Smart Contracts Integration between Blockchain and Internet of Things: Opportunities and Challenges

Azam Rashid
Computer Department.
Board of Intermediate and Secondary Education, Lahore.
Lahore, Pakistan.
azamrashid@gmail.com

Muhammad Jawaid Siddique
Faculty of Information Technology.
Pakistan Institute of Management.
Lahore, Pakistan.
jawaid@imforhelp.org

***Abstract*—A Smart Contract is self-executable and self-enforceable program code that runs on the top of blockchain to manage complex business logic. It eliminates the need of extrinsic enforcement of legal agreements. Furthermore, it enforces the terms and conditions of an agreement that lies between untrustworthy parties in which the trusted third parties cannot interfere. The cryptography logic used in smart contract enables the blockchain network to provide trust and authority to all parties in transaction. Network decentralization, data immutability and transparency, resiliency and security make blockchain technology more versatile. Recently, it has become a potential quality and capability of IoT to connect uncountable electronic objects or devices at the same time. The most prominent feature of blockchain-based IoT applications is the integration of smart contracts between blockchain and IoT.**

A brief comparison has been given in the paper that how the smart contracts react on multiple blockchain platforms with respect to scalability, system complexity and consensus protocol factors. Furthermore, the context of Smart contract integration between blockchain and IoT with highlighting the integration opportunities and challenges along with future research directions. Therefore, we have concluded in the current paper that amalgamation of Blockchain with IoT through Smart Contract can provide a strong framework for distributed application and the newly introduced business communities.

***Index Terms*—Smart Contracts, Internet of Things (IoT), Blockchain, Decentralize Applications (DApps).**

I. Introduction

Smart Contract [1] is spontaneous which we can call a computer program or protocol that is self-executing, self-enforceable and self-verifiable script that resides on the top of blockchain distributed ledger to handle complex transactions between untrusted parties in decentralized network environment and allow automation in multi-steps mechanism. It eliminates the extrinsic enforcement of legal agreements and promotes self-enforcement criteria for the enforcement of terms and conditions of an agreement without involving third party intermediaries. The massive use of cryptography logic in the form of smart contracts, blockchain network brings interactions in the network, interest in its use, and authoritativeness behind all transactions.

Before the innovation of Blockchain technology [2], applications were run through trusted intermediaries, now operates decentralized network platforms without the need of centralized authority. Blockchain provides the interest to stakeholders like finance, healthcare, real-estate, utilities, government and private industrial sector etc.

IoT paradigm has extended the idea of the internet connectivity, where billions of devices connected simultaneously with a centralized client/server model. Blockchain technology decentralized computation architecture, immutability of data, transactional security and privacy has resolved many issues related to IoT. An authentic overview of integrating blockchain with the IoT through smart contracts has been put forth in the present study. During this study, from the process of integration, we examined the opportunities and encountered the challenges related to the implementation.

We have categorized this paper into multiple sections. In section II we highlighted different techniques, architectures and systems used in blockchain based IoT applications. In section III & IV, we examined the real definition of blockchain and discussed how its network operates. Similarly, the discussion about the historical background of blockchain is done. Consensus and type of blockchain are also discussed in these sections respectively. In section V we examined what is a smart contract, historical background of smart contracts, how it works and reacts on multiple blockchain platforms. In section VI we discussed IoT and Blockchain based IoT applications. In section VII and VIII, we discussed the opportunities and challenges of smart contract integration between blockchain and IoT and in last sections IX & X we briefly focused on future research directions and concluded our paper.

II. Related Work

Smart Contract plays a vital role for the integration of blockchain with IoT devices. Investigation about it has been done at very low rate in [3,5,6,7,8,9,10] papers. For example, IBM proposed the blockchain-based project named (ADEPT) which stands for Autonomous Decentralized Peer-to-Peer

Telemetry [3] to the IoT, in order to boost the blockchain network and to attain greater robustness, scalability, and security, along with the privacy by its design. As for the ADEPT project, there are a number of approaches which have been trying hard to build some design for merging all different blockchain based applications through smart contracts.

A. Slock.it [5] proposed the system for the enforcement of blockchain and IoT by using the Ethereum Platform [4]. It works to indicate the real-world objects and IoT devices that blockchain technology can control easily. Ethereum expands upon the blockchain idea with the concept of self-enforcing smart contracts. When someone wants to get a house on rental basis in Slock, he joins the Slock blockchain network. In Slock system, the property owner can fix a rent price and a deposit amount of his precious property, and the fix amount is deposited by client through a suitable transaction in blockchain. Further, the system authorizes the client to close and open the smart locks by the help his/her smart phone. Hence, the system provides the opportunity to the tenant to deal with the owner without interference of the intermediaries.

B. Gupta et al. [6] have proffered a technique to elaborate the blockchain that enabled to make a secure e-healthcare records exchange possible for the real owners of the health consumers. They have suggested the model that only stores the metaphor data about medical and health events on blockchain through smart contracts. Metadata fields are used for smart contract script such as patient id, doctor id, etc. but the actual information regarding patient must be stored in a separate universal e-health cloud.

C. Ekblaw et al. [7] have proposed a prototype to store the medical research data and e-health records. Ethereum's smart contracts have used by them to generate the suitable representations of pre-existing medical records. Within the individual nodes, this data is recorded directly on the network named as "MedRec". The earlier mentioned solution can structure a huge amount of this data into the well-known three contracts such as Registrar contract, Patient-Provider Relationship contract and Summary contract.

D. Dorri et al. [8] suggested a private, secure, lightweight and decentralized architecture for the blockchain technology that is based upon IoT. It eliminates the overhead of Blockchain during the maintenance of security and privacy. The proposed three tiers architecture is in some specific order like a hierarchy, and consists of an overlay network and smart homes.

E. WAVE [9] (Wide Area Verified Exchange) is a decentralized approval granting system designed for IoT devices in blockchain network, without relying on a central authority that operates data globally. It is providing solid permissions and non-interactive delegation that can be efficiently verified. Smart contacts resist DDoS attacks, because it does not allow relying on the central trusted parties. Similarly, it does allow complex and rich policies to reveal, and used on public blockchain.

F. TransActiveGrid [10] the blockchain-based peer-to-peer energy transaction and control system. For mechanical selling and purchasing system, help is needed from the integration of blockchain with IoT because it is the only reasonable thing that allows peer-to-peer marketing. For sure, machines are able to sell and buy the energy in an automatic way there. It also works on the top of existing infrastructure in the form of smart contracts. It is auditable, immutable, peer-to-peer and secure blockchain network.

III. Blockchain and How it Works

In 1991, Stuart Haber & W. Scott Stornetta had presented his work on chain of blocks. In 1992, Bayer, Haber and Stornett had completed the integration of Merkle tree with blockchain. They thought it would help them to improve the efficiency of one block. Satoshi Nakamoto proposed the concept of distributed blockchain in 2008, that titled as "Bitcoin: A Peer-to-Peer Electronic Cash System" [11]. Innovation in blockchain came when he resolved some complex game theory conundrum, named as byzantine generals problem. In this he observed that any block of assets can easily be transferred to anybody else without any interruption created by some third party.

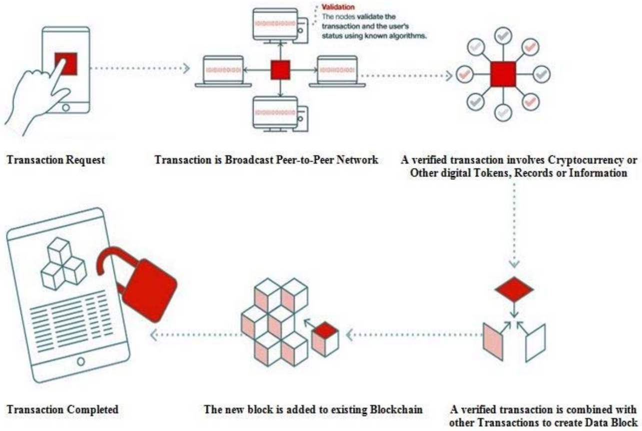
Validation
The nodes validate the transaction and the user's status using known algorithms.
Transaction Request
Transaction is Broadcast Peer-to-Peer Network
A verified transaction involves Cryptocurrency or Other digital Tokens, Records or Information
Transaction Completed
The new block is added to existing Blockchain
A verified transaction is combined with other Transactions to create Data Block

Fig. 1. How Blockchain Works

There are three generations for the evolution of blockchain technology networks that has been categorized as blockchain 1.0 to 3.0 [12]. In first generation, the innovation in the concept of distributed blockchain had released and implemented in the form of digital currency named as "Bitcoin" by Satoshi Nakamoto. In second generation, Ethereum platform had launched in 2013. It has improved blockchain architecture and it proposed a faster "Proof-of-Stake" protocol along with the idea of smart contracts and Ethereum self-governing application.

The first two generations of blockchain promises the high scalability, interoperability, sustainability, security, cost-effectiveness and governance in the blockchain networks but they can't meet the commitments completely. Therefore, the third generation of blockchain networks has launched in the form of many new cryptocurrencies. The idea of Directed Acyclic Graph (DAG) is implemented by IoT chain (ITC), IOTA, and Byteball in which transactions can be confirmed almost instantaneously. DAG allows for flexibility and scalability. IOTA has launched as a cryptocurrency platform optimized for the demanding Internet of things (IoT) ecosystem. Zilliqa is also 3rd generation high throughput blockchain platform that solves the scalability problem. It processes the 100-1000 tx/sec. EOS is also 3rd generation blockchains that has the ability to secure huge amount of data.

Blockchain is a ledger database which is peer-to-peer distributed. It is a decentralized system but is inter-connected with data blocks. The Header Hash is a connection pointer in blocks which is processed by cryptographic Hash function. In this way, the transaction is protected in each and every block and case with the connected blocks. Hence; there cannot be any change occurred until and unless a chain of Header Hash is validated.

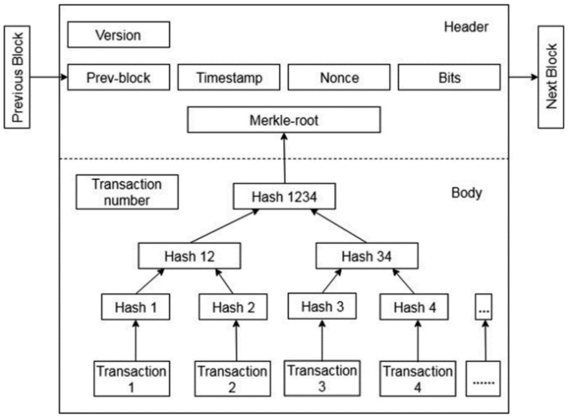

Fig. 2. Block Structure in Blockchain.

In bitcoin system, one block is created approximately in every ten minutes that save all the transactions. A body and a header are also contained by a block. This has been shown in "Fig .2", Metadata of the block is contained by the Header. It shows the version contains prev-block to Bits (Bits, Nonce, Timestamp, previous block, and Merkle-root etc.)

III-A. Types of Blockchain

A. Public / Permissionless Blockchain

Public blockchain networks are available for everyone that can join them to post transactions and also participate the consensus and mining process for new block of transaction in a blockchain. These blockchain networks are used the PoW and PoS protocols for consensus mechanism.

B. Private / Permissioned Blockchain

In Private Blockchain, the owner of the blockchain is an enterprise or an individual entity that has authority to delete/override commands on blockchain system. The private blockchain is also centralized but works as database and distributed ledger. Due to trusted nodes, there is no requirement for consensus protocol in private block chain system. Access to information, cheaper transactions and control on privacy level are easier things in the private ledgers.

C. Hybrid Blockchain

Hybrid Block is a Consortium ledger that contains both private and public blockchain ledgers to achieve more benefits in blockchain technology. In hybrid blockchain, the record of all the transactions is generated by the private network verified and stored on public network. This system is assumed to be partially centralized and partially decentralized. Hybrid network runs on a delegated proof-of-stake consensus (DPoS) between trusted master nodes with both IoT and smart contracts a top of the protocol.

IV. Consensus Protocols in Blockchain

Consensus means an agreement with the single version or aspect of the truth. This agreement is done by all the peers who are working on block chain. The concept of consensus is basically distributed computation or computing to search out such a value on which all the participants working. Consensus protocols [13] used in blockchain network are as follows.

A. Proof of Work (PoW)

PoW demands for the authentic proof. The proof in the sense, that enough resources have been spent in computational process before finding some specific value.

B. Proof of Stake (PoS)

This calculation takes a shot at the possibility that a hub or client has enough stake in the framework with the goal that any malevolent endeavor would exceed the advantages of playing out an assault on the framework.

C. Proof of Importance (PoI)

This thought is critical and not quite the same as Proof of Stake. Evidence of significance not just depends on how much stake a client has in the framework yet it likewise screens the utilization and development of tokens by the client to set up a level of trust and significance.

D. Delegated Proof of Stake (DPoS)

In DPoS, the stake holders in the system can elect leaders (witnesses) who will vote in their behalf. This makes it faster than the normal PoS.

E. Practical Byzantine Fault Tolerance (PBFT)

PBFT (Practical Byzantine Fault Tolerance) gets the state machine replication, because of which tolerance is provided against Byzantine nodes. Different conventions, including however are not constrained to PBFT, PAXOS, RAFT, and

Federated Byzantine Agreement (FBA), are additionally being utilized or have been proposed for use in a wide range of usage of disseminated frameworks and blockchains.

V. SMART CONTRACT

In the late 1990s, Nick Szabo theorized an article on smart contracts named formalizing and securing relationships on public networks [1] but their real benefits and potentials were attained and appreciated almost two decades later on, with the creation of bitcoin and subsequent development in blockchain technology.

Smart contracts are described by Szabo [1] as follows:
"A smart contract is an electronic transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs."

An enforceable and automatable agreement is called a smart contract. Automatable in the sense that some parts of it need human efforts and some parts of it do not, rather it is automatable by computer. Tamper-proof execution of computer code comes under the term "enforcement" [14].

V-A. HOW SMART CONTRACT WORKS

A smart contract is executable piece of code that runs on the blockchain to execute, expedite, and implement the terms of a contract. The implementation of the conditions for the agreement in an automatic way is assumed the main focus of a smart contract.

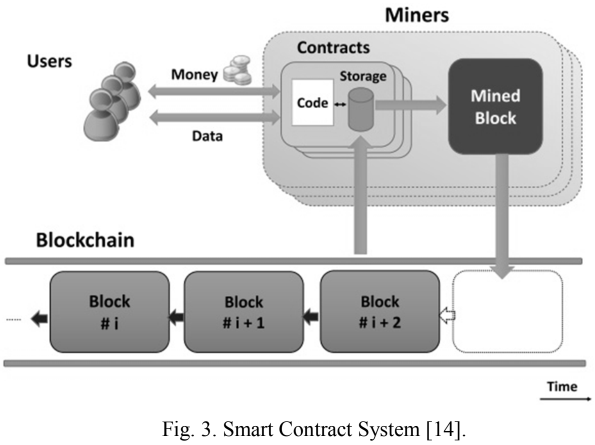

Fig. 3. Smart Contract System [14].

"Fig. 3", shows that how smart contract works in blockchain network. In literature, different explanations and interpretations of the term "smart contract" have been put forth by different people accordingly. In [14], all the debated definitions have been categorized in two types. First is SLC which stands for Smart Legal Contract and second is SCC which stands for Smart Contract Code. SCC means "a code that is verified, stored, and executed on a blockchain". A smart contract has the following four properties: 1) Self-executable. 2) Self-enforceable. 3) Strong Semantics. 4) Secure and unstoppable

V-B. BLOCKCHAIN-BASED SMART CONTRACT PLATFORMS

Lately, blockchain innovation has empowered another type of smart contracts with immutable storage of agreement terms, cryptographic approval, and coordinated transfers of significant worth. Smart contracts can be developed and deployed in different blockchain platforms (e.g., Ethereum, Bitcoin, Hyperledger Fabric, Steller, Waves, NXT etc). Different platforms provide specific features for developing smart contracts as follows.

A. ETHEREUM

Ethereum [4] is distributed public/permissionless blockchain-based platform for running smart contracts in distributed applications interact to one or more blockchain networks. Ethereum had proposed by Russian-Canadian programmer "Vitalik Buterin" in 2013 and went live in July 2015. It used ERC-20 token standard. Ethereum is a permission less blockchain associated with a cryptocurrency called "ether". Ethereum provides the opportunity for the creation of smart contracts in blockchain network and the changes or modification is performed through program.

The first language had been designed on ethereum platform for writing smart contract program code is solidity but now many smart contract platforms invented their own languages such as DAML, DSCL, RIDE, Go etc.

B. BITCOIN

Being a public blockchain, Bitcoin [11] is normally used to process the cryptocurrencies transactions. Bitcoin uses a IVY stack-based scripting language that processed from left to right. The ability of making a smart contract with rich rationale using bitcoin scripting language is exceptionally restricted. For a single transaction, multiple signatures are required in bitcoin to make the payments conceivable. On the other hand, complex logic to compose contracts seems impossible because scripting language of bitcoin has a number of limitations.

C. HYPERLEDGER FABRIC

The Linux Foundation along with the collaboration of IBM launched Hyperlegder project [15] in 2015. It is permissioned (Private) blockchain-based network. It is an open source project that has the expressed objective of supporting the improvement of blockchain-based distributed ledgers. Hyperledger Fabric is remarkable smart contract execution platform that has proven itself as real alternative of Ethereum Platform. The developers of Hyperledger fabric have created many JavaScript based tools that allows developers to create smart contract program code more logically and accurately.

D. NEM

NEM is Permissionless (Public) decentralized blockchain network. It was developed in object-oriented language Java and launched on March 2015. NEM does not depend upon the solidity language for the creation and execution of smart contract byte-code. NEM developer released new updates for smart contract programming named as Catapult or Mijin v.2 that is more secure for smart contract platform. NEM technology allows for combining multiple distributed ledgers in one blockchain.

E. STELLAR

Stellar [16] is the decentralized protocol used for sending and receiving money in pair of currencies. It had firstly launched in 2014 and updated by stellar development foundation. It is an encouraging universal payment platform. The implementation of smart contract in stellar platform is ostensibly less difficult and simplest than Ethereum. Stellar is not feasible for the development of more sophisticated SC decentralized application.

F. WAVES

WAVES is public, decentralized and open source blockchain platform. It was launched in June 2016. It expected to address a significant number of the current obstructions that hinder more standard blockchain usage, to be specific speed and scalability. Much like Ripple, Wave has positioned itself as a platform to encourage token operations, and excellent platform for ICOs. It takes some time to create your own tokens on the platform without having sufficient technical knowledge.

G. LISK

LISK [16] is a public decentralized blockchain platform that allows the smart contracts to utilize the turing complete with Node.js or JavaScript but the smart contracts are validated by programmers. It managed blockchain-based decentralized applications by deploying their own sidechain linked to the Lisk mainchain. It's the best approach for solving scalability problem has is facing by many cryptocurrency platforms.

H. NXT

NXT was released in November 2013 and idea proposed by bitcointalk.org. It's advanced public decentralized blockchain platform provides the environment to build the better functionality cryptocurrencies and also includes the built-in smart contract templates. NXT trusts the smart contracts made from these formats should cover most business applications;

be anything but difficult to code, and guaranteed safety in the system. It provides the full independency to create their own smart contract for financial systems, crowdfunding and cryptocurrencies DApps.

I. MONAX

Monax [16] is a private blockchain platform that enables clients to characterize particular approval strategies to get to the blockchains. Monax has characterized smart contracts as code representing unilateral promises to give deterministic calculation based on transactions which are sent to the blockchain content code. Monax smart contract designs are modular, repeatable and have autonomous scripting which can be used to build applications.

J. QTUM

Qtum is pubic bitcoin-ethereum hybrid functioning decentralized blockchain platform for smart contracts and value transfer protocol. It was launched in 2017. It used Proof of Stake (PoS) consensus algorithm. Qtum will have an account abstraction layer, fused in their smart contract outline, which deciphers the UTXO-based model to an account-based interface for the EVM. Qtum made DGP to have preferable governance over Bitcoin and Ethereum, where clashes inside the community prompted the launch of bitcoin cash and Ethereum classic.

VI. INTERNET OF THINGS (IOT)

IOT [17] is the centralized network of electronic devices, smart connected objects, embedded system in appliances etc. that are interconnected to share or exchange data from each other simultaneously. The rise of the Internet of Things (IoT) wipes out every model and predetermined idea of network architecture. Recently, the systems have been created by architects talented in conventions and steering hypothesis. So the engineering and development in the IoT devices will depend upon the exercises got from nature than customary organizing plans. The IoT devices system architectures and developers are investigating the reasons that why the design for the Internet of Things must fuse on basic level diverse engineering from the customary Internet.

A. Blockchain based IoT Applications

IoT implies the internet to which "things" (gadgets, sensors, actuators, and so forth.) are associated. The information from the physical world is accumulated by sensors, conveyed through the internet. The clients of IoT frameworks can examine the accumulated information to find patterns or examples, or change the status of actuators dependent on the information. IoT technology has been developing quickly these years. Gartner, Inc. predicted that by 2020, 20.8 billion IoT devices will be linked to the Internet [18].

TABLE I
COMPARISON BETWEEN BLOCKCHAIN-BASED SMART CONTRACT PLATFORMS

Platform	Blockchain	Smart Contract Language	Consensus Protocol	Cryptocurrency	System Complexity	Scalability
BitCoin	Public & Private	IVY for Bitcoin Language	PoW	BTC	Medium	Block size 3-7 Tx/Sec
Ethereum	Public & Private	Solidity	PoS	Ether (ETH)	High	Block size 5-20 Tx/Sec
HyperLedger Fabric	Private	Java, Node.js and Go	PBFT/SIEVE	None	High	Block size 100-3000 Tx/Sec
NEM	Public	Java and Node.js	PoI	XEM	Medium	Block size 1,000-10,000 Tx/Sec
Stellar	Public	Stellar SDK & Go	PBFT / FBA	Lumens (XLM)	High	Block size 1,000-1,500 Tx/Sec
Waves	Public	RIDE	LPoS	WAVES	Medium	Block size 100 Tx/Sec
Lisk	Public	Lisk JScript	DPoS	LSK	Medium	Block size 25Tx/Sec
NXT	Public	TC Script	PoS	NXT	Medium	Block size 5-20 Tx/Sec
Monax	Private	Monax SDK and Solidity	PoS	MultiAsset	High	-
Qtum	Public	QSCL and Solidity	PoS	QTUM	Medium	Block size 70-140Tx/Sec

Atonomi is one these organizations that has introduced a security protocol in blockchain-based IoT networks that root the identity and reputation of electronic devices) blockchain-based immutable ledger. Atonomi is also providing token-based economy for the enrollment of electronic devices.

VII. OPPORTUNITIES FOR SMART CONTRACT INTEGRATION BETWEEN BLOCKCHAIN AND IOT

A. Immutability

The replicated and immutable shared ledger is achieved by the blockchain technology. The purpose of it is to record the transactions safely. Verification from a number of network nodes is very necessary to save any changes in the distributed ledger. However, alteration and deletion of the already existing transactions is impossible here without the verification done by the majority of the nodes on the network. There are more benefits for reporting and recording data actively in the immutability of the block chain records. These are as follows, 1) Regulatory compliance is handling through 'smart code'. 2) Providing a clear financial trail for auditors. 3) Enabling tamper-proof distributed platforms in order to reduce error and fraud in data. 4) Transparency mechanism is improving during the recording of trail of transactions in permission less ledgers [19].

B. Smart Auditing

It refers to auditing of services and goods in an automatic way, using technology particularly computer methods. For example, smart sensors, smart contract and IDA (intelligent data analysis) are very fruitful and beneficial things in his regard. Smart contract is applied through blockchain technology that may allow self-execution and self-enforcement of mutual and personal different kind of agreements among individuals, businesses, or machines. It may help for reducing risks in transactions and minimize the costs at administrative level in different business industries [19].

C. Innovations for New Programmable Money / Cryptocurrencies

Smart contracts and blockchains are likely to adopt a possible form of programmable money. It may help in attaching the policies about spending money digitally and unrevealed other methods in contribution with the digital currency and distributed integrity. Smart contract in block chains can further introduce the innovative kinds of programmable money. Through smart contract in block chain, the financial institutions and investors could make policies to get the parcel of money transferred or spent. This would be self-executable and self-enforceable smart contract in blockchain. The expiry of the policy constraint for parcel of the money would be configured and monitored. For example, the payment ecosystem restricted the payment to a third-party or else be carried by implementing the policy.

D. Improving Resiliency and Security

Through blockchain, the security and resilience of the systems particularly storage of data could be increased because it has the potential for that. This is because blockchain technology has a distributed nature protection in the term failure of central point [24]. As it is not owned and controlled by a single body or entity, according to Mainelli, everybody may have their own transaction and data copy in the occasion of failure in system. Here all the members holding data do have their own identity systems which cannot be destroyed and remains consistent universally. And opportunity is possible only by this kind of security and resilience.

E. Innovations in Supply Chain Management

Regarding the application of the blockchain technology, very promising and suitable domains is supply chains. The self-execution system of smart contract in block chain allows integrating the exchange of information, helps in the improvement of the operational efficiencies across some vide and diverse industry. In addition, it minimizes the expense endorsement regarding administration. In the same way, blockchain technology improves the supply chain quality for marked products. Anyhow, there is a dire need of researches issues related to commercial confidentiality.

F. Saving the Cost and Time of Remittances

Decentralization feature of Blockchain technology and usage of smart contracts between transactions provides the capability for financial institutions to reduce the cost and time of remittances but significant challenges still remain in finding solutions to KYC (Know Your Customer) and achieving acceptance of those solutions by international law regulatory bodies.

G. Decentralization of Records

Smart contracts are the executable and enforceable code that includes in blockchain script that runs into peer-to-peer network of computers similar like DApps (Decentralized Applications). Actually, DApps are computer programs that are deployed on blockchain to perform more complex tasks than smart contracts. Therefore, in future role of DApps for IoT devices will support the decentralization of records and the verification process of transactions on different nodes of blockchain distributed ledger. In this way, the network provides the trust for majority of the participants have to reach an agreement to validate transactions without any single centralized authority.

H. Speed and Accuracy

Smart contracts are encoded on the top of every blockchain network and executed in the form of transactions across the network in partial time period; it will be processed at any time in distributed network.

I. Data Protection Regulation

The European Union brought in the General Data Protection Regulation (GDPR), to standardize and update the previous data protection and privacy regime, which dated back to the Data Protection Directive (DPD) of 1995.

GDPR and blockchains share the motivation of empowering individuals and reduce the asymmetry between them and the organizations that process their data and transactions. However, some of the technological advancements that make possible decentralization in blockchains require data processing and storage to be distributed among members of a community or outsourced to unknown individuals or organizations.

VIII. Challenges of Smart Contract for Blockchain with IOT

A. Scalability

Scalability advances the centralization of blockchain innovation which is throwing the shadow over the fate of digital currency. Because of the expansion of IoT gadgets, the quantity of blockchain based IoT systems upgrades and the rate of blockchain exchanges will increment with the progression of time so the factor of scalability limitations in IoT applications make these challenges much greater, however there are many proposed approaches that could be alleviated or avoided these limitations in IoT devices. It is realized that some present blockchain executions can just process a couple of exchanges for each second, so this could be a potential bottleneck for the IoT. The issue is serious regarding the integration of smart contracts between blockchain based IoT networks in large number of nodes.

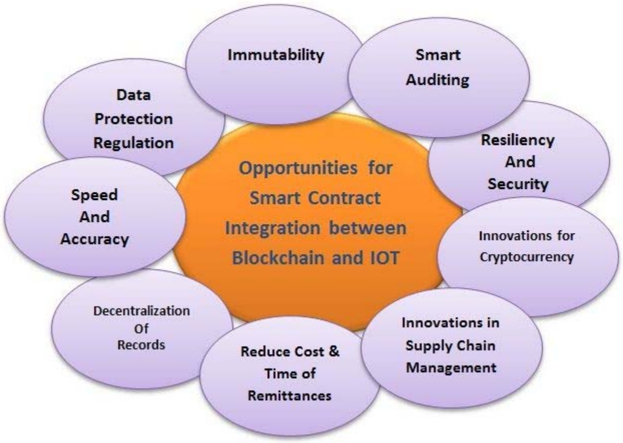
Opportunities for Smart Contract Integration between Blockchain and IOT
Immutability
Smart Auditing
Resiliency And Security
Innovations for Cryptocurrency
Innovations in Supply Chain Management
Reduce Cost & Time of Remittances
Decentralization Of Records
Speed And Accuracy
Data Protection Regulation

Fig. 4. Opportunities for Smart Contract Integration between Blockchain and IoT.

Scalability is a noteworthy roof for current blockchain executions, making it troublesome for the innovation to be connected at scale for applications like payments. For example, VISA forms 1,667 transactions each second. Bitcoin has a capacity of 5-7 transactions per second, and Ethereum supports up to 15 per second. Considerably more fundamentally, blockchains today require huge measures of power.

B. Legal Issues and its Compliance

There are number of lawful and functional issues that can emerge from the utilization of smart contracts in their present phase of development. Parties must provide the evidence for the offer and acceptance of terms and conditions of the agreement during smart contract transactions. The Electronic Signatures in Global and National Commerce Act ("ESIGN Act"), the Uniform Electronic Transactions Act ("UETA");

and equivalent statutes in several states provide grounds for enforcement of smart contracts once electronically signed.

Due to the immutability of blockchain technology, once smart contract added to the blockchain, it can't be altered. It is essential that legal counsel and its software coding counterparts establish procedures so there are no gaps or mistakes as between the two versions.

C. Data Security and Privacy

The IoT area is likewise influenced by a nation's laws or controls with respect to data security and privacy. The first cryptocurrency focused on anonymity and privacy is known as Dash. The cryptographic accountability mechanisms and randomized mixing fee is introduced by MixCoin [19] to increase security features. Numerous specialists see blockchain as a key innovation to give the genuinely necessary security changes in IoT. One of the fundamental difficulty in the joining of the IoT with blockchain is the unwavering quality of information created by IoT. Blockchain can insure the guarantee that the information in the chain is permanent and can recognize their changes, nevertheless when information arrives officially corrupted source in the blockchain.

D. Jurisdictional Issues

Enforceability of smart contracts in cross border transactions when different rules apply in the relevant jurisdictions, including choice of law provisions is a biggest challenge for present and future smart contracts. This issue is debatable globally.

E. Uniformity of Contracts at Blockchain Platforms

The front-end complexity associated with building out smart contracts will accelerate the drive to adopt uniform contracts in industries; to maximize interoperability and scalability just as with any other standard technologies. Growing convergence in standardizing commercial contracts such as non-disclosure agreements (NDAs), supply agreements, online terms and conditions. It is inevitable that smart contract and distributed ledger technologies will accelerate this convergence to uniform contract standards.

F. Irrevocability of Smart Contract Code

Once the smart contract is embedded into the distributed ledger it is irrevocable and cannot be changed or deleted and will be self-executing. This is the equivalent of a transactional doomsday machine. This can be corrected by the parties adopting and embedding a revised smart contract to supplement the existing block-chained one but only if both agree.

G. Consensus

Some legacy IoT devices have limited capacity for storing blockchain information and executing smart contracts. Therefore, it makes them unsuitable for taking part in consensus mechanisms, such as PoW, PoS etc. In spite of the fact that there are activities to consolidate blockchain full nodes into IoT devices, mining is as yet a major challenge in the IoT because of its constraints. IoT is mostly made out of resource constrained devices yet all-inclusive the IoT has a possibly enormous processing power.

H. Complexities of Business Ecosystem

The introduced base of business innovations, procedures, and methodology reflects numerous assumptions that would need to be returned to while considering how to incorporate smart contract capabilities into specific business processes.

I. Resource Constraints

There are very limited resources for communication, computation and storage at IoT platforms whereas excessive and large number of resources is demanded by the blockchain technologies. Class A low-power IoT platforms have fewer than 10 KB of data memory and under 100 KB of program memory, while a Blockchain node requires memory in the order of GBs. Proof-of-Work which is the basic requirement of the computational consensus algorithm does not come under the capacities of a low power and resource constrained devices of IoT.

J. Latency and Performance

Blockchain technology is supported the decentralized networks where transactions are committed in parallel order but smart contracts are executed sequentially. However, this would influence the execution of the blockchain systems adversely as the quantity of smart contracts that can be executed every second will be constrained. With the developing number of smart contracts later on, the blockchain frameworks won't have the capacity to scale. Vukolić [21] proposed the framework that smart contracts are executed in parallel order as long as they are independent. Thusly, the execution of blockchain systems would be enhanced as more contracts can be executed every second.

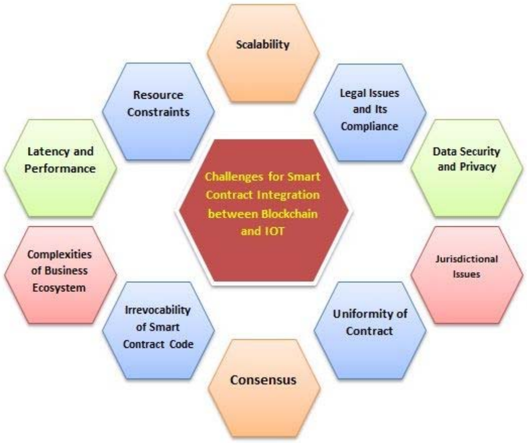
Scalability
Resource Constraints
Legal Issues and Its Compliance
Latency and Performance
Challenges for Smart Contract Integration between Blockchain and IOT
Data Security and Privacy
Complexities of Business Ecosystem
Jurisdictional Issues
Irrevocability of Smart Contract Code
Uniformity of Contract
Consensus

Fig. 5. Challenges for Smart Contract Integration between Blockchain and IoT.

IX. Future Research Directions

Recently the smart contracts are emerging key feature of every decentralized application and playing prominent role to solve complex business logics but many research directions are vacant in future some of them are as follows.

1) Resiliency against Hybrid Attacks
2) Optimal Platform for IOT objects
3) Security and Privacy Auditing Protocols
4) Trust and Reliance Management in Social Networks
5) Smart Energy-efficient Mining
6) Innovation of Hybrid Consensus Protocols

X. Conclusion

A smart contract is an automatable and enforceable agreement provides opportunity to integrate blockchain with IoT. Many previous research studies focus on the smart contract execution and performance in blockchain networks but in present development and innovations of decentralized applications, smart contract plays a vital role to solve complex business logics.

In this paper, we provide a brief comparison that highlights how Smart Contract react on multiple blockchain platforms with respect to scalability, system complexity, and consensus protocols. We have also highlighted the smart contracts integration between blockchain and IoT with emphasizing the opportunities and challenges. The discussion also focused on future research directions. We have concluded that the amalgamation of Blockchain with IoT through Smart Contract can provide strong frameworks for new business communities and distributed application (DApps).

However, as there are still many problems and limits in smart contract languages and frameworks. Many innovative Blockchain-IoT based applications are hard to implement currently. We plan to take a concrete in-depth study on smart contracts in the future.

References

[1] N. Szabo, "Formalizing and Securing Relationships on Public Networks," *First Monday,* vol. 2, 1997.

[2] Michal, J., Cohn, A., & Butcher, J. R. (2018). Blockchain technology. *The Journal*.

[3] Panikkar, S., Nair, S., Brody, P., & Pureswaran, V. ADEPT: An IoT Practitioner Perspective (2015).

[4] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*.

[5] Prisco, G. (2016). “Slock.it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy”. *Bitcoin Magazine. Nov-2015*

[6] N. Gupta, A. Jha, and P. Roy, “Adopting Blockchain Technology for Electronic Health Record Interoperability”, 2016

[7] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). “Medrec: Using blockchain for medical data access and permission management”. In *Open and Big Data (OBD), International Conference on* (pp. 25-30). IEEE.

[8] A. Dorri, S. S. Kanhere and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," CoRR, vol. abs/1608.05187, 2016.

[9] WAVE, Dec 29, 2017
http://www2.eecs.berkeley.edu/Pubs/TechRpts/2017/EECS-2017-234.html

[10] Grid, T. (2015). “Peer to Peer Energy Transaction and Control”. *New York: TransActive Grid*.

[11] Nakamoto, S. (2008). “Bitcoin: A peer-to-peer electronic cash system”.

[12] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). “A survey on the security of blockchain systems”. *Future Generation Computer Systems*.

[13] Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017, January). “Survey of consensus protocols on blockchain applications”. In *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on* (pp. 1-5). IEEE.

[14] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, “Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in International Conference on Financial Cryptography and Data Security, pp. 79-94, Springer, 2016.

[15] Cachin, C. (2016, July). “Architecture of the hyperledger blockchain fabric”. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers* (Vol. 310).

[16] Clack, C. D., Bakshi, V. A., & Braine, L. (2016). “Smart contract templates: foundations, design landscape and research directions”. *arXiv preprint arXiv:1608.00771.*

[17] The Internet of Things Industrie 4.0 Unleashed, https://doi.org/10.1007/978-3-662-54904-9

[18] M. Swan, *Blockchain: blueprint for a new economy*. Beijing: O’Reilly Media, Inc., 1st ed., 2015

[19] Deloitte. 2016. Blockchain: Enigma. Paradox. Opportunity. London: Deloitte LLP. As of 14 March 2017: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf

[20] Diana Asatryan, “4 Challenges to Blockchain Adoption from Fidelity CEO,” 2017. (Legality& Compliance).

[21] M. Vukolić, "Rethinking permissioned blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, 2017.