Blockchain in Smart Power Grid Infrastrusture

Mohit Vashistha
Computer Science and Engineering
Indian Institute of Information Technology Guwahati
Assam, India
mohit6b@gmail.com

Dr. Ferdous Ahmed Barbhuiya
Computer Science and Engineering
Indian Institute of Information Technology Guwahati
Assam, India
ferdous@iiitg.ac.in

***Abstract*—Internet of Things(IoT) is playing a vital role in making the digital world smarter with widely adopted applications in industrial and manufacturing such as supply chain management, manufacturing automation, remote machine diagnostics and prognostic health management of industrial machines. Internet of Things is the network of the physical devices embedded with sensors, electronics, software, actuators and connectors for the connectivity of these devices to connect, collect and process/exchange the data among them and with other devices. Existing solutions are leveraging IoT technologies at a large scale but with the requirement of third party intermediary and with a lot of compromises with security of data. This paper represents a system which will help to rectify these existing concerns about security, privacy and third party requirement. It represents a system which will allow exchange and collection of data in a decentralized, peer-to-peer, trustless network of devices with the help of the BlockChain technology consisting of these vital properties.**

***Index Terms*—BlockChain, IoT(Internet of Things), decentalized**

I. Introduction

Internet of Things (IoT) comprises "Things" (or IoT devices) which have remote sensing and/or actuating capabilities, and can exchange data with other connected devices and applications (directly or indirectly). IoT devices can collect data and process the data either locally or send the data to centralized servers or cloud-based application back-ends for processing [1]. But the problem arises while storing and processing data in secure manner. There are several security and trust issues associated with the IoT data. In order to rectify these above problems, blockchain plays an important role because of the underlying properties of blockchain in section 1.2.1. Because of the power of these properties of blockchain our system enables peers in a decentralised, trust-less, peer-to-peer network to interact with each other without the need for a trusted intermediary [3].

In this paper, we proposed a architecture which provides secure data processing and storage with the use of blockchain technology. This technology provides a decentralized, peer-to-peer, trust-less and secure environment to the whole processed and the stored data. Blockchain will store the data in the form of hashes which are being generated by the various cryptographic algorithms to secure the data. The whole data will be processed in the form of transactions which will produce a unique transaction hash for all types of different types of transactions. This system will also provide the decentralised environment to all the peers present in the network which will remove the dependency of the system on the centralised systems/servers. It also automates the process flow with the help of the mining process which is happening as a background process for all types of transactions to verify the transactions by running a consensus algorithm to check whether a transaction is liable to enter in the blockchain or not.

Section II will give the insight on the works which has already been tested and published.

Section III describes how Blockchain support Iot due to it's properties.

Section IV has the description of all the blockchain related terminologies to under the basic terms/concepts used in blockchain.

Section V describes the application and architecture of the distributed application for Smart Power Grid. It also explains all types of events and functionalities, event attributes and the overall architecture and the event flow involved in the application.

Section VI describes the whole process flow which is taking place in the application development. It also includes all the algorithms involved for all the events.

Section VII is showing the performance and the results for the considered ethereum blockchain.

Section VIII concludes the whole architecture along with analysis and factors effecting the application.

In the end, this paper cited all the important and noteworthy refrences which helped during the production of the underlying application.

II. Related Work

The Bitcoin transactions are recorded in a public ledger called the Blockchain. The Blockchain technology was introduced along with Bitcoin by Satoshi Nakamoto. IBM and Samsung have announced a collaboration to build decentralized IoT solutions by leveraging the Blockchain technology.

Trans Active Grid has developed a combination of software and hardware technologies that enable users to buy and sell solar energy from each other securely and automatically, using smart contracts and the Blockchain [10]. Filament

has built an open technology stack based on Blockchain technology, to enable devices to discover, communicate, and interact with each other in a fully autonomous and distributed manner [4].

Slock it has developed a smart lock technology called Slocks which enables real-world physical objects to be controlled by the Blockchain [9]. The owners of a Slock who wants to rent their real-world physical objects (such as houses, cars or bikes) set a deposit amount and a price for using the objects. Users can find the Slocks using the mobile app and then make a payment in Ethers to rent the objects. After the transactions are validated on the Ethereum Blockchain network, the users get permission to open or close the Slocks with their smartphone. A smart contract is automatically enforced between the owner and the user. After the object is returned, the deposit minus the cost of the rental is returned to the user.

III. Blockchain supporting IoT properties

- Integrity of ledger (Cryptographic hash function)
  A cryptographic hash function is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value', 'message digest', 'digital fingerprint', 'digest' or 'checksum'.[5]
- Authenticity of transactions (Elliptic Curve Digital Signature Algorithm)
  Elliptic Curve Digital Signature Algorithm or ECDSA is a cryptographic algorithm used by Bitcoin to ensure that funds can only be spent by their rightful owners.
  A few concepts related to ECDSA:
  1). private key, 2). Public key and 3). Signature [20]
- Privacy of transactions (Pseudonymity through crypto tools)
  A key aspect of privacy in blockchains lies in the use of private and public keys. Blockchain systems use asymmetric cryptography to secure transactions between users. [21]
- Identity of participants (Cryptographic signatures)
  A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender(authentication), and that the message was not altered in transit (integrity). [7]
- Auditability and Transparency (Cryptographic hash chain)
  A hash chain is the successive application of a cryptographic hash function to a piece of data. In computer security, a hash chain is a method to produce many one-time keys from a single key or password. For non-repudiation a hash function can be applied successively to additional pieces of data in order to record the chronology of data's existence. [8]

IV. Terminology

A. BlockChain

Blockchain is a distributed data structure comprising a chain of blocks. Blockchain acts as a distributed database or a global ledger which maintains records of all transactions on a Blockchain network. The transactions are time stamped and bundled into blocks where each block is identified by its cryptographic hash. The blocks form a linear sequence where each block references the hash of the previous block, forming a chain of blocks called the Blockchain. A Blockchain is maintained by a network of nodes and every node executes and records the same transactions. The Blockchain is replicated among the nodes in the Blockchain network. Any node in the network can read the transactions. Figure 2(a) shows the structure of a Blockchain. [3]

B. Smart Contracts

A smart contract is a piece of code that resides on a Blockchain and is identified by a unique address. A smart contract includes a set of executable functions and state variables. The functions are executed when transactions are made to these functions. The transactions include input parameters which are required by the functions in the contract. Upon the execution of a function, the state variables in the contract change depending on the logic implemented in the function. Contracts can be written in various high-level languages (such as Solidity or Python) [11]. Language-specific compilers for smart contracts (such as Solidity or Serpent) are used to compile the contracts into byte code. Once compiled the contracts are uploaded to the Blockchain network which assigns unique addresses to the contracts. Any user on the Blockchain network can trigger the functions in the contract by sending transactions to the contract. The contract code is executed on each node participating in the network as part of the verification of new blocks. Figure 2(b) shows the structure of a smart contract. [3]

C. Ethereum

Ethereum is an open and programmable Blockchain platform. Anyone can sign up for the platform and create an Ethereum account. Users can create and deploy smart contracts to the Ethereum platform and build decentralized applications. The platform is not owned or controlled by a single entity and is powered by the peers who run the Ethereum nodes. [3]

D. Ethereum Virtual Machine

Ethereum Virtual Machine (EVM) is the runtime environment for smart contracts in Ethereum. The nodes in the Ethereum network run the EVM. The EVM runs as a sandbox and provides an isolated execution environment. All the nodes in the Blockchain network perform the same computations thus providing redundancy in the execution of smart contracts. While this massive amount of redundancy is not an efficient

approach for execution, but it is required to maintain consensus in the network where there is no centralized authority or a trusted third-party. [3]

E. Accounts

Ethereum has two types of accountsExternally Owned Accounts (EOAs) and Contract Accounts. EOAs are the accounts which are owned and controlled by the users. Each EOA has an Ether balance associated with it. These accounts can send transactions to other EOAs or contract accounts. The contract accounts are controlled by the associated contract code which is stored with the account. The contract code execution is triggered by transactions sent by EOAs or messages sent by other contracts. [3]

F. Ether

Ether is the currency which is used in the Ethereum Blockchain network. The miners in the Ethereum network receive mining rewards in the form of Ethers. The base unit of Ether is called Wei (where 1 Ether = 10 18 Wei). [3]

G. Gas

Gas is the name of the crypto fuel which is consumed for performing the operations on a Blockchain network. All the transactions on the network are charged a certain amount of gas. While sending a transaction, the sender sets a gas price which represents the fee the sender is willing to pay for gas. The senders of the transactions are charged a gas fee, which is paid to the miners and the balance is refunded to the sender. The gas fee paid is proportional to the amount of work that is needed to execute the transaction, in terms of the number of atomic instructions. [3]

H. Blocks

The transactions in a Blockchain network are bundled into blocks and executed on all the participating nodes. A block contains a transaction list, the most recent state, a block number and a difficulty value. If there are conflicting transactions on the network (for example, transactions that do double spending), only one of them is selected to become a part of the block. The blocks are added to the Blockchain at regular intervals. [3]

I. Transactions

Transactions are the messages which are sent by Externally Owned Accounts (EOAs) to other EOAs or contract accounts. Each transaction includes the address of the recipient, transaction data payload and a transaction value. When a transaction is sent to an EOA, the transaction value is transferred to the recipient. When a transaction is sent to a contract account, the transaction data payload is used to provide input to the contract function to be executed. Transactions aresigned by the sender's private key. Transactions are selected and included in the blocks in the mining process. The state of the network is changed only by the transactions which are selected for inclusion in the blocks. The transactions on a Blockchain network can be read by all the participant nodes in the network. [3]

J. Mining

The transactions on a Blockchain network are verified in a process called mining. The participating nodes in the network are given incentives in the form of Ethers for performing the mining operations. Miners compete to do a complex mathematical computation and the node that wins, earns a reward in Ethers. Miners produce blocks which are verified by other miners for validity. A valid block is one which contains proof of work (PoW) of a given difficulty. In Ethereum, a proof-of-work algorithm called Ethash is used. The PoW algorithm finds an nounce input to the algorithm so that the result is below a certain difficulty threshold. The time for finding a new block can be controlled by manipulating the difficulty. A successful PoW miner is one whose block is selected to be next on the Blockchain. Once a winning block is selected all other nodes update to that new block. [3]

K. Dapp

A Decentralized Application (or Dapp) is an application that uses smart contracts. Dapps provide a user-friendly interface to smart contracts. A crypto currency application is an example of a Dapp that runs on a Blockchain network. [3]

L. Key Infrastrusture

Each Externally Owned Account (EOA) has a public-private key pair associated with it. The account address is derived from the public key. When a new EOA is created, a JSON key file is created which has the public and private keys associated with the account. The private key is encrypted with the password which is provided while creating the account. For sending transactions to other accounts, the private key and the account password are required. [3]

M. Messages

Contracts deployed on a Blockchain network can send messages to other contracts. A message contains the address of the sender, address of the recipient, value to transfer and a data field which contains the input data to the recipient contract. The difference between a transaction and a message is that a message is produced by a contract while a transaction is produced by an EOA. [3]

V. Distributed Application for Smart Power Grid with IoT

Smart Grid distributed application using blockchain is build to showcase the importance of blockchain in the security of the collected data and also for the processing of that data. As we are using blockchain for all the data which will be processed as transactions between machine-to-machine, peer-to-machine and peer-to-peer. Blockchain will act as a tamperproof and immutable storage for the data of all the transactions among several peers inside the system. The data present inside the network will be publicly accessible which is hashed and encrypted using various cryptographic techniques like public-private key, digital signature, etc. All the transactions are replicated over all the nodes in the network which will provide

a heavy resistance to modify, update or delete the data over the blockchain. There will not be any requirement of third party indermidiary as all the transactions will be verified using the process of mining(section IV(J)). It also prevents the peers from modifying, updating and deleting the transaction because of the immutable nature of the blockchain. This property will help to build trust among the peers. Every transaction is associated with a time-stamp which will help the peers to track the transactions and the miners to verify the transaction.

A. Events and Functionalities

This Dapp mainly consists of 4 important types of events for the transactions inside a smart grid for the distribution of supply among the peers.

Storage Event - These events cover all the storage done by the producer inside the grid. These events will occur whenever storage type of event will happen inside the system. These storage can be sensed by the various types of sensors by detecting the capacity of the grid at various timestamps. As soon as storage event will occur, a alert and storage will be generated on the both side of the application, one is purchaser side and other is the generator/producer side. Ref. Algorithm 1

Purchase Event - These events covers all the purchasing done by the buyer after the creation of the storage event. This event can only occur when a storage event has already been occurred. These event includes all the details about the purchasing transaction done by the customer of the supply. These can be easily captured by a sensor for all the supply request appeared after storage. Ref. Algorithm 2

Transfer Event - These events covers all the transfer of supply from the power grid to the customer after the request of supply from customer. An alert will be be produced as soon as we see a reduction from storage and an acknowledgement from the customer for this particular transfer. There will always be cost associated with each transfer which directly depends on the rate of the power supply and the amount of supply requested by the customer. Ref. Algorithm 3

Bill Creation Event - This events occurs when all the above three events has already been occurred. This event will have all the data captured by a sensor during storage, purchase and transfer event. All these inputs from sensors will make a file. Then a Bill creation event will occur in which the bill will be captured as a file. Then a request will generate to store that file in the inter-planetary file system(IPFS). As soon as this bill gets stored in IPFS, it will generate a unique document hash. Then a event will be generated to store this unique document hash in the blockchain under the name of the purchaser. Ref. Algorithm 4

B. Event Attributes Table

Storage	Purchase	Transfer
Grid Capacity	Purchase Quantity	Device Name
Available storage	Purchase Date	Transfer Amount
Grid Location	Associated Cost	Start Time
Rate		End Time

C. Architecture

a) System Architecture: "Fig. 1".

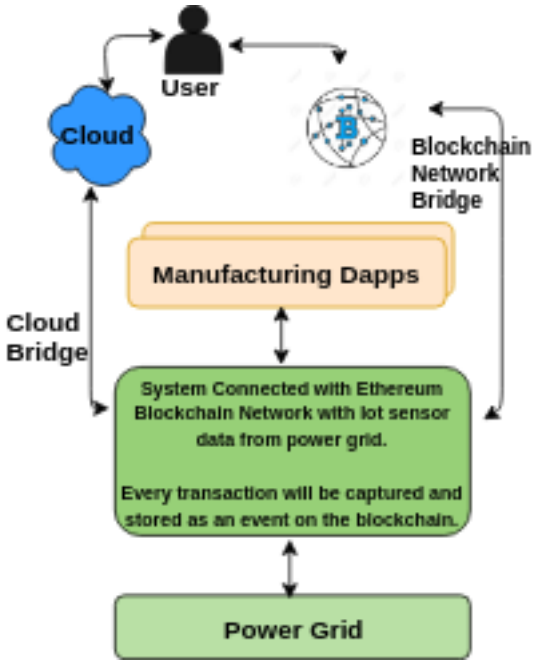

Fig. 1. Overall Architecture.

b) Event Flow Diagram: "Fig. 2".

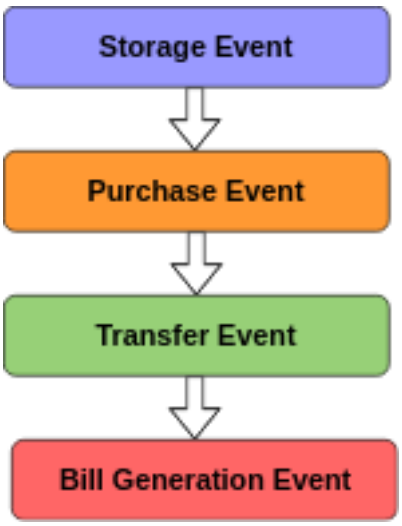

Fig. 2. Event Flow.

c) Bill Event Diagram: "Fig. 3".

VI. PROCESS FLOW

Different types of processes will be involved which will play a huge role in the enhancement over existing cloud based manufacturing models using blockchain technology by enabling consumer-to-machine and machine-to-machine transactions without a trusted intermediary, by automating machine maintenance and diagnostics tasks, by providing a

Fig. 3. Bill Event

Result: Write here the result
String gridCapacity, availableStorage, gridLocation, rate;
if *((gridCapacity) & (availableStorage) & (gridLocation) & (rate) are valid)* **then**
  sendRequest(gridCapacity, availableStorage, gridLocation, rate);
  publishToBlockChainRequest(gridCapacity, vailableStorage, gridLocation, rate) =>txnHash, timestamp;
  mining(txnHash, timestamp)
  if *(mined properly)* **then**
    publish the data to the blockchain;
    return blockNumber;
  else
    return "Error message - Could not mine";
  end
else
  return Input Error;;
end

Algorithm 1: Storage Event Algorithm

Result: Write here the result
String purchaseQuantity;
if *((purchaseQuantity is valid) & (purchaseQuantity <= availableStorage))* **then**
  associatedCost = rate x purchaseQuantity;
  sendRequest(purchaseQuantity, associatedCost);
  publishToBlockChainRequest(purchaseQuantity, associatedCost) =>txnHash, timestamp;
  mining(txnHash, timestamp)
  if *(mined properly)* **then**
    publish the data to the blockchain;
    return blockNumber;
  else
    return "Error message - Could not mine";
  end
else
  return Input Error;;
end

Algorithm 2: Purchase Event Algorithm

Result: Write here the result
String deviceName, transferAmount, startTime, endTime;
if *((deviceName) & (transferAmount) & (startTime) & (endTime) are valid)* **then**
  totalCost = associatedCost;;
  sendRequest(deviceName, transferAmount, startTime, endTime, totalCost);
  publishToBlockChainRequest(deviceName, transferAmount, startTime, endTime, totalCost) =>txnHash, timestamp;
  mining(txnHash, timestamp)
  if *(mined properly)* **then**
    publish the data to the blockchain;
    return blockNumber;
  else
    return "Error message - Could not mine";
  end
else
  return Input Error;;
end

Algorithm 3: Transfer Event Algorithm

Result: Write here the result
file selectedFile;
if *(selectedFile is not currupt & empty)* **then**
  sendBillToIPFS(selectedFile) =>ipfsHash;
  publishipfsHashToBlockChain(ipfsHash) =>txnHash, timestamp;
  mining(txnHash, timestamp)
  if *(mined properly)* **then**
    publish the ipfsHash to the blockchain;
    return blockNumber;
  else
    return "Error message - Could not mine";
  end
else
  return Input Error;;
end

Algorithm 4: Bill Event Algorithm

distributed, secure and shared ledger of all transactions, assets and inventory records, all through the existence of a decentralized, trustless, peer-to-peer blockchain network. The key enabler component for the industrial machines in the proposed platform is the IoT device. The IoT device enables existing machines to communicate with the Blockchain network. The IoT device is a plug and play solution that allows machines to exchange data on their operations, send transactions to the associated smart contracts and receive transactions from the peers on the Blockchain network.

Storage event will perform a machine-to-machine type of transaction in which IoT device will sense the capacity of the added storage and will pass the information to the blockchain network through smart contract in the form of a blockchain event. As soon as the storage event gets added

into the blockchain after the validation of the transaction in the blockchain network, it will reflect inside the whole blockchain network. After the addition of storage event, purchase event will be of the consumer-to-machine type of transaction in which a event will be fired from the consumer end as soon as the IoT sensor sense the requirement on the consumer end to purchase the amount of power supply. An event will be generated to be stored into the blockchain through the underlying smart contract. As soon as this purchase event occurs, an alert will be generated which will be sensed by the IoT sensor and a machine-to-machine transaction will be generated in the form of transfer event which will send the requested amount of supply, IoT sensor will be activated throughout the supply period to sense any fault or the quantity of supply transferred to the user during the transfer period. Based on the supplied amount of quantity sensed by the IoT device, a bill event will get generated through the already written smart contract and and the cycle will get complete.

Underlying system will also provide the functionality of storing the document of the bill in the inter planetary file system which provides an unique document hash which can be stored in blockchain to give the ownership of the data attached with a bill to the user itself by removing the need of third party intermediary.

VII. Results

A. Performance Table

Type of Transaction	Minimum	Maximum
push/storage	3x60x24=4320	4x60x24=5760
get/subscribe	6x60x24=8640	10x60x24=14400

B. Performance Analysis

From the analysis of the application we got the above results given in the performance table for both type of transactions in ethereum. As our application has 4 types of push transactions. As soon as the number of transactions happening are within limits of the results shown, the system will perform in fluent manner. As we are also conidering the IoT sensors attached with the application which are supporting machine-to-machine types of transcations. for example, detection of faults during power transmission. For all such type of events we had to consider the constraints associated with the scalability of the blockchain. For these types of situations we can consider either other types of blockchain like private blockchain, MultiChainDB which provides a faster rate than the ethereum transaction rate. Also, Vitalik Buterin, the creator of Ethereum, has explained in a recent OmiseGO AMA session that with second-layer solutions such as Sharding and Plasma, the Ethereum network will eventually be able to process 1 million transactions per second and potentially more than 100 million transactions per second which will help in the increase of performance of the application.[23] Other than the performance, all other features of blockchain like robustness, immutability of ledger provides the highly secured environment to the whole critical vulnerable data involved in the application.

VIII. Conclusion

Underlying platform enables users with services where the machines have their own Blockchain accounts and the users are able to provision and transact with the machines directly to avail the services [1]. This platform is built on the Ethereum platform with the smart contracts for various events written in Solidity.

The benefits of using Blockchain which make it suitable for Industrial Internet of Things and secure Smart Power Grid are as follows:

Decentralized and Trustless : Blockchain is a public ledger of all transactions on the network which is maintained by different decentralized nodes. Blockchain technology enables a decentralized and trustless peer-to-peer network where the peers do not have to need a trusted intermediary for interacting with each other. Since a Blockchain network is not controlled by a central authority and all the transactions are verified and validated by a consensus among the peers, the peers do not need to trust each other.

Resilient : Blockchain network is resilient to failures, as it is a decentralized peer-to-peer network with no single point of failure. The Blockchain itself is an immutable and durable ledger and the transactions once recorded on the Blockchain after a consensus among the peers cannot be altered or deleted.

Secure and Auditable : All the transactions in a Blockchain network are secured by strong cryptography. Furthermore, the transparent nature of the public ledger maintained by a Blockchain network makes it secure and auditable as everyone on the network knows about all the transactions and the transactions cannot be disputed.

Autonomous : Blockchain can enable IoT devices to communicate with each other and do transactions autonomously as each device has its own Blockchain account and there is no need for a trusted third-party.

References

[1] Bahga, A. and Madisetti, V. (2014) Internet of Things: A Hands-On Approach. VPT/Create Space Inc., Atlanta.

[2] *Kamanashis Biswas, School of Information and Communication Technology, Griffith University, Gold Coast, Australia* and *Vallipuram Muthukkumarasamy Institute for Integrated and Intelligent Systems, Griffith University, Gold Coast, Australia, Securing Smart Cities Using Blockchain Technology*

[3] *Arshdeep Bahga, Vijay K. Madisetti* Georgia Institute of Technology, Atlanta, GA, USA, Blockchain Platform for Industrial Internet of Things

[4] Filament (2016) Foundations for the Next Economic Revolution Distributed Exchange and the Internet of Things. *https://filament.com/assets/downloads/Filament%20Foundations.pdf*

[5] https://simple.wikipedia.org/wiki/Cryptographic_hash_function.

[6] *https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm*

[7] https://en.wikipedia.org/wiki/Digital_signature.

[8] https://en.wikipedia.org/wiki/Hash_chain

[9] Slock.it. https://slock.it

[10] TransactiveGrid. http://transactivegrid.net

[11] Bahga, A. and Madisetti, V. (2014) Internet of Things: A Hands-On Approach. VPT/Create Space Inc., Atlanta.

[12] Wu, D., Rosen, D.W., Wang, L. and Schaefer, D. (2015) Cloud-Based Design and Manu- facturing: A New Paradigm in Digital Manufacturing and Design Innovation. Comput- er - Aided Design , 59, 1-14.

[13] Xu, X. (2012) From Cloud Computing to Cloud Manufacturing. Robotics and Computer - Integrated Manufacturing , 28, 75-86. *http://dx.doi.org/10.1016/j.rcim.2011.07.002*
[14] Colombo, A., Bangemann, Th., Karnouskos, S., Delsing, J., Stluka, P., Harrison, R., Jammes, F. and Lastra, J.L. (2014) Industrial Cloud-Based Cyber-Physical Systems. The IMC-AESOP Approach, Springer, Switzerland. *http://dx.doi.org/10.1007/978-3-319-05624-1*
[15] Solidity Documentation. *https://solidity.readthedocs.io*
[16] Ethereum Homestead Documentation. *http://www.ethdocs.org/en/latest/*
[17] Wu, D., Thames, J.L., Rosen, D.W. and Schaefer, D. (2013) Enhancing the Product Realization Process with Cloud-Based Design and Manufacturing Systems. Journal of Computing and Information Science in Engineering , 13, 1-14. *http://dx.doi.org/10.1115/1.4025257*
[18] Ethereum Go Client. *https://github.com/ethereum/go-ethereum*
[19] A Next-Generation Smart Contract and Decentralized Application Platform (2016) *https://github.com/ethereum/wiki/wiki/White-Paper*
[20] *https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm*
[21] *https://en.wikipedia.org/wiki/Privacy_and_blockchain*
[22] *https://en.wikipedia.org/wiki/InterPlanetary_File_System*
[23] *https://www.ccn.com/vitalik-buterin-ethereum-will-eventually-achieve-1-million-transactions-per-second*