentralized Marketplace's System Architecture is systematically shown in Figure 5.

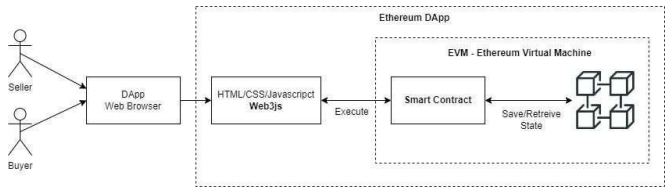

Fig. 5 System Architecture Design

The system's front-end was built as a web application using HTML/CSS/JavaScript programming language. Web3.js enables the user interface to connect to the blockchain network and communicate. Solidity, a programming language, was used to create the smart contract. The Ethereum network will be used to construct the blockchain backend. However, a local blockchain network called Ganache was developed and utilized for development and testing reasons.

2) Definition of Requirements: We have created a simple marketplace system with the following functionality.

- Sellers can add items and edit product information.
- Buyers can view a list of items that are offered as well as their costs.

- Buyers can purchase things that are currently available.

3) Sellers can earn from successfully acquired items from purchasers. *Participant Identification.* This section will identify the network's participants. Participants are chosen depending on the requirements of system actors. The following is a list of the network's participants.

TABLE II
PARTICIPANT LIST

No	Participant
1	Seller
2	Buyer

4) Assets Determination: The assets will be determined in this section. Everything that has worth is referred to as an asset. The data from the transaction process is stored in these assets. The materials and content required for this system are listed below.

TABLE III
ASSET LIST

No	Asset
1	Products
2	Product purchased

5) Transaction Determination: The transaction will be determined in this section. A transaction is a collection of actions taken by parties to alter the contents of an asset. The following is a list of the system's transactions.

TABLE IV
TRANSACTION LIST

No	Transaction	Participant
1	Create Product	Seller
2	Purchase Product	Buyer

6) Access Control Determination: Each participant's access permissions will be determined in this section. This access permission is granted under the system architecture's requirements. The following is a list of each participant's access permissions.

TABLE V
ACCESS CONTROL DETERMINATION

No	Participant	Permission
1	Seller	Perform the Create, Read, Update functions on the product asset
2	Buyer	Perform Read List Products and Purchase Product

III. RESULTS AND DISCUSSION

The design of the smart contract is carried out using a class diagram. The design includes the data structure and functions in the smart contract, as seen in figure 6. The Decentralized Marketplace System is composed of a single primary smart contract containing the CreateProduct and PurchaseProduct capabilities. A struct represents the data structure for the product. The following is an explanation for each smart contract and struct:

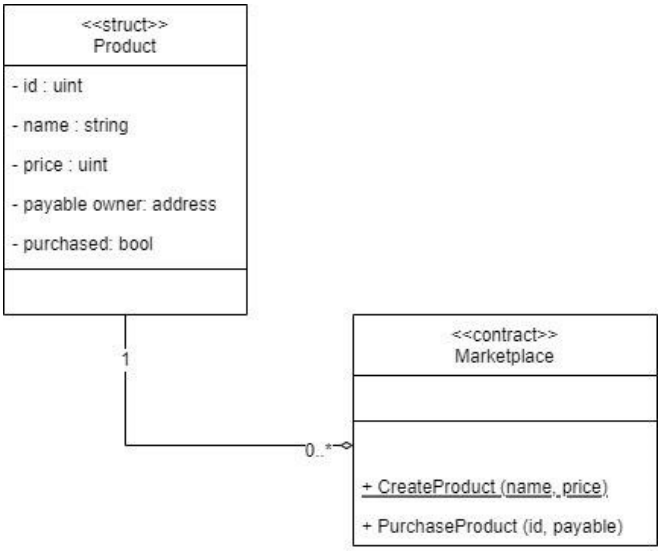

Fig. 6 Smart Contract Class Diagram.

A. Composing Data Structure

The smart contract data format in the Decentralized Marketplace is constructed in a simplified way to demonstrate the essential logic of the marketplace system using smart contracts. The architecture for the smart contract data structure is as follows:

1) Product Data Structure: Sellers must add items to the marketplace before they can sell them on the marketplace, which requires us to create a product data structure.

```
struct Product {
    uint id;
    string name;
    uint price;
    address payable owner;
    bool purchased;
  }
```

2) Event ProductCreated: Events are used to notify customers that contact this function that this product has been added to the blockchain.

```
event ProductCreated(
    uint id,
    string name,
    uint price,
    address payable owner,
    bool purchased
  );
```

3) Event ProductPurchased: Clients that call the product purchased Event function will receive a message that the product has been successfully purchased on the blockchain.

```
event ProductPurchased(
    uint id,
    string name,
    uint price,
    address payable owner,
    bool purchased
  );
```

B. Composing Function

In terms of the contract, the following function is defined:

1) Create Product:

```
function createProduct(string memory _name, uint _price)
public {
    // Require a valid name
    require(bytes(_name).length > 0);
    // Require a valid price
    require(_price > 0);
    // Increment product count
    productCount ++;
    // Create the product
    products[productCount]=Product(productCount,_name,
    _price, msg.sender, false);
    // Trigger an event
    emit ProductCreated(productCount, _name, _price,
    msg.sender, false);
  }
```

There is a Product Field validation in the CreateProduct method, which states that the supplied name cannot be empty, and the price must not be empty; if it is, the needed function will be refused.

2) Purchase Product:

```
function purchaseProduct(uint _id) public payable {
    Product memory _product = products[_id]; address
    payable _seller = _product.owner;
    require(_product.id > 0 && _product.id <=
productCount);
    require(msg.value >=_product.price);
    require(!_product.purchased);
    require(_seller != msg.sender);
    _product.owner = msg.sender;
    _product.purchased = true;
    products[_id] = _product;
    address(_seller).transfer(msg.value);
    emit ProductPurchased(productCount,
_product.name, _product.price, msg.sender, true);
  }
```

When someone buys a product using the Purchase Product function, the product owner's status is automatically updated to the person who purchased the product, and the buyer's money is sent to the seller of the goods. The parameter for this function is the product's id to be purchased, and then money will be sent in the form of ether will be done automatically.

IV. Conclusion

This paper suggests a blockchain-based strategy based on Ethereum smart contracts for constructing DApps that are open, transparent, and responsible. Smart contracts, which are digital contracts that can be implemented independently and are saved and executed on blockchain nodes, allow for the construction of safe decentralized applications. The necessity for a third-party business to function as a mediator to organize the course of the marketplace can be eliminated in a distributed marketplace, allowing sellers and buyers to execute transactions directly.

This paper demonstrated how the marketplace system is developed holistically, beginning with system architecture design and continuing with requirements, participant preparation, asset list preparation, transaction list preparation, and access control. This study has examined the procedures involved as well as the needs of the marketplace system using a solidity program. This study could compile a smart contract composed of data structures and functions, and future research could concentrate on putting smart contracts to the test in the performance section.

References

[1] S. Sfenrianto, T. Wijaya, and G. Wang, "Assessing the buyer trust and satisfaction factors in the E-marketplace," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 13, no. 2, pp. 43–57, Jun. 2018, doi: 10.4067/S0718-18762018000200105.

[2] A. N. Hidayanto and M. R. Shihab, "Trust Transfer and Its Effects on The Continuance Usage of Mobile Service in B2C E-marketplaces Comparing the approaches of small, medium, and large organisations in achieving IT and business alignment View project IT Governance on Higher Education View project." 2017. [Online]. Available: http://aisel.aisnet.org/pacis2017

[3] I. Staff, 2018 International Conference on Information Management and Technology (ICIMTech). IEEE, 2018.

[4] W. Wang, R. Chen, and C. Rui, "Association for Information Systems AIS Electronic Library (AISeL) How to Retain Your Customers: The Impact of Consumer Trust and Commitment in E-marketplaces Recommended Citation How to Retain Your Customers: The Impact of Consumer Trust and Commitment in E-marketplaces." [Online]. Available: http://aisel.aisnet.org/whiceb2011http://aisel.aisnet.org/whiceb2011/41

[5] H.-S. Doong, H.-C. Wang, and H.-C. Shih, "Exploring Loyalty Intention in the Electronic Marketplace," Electronic Markets, vol. 18, no. 2, pp. 142–149, Jun. 2008, doi: 10.1080/10196780802044792.

[6] M. E. Greiner and H. Wang, "Building consumer-to-consumer trust in E-finance marketplaces: An empirical analysis," International Journal of Electronic Commerce, vol. 15, no. 2, pp. 105–136, Jun. 2010, doi: 10.2753/JEC1086-4415150204.

[7] A. Safari, "Customers' international online trust - Insights from focus group interviews," Journal of Theoretical and Applied Electronic Commerce Research, vol. 7, no. 2, pp. 59–72, 2012, doi: 10.4067/S0718-18762012000200007.

[8] K. C. Ling, D. bin Daud, T. H. Piew, K. H. Keoy, and P. Hassan, "Perceived Risk, Perceived Technology, Online Trust for the Online Purchase Intention in Malaysia," International Journal of Business and Management, vol. 6, no. 6, Jun. 2011, doi: 10.5539/ijbm.v6n6p167.

[9] M.-S. Kim and J.-H. Ahn, "A Model for Buyer's Trust in the E-marketplace."

[10] V. P. Ranganthan, R. Dantu, A. Paul, P. Mears, and K. Morozov, "A decentralized marketplace application on the ethereum blockchain," in Proceedings - 4th IEEE International Conference on Collaboration and Internet Computing, CIC 2018, Jun. 2018, pp. 90–97. doi: 10.1109/CIC.2018.00023.

[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: www.bitcoin.org

[12] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4. Institute of Electrical and Electronics Engineers Inc., pp. 2292–2303, 2016. doi: 10.1109/ACCESS.2016.2566339.

[13] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[14] 2019 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT-NCON). IEEE, 2019.

[15] D. J. T. G. (Japan), I. C. E. Society, I. of Electrical, and E. Engineers, 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE) : 27-30 Oct. 2015.

[16] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "Cryptographic primitives in blockchains," Journal of Network and Computer Applications, vol. 127, pp. 43–58, Feb. 2019, doi: 10.1016/j.jnca.2018.11.003.

[17] B. M. Goi, M. U. Siddiqi, and H. T. Chuah, “Computational complexity and implementation aspects of the incremental hash function,” IEEE Transactions on Consumer Electronics, vol. 49, no. 4, pp. 1249–1255, Jun. 2003, doi: 10.1109/TCE.2003.1261226.

[18] P. Tasatanattakool and C. Techapanupreeda, “Blockchain: Challenges and applications,” in International Conference on Information Networking, Jun. 2018, vol. 2018-January, pp. 473–475. doi: 10.1109/ICOIN.2018.8343163.

[19] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything You Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems,” IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6–14, Jun. 2018, doi: 10.1109/MCE.2018.2816299.

[20] K. Wust and A. Gervais, “Do you need a blockchain?,” in Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018, Jun. 2018, pp. 45–54. doi: 10.1109/CVCBT.2018.00011.

[21] C. Cachin and M. Vukolić, “Blockchain Consensus Protocols in the Wild,” Jun. 2017, [Online]. Available: http://arxiv.org/abs/1707.01873

[22] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang, “Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266–2277, Jun. 2019, doi: 10.1109/TSMC.2019.2895123.

[23] J.-Y. Nie, Institute of Electrical and Electronics Engineers, and IEEE Computer Society, 2017 IEEE International Conference on Big Data : proceedings : Dec 11- 14, 2017, Boston, MA, USA.