World Academy of Science, Engineering and Technology
International Journal of Economics and Management Engineering
Vol:16, No:11, 2022

Ethereum Based Smart Contracts for Trade and Finance

Rishabh Garg

Abstract**—**Traditionally, business parties build trust with a centralized operating mechanism, such as payment by letter of credit. However, the increase in cyber-attacks and malicious hacking has jeopardized business operations and finance practices. Emerging markets, due to their high banking risks and the large presence of digital financing, are looking for technology that enables transparency and traceability of any transaction in trade, finance or supply chain management. Blockchain systems, in the absence of any central authority, enable transactions across the globe with the help of decentralized applications. DApps consist of a front-end, a blockchain back-end, and middleware, that is, the code that connects the two. The front-end can be a sophisticated web app or mobile app, which is used to implement the functions/methods on the smart contract. Web apps can employ technologies such as HTML, CSS, React and Express. In this wake, fintech and blockchain products are popping up in brokerages, digital wallets, exchanges, post-trade clearance, settlement, middleware, infrastructure and base protocols. The present paper provides a technology driven solution, financial inclusion and innovative working paradigm for business and finance.

Keywords**—**Authentication, blockchain, channel, cryptography, DApps, data portability, Decentralized Public Key Infrastructure, Ethereum, hash function, Hashgraph, Privilege creep, Proof of Work algorithm, revocation, storage variables, Zero Knowledge Proof.

I. Introduction

THE fundamental concern to create blockchain was to solve the double-spend problem or duplication of digital currency. Blockchain, in this context, was presumed to act as a ledger of the currency transaction, and each transacting person, act as node in the network, registering his activity. The complete process involved each person in the network, given the power to write on a ledger, with the consensus in the network, thus enabling decentralization. So, the more people are involved in the network, the more difficult it is to change the authenticity of information, as it would require approval from 'majority' of the network, making blockchain, a steady and secure way of protecting the data.

The data in a block seem locked as they get recorded in it, and cannot be changed. To make changes, one need to write to the blockchain and that is done only after the consensus of the network. It entails that in order to rectify any bit of information, all the blocks, created after that block, need to be changed and that too, on receiving the consensus. This would require enormous computing power to change the blocks as they are created every minute, so to bring change, at a particular point, the newly added blocks change till the specific block that needs to be changed, is rectified. The added change exists in the chain as new branch of information referred to as the 'source of truth'.

The main objective of the present study is to leverage this surefire technology for business and finance by employing any open source software such as Linux or Windows through virtual machines.

Rishabh Garg is with Department of Electrical & Electronics Engineering, Birla Institute of Technology & Science, K.K. Birla Goa Campus, Sancoale, Goa – 403726, India (e-mail: rishabhgargdps@gmail.com).

II. Software Requirements

Almost all of the software used in blockchain applications are open source, actively maintained and developed. However, most of these are designed to run on the Linux operating systems, and the preferred way to run this software on Windows machines is to use virtual machines or Docker containers that provide a Linux environment in which they can run. This is not a constraint for business applications because financial service companies already run a large number of Linux machines for other applications.

For permissioned blockchain applications, the most common software platforms are Hyper-ledger Fabric, an open source collaborative effort by a consortium of large technology companies and banks, and R3 Corda, an open source platform with a commercial version.

While permissionless blockchains have found it challenging to achieve high throughput because of the inherent limitations of proof-of-work, the permissioned systems have no difficulties on this score. Some report depict that distributed ledgers were able to 'perform at levels necessary to process an entire trading day's volume at peak rates, which equates to 115,000,000 daily trades, or 6,300 trades per second for five continuous hours' during test conditions [1].

III. Proposed Gateway

Blockchain realizes trust by validation, verification and consensus algorithms. It works in the following manner [2], [3]:

- The user, who wants to join the blockchain network, first creates an account.
- Then the genesis file is created and a genesis block is initialized.
- After starting the nodes, peers are added using the blockchain APIs.
- Using these unlocked accounts, transactions can be initiated on the blockchain.
- Transactions, the basic element of the blockchain, are validated and broadcast.
- Many transactions form a block and many blocks form a

chain through a digital data link.

- Blocks go through a consensus process to select the next block that will be added to the chain.
- Chosen block is verified and added to the current chain.
- Validation and consensus process are carried out by special peer nodes called miners.
- Miners are powerful computers executing software defined by the blockchain protocol.
- Blocks are joined together with links created by referenced hashes.

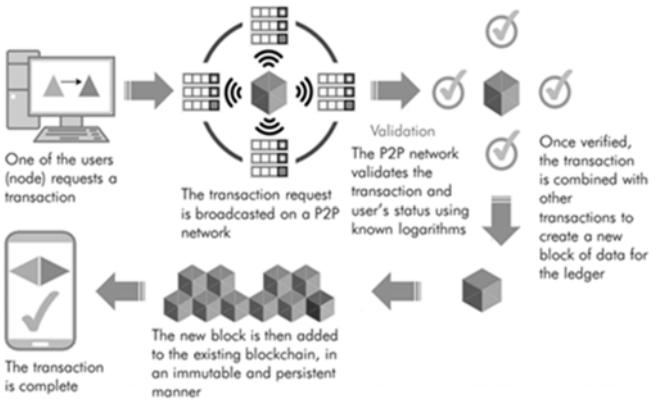

Fig. 1 Working of Blockchain [4]

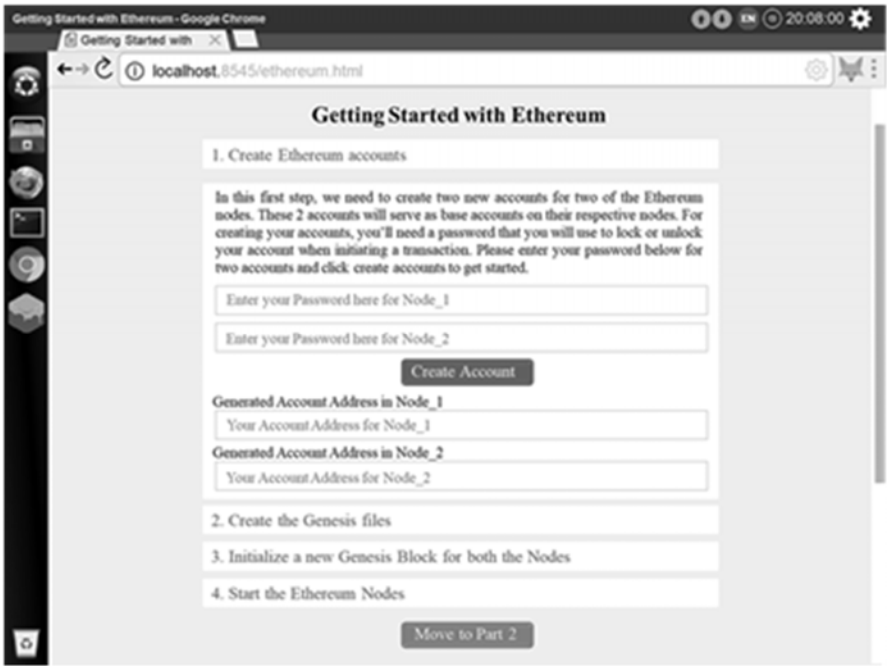

Fig. 2 Creating Blockchain Account [4]


```
{
    "config": {
        "chainId": 12,
        "homesteadBlock": 0,
        "eip155Block": 0,
        "eip158Block": 0
    },
    "difficulty": "0x20000",
    "gasLimit": "0x2feed8",
    "alloc": {},
    "nonce": "0x0000000000000041",
    "timestamp": "0x0",
    "parentHash":
"0x0000000000000000000000000000000000000000000000000000000000000000
00000000000",
    "extraData": "",
    "mixhash":
"0x0000000000000000000000000000000000000000000000000000000000000000
00000000000",
    "coinbase":
"0x0000000000000000000000000000000000000000"
}
```


Fig. 3 Content of Genesis File [4]

A. Ethereum

The Ethereum Network provides a flexible development environment. It is a P2P network that can process any type of smart contract, which can be easily created with a few lines of code, and without the necessity of creating your own special-purpose blockchain infrastructure. As opposed to Bitcoin and other single-purpose blockchains, Ethereum decoupled this smart contract layer, which now runs on top of the underlying Ethereum blockchain, making it easy to create smart contracts with just a few lines of code.

B. Smart Contracts

Smart Contracts are used for automation of common centralized processes like conditional transfer of digital assets, Multisig asset exchange or waiting for specific time to execute transaction.

Fig. 4 Adding Peers on the Blockchain [5]

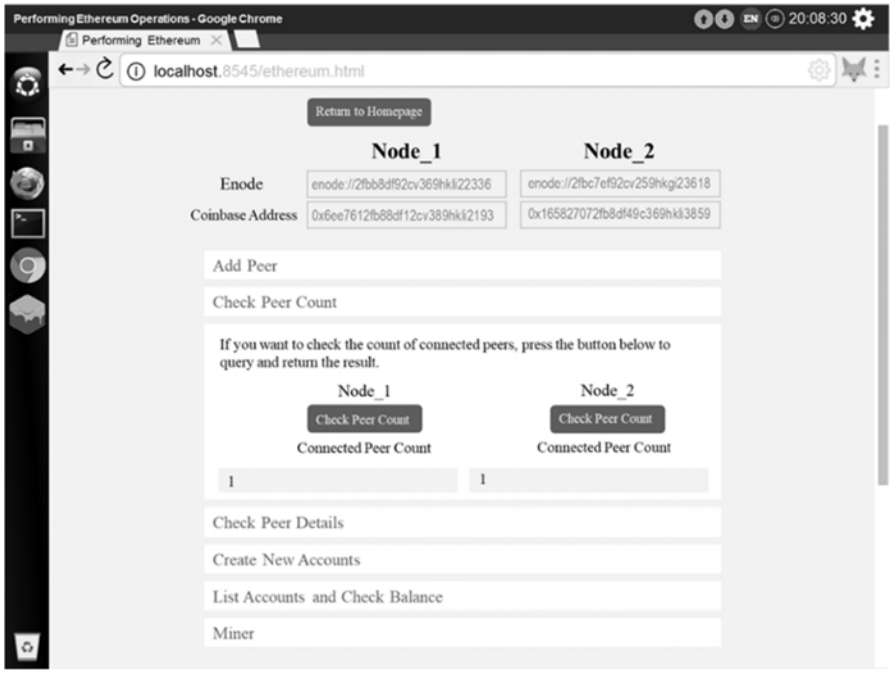

Fig. 5 Checking Peer Account [5]

Ethereum virtual machine is used to run smart contracts. Smart contracts are written in Solidity language for functionality which is typically like an Object Oriented Programming language. To be able to execute a smart contract in any hardware or software, an abstraction layer is required. This is provided by Ethereum Virtual Machine (EVM) which converts the high level language to EVM byte code.

A smart contract is represented by a Contract account. This can be invoked by an Externally Owned Account (EOA) which is needed to participate in the Ethereum blockchain. The invocation process is done using transactions sent by EOA in the form of Ether and Gas. When the target address in a transaction is a smart contract, the execution of smart contract happens on validation (e.g. checking nonce combination and fees) and verification of transaction.

Transaction in Ethereum contains:

1. Amount of Wei (1 Ether = 10^{18} Wei)
2. STARTGAS (max computational steps)
3. GASPRICE (fees per different steps of code execution)

Around 21000 gas points are paid to miner for adding transaction to block. Note: Computation requirements are specified in gas as it is a standard crypto currency. Unlike Ether, its value does not change as per market swings. State of Ethereum blockchain changes when state hash and receipt hash of smart contract changes.

TABLE I
COMPUTATION FEE IN GAS POINTS

1.	Operation name	Gas Cost
2.	Step	1
3.	Load from memory	20
4.	Store into memory	100
5.	Transaction base fee	21000
6.	Contract creation	53000

Like a programming language, Solidity class contains state of variable and methods to access the public variables. When methods are called during smart contract execution, the values of variables change, which in turn changes the state of the smart contract. This change is recorded in the form of state hash. The final result of the execution is stored in the form of receipt hash.

C. Decentralized Applications

Decentralized Applications or DApp solves the problem that requires blockchain services and blockchain infrastructure for its purpose. DApp has a front-end, a blockchain back-end and middleware, i.e. code connecting the two. The front end of a DApp is used to invoke functions/methods on the smart contract which, in turn, changes the state of the smart contract. The front-end can be a sophisticated web app or mobile app. The web app can employ technologies such as HTML, CSS, React and Express. It can be considered as a web client embedded with web3.js script communicating over RPC pipeline. To maintain the standards of DApp, tokens are used.


```
[
  {
    "id":
"85eae04bb7cc52c04ddc78b37e564055098dbc6a6118f469d918742
8e2f3802202ed147ccb44aca7a824b8fa171c8f2d28131ef4d12aa92
e56241dd0a6448a68",
    "name":          "Geth/v1.8.2-stable-4bb3c89d/linux-
amd64/go1.9",
    "caps": [
      "eth/63"
    ],
    "network": {
      "localAddress": "[::1]:35849",
      "remoteAddress": "[::1]:30302"
    },
    "protocols": {
      "eth": {
        "version": 63,
        "difficulty": 131072,
        "head":
"0x5e1fc79cb4ffa4739177b5408045cd5d51c6cf766133f23f7cd72
ee1f8d790f0"
      }
    }
  }
]
```


Fig. 6 Connected Peer Node - 1

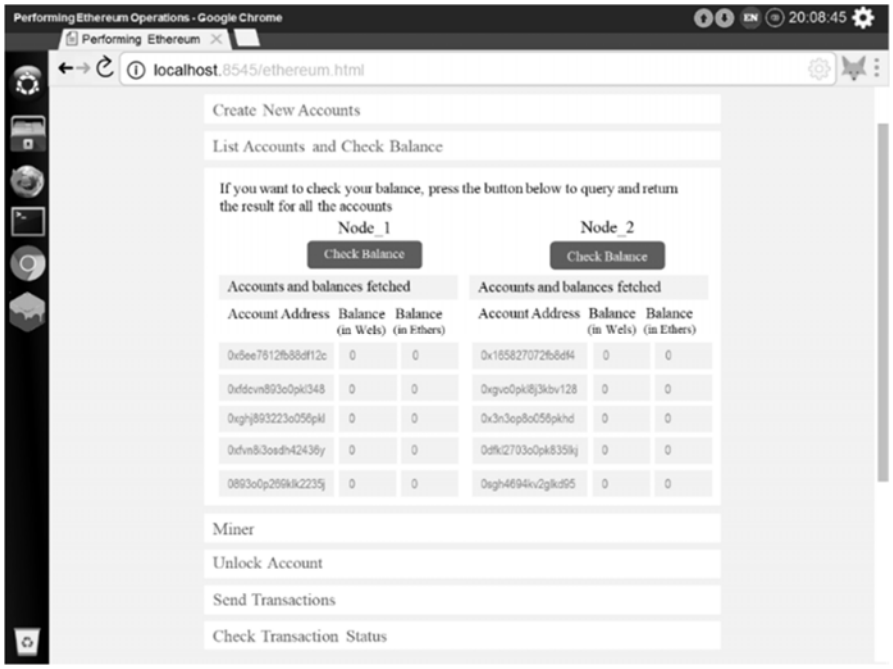

Fig. 7 Checking Account Balances [5]

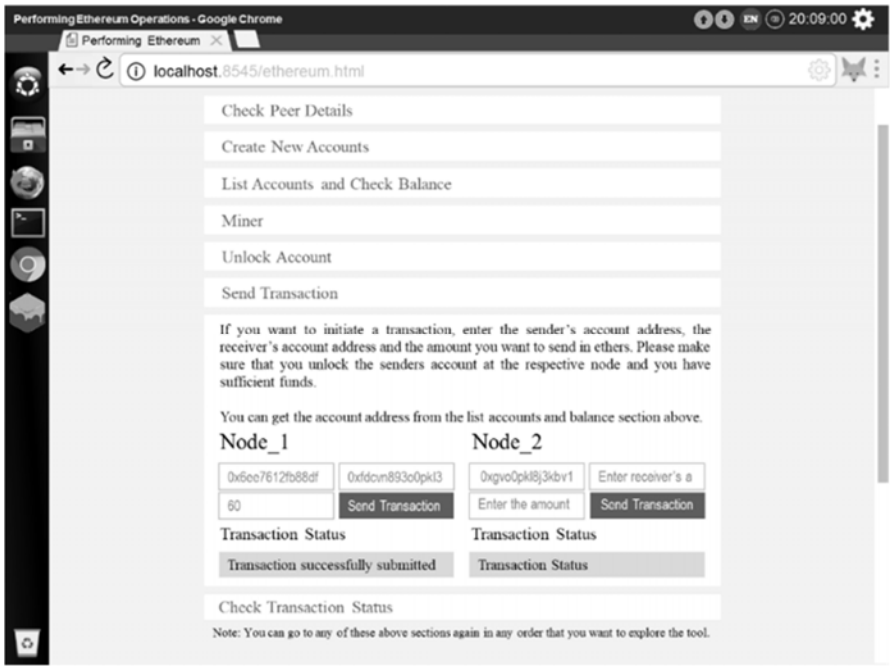

Fig. 8 Transacting on the blockchain [5]

D. Tokens

It is a type of DApp associated with asset or utility. Tokens can be of two types - fungible or non-fungible. Fungible tokens carry equal value and can be replaced with each other. ERC20 guidelines are considered as standards for fungible tokens. Non-fungible tokens have their standards inherited from ERC721 guidelines. DApps built on Ethereum such as Augur and Grid+ make extensive use of tokens to resolve disputes in the case of market prediction and payment for electricity usage respectively.

IV. Efficiency in Trade Finance

Trade finance plays a significant role in international trade. An international consignment comprises three major flows - documentation, cash flow and shipment, involving exporters (manufacturers, sellers, suppliers), importers (retailers, buyers, consumers), transporters (shippers, logistic movers) and credit operators (banks, financers), insurance companies and agents. Traders often choose payment modalities, according to diverse risk level and strategic concerns, and create a sale contract between the seller and the buyer. Among various payment methods (letter of credit, open account, telegraphic transfer, cash on delivery), Letter of Credit is usually preferred by exporters owing to lower risk probability.

Banks in the countries of the seller and buyer act as trusted intermediaries to handle cash in exchange of goods. The buyer asks his bank to issue a Letter of Credit to the seller's bank, for the exchange of goods. However, it involves redundant documentation, higher bank charges and likelihood of forgery.

A. Smart Contracts

Trade contract is a business agreement, in physical or written form, between commercial minds in a complicated legal language, which either of the parties hardly understand. Instead of legal terms, these contracts can better be described by computer code in the Python programming language so that traders could understand them better. In 2010, the US Securities and Exchange Commission [6] also suggested to disclose the terms and conditions laid down in Asset Backed Securities in the form of computer code.

In this milieu, blockchain provides an ideal platform for smart contracts. Smart contracts combine protocols with user interfaces to formalize and secure new relationships such as business forms, contract law and account controls. Though it is possible to share database between two parties or deploy a smart contract even without the blockchain, it can be difficult to build trust in the absence of a trusted intermediary. Neither of the parties will trust each other's data, formats, standards and procedures nor let the smart contract run on the other's node. This is where the blockchain comes into being - it is not only a computer in the cloud, rather it is shared platform across several nodes, backed by consensus algorithms and protected by cryptography. It is inherently designed to audit each transaction with no room for modification or omission.

By automating key contractual phases: search, negotiation, commitment, performance, and adjudication, transactions may be secured, overheads may be reduced and petty transactions can be made viable. Today, many financial transactions, including stock trading, are done largely by algorithms that decide to buy or sell on the basis of price signals. A momentum-based algorithm sends a buy order to the stock exchange, while another contrarian algorithm sends a sell order. The stock exchange's software, without any human intervention, takes decision between the two algorithms on certain complex rules. Smart contracts deployed on a blockchain can achieve similar output in OTC markets without an exchange. Thus, the

blockchain, in amalgam with smart contracts, provides a secure, transparent, auditable, and automatic transactional environment for trade investors. Smart contracts may be automated in line with the terms of trade contract, logistics status may be updated as an event driven mechanism and payments may be activated as per predetermined procedures. This is how, blockchain network may alleviate the need of a central authority to verify transaction in a brick and mortar operation.

In the upcoming code cell (see Fig. 9), a smart contract to automate trade (auction process), after Garg [5].

B. Enterprise Resource Planning

Organizations mostly use an Enterprise Resource Planning (ERP) software with a common database that provides a single version of the truth, across numerous departments, in real time. It ensures better management and internal controls. Once again, blockchain itself is a distributed ledger that shares a common database and provides a single version of the truth to all participating nodes irrespective of any geographical or administrative precincts. An added advantage is that, in absence of a trusted intermediary, it would be easier for either of the parties to adopt a neutral platform like blockchain. At the same time, other players - clearing agents, insurance companies, shippers, forwarding agents will also have an access to same version of truth, in real time. Thus, it is an area, where the blockchain can move from pilots to real world applications [6], [7].


```
pragma solidity ^0.4.17;
contract Auction {

    // Data
    //Structure to hold details of the item
    struct Item {
        uint itemId; // id of the item
        uint[] itemTokens;  //tokens bid in favor of the
item
    }

   //Structure to hold the details of a persons
    struct Person {
        uint remainingTokens; // tokens remaining with
bidder
        uint personId; // it serves as tokenId as well
        address addr;//address of the bidder
    }

    mapping(address => Person) tokenDetails; //address
to person
    Person [4] bidders;//Array containing 4 person
objects

    Item [3] public items;//Array containing 3 item
objects
    address[3] public winners;//Array for address of
winners
    address public beneficiary;//owner of the smart
contract

    uint bidderCount=0;//counter

    //functions

    function Auction() public payable{    //constructor

        //Task 1.1. Initialize beneficiary with address
of smart contract's owner
        //In the constructor,"msg.sender" is the address
of the owner.
        // ** Start code here. 1 line approximately. **/
        beneficiary = msg.sender;
          //** End code here. **/
        uint[] memory emptyArray;
        items[0] =
Item({itemId:0,itemTokens:emptyArray});

        //Task 1.2. Initialize two items with at index 1
and 2.
        // ** Start code here. 2 lines approximately.
**/
        items[1] =
Item({itemId:1,itemTokens:emptyArray});
        items[2] =
Item({itemId:2,itemTokens:emptyArray});
        //** End code here**/
    }

    function register() public payable{


bidders[bidderCount].personId = bidderCount
```

```
//Task 1.3. Initialize the address of the bidder
        /*Here the bidders[bidderCount].addr should be
initialized with address of the registrant.*/

        // ** Start code here. 1 line approximately. **/
        bidders[bidderCount].addr = msg.sender;
        //** End code here. **

        bidders[bidderCount].remainingTokens = 5; //
only 5 tokens
        tokenDetails[msg.sender]=bidders[bidderCount];
        bidderCount++;
    }

    function bid(uint _itemId, uint _count) public
payable{
        /*
            Bids tokens to a particular item.
            Arguments:
            _itemId -- uint, id of the item
            _count -- uint, count of tokens to bid for
the item
        */

        /*
        Task 1.4. Implement the three conditions below.
            4.1 If the number of tokens remaining with
the bidder is < count of tokens bidded, revert.
            4.2 If there are no tokens remaining with
the bidder, revert.
            4.3 If the id of the item for which bid is
placed, is greater than 2, revert.

        Hint: "tokenDetails[msg.sender].remainingTokens"
gives the details of the number of tokens remaining with
the bidder.
        */

        // ** Start code here. 2 lines approximately.
**/
        if
(tokenDetails[msg.sender].remainingTokens<_count ||
tokenDetails[msg.sender].remainingTokens == 0 || _itemId
> 2) revert();

        //** End code here. **

        /Task 1.5. Decrement the remainingTokens by the
number of tokens bid and store the value in balance
variable.
        "tokenDetails[msg.sender].remainingTokens"
should be decremented by "_count". */

        // ** Start code here. 1 line approximately. **
        uint
balance=tokenDetails[msg.sender].remainingTokens -
_count;
        //** End code here. **


tokenDetails[msg.sender].remainingTokens=balance;

bidders[tokenDetails[msg.sender].personId].remainingToke
ns=balance;//updating the same balance in bidders map.
```

```
Item storage bidItem = items[_itemId];
        for(uint i=0; i<_count;i++) {

bidItem.itemTokens.push(tokenDetails[msg.sender].personI
d);
        }
    }

    // Task 2.1. Create a modifier named "onlyOwner" to
ensure that only owner is allowed to reveal winners
    //Use require to validate if "msg.sender" is equal
to the "beneficiary".
    modifier onlyOwner {
        // ** Start code here. 2 lines approximately. **
        require(msg.sender == beneficiary);
        _;
        //** End code here. **
    }

    function revealWinners() public onlyOwner{

        /*
            Iterate over all the items present in the
auction.
            If at least on person has placed a bid,
randomly select          the winner */

        for (uint id = 0; id < 3; id++) {
            Item storage currentItem=items[id];
            if(currentItem.itemTokens.length != 0){
            // generate random# from block number
            uint randomIndex = (block.number /
currentItem.itemTokens.length)%
currentItem.itemTokens.length;
            // Obtain the winning tokenId

            uint winnerId =
currentItem.itemTokens[randomIndex];

            /Task 1.6. Assign the winners.
            " bidders[winnerId] " will give you the
person object with the winnerId.
            you need to assign the address of the person
obtained above to winners[id] */

            // ** Start coding here *** 1 line
approximately.
            winners[id] = bidders[winnerId].addr;

            //** end code here*

            }
        }
    }

  //Miscellaneous methods: Below methods are used to
assist Grading. Please DONOT CHANGE THEM.
    function getPersonDetails(uint id) public constant
returns(uint,uint,address){
        return
(bidders[id].remainingTokens,bidders[id].personId,bidder
s[id].addr);
    }
```

Fig. 9 Auction Process using Smart Contracts

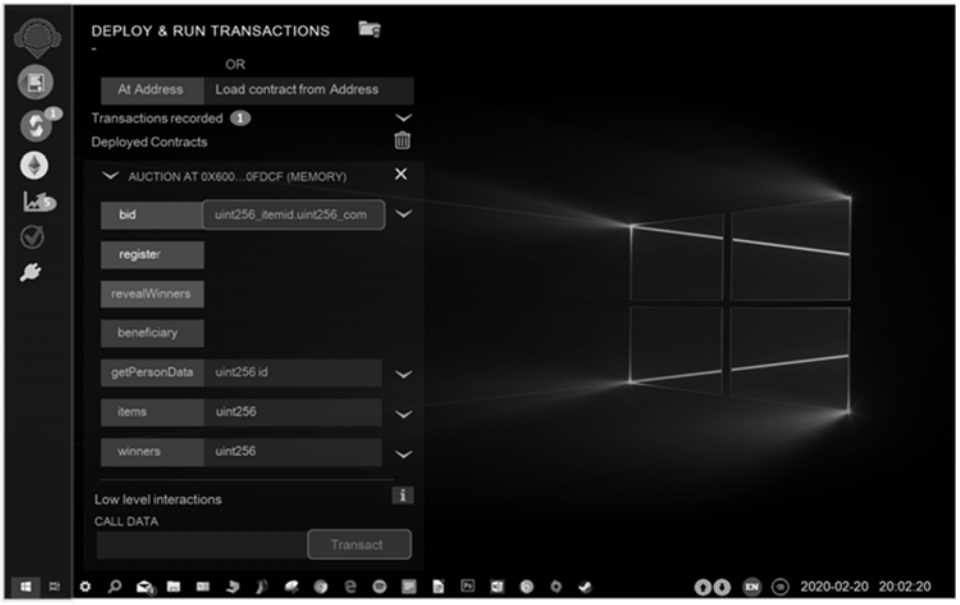

Fig. 10 Deployment of Smart Contracts using Remix IDE, after Garg [5]

C. Data Repositories and Registries

After the Global Financial Crisis 2008, trade repositories have been formed to make sure that regulators have requisite information about the risk and interconnectivity of the financial system. Post 2008 finance largely depends on data repositories (e.g. credit bureaus) and registries (e.g. loan registries) that provide verified data for a variety of transactions. Though such information is decisive for providing credit, the data stored by credit repositories contain inadvertent errors like duplication, and the system has been suffering from lack of accountability, loss of privacy and excessive cost. Blockchain, being permanent and auditable, can provide a real solution.

D. Tokenization of Fiat Money

Finance is all about money, and in due course of time, it can achieve better liquidity and scale, if fiat money (dollars, euros, rupees etc.), in place of crypto currency, be transacted directly on the chain. At the outset, the central banks itself can issue digital money that flows on a blockchain. Albeit, it is not easy to cover the initial operation costs and returns, until the issuance reaches a sufficiently large scale.

It is evident from reports that Blockchain has captured a vast landscape with 200 million crypto users worldwide [9]. Japan, the harbinger of crypto currency trading, has announced the Payment Services Act to rule crypto currencies and their usage for trading purposes. Following the trail of Japan, Mastercard and Bank of New York Mellon, in the United States, have allowed users to transact in certain crypto currencies. Likewise, Amazon, Subway, Microsoft Store, etc. have started accepting payments in Bitcoin. As of 2021, over 18,000 trades have adopted crypto currency payments [10].

In European Union (after France in 2014), Germany has also legalized bitcoin, and is steadily involved in pioneering blockchain solutions. Further, Canada has validated bitcoin exchanges, but refrained its use for money laundering. Australia is one of the countries that have legalized crypto currency effectively. The government has imposed capital gains tax and given acceptance as a property.

According to the Statista Global Consumer Survey [11] conducted by the World Economic Forum (2021), Nigeria is leading among the top most countries using crypto currency. The primary reason seems to be high remittance fee, to send money, across borders. With relatively small legacy systems in the region, the prospects for emerging blockchain technology into a full range of financial products, is highly probable, due to strong support from financial players and local governments. Stakeholders are gradually diagnosing blockchain as an emerging disruptor and enabler, and they are investigating and fostering the technology to ensure that they are not excluded from its potential benefits.

Philippines, as a big surprise, has the third highest number of crypto users in the country, after Vietnam. Ukraine and Russia are the leaders in crypto currency adoption, despite infrastructure challenges.

Asia is a global leader with 59 million crypto users. There are nevertheless stark differences across Asian nations with China, Hong Kong and Singapore leading the way. China's voracious thirst for blockchain goes far beyond crypto currencies. It strongly supports adoption of blockchain technology, as announced in its recent five year plan, and is providing a conducive regulatory environment. The government is piloting a sovereign blockchain digital currency, led by the central bank, the People's Bank of China [12]. Other countries, such as Vietnam, Thailand, Pakistan, are also in the list, with India surpassing 100 million crypto users [13]. Asia has evolved the most comprehensive ecosystem for blockchain development with regulatory support, and mobilization of capital from venture capitalists as well as industry players. The Middle East is also catching up, despite the fact that many states in the region still do not allow activities related to blockchain.

In Latin America, political uncertainty and the impact of de-risking are tantalizing blockchain-based financial products. Some countries, like Peru, Argentina, Brazil and Chile have made a start; yet, the region as a whole lacks technological infrastructure, adequate access to venture capital funding, and the regulatory sandboxes for open adoption.

By the time crypto currency forms a substantial base, as an alternative to fiat money, it is worthwhile to deliberate over, and adopt, regulated tokenization of fiat money.

E. Lightning Network

The Lightning Network, which depends upon the underlying technology of blockchain, using its native smart-contract language, can create a secure network of participants to transact at high volume and high speed. Suppose, two participants wish to transact frequently, may be a number of times a day. Initially, they would create a multi-signature wallet, which both of them can access using their respective private keys. Then, they would deposit a certain amount into that wallet, and thereafter, they can perform unlimited transactions between them. Since, all the transactions would happen between the two only, it would be more of a redistribution of fund, within the shared wallet. Whatever transactions they make, both of them use their private keys to sign for an updated balance sheet. But, the actual distribution of funds would happen when the channel gets closed. Once the channel is closed, then only the information is broadcasted about the initial contribution and the final balance on the blockchain. In this way, the Lightning Network enables users to conduct countless number of transactions outside of the main chain and then record them as a single on the blockchain. This is how volume and speed, both are met with confidence of on-blockchain enforceability.

F. Pre- and Post-Trade Processes

Securities are traded and settled in three stages: (a) pre-trade authorization and approval, (b) trade execution, and (c) clearing and settlement. With enormous investment in technology infrastructure, trade execution has been highly automated to minimize latencies to the tune of microseconds. Blockchain works at a speed of 07 transactions per second [14] and it would be next to impossible for any blockchain to achieve the speed of stock exchange. So, exchanges may be continued but the pre- and post-trade processes, that involve inefficient and fragmented legacy systems, can be boosted by implementing blockchain.

Blockchain can remove opacity on the cash and securities in pre-trade checks and trade confirmations. With dividends and stock splits being controlled by smart contracts, and settlements occurring on delivery versus payment basis, we will not require depositories, brokers or custodians, anymore. The novation - short selling, margin trading and net settlement, provided by the Central Counter Parties can be replicated through smart contracts and the depository could run the permissioned blockchain on which the settlement happens.

Though it is little early to predict things, however, there may be new ways of business organizations and corporate governance, in the days to come. It could be an algorithmic governance [15]; an enterprise without entities [16] or a decentralized autonomous organization (DAO) with fool-proof codes.

V. Potential Benefits

The blockchain provides possibility of improvements in various aspects of trade finance.

A. Decentralization

In conventional trade finance, if the central trusted institution shuts down for a while, the entire system grinds to a halt. In 2014, the RTGS (real time gross settlement system) of the United Kingdom experienced a downtime of nine hours [17]. Though all banks and other entities were operational, high-value payments could not happen during this period. Advantage of using a distributed ledger [18] is that blockchain is partition resistant, wherein if some nodes fail or are disengaged from the network, the rest of the nodes continue to function since all nodes carry a copy of the same data.

B. Information Transmission

Blockchain allows trade associated parties - banks, transporters, agents, exporters and importers, to share a common distributed ledgers for trade practices. Trade documents may be digitized to enable the automatic implementation of trade processes through smart contracts. Since the flow of vital information among parties will be carried out through an event-driven mechanism, most of the trade frictions and painful handovers of merchandises could be transformed into a real-time response of workflow status. This would eliminate repetitive manual checks, to verify trade logistics, goods delivery and payment contexts.

C. Incorporation of IoT

Traders often make payment upon the arrival of goods or presentation of bills. It implies that the activities, that are resultant upon shipment handovers, or notifications, deter the smooth trade practices. Blockchain provides parallel notification of status for goods and documents, in real time, through deployment of Smart contracts [19]. Further, IoT enabled operations, such as machine-to-machine transactions, source tracking, logistics, shipping [14], can facilitate trade associates to make accurate tracking of goods and supplies.

D. Defense Mechanism

Over the years, there has been a gush of hacks and cyber-attacks, either to steal personal information or inflict colossal damage to the system. Byzantine fault tolerance, which deals with nodes that function maliciously, provides a strong defence by virtue of (a) replication of the data across large number of nodes running on completely different computer networks and (b) cryptographic integrity checks.

E. Transparency

Blockchain ledger is not only irreversible, but trustworthy too. It averts any scope for malicious activity or fraudulence, thereby alleviates an obligation of any certified trusted party or a consensus mechanism [15]. Further, it allows users to validate

their identity, irrespective of any geographical border, and creates a traceable audit for authentication [16]. Thus, transfer of ownership and verification of identity will be more accessible, transparent and auditable.

F. Disintermediation

In trade practices, numerous intermediaries, play their roles and in turn, impede process of transactions. The blockchain unites diverse trade groups into a single transactional network without intermediaries, automates the confirmation of trade documents and expedites the process of cash settlements.

G. Cost

In Letter of Credit finance, trade-related administrative and logistic handovers, across shipping routes, obstructs the flow of business and make it less competitive under payment options, such as inter-firm trade credit [17]. Blockchain will streamline trade processes and reduce over-heads by curtailing the cost of documentation and payments for central service providers.

TABLE II
GLOBAL TRADE PAIN POINTS AND POTENTIALS BENEFITS OF USING BLOCKCHAIN ENABLED TRADE

	Issues	Global Trade Pain points	Potentials utilizing blockchain L/C
1	Trust mechanism	Rely on an authorized central party (e.g., banks) as intermediary to deal with trade finance.	Immutable, consensus-based and distributed ledger network for a conducive trade environment
2	Tampering issues	Malicious attempts may cause fraudulence and trade disputes; Authorities build trust among trade parties.	Preserve contract terms and amendments, if any, on blocks for ever; Alleviate tampering issues.
3	Instruments used	Paper-based, manual process; Lengthy delivery.	Digitized documents deployed on a secured and shared ledger.
4	Transaction risk	Risk-sensitive; Rely on authorized third parties.	Risk mitigation. Trust ensured through consensus mechanisms
5	Bill(s) of lading (B/Ls)	Intensive paperwork for presentation of B/Ls. Lengthy delivery across borders; Complex ownership transfer across handovers.	Digitized operation; Minimum time of transfer and delivery; Blockchain-based identification without presentation of B/Ls
6	Information transmission	Manual process, which takes time and cost; Centralized data, susceptible to cyber-attacks or system malfunction.	Event-driven consensus with smart contracts; Tamper-proof features. Less security and privacy concerns on consortium chain
7	Traceability	Complex trade processes due to multiple participants; Uncertainties in tracking asset identities, ownership, and shipment status.	A member database, easily traceable; with provision of credit ratings, promises better user experience

VI. CHALLENGES AND WAYS TO OVERCOME

A. Security

Security is a prime concern with identity as well as finance. A participant, who has more than 50% of the mining capability, can plan an attack by virtually holding full control on the blockchain. Despite having a fork on the blockchain, the attacker can make step-wise false transaction : i) publication of a mining software with expected value; ii) creation of a pool with stickiness (Ponzi scheme); iii) creation of unwanted coalitions; iv) assault of other pools with cannibalized pools; and v) an eventual switch to members only.

TABLE III
IMPACT DIMENSION OF THE USE OF BLOCKCHAIN IN TRADE FINANCE AND L/C PAYMENT

	Dimension	Blockchain's Impact
1.	Transparency	Auditable trail of transactions through global ledger Digitization of Physical property and Collaborative verification of critical transactions by participating nodes using a shared database Immutable transactions on a common distributed ledger Lessen fake and counterfeit goods or document across transaction journey Providing participants with access to transaction records
2.	Information transmission	Enable broadcast of verified and time-stamped transactions Automatic execution of Trade activities through Smart Contracts
3.	Traceability	Physical flow of goods Real-time notifications
4.	Disintermediation	Cash settlement and validity check of trade documents without intervention of third party
5.	Cost	Streamline administrative processes Shorten latency and curtail transaction fees
6.	Incorporation of IoT	Facilitate storage of tracking records

Under such circumstances, Wallet security - a multiple signature process, called multisig, can be adopted. Although, the creation of scripts helps to resolve hoards of problems, there is a possibility that a transaction may not correctly configure due to complexity of the scripts. If it occurs, the Bitcoin that uses an incorrectly configured script would be discarded, since the unlocking script will not be able to generate [18].

B. Scalability

With the ever increasing volume of transactions, the blockchain becomes bulky. Due to the inherent restriction of block size and the time interval to generate a new block, the Bitcoin blockchain can process, about seven transactions per second, which fails to meet the requirement of processing millions of transactions on real-time basis. Hence, there are only two way-outs: one is storage optimization and the other is re-designing.

Bruce [19] proposed a novel crypto currency scheme, in which the old transaction records are removed (or forgotten) by the network. It is significant because it is quite difficult for node to operate full copy of ledger. Eyal et al. [20] presented Bitcoin-Next Generation to decouple conventional block into two parts: key block for leader election; and microblock for transaction storage. The time has been divided into epochs, and in each epoch, the miners need to hash to generate a key block. Once a key block is generated, the node becomes the leader, who is liable to generate microblocks. Bitcoin-NG also extended the longest chain strategy in which microblocks carry no weight. This is how, by redesigning blockchain, the tradeoff between block size and network security has been addressed.

Another concern regarding scalability is related to the

technical extension of the system. The non-scalable technical extension of the design of Bitcoin does not allow other features or applications to be incorporated. For example, creators that want to incorporate the Bitcoin system to smart contracts, find it extremely complicated. This is how other systems were born, Ethereum being one of the most relevant examples today [21].

In the near future, blockchain can have an issue regarding storage capacity as transactional histories are constantly added onto one another [22]. The problem can be resolved by providing access to write information, only to a central intermediary. This would reduce consensus needs [23].

C. Block Time

Currently, Bitcoin processes 4.6 transactions per second and Visa does around 1,700 transactions per second (150 million transactions per day) with a small fraction of the electrical power that used by Bitcoin [24]. The reasons for this dormancy are cryptographic verification and blockchain's consensus algorithms, which delay the amount of transfers.

Nowadays, Bitcoin block puzzles are solved at a minimum time of 03 seconds and a maximum of ≥ 50 minutes. Subsiding the complexity of PoW would reduce the time spent, but may lead to blockchain forks if the block generation timeframe is very narrow [21]. Lin et al. [25] proposed an improved blockchain consensus algorithm based on the mortgage model instead of probability model; a cross-chain protocol with transverse expansion capacity, which would support the message transmission among chains; and a high-performance cross-chain blockchain network structure, which could handle more than a thousand transactions per second per chain by verification.

D. Privacy

Though transparency is one of the virtues of blockchain, yet it frightens privacy. A holder of crypto currency can be tracked by making the use of public keys related to his payments. Using software tools, anyone can have an access to and create a behavioral map on the basis of information gathered through public keys, about his shopping choices, spending capacity and the frequency of transactions.

In order to resolve privacy concern, Del Rio [22] proposed a notary based blockchain system, in which no node in the system has the complete set of information. Since a trusted third party would contribute in validating the transactions, this would ensure greater privacy. The only disadvantage is that if there is any fake information in one or more nodes, the system would collapse and verification will not be possible as nobody would have a full copy of the ledger. In such cases, Bitcoin Fog or Dark Wallet that fosters anonymity through a series of scripts, can be used as an alternative [25].

E. Technology Development

Blockchain technology has certain teething troubles, since the idea is years ahead of the actual technological development. Rodrigues et al. [26] have cautioned the blockchain based start-ups to make sure that the technology, used to develop the applications, must be compatible in terms of decentralization and transparency without compromising with performance and privacy, in order to prevent financial losses. However, the PoW serves no other purpose than assuring the security inside the network, hence it is a wastage of resources in the early stage of the technology development A higher computational power for mining would result in high-energy expenditure. Though development models like, Standards Development Organizations and National Standards Organizations, are only open to users who have paid a subscription, yet this restricts the number of users that can make developments into a specific area. In order to survive through this situation, Marsal-Llacuna et al. [27] have presented a blockchain model for drafting with a token to administer open to sharing.

F. Cyber-Risks

Blockchain system, in absence of any central authority, qualifies transactions across the globe, without verifying one's identity. This can encourage the development of illegal activities such as drug trafficking, money laundering and financial terrorism [21].

In recent years, ransomware attacks, such as WannaCry, affected more than 300,000 computers in 150 countries. Investors may incur huge financial losses, if their cryptographic keys are lost, because in most cases the attack is instant and irreversible [23]. Irwin & Turner [25] and Stefan [28] pointed out the necessity for regulation procedures to prevent fraud and money laundering activities.

G. Robustness

Trade and Finance require 24 x 7 service for transactions, with no downtime. Another concern is to envisage ever-growing software requirements of blockchain based products for startups, in order to grow their business. This would require enhancement in software capacity for decision-making, higher degree of automation, and up-gradation of traditional software concepts to make them blockchain compliant [29]. The optimization of smart contracts in the blockchain would help the network achieve its robustness [30].

H. Legal Enforcement

Blockchain system has so far been dominated by ideologically motivated computer professionals or geeks who are not sufficiently meticulous about commercial aspects. In real world finance, they have to face competition from incumbent players who are not only rich and powerful, but also well-rooted in the current legal and regulatory framework. Thus, in order to push real world finance into the blockchain, code and law must co-exist.

Policy-makers are in a state of dilemma whether to continue with an unregulated state of affairs or to incentivize the new technology. An unfettered situation may embolden illegal organizations to make profit in absence of regulations that govern these activities [31]. On the other hand, development of an adapted regulation could lead to loss of a country's competitive advantage, as FinTech start-ups may end up migrating to more favorable jurisdiction in some other part of the globe.

I. Miscellaneous

Other issues are associated with the dark net, financial risks (credit or liquidity risk), cyber-security, and crypto currency volatility. However, the darknet escapes common users, as only one out of 3,000 web pages are visible to everyday search engines, and between 80%-98% of the information on the Internet exists in in the darknet. All at once, it is also necessary to address issues like instability of crypto currencies that has experienced unprecedented growth, accompanied with violent volatility, during the last two years.

VII. Conclusions

The adoption of any new technology is often difficult to understand in terms of the path that it will take. The history is full of instances, when there is a delay between early implementation and regulatory acknowledgment while dealing with important market innovations. Legal compliance and regulation by the authorities, which rely on stable and optimal choices, are a pre-requisite for any such innovation to make its way into the financial system. Currently, this framework seems inadequate especially when introducing a disruptive technology such as blockchain in the equation. However, recent market trends indicate that a proof-of-concept phase is happening across emerging markets, coercing governments and policy-makers to observe and devise regulatory procedures for blockchain to thrive.

While blockchain can have a decisive impact on all emerging market regions, Asia appears to be a rising champion for blockchain implementation. China and Singapore are emerging leaders, as they have prospered in bringing together a robust infrastructure, administrative support, regulatory frame-work, symbiotic relations between industry & enterprise, and continued access to venture capital.

References

[1] Depository Trust & Clearing Corporation, DTCC unveils groundbreaking study on DLT. Retrieved from http://www.dtcc.com/27 October 2018.
[2] R. Garg, “Self-Sovereign Identities”. Lambert Heinrich-Böcking-Str. 6-8 | 66121 Saarbrücken, Germany, 2021: 1-96.
[3] R. Garg, “Digital Identity Leveraging Blockchain”, Barnes & Noble USA, 2021: 1-124.
[4] R. Garg, “Blockchain based Decentralized Applications for Multiple Administrative Domain Networking”. BITS - Pilani, KK Birla Goa Campus, India, 2021: 01-69.
[5] R. Garg, “Blockchain for Real World Applications,” John Wiley & Co. USA, 2022: 01-300.
[6] D’Monte, L. How blockchain puts trade finance deals in fast lane. Mint. Retrieved from https:// www.livemint.com/Money/aeuKOy0BpNrlFgXyjzTIqJ/How-blockchain-putstradefinance-deals-in-fastlane.html.
[7] Sanghvi, N. The truth about reliance and India’s first blockchain transaction. Retrieved from https://coincrunch.in/2018/11/06/the-truth-about-reliance-and-indias-first-blockchain-transaction.
[8] CB Insights, 2017. “Global Ledger: Mapping Bitcoin and Blockchain Startups around the World.” CB Insights Research Briefing.
[9] DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of ‘The DAO’, a failed decentralized autonomous organization. In Malcolm Campbell-Verduyn (Ed.), Bitcoin and Beyond (pp. 157–177). Routledge.
[10] Verstein, A. (2017). Enterprise without entities. Michigan Law Review, 116(2), 247.
[11] Deloitte. (2014), Independent review of RTGS outage on 20 October 2014. Bank of England.
[12] Bank of England. (2016). A new RTGS service for the United Kingdom: Safeguarding stability, enabling innovation.
[13] Wu, H. Li, Z. King, B. Ben-Miled, Z. Wassick, J. Tazelaar, J. A distributed ledger for supplychain physical distribution visibility. Information 2017 (8) 137.
[14] Panarello, A. Tapas, N. Merlino, G. Longo, F. Puliafito, A. Blockchain and IoT integration: A systematic survey. Sensors 2018 (18) 2575.
[15] R. Garg, “Global Identity through Blockchain”. International Webinar on Blockchain. Scholars Park, IN 2021: 1-60.
[16] Mainelli, M. Blockchain will help us prove our identities in a digital world. Harv. Bus. Rev. Digit. Artic. 2017, 2-6.
[17] Clark, J. Trade finance: Developments and issues. CGFS Paper. 2014, 50.
[18] Park, JH. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry 2017 (9) 164.
[19] Bruce JD. The Mini-blockchain Scheme, 2014.
[20] Eyal, I. Gencer, AE, Sirer, EG. Van Renesse, R. Bitcoining: A Scalable Blockchain Protocol. Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI-16), Santa Clara, CA, 2016: 45-59.
[21] Chen, G. Xu, B. Lu, M. and Chen NS. Exploring blockchain technology and its potential applications for education. Springer open Chen et al. Smart Learning Environments, 2018 (5) 1.
[22] Del Rio, CA. Use of distributed ledger technology by central banks: A Review. Enfoque Ute 2017 (8) 1-13.
[23] Mills, D. Wang, K. Malone, B. Ravi, A. Marquardt, J. Chen, C. Badev, A. Brezinski, T. Fahy, L. Liao, K. Distributed Ledger Technology in Payments, Clearing and Settlement. Finance and Economics Discussion Series. 2016.
[24] Jeffrey, C. What Is Transactions per Second (TPS): A Comparative Look at Networks. https://phemex.com/blogs/what-is-transactions-per-second-tps.
[25] Lin, T. Xu, Y. Wang, T. Peng, T. Xu, F. Lao, S. Ma, S. Wang, H. and Hao, W. Implementation of High-Performance Blockchain Network Based on Cross-Chain Technology for IoT Applications. Sensors (Basel), 2020.
[26] Irwin, AS. Turner, AB. Illicit Bitcoin transactions: Challenges in getting to who, what, when and where. J. Money Laund. Control 2018 (21): 297-313.
[27] Rodrigues, B.; Bocek, T.; Stiller, B. The Use of Blockchains: Application-Driven Analysis of Applicability. Blockchain Technol. 2018: 111, 163–198.
[28] Marsal-Llacuna, M.-L. Future living framework: Is blockchain the next enabling network? Technol. Forecast. Soc. Chang. 2018: 128, 226–234.
[29] Stefan, C. Tales from the crypt: Might cryptocurrencies spell the death of traditional money? A quantitative analysis. In Proceedings of the International Conference on Business Excellence, Bucharest, Romania, 2018 (12): 918-930.
[30] Almeida, S. Albuquerque, A. Silva, A. An Approach to Develop Software that Uses Blockchain. Software Engineering Algorithms Intelligence Systems, 2019 (763): 346–355.
[31] Kumar, S. Mookerjee, V. Shubham, A. Research in Operations Management and Information Systems Interface Productivity & Operation Management 2018 (27): 1893-1905.
[32] Ducas, E.; Wilner, A. The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. Int. J. Can. J. Glob. Policy Anal. 2017: 72, 538–562.