An Overview of Smart Contract and Use cases in Blockchain Technology

Bhabendu Kumar Mohanta
IIIT Bhubaneswar
Odisha,India 751003
C116004@iiit-bh.ac.in

Soumyashree S Panda
IIIT Bhubaneswar
Odisha,India 751003
C117011@iiit-bh.ac.in

Debasish Jena
IIIT Bhubaneswar
Odisha,India 751003
debasish@iiit-bh.ac.in

***Abstract*—In the last decade blockchain technology become mainstream research topic because of its decentralized, peer to peer transaction, distributed consensus, and anonymity properties. The blockchain technology overshadows regulatory problem and technical challenges. A smart contract is a set of programs which are self-verifying ,self-executing and tamper resistant. Smart contract with the integration of blockchain technology capable of doing a task in real time with low cost and provide a greater degree of security. This paper firstly, explains the various components and working principle of smart contract. Secondly, identify and analyse the various use cases of smart contract along with the advantage of using smart contract in blockchain application. Lastly, the paper concludes with challenges lie in implementing smart contract the future real-life scenario.**

***Index Terms*—Smart Contract,Blockchain,Event Driven,Distributed**

I. INTRODUCTION

In the year 2008,Satoshi Nakamoto explain peer to peer cash transaction without the centralized system [1].Till date 1639 different cryptocurrency available in the digital currency market. The growth of cryptocurrency is changing rapidly. Bitcoin being the first as well the mostly capture market share [2].Blockchain technology concept derived from initial Bitcoin transaction system. A blockchain is a digital ledger which store transaction publicly after verifies the transaction by nodes. The basic structure of the blockchain technology is shown in this figure [1]. Each transaction is validated by the nodes and transactions are secured by cryptography hash function. A transaction is link by their previous transaction hash value. Once transaction added to the blockchain no one can modify or alter it, but that transaction can be view openly which bring transparency to the system. Blockchain uses some of the proof of concept and proof of work as well as proof of stake concept to validate the transaction.

A smart contract is a computer program consists of a set of rules run on the blockchain [4].With the rise of blockchain technology in the last decade which shows it has many application areas. The integration of blockchain technology and smart contract give lots of flexibility to develop and design as well as implement some of the real world problems in less cost and time without involves of traditional third party based system.

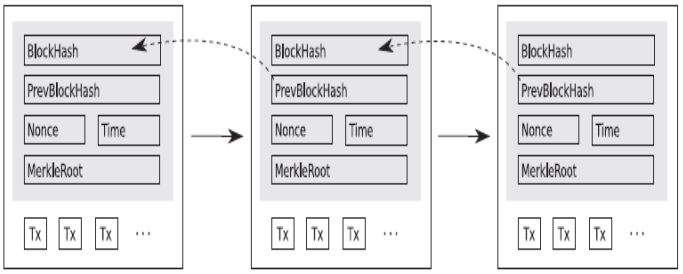

Fig. 1. A basic blockdiagram of Blockchain [3]

II. BACKGROUND STUDY AND RELATED WORK

A smart contract is a computer program having self-verifying, self-executing, tamper-resistant properties. The smart contract concept was proposed by Nick Szabo in 1994 [5]. It allows executing code without the third parties. A smart contract consists of the value, address, functions, and state [6]. It takes transaction as a input, executes the corresponding code and triggers the output events. Depending upon the function logic implementation states are changes. Since 2008 when blockchain technology come into existence through Bitcoin cryptocurrency. The importance of smart contract integration of blockchain technology become a focus area to develop because it give peer to peer transaction and database can be maintained publicly in a secure way in a trustful environment. Smart contracts are trackable and irreversible. All the transaction information are present in a smart contract and it executes automatically. The programming language Solidity is used to implement the smart contract in various blockchain platforms. Some characterizes of a smart contract are:

- Smart contract are machine readable code run on blockchain platform
- Smart contracts are part of one application program
- Smart contracts are event driven program
- Smart contracts are autonomous once created no need to monitor
- Smart contracts are distributed

Solidity is a high level language used to implement smart contracts.Developing blockchian platform of solidity are Ethereum,ErisDB,Zeppelin and Counterparty.

The work by Tatsuya Sato and Yosuke Himura in [8]design

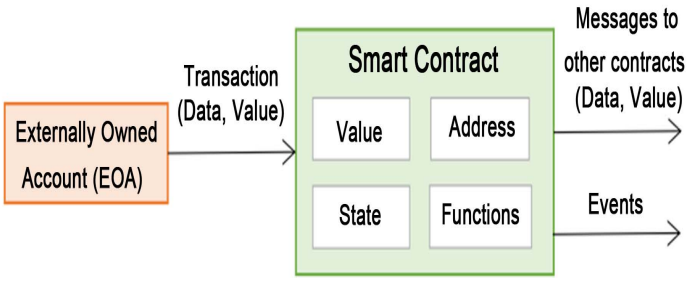

Fig. 2. A basic structure of Smart Contract [5]

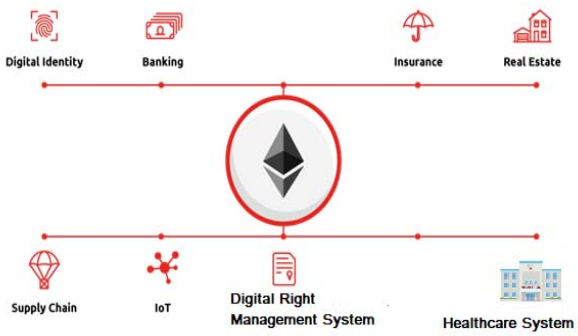

Fig. 3. Different use cases of smart contract

an operation based smart contract in a permission blockchain and execution of these services is considered as unified and synchronized way. In [9], Hiroki Watanabe et.al explains the smart contract in digital right management application and proposed consensus method. Ahmed Kosba et.al in [10] proposed a Hawk which provides a new way to write a smart contract in a cryptographically secure way. Joshua Ellul and Gordon J. Pace in [11] explain virtual machine AlkylVM to create a smart contract in Internet of Things application. The authors in [12] and [13] explain about the smart contracts execution process and some security issue.Similarly Authors in [14], [15] and [16] described the financial uses of smart contracts.The authors in [17] and [18] online detection of effective call back and scalable issue of smart contracts are explained. From the study of various article related to smart contracts ,we found most of these are have security issues and are implemented on financial domain.

Our contributions are:

- We analyze the smart contract properties and working principle.
- We Identify 7 different Important use case of smart contract enable blockchain application.
- We design and proposed the architecture of 7 different smart contract enable blockchain application.

III. WORKING PRINCIPLE OF SMART CONTRACT

The concept of smart concept was introduced by Nick Szabo in the year 1994, who defined it as a computerized transaction protocol that executes the term of a contract. According to him, the contractual clauses (collateral, bonding, delineation of property rights, etc.) should be encoded and embedded in the required hardware and software. This helps to minimize the requirement of any trusted third party for communication using smart contracts and at the same time makes the system secure against any malicious attack. In case of blockchain based smart contracts, contracts are nothing but scripts residing on the blockchain, which has the ability to execute them. One can trigger a transaction to a smart contract by using the unique addresses assigned to it by the blockchain technology. Let us take an example to better understand the working of smart contracts. Suppose you want to sale your house or rent your apartment to someone, then you can simply deploy a smart contract in an existing blockchain network. Information regarding the property can be stored in the blockchain and anyone belonging to that network can access those information but they cannot change it. In this way you can find a buyer for your property without the need of any third party. For a wide range of potential applications, blockchain-based smart contracts could offer a number of benefits:

- Speed and real-time updates.
- Accuracy.
- Lower execution risk.
- Fewer intermediaries.
- Lower cost.
- New business or operational models.

IV. USES CASES

A smart contract is pieces of a program executed in blockchain system that uses consensus protocol to run a sequence of events. A smart contract can be used different filed to eliminate the third party transaction as well as automate the system. In this work, we have identified 7 different use cases of smart contract and blockchain based application shown in Figure [3]. The various type of application area of blockchain technologies already discussed [19].

A. Supply Chain

The supply chain management system is consists of the different level of the transaction. Each level consists of some term and condition. Multiple systems are engaged in supply chain system. The various sector of supply chain systems like food processing system, transport sector, shipment system. In all these case digital ledger database makes a system more transparent, reliable and most importantly without third party involvement. Blockchain system makes supply chain sector more reliable and trustful, everything is present in open system in a distributed manner. If a smart contract is used along with the blockchain system like shown in Figure [4] then system become autonomous as well as secure .some smart conditions are needed to developed in the form of program and put into the blockchain system whenever any transaction occurs these smart contract will be executed.The verification and validation are done by the blockchain nodes. If conditions are agreed

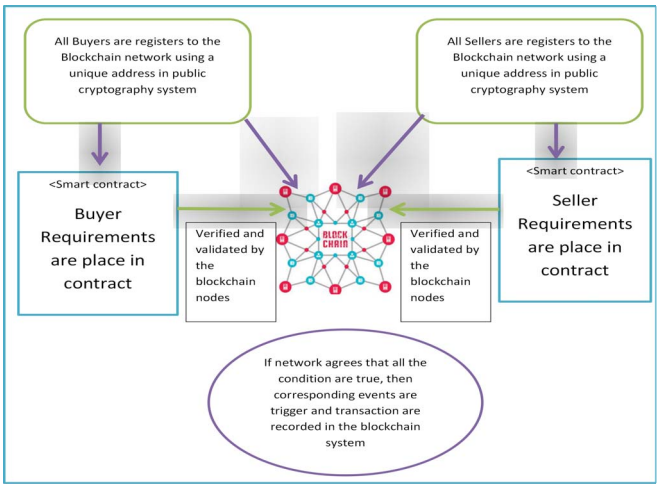

Fig. 4. A Smart contract based Supply chain system

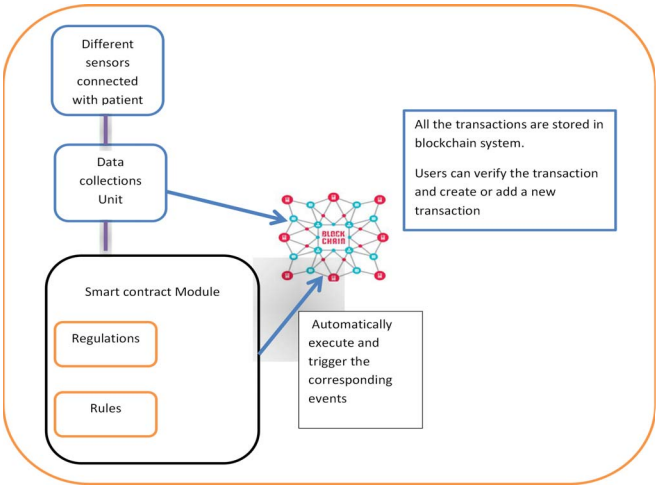

Fig. 5. A Smart contract based Healthcare system

by the network node then smart contract events are triggered. Finally, a transaction is recorded into the blockchain system. Making supply chains more transparent via smart contracts is helping to smooth out the movement of goods and restore trust in trade.

B. Internet of Things

The internet of Things is one of the promising areas of research. The IoT devices are resource constraint device having less memory power as well as less processing power. The number of IoT devices connected to the different application are already cross the number of total population of the world as mention by CISCO report. Blockchain technology-based smart home, smart city, smart transportation, smart monitoring of environment application are already some research being done. If smart contract concept integrates with the blockchain system then IoT become more autonomous.

C. Healthcare System

With the technology growing fasting human living standard also growing fastly. The using recently developed devices and supporting technology human can monitoring his or her health condition in sitting home. There are lots of devices are already developed to read different attributes in human body. These data can be collected using low-end device and processing locally to get quick information [20]. Blockchain technology helps to maintain the privacy of the patients and maintained data in digital ledger format. A smart contract can be used in that system to make the system more reliable and automated. Using Smart contract human can write some term and condition which could be applied once data are collected. Then it will execute these smart contracts and trigger corresponding events.the details is shown in Figure[5].

D. Digital Right Management

Digital right industry involves multiple parties to create an event. The percentage of payment and copyright is one of the issues arises. Using smart contract-based system guarantee that

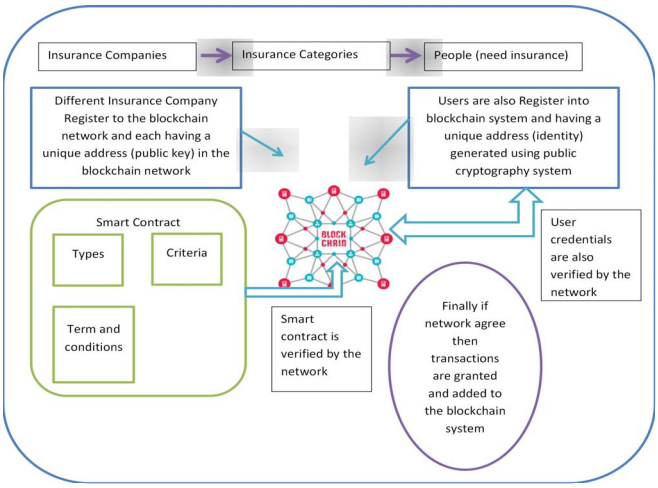

Fig. 6. A Smart contract based Insurance system

royalties go to actual recipients by using ownership right in blockchain system.

E. Insurance

Traditional insurance system takes very long time process a claim. There is much ambiguity arises between different stakeholder during processing. A smart contract-based system can streamline the process and using blockchain technology everything can be made transparent as well as system secure without third-party intervention. whenever smart contract execute successfully it trigger the corresponding events the details shown in Figure[6].

F. Financial System

Blockchain technology invented by Bitcoin cryptocurrency system, initially used for the financial system only. Traditional banking system involves a third party to transfer money from one account to another account. But in blockchain system, it is a peer to peer transaction and no central storage is used. Using smart contract and blockchain technology financial sector can

be beneficial.but still, a lot of research needs to be done in this sector to implement the smart contract.

G. Real Estate

Real estate system in the traditional way of involves lots of risks as well as time taking. It also passes through different stages of legal action are also need to lot of paper signings as well as manual verification of the documents. Blockchain technology and a smart contract can overcome the problem associated with real estate sector. A centralized system can allow buying as well as sell properties without the third party. The document is also verified and validated digitally. All the documents are also stored digital ledger distributed database where everyone can see.

V. CONCLUSION

Research point of view smart contract is still in early stages. Some of the issues need to be addressed like scalability, flexibility, privacy issue as the code is available publicly in the network it may not be suitable in some application In this paper, we have explained the integration of blockchain and smart contract can be more powerful. Blockchains provides secure, tamper-proof, distributed architecture platform for peer to peer transaction in a trustful environment. Smart contracts provide automatic, deterministic program unit to process various modules in a certain way and trigger the corresponding events. The smart contract taxonomy and architecture workflow are discussed clearly in this paper. Finally, 7 different application areas are considered as the use case of smart contract. Each of these application areas is discussed benefit of Smart contract. In future work, we would try to implement these application areas in term of blockchain Smart contract.

REFERENCES

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[2] https://coinmarketcap.com/all/views/all/

[3] Tschorsch, Florian, and Bjrn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." IEEE Communications Surveys Tutorials 18.3 (2016): 2084-2123.

[4] https://www.ambisafe.co/blog/smart-contracts-10-use-cases-business/

[5] Szabo, Nick. "Formalizing and securing relationships on public networks." First Monday 2.9 (1997).

[6] Bahga, Arshdeep, and Vijay K. Madisetti. "Blockchain platform for industrial Internet of Things." Journal of Software Engineering and Applications 9.10 (2016): 533.

[7] https://solidity.readthedocs.io/en/v0.4.24/

[8] Sato, Tatsuya, and Yosuke Himura. "Smart-Contract Based System Operations for Permissioned Blockchain." New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on. IEEE, 2018.

[9] Watanabe, Hiroki, et al. "Blockchain contract: Securing a blockchain applied to smart contracts." Consumer Electronics (ICCE), 2016 IEEE International Conference on. IEEE, 2016.

[10] Kosba, Ahmed, et al. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." Security and Privacy (SP), 2016 IEEE Symposium on. IEEE, 2016.

[11] Ellul, Joshua, and Gordon J. Pace. "AlkylVM: A Virtual Machine for Smart Contract Blockchain Connected Internet of Things." New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on. IEEE, 2018.

[12] Dickerson, T., Gazzillo, P., Herlihy, M., Koskinen, E. (2018). How to add concurrency to smart contracts. BULLETIN OF THE EUROPEAN ASSOCIATION FOR THEORETICAL COMPUTER SCIENCE, (124), 22-33.

[13] Cruz, J. P., Kaji, Y., Yanai, N. (2018). RBAC-SC: Role-Based Access Control Using Smart Contract. IEEE Access, 6, 12240-12251.

[14] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., Santamara, V. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?. Future Internet, 10(2), 20.

[15] Chen, T., Li, Z., Zhou, H., Chen, J., Luo, X., Li, X., Zhang, X. (2018, May). Towards saving money in using smart contracts. In Proceedings of the 40th International Conference on Software Engineering: New Ideas and Emerging Results (pp. 81-84). ACM.

[16] Nissen, B., Pschetz, L., Murray-Rust, D., Mehrpouya, H., Oosthuizen, S., Speed, C. (2018, April). GeoCoin: Supporting Ideation and Collaborative Design with Smart Contracts. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (p. 163). ACM.

[17] Grossman, S., Abraham, I., Golan-Gueta, G., Michalevsky, Y., Rinetzky, N., Sagiv, M., Zohar, Y. (2017). Online detection of effectively callback free objects with applications to smart contracts. Proceedings of the ACM on Programming Languages, 2(POPL), 48.

[18] Gao, Z., Xu, L., Chen, L., Shah, N., Lu, Y., Shi, W. (2017, December). Scalable blockchain based smart contract execution. In Parallel and Distributed Systems (ICPADS), 2017 IEEE 23rd International Conference on (pp. 352-359). IEEE.

[19] Tama, Bayu Adhi, et al. "A critical review of blockchain and its current applications." Electrical Engineering and Computer Science (ICECOS), 2017 International Conference on. IEEE, 2017.

[20] Jaiswal, Kavita, Srichandan Sobhanayak, Bhabendu Kumar Mohanta, and Debasish Jena. "IoT-cloud based framework for patient's data collection in smart healthcare system using raspberry-pi." In Electrical and Computing Technologies and Applications (ICECTA), 2017 International Conference on, pp. 1-4. IEEE, 2017.