Defence Science Journal, Vol. 71, No. 4, July 2021, pp. 491-498, DOI : 10.14429/dsj.71.16454

Blockchain Enabled Reparations in Smart Buildings-Cyber Physical System

Anupam Tiwari* and Usha Batra

GD Goenka University, Gurugram – 122 103 , India
**E-mail: anupam.tiwari@gdgu.org*

ABSTRACT

Blockchain technology is evolving across the globe and is being looked upon as a definite part of the future. Blockchain is often associated with bitcoin and finance's domain. But over the last decade, this backend technology to bitcoin has spread its association in almost all domains that we can think of. Further to this, smart contracts are making the blockchain ecosystem better. Other evolving technologies like Internet-of-things, Industrial Internet-of-things, Cyber physical systems are also making their onset on the global platform. Smart buildings link Internet-of-things connectivity, sensors and the cloud to remotely supervise and assure efficient heating- air conditioning, lighting and security systems etc to improve efficiency and overall sustainability. The global buildings sector over the next 40 years is expected to add 230 billion square meters of fresh construction, i.e., adding the equivalent of Paris every week. Thus integrating these technologies right at the onset, before they grow in isolation, is a coveted need today. This paper proposes a prototype to simulate architecture and discusses how blockchain enabled smart buildings can further expedite automation, security and transparency. For an apprehension purpose, the paper focuses on smart contracts enabled repairs and service in smart buildings.

Keywords: Blockchain; Smart contracts; Smart building; Cyber physical systems; Internet of things

1. INTRODUCTION

The last decade is witness to a horde of technologies which have altered the world with better and efficient functioning systems. These primarily include robotics, big data, machine learning, Internet of things (IoT), cyber-physical systems (CPS), blockchain to mention a few. The good thing is that these technologies are still evolving into newer possibilities for improving future. So, today is the right time to associate-integrate maximum of these technologies in right schema to reap maximum benefits ahead.

A lot of work is currently on associating blockchain and smart buildings. Blockchain smart contracts have been proposed[1] to describe, grant, and revoke fine-grained permissions for smart building occupants in a decentralised mode with resource description frameworks. Krishnan & Anjana [2] propose blockchain technology for secure migration of data within the smart building enabled on software-defined networking technology. Costantino[3] applies blockchain as an option to secure the integration of IoT and building information management. Stroulia[4], *et al.*, propose a model in context of a real office smart building and argue that it can reduce the administration overhead enabled with smart contracts.

While S.Li[5] works are not specific to smart buildings, but peculiar to smart cities, it proposes architecture of peer to peer light-heavy backup to overcome the high cost of blockchain data storage. Biswas and Muthukkumarasamy[6] apply blockchain to ascertain the security of data transmitted and furnish a secure communication platform in a smart city ecosystem. All these and similar other works have different applications of blockchain peculiar to smart buildings ecosystem. The fact that all these are recent works emphasizes the focus on blockchain technology being realised globally by research community.

This paper will be focusing on associating smart contracts built on solidity with specific scope of enabling repairs of devices on ethereum blockchain. Before taking on the proposed architecture and design to propose blockchain enabled smart building CPS (SB-CPS), these technologies are briefly discussed in section 2 followed by section 3 which is peculiar to recent works and challenges about SB-CPS. This section also discusses the traditional methods involved for coordinating repairs in a smart building. This is followed by section 4 which discusses the tools and simulation works conducted in detail. Section 5 and 6 discusses the results obtained followed by conclusion in section 7.

2. BLOCKCHAIN, SMART CONTRACTS AND CYBER-PHYSICAL SYSTEMS

2.1 Blockchain

The term blockchain comprises of two words "*Block*" and *Chain*". The "*Block*" consists of transactions and hashes while "*Chain*" refers to cryptographically linked blocks. The technologies behind these two words "Bitcoin" and "Blockchain" have independently evolved to otherwise unforeseen possibilities. Bitcoin has made way for around 2000+ cryptocurrencies with multiple variants of consensus

Received : 29 October 2020, Revised : 09 February 2021
Accepted : 10 February 2021, Online published : 01 July 2021

algorithms. Blockchain has made way ahead with blockchain 2.0 and blockchain 3.0 visions. These visions do not look far sighted with technical communities and leading IT corporates investing arduous research efforts and investments to expedite technological realisations.

2.2 Smart Contracts

Smart contracts[7], a term first coined by Nick Szabo, an American computer scientist, who recognised that the decentralised ledger could be applied for implementation of self-executing contracts. Many years later, after introduction of the bitcoin blockchain, in 2013, Vitalik Buterin, came up with ethereum[8], primarily planned for smart contracts. Ethereum is a worldwide network of computers which execute smart contracts. Smart contracts are self-executing terms of the agreement between seller and buyer interpreted into written lines of code. Solidity, Golang, Javascript, C++ are few main languages used for writing smart contracts.

2.3 Cyber Physical Systems

Often used interchangeably with IoT or Industrial IoT, CPS[9] denotes combining digital capacities, including network connectivity and computational capacity, with physical devices and systems. CPS components are enabled to communicate with their environment in real time mode to offer agility and sustainability of participating systems. While IoT, Industrial IoT (IIoT) are not architectured to attain a certain common task as they function i.e. they do not constitute a "system" in the classical sense. The word "system" implies a set of things working together as parts of a mechanism or an interconnecting network. CPS[10] are "systems of system" and are holonic in nature i.e. they are self-contained entities and a part of a larger system. CPS are incorporated into interfacing analogue, digital, physical, and human components machinated for operating through fusion of physics and logic.

3. SMART BUILDINGS-CYBER PHYSICAL SYSTEM (SB-CPS)

A CPS smart building[11] is any construction that applies automated operations to ascertain the building's functioning by employing actuartors, building management systems (BMS), sensors, IoT gateways etc to collect and manage data.

A schematic representation of smart building components is seen in Figure 1. An automated home will be able to mechanize things and do as directed but not intelligently. The term automation refers the transference of work from manual based mode to machines that are capable to accomplish the assigned jobs independently. Thus building automation denotes the interconnectedness of actuators, sensors and devices inside a building by communication protocols and networks.

3.1 Challenges in SB-CPS

The envisaged smart homes inside a smart building are enabled by intelligent systems for the occupants desired requirements and demands. An ecosystem of such a setup would have homes and buildings which constitute of living beings, well-informed technical devices and physical devices communicating with each other as a functional unit. This setup of things will be enabled with self-regulation to a limited extent and critically dependant on human computer interaction (HCI)[12] that centers on the interaction between humans and computer technology. Various architectures have been proposed for setting up SB-CPS but all of them are characterised by few common drawbacks and challenges briefly discussed below.

3.1.1 Security

New generation building automation service (BAS) have an underlying challenge of resolving security threats from cyber space[13]. Lohia[14], *et al.* focus on improving most popular BAS protocols KNX/EIB, ZigBee, BACnet, and EnOcean while Morenas[15], *et al.* identifies eavesdropping, physical attacks,

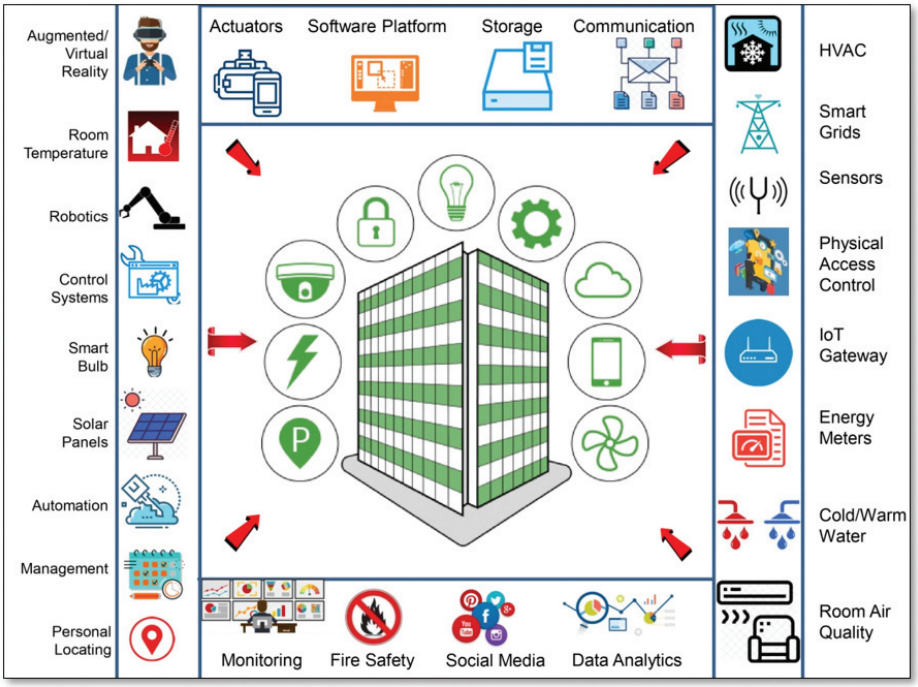

Figure 1. Smart building components

denial -of -service, spoofing, replay attack, data manipulation or injection and packet rerouting.

3.1.2 Interoperability

Communications between heterogeneous IoT devices and platforms in a SB-CPS context will be a huge challenge owing to big diversity. Multiple systems enabled with different protocols would deem a way out to exchange data and work in an interoperable way. Chituc[16] has proposed that integration in IoT-based systems is not an easy task and has identified numerous challenges.

3.1.3 Distributivity

CPS will eventually evolve in a highly distributed environment wherein data transfer will be derived from multiple sources and processed by distributed entities in a distributed manner. While peculiar to an SB ecosystem, retrieving data in distributed sensing search, Sriraghav[17], *et al.* have proposed clustered-tier architecture.

3.1.4 Scalability

The increasing number of sensors and devices will not just be confined to one smart building, but it will also be connected to other smart buildings to create an ecosystem of SB-CPS devices. This ecosystem is expected to scale to a billion plus devices and sensors. Fog computing is seen as one of the viable options to extend the scalability of IoT devices in the cloud[18].

3.1.5 Resources Scarcity

Resources for an operationally efficient CPS ecosystem would primarily encompass computational and power resources. With miniaturised devices only getting smaller, computational expectation will be a challenge while for smooth running of an entire ecosystem of IoT, powering devices will be a key contributor and wireless power is option[19].

3.2 Facility Management and Need of Blockchain Enabled SB-CPS

Facility Management in a smart building, as per BS EN ISO 41011:2018 is defined as 'consolidation of operations within a smart building organisation to maintain and workout the accorded services which abide and better the effectiveness of its main activities'. Almost in all BMS and BAS, it is normal to outsource facility management services. These facility management services are critical to routine and real time operations of the building. This may involve the technical control on automation and likewise various other services as bought out in Table 1. After making huge investments in building construction, setting up sensors, devices and intensive IT infrastructure, expecting a third party to decide the efficiency and performance of smart building-CPS ecosystem is indeed a dubitable choice. But then there doesn't seem to be a solution for this and perforce the BMS and BAS are seen outsourced, giving away significant fund divergences to third parties.

Blockchain may eliminate the need for such third party outsourcing by coding specific smart contracts to automatically execute functions as anticipated per requirement. This would supersede the legal contract or any other document agreement in place. Smart contracts ascertain a very specific set of results as per the executed code and thus there's never any mix-up in outputs. It's merely a very determined, computer-guaranteed set of outcomes. Smart contracts can thus be applied to a variety of situations including coordinating repairs in SB ecosystem.

Assuming a device is detected defective by the sensor control mechanism existing in the BAS, the following options of coordinating repairs exist, that range from the traditional (scenario 1 and 2) to smart contracts enabled (scenario 3), depicted in Fig. 2.

Scenario 1: **Traditional**: The occupant manually realises that the device is not working. He calls up the maintenance section which follows up repair by physical visit, checking the device and advising suitable action. Subsequently, books spare, replaces and resolves the defect. The payment is made by the occupant and the complaint closes.

Scenario 2: **Automated building system**: The device is reported faulty by the BMS to the maintenance section and the traditional way follows subsequently.

Scenario 3: **Smart contract enabled**: The device is detected defective by the sensor, which is immediately communicated in real-time vide the smart contract to the maintenance agency. If the sensor is also able to detect the defective part, effected order is placed too, thereby reducing the turnaround time. The smart contract also facilitates payment immediately on closure of the defect as seen in Fig. 2.

In scenario 3, we observe the negation of the middle men

Table 1. Facility Management Functions

Estates strategies	Asset management	Space management	Masterplanning
Service provisions	Provision of infrastructure and information technology	Maintenance, cleaning, testing	Restoration, retrofitting and renovation
Enabling changes in working practices	Quality judgment	Brand management	Rationalisation of services and assets
Assuring business continuity	Assuring safety and security and instituting emergency procedures	Traffic, parking and transport	Budget management
Accounting finances	Performance and usage assessment, optimisation	Sustainability	Procurement and project management
Contract management	Regulatory abidance and liaison with local authorities and emergency services	Mechanical ,electrical, plumbing and technical services	Help desk and other support services

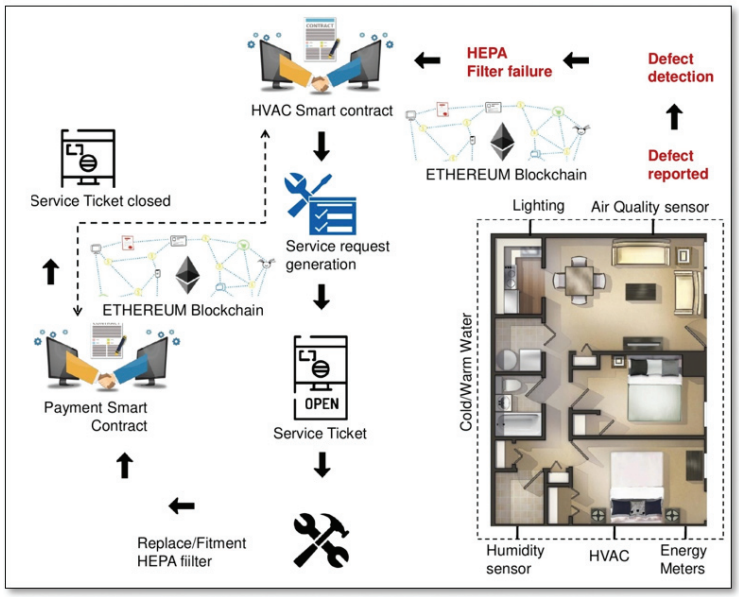

Figure 2. Smart contract enabled repairs.

i.e. the facility management personnel's and its intervention in an expedited manner. Blockchain enabled facility management would thus provide a potent self-activating, self-supervising, and cyber-hardened data transaction functioning, ensuring a truly effective data exchange system. This schema of proposed design is simulated in steps ahead.

4. MATERIALS & METHODS

The following setup of hardware and software applications has been used for the simulation part in this work. Details of the applications are seen below.

Hardware

Dell PowerEdge T440 Server, 10 Core Processor with 16 GB RAM, Intel Xeon 4210 (2nd Gen) & 1.2TB 10k RPM SAS Hard Disk and 5.0.0-29-generic #31~18.04.1-LTS GNU/ Linux

Software

- Truffle Suite[20]
- Ganache[21]
- Sublime code editor
- Cupcarbon IoT simulator[22]

Figure 3 depicts a simulated general area mapped on *cupcarbon* simulator with 10 sensor nodes[S1-S10] routed with one mobile sensor on a identified route marked. The 10 sensor nodes are simulated in a campus residential building with device IDs marked. The markers on the route were simulated with complete sensor nodes run for 86400 seconds with simulation speed of 100 ms and arrow speed of 200 ms in cupcarbon simulation. The sensor nodes were set with parameters as seen in Table 2.

The algorithm steps executed in *cupcarbon* simulator is seen in algorithm 1.

Algorithm 1 : Sensor nodes simulation fault loop

```
1   detect fault loop
2   dreadsensor HEPA
3           println  HEPA
4                    if($HEPA==1)
5                    send A2
6                           else
7                    send B2
8           end
9   delay 500
```

The simulated smart building in Figure 3 depicts a relatively small area with just one sensor reporting defect unlike a real time scenario which will have thousands of interconnected buildings with millions of IoT sensors communicating with each other.

5. RESULTS

Table 2. Sensor specifications

Longitude	28.2648° N
Latitude	77.0645° E
Sensor Radius	60 meters (radius for sensing unit)
Energy max	20160 (Initial energy of the battery)
UART Data rate:	9600 (represents the necessary time to send data (bytes) to the buffer of the radio module.
Drift (sigma)	3.0E-5 represents the clock drift.
Direction	5 represents the direction (rotation) of a sensing unit (case of directional sensor node)
Coverage	50 meters represents the coverage of a sensing unit

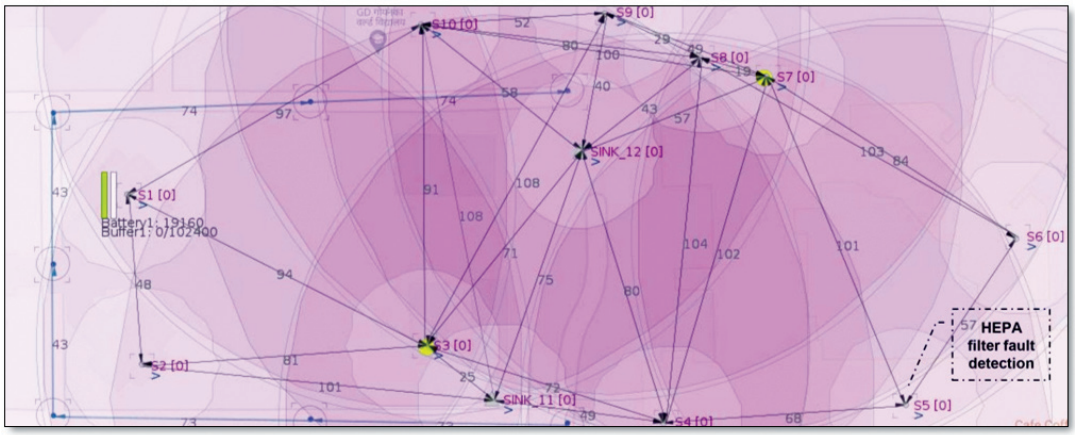

Figure 3. Campus general area simulated with sensors

The fault detection by node simulated at S5 reported with HEPA filter defect and the scenario 3, thus observed a defective HEPA (High-efficiency particulate air) filter. HEPA filters ensure that the air that passes through in the room environment has at least 99.95% of particles whose diameter is greater than or equal to 0.3 µm. This is detected by the sensor and the smart contract *HEPAfilterreplace* is activated as seen in Fig. 4. The sequence of operations that follows is enumerated below:

- Detection by sensor
- Reporting of defect to smart contract
- Activation of smart contract and execution
- Placing of demand of HEPA filter to vendor
- Service generation request
- Replacement and repair completed
- Conclusion of smart contract *HEPAfilterreplace*
- Finance smart contract executed and payments made.
- Conclusion of repair chain.

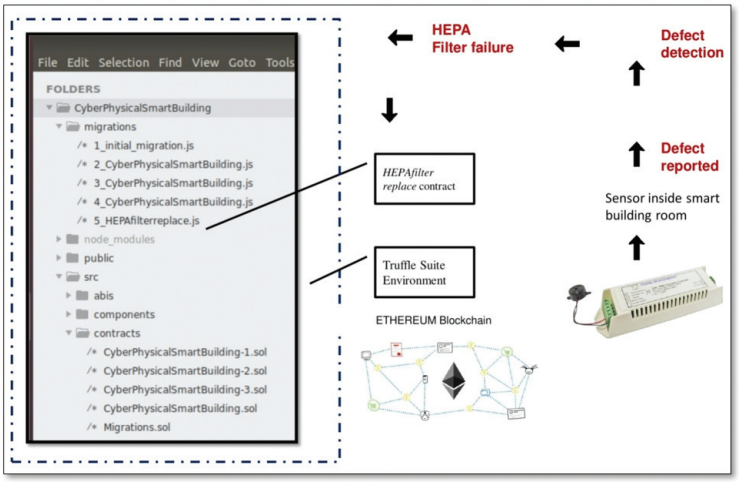

Figure 4. Repair chain enabled with Smart Contract.

5.1 Contract Compilation

Further to activation of the *HEPAfilterreplace* contract, the contract is compiled and migrated to *ganache* blockchain as seen in Figure 5.

Once compiled, the mining details were observed in block number 23, generated in this simulated environment. The contract address generated as the smart contract *HEPAfilterreplace* gets executed is seen in the Figure 5. Once the address is generated, the same is seen deployed on the blockchain. The address generated and seen for the deployment is *0Xe89c06815c38c4BFdA71823539A8Bd541B6c8BA1*. The transaction hash *0x4fb6238d11aa2a4271d17e6cacb43f-77d8c0fbe26f9f4708f3cd-f65869281a6c* as seen in Fig. 6. It is pertinent to mention that these unique transactions IDs play a significant role in querying a blockchain.

While the information seen in Figs. 5 and 6 w.r.t transaction IDs and contract address of *HEPAfilterreplace* look similar, it is observed that both pertain to different blocks 23 and 24. This re-affirms the connectivity between blocks in the blockchain and confirms the ubiquitous deployment and access of smart contract in blockchain. The above details are seen under the transactions tab of *ganache* interface as executed vide the Truffle suite.

5.2 Executions and Block creations

34 rounds of simulations effected into 34 blocks creation with as many number of transaction hashes. A sample execute of the smart contract *HEPAfilterreplace* is produced below for block number 33.

Transaction hash

0xfca9446d559fb7fd270d980a0c48a6698d78ee105322-a95ef44d6c28d248798f

Contract address

0xedF572101c57b730bBfdaC1f0a13e743513308b5

Block number: 33

Block timestamp: 1599367863

Account: 0xe6d1ECd330D536f421C1A150834357-164a51C6Cf (Sender address) at Fig. 5

Balance: 99.92077838

Gas used: 261393

Gas price: 20 gwei

Value sent: 0 ETH

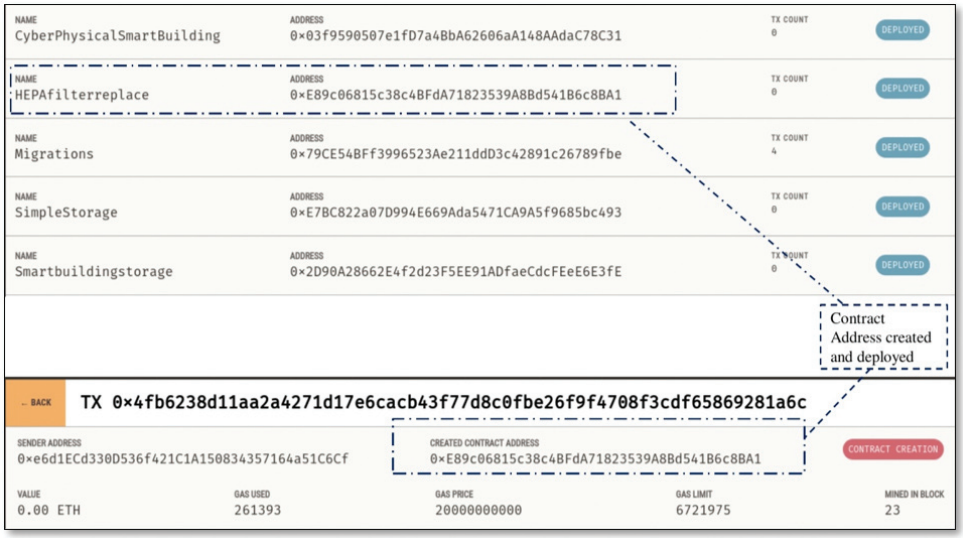

Figure 5. *HEPAfilterreplace* contract and deployment details.

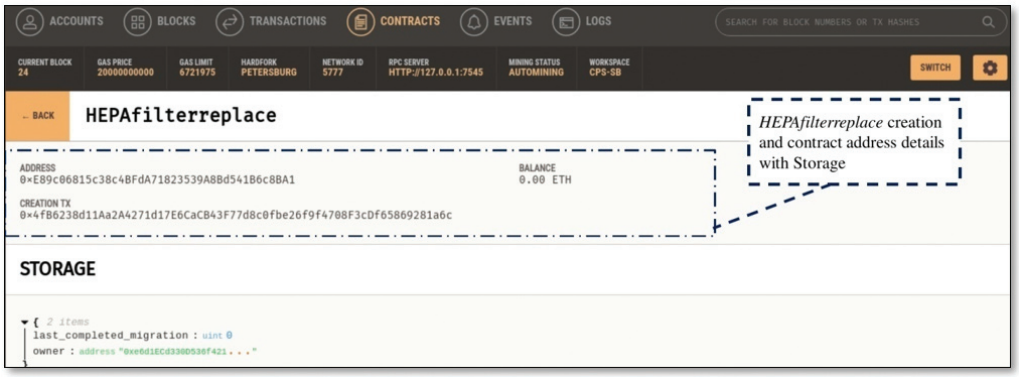

Figure 6. Smart contract *HEPAfilterreplace* address details at Block 24.

Total cost: 0.00522786 ETH

Block time-stamp *1599367863* is the epoch timestamp and the GMT equivalent is "Sunday, 6 September 2020 04:51:03" i.e the day of mining of this block. These time stamps again are invaluable information for data associations and smart contracts activations.

5.3 Gas Expansion

Gas expansion in transactions conducted in the ethereum blockchain are based on quantified computational effort taken to coordinate operations. In the simulations conducted, the set parameters were with gas price=20000000000 and gas limit= 6721975. The concept of gas is currently used only in the ethereum blockchain, thus such parameters may not exist if any other blockchain platform is used for associating with BMS. Study of design patterns of gas optimisation is an area of evolving research work since gas optimisation is a complex challenge in the ethereum ecosystem[23].

6. DISCUSSIONS

The simulation conducted in this work envisages a smart building environment with facility controls being coordinated by smart contracts. The simulated model schema of sensors and blockchain worked fine in the limited environment setup. The detection of defect, activation of the smart contract, generation of transaction IDs, creation of smart contract addresses and deployment of smart contracts on the blockchain have been successfully realised in the work.

However, the real time conditions in actual will face a horde of challenges as discussed in section 3.1 earlier. Apart from these discussed challenges, few peculiar challenges in a blockchain ecosystem of things will include the following

- *Unique digital Identification of devices on IoT :* All the devices on the network and participating in such a SB-CPS architecture are expected to have unique digital identification based on strong PKI or any alternative standard to negate any scenario of being plugged in with malicious devices[24].
- *Expedited versions :* Solidity language for smart contracts used in this work has got an extra ordinary version speed release[25]. The version has seen 53 versions since its introduction with major challenge of backward incompatibility. During the course of this work, the version has changed more than 12 times since Jan 2020. It is undoubtedly a good thing for expediting into stable versions but as on date the challenge remains for researchers and programmers.

7. CONCLUSION

Critical infrastructures of national importance are crucial to the operation of modern societies and economies and so is the need for security by design at the onset[26].

Blockchain is an evolving technology phenomenon and it should be endeavored to associate it along with IoT into CPS. The interconnection of CPS devices and components sets the way ahead to collectively perform intelligent smart contract based decisions and executions. In this paper, the possibility of introducing smart contracts in the facility management system in a smart building environment has been discussed and a small scenario problem has been solved.

An approach is discussed with proof-of-concept to generate and exploit ethereum smart contracts based on solidity on ganache blockchain. In this paper a defective HEPA filter has been simulated for repairs vide activation of smart contracts while the sensor informs about the defect. While the approach is partial and the scenario envisaged is simulated which does not fulfill the real ground situations as would deem. The challenges bought out vide the paper remain a big road block in the way ahead for the realisation of smart contracts environment in a smart building part of CPS.

The technologies discussed are all evolving at an expedited pace and it's perhaps the right time that smart contracts be explored at the onset to achieve true realisation of SB-CPS. In the current state of development, though many projects are evolving in the domain viz Ethereum, Hyperledger[27], NEM[28], Stellar[29] ,Waves[30] etc. But each of these projects has it's advantages and disadvantages to resolve. Developing right and hardened smart contracts, with the right platform, for such use cases as HEPA filter repair looks a near future vision for realisation. This paper presents an initial approach for generating smart contracts for coordinating the usage of cyber-physical system elements from smart contracts. While the platform testing in this paper is limited to solidity i.e. Ethereum, the approach and architecture can easily be worked out with other blockchain platforms.

REFERENCES

1. Houbing, Song; Glenn ,A. Fink & Sabina, Jeschke. Cyber Security of Smart Buildings. Security and Privacy. *In* Cyber-Physical Systems: Foundations, Principles, and Applications , IEEE, 2017. pp.327-351. doi: 10.1002/9781119226079.ch16.
2. Krishnan, S & Anjana, M. S. Security Considerations for IoT. In Smart Buildings. *In* IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, 2017. pp. 1-4. doi: 10.1109/ICCIC.2017.8524450.
3. Costantino, D. Solving Interoperability within the Smart Building: A Real Test-Bed. *In* IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, 2018, pp. 1-6. doi: 10.1109/ICCW.2018.8403751.
4. Stroulia, E.L. Bindra, C. Lin, & O. Ardakanian. Decentralized Access Control for Smart Buildings Using Metadata and Smart Contracts. *In* IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS),Canada, 2019. pp. 32-38. doi: 10.1109/SEsCPS.2019.00013.
5. Li, S. Application of Blockchain Technology in Smart City Infrastructure. *In* 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi'an, China, 2018 pp. 276-2766. doi: 10.1109/SmartIoT.2018.00056
6. Biswas, K. & Muthukkumarasamy, V. Securing Smart Cities Using Blockchain Technology. *In* IEEE 18th International Conference on High Performance Computing and Communications, Sydney, 2016.pp. 1392-1393. doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.
7. S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin & F. Wang. An Overview of Smart Contract: Architecture, Applications, and Future Trends. *In* IEEE Intelligent Vehicles Symposium (IV), Changshu, 2018. pp. 108-113. doi:10.1109/IVS.2018.8500488
8. D. Vujicic, D. Jagodic & S. Randic. Blockchain technology, bitcoin, and ethereum: A brief overview. *In* 17th International Symposium Infoteh-Jahorina, East Sarajevo, 2018.pp. 1-6. doi :10.1109/INFOTEH.2018.8345547
9. Y. Liu, Y. Peng, B. Wang, S. Yao and Z. Liu. Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica,* 2017, **4**(1), 27-40. doi: 10.1109/JAS.2017.7510349
10. Humayed, A.; Lin, J.; Li, F. & Luo, B. Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, 2017, **4**(6), 1802-1831. doi: 10.1109/JIOT.2017.2703172
11. Havard, N.; McGrath, S.; Flanagan, C. & MacNamee, C. Smart Building Based on Internet of Things Technology. *In* 12th International Conference on Sensing Technology (ICST), Limerick, 2018. pp. 278-281. doi: 10.1109/ICSensT.2018.8603575
12. Pitale, A. & Bhumgara, A. Human Computer Interaction Strategies - Designing the User Interface. *In* International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2019, pp. 752-758, doi: 10.1109/ICSSIT46314.2019.8987819
13. Rai, N. & Chansarkar, S. Cyberspace Security : An Overview for Beginners. *Def. Sci. J.,* 2017, **67**(4),483-484, doi: 10.14429/dsj.67.11542
14. Lohia, Karan; Jain, Yash; Patel, Chintan & Nishant. (2019). Open Communication Protocols for Building Automation. *In* Procedia Computer Science. 160. 723-727. doi: 10.1016/j.procs.2019.11.020.
15. Morenas, J. de las; Silva, C.M. da & Leitao P. Security Experiences in IoT based applications for Building and Factory Automation. *In* IEEE International Conference on Industrial Technology (ICIT), Argentina, 2020. pp. 322-327. doi: 10.1109/ICIT45562.2020.9067229.
16. Chituc, C. Interoperability Standards in the IoT-enabled Future Learning Environments: An analysis of the challenges for seamless communication. *In* 13th International Conference on Communications , Romania, 2020, pp. 417-422, doi: 10.1109/COMM48946.2020.9141959.
17. Sriraghav, K.; Vidya, N. & Chandran, K. R. Sarath. Sub-system model for data collection and distributed sensing search technique for Internet of Things applications. *In* Third International Conference on Sensing, Signal Processing and Security (ICSSS), Chennai, 2017, pp. 9-14, doi: 10.1109/SSPS.2017.8071556.
18. Tseng, C. & Lin, F. J. Extending scalability of IoT/M2M platforms with Fog computing. *In* IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 825-830. doi: 10.1109/WF-IoT.2018.8355143.
19. Molefi, M.; Markus E. D. & Abu-Mahfouz, A. Wireless Power Transfer for IoT Devices - A Review. *In* International Multidisciplinary Information Technology and Engineering Conference, South Africa, 2019. pp.1-8, doi: 10.1109/IMITEC45504.2019.9015869.
20. Truffle Overview. Accessed from https://www.trufflesuite.com/docs/truffle/overview dated 03 Sept 2020.
21. Ganache. Accessed from https://github.com/trufflesuite/ganache dated 03 Sept 2020.
22. M. Akkurt and K. Küçük. Simulation of Smart City Applications Based on IoT Technologies with CupCarbon. *In* 3rd International Conference on Computer Science and Engineering , Sarajevo, 2018. pp. 179-184. doi: 10.1109/UBMK.2018.8566291.
23. Marchesi, L.; Marchesi, M.; Destefanis, G.; Barabino G. & Tigano, D. Design Patterns for Gas Optimisation in Ethereum. *In* IEEE International Workshop on Blockchain Oriented Software Engineering, Canada, 2020. pp. 9-15. doi: 10.1109/IWBOSE50093.2020.9050163
24. Aksoy, A. & Gunes, M.H. Automated IoT Device Identification using Network Traffic. *In* IEEE International Conference on Communications (ICC), Shanghai, China,

2019, pp. 1-7.
doi: 10.1109/ICC.2019.8761559.
25. Solidity releases. Accessed from https://github.com/ethereum/solidity/releases dated 31 Aug 20
26. Ravishankar, M., Rao, D. & Kumar, C. R. S. . A Game Theoretic Software Test-bed for Cyber Security Analysis of Critical Infrastructure. *Def. Sci. J.,* 2018, **68**(1), 54-63. doi:10.14429/dsj.68.11402
27. D. Li, W. E. Wong & J. Guo. A Survey on Blockchain for Enterprise Using Hyperledger Fabric and Composer. *In* 6th International Conference on Dependable Systems and Their Applications ,China, 2020. pp. 71-80. doi: 10.1109/DSA.2019.00017
28. NEM – Distributed Ledger Technology (Blockchain). Accessed from https://nem.io/ dated 21 Nov 20.
29. Stellar Consensus. Accessed from https://www.stellar.org dated 21 Sept 2020.
30. Waves Platform. Accessed from https://wavesplatform.com/ dated 05 Sept 2020.

CONTRIBUTORS

Mr Anupam Tiwari, is M.Tech in Computer Science from JNTU Hyderabad, India. He also holds three post graduation qualifications in Information Security, ERP and Operations & Systems. He has 16 years plus experience in the field of Cyber Security domain and for last 5 years has been exploring Blockchain domain and cryptocurrencies. He has more than 25 articles and papers in International , national and defense journals/ magazines.
Contribution in the current study, he carried out the experimental and simulation part along with manuscript writing.

Dr Usha Batra is PhD (Computer Science and Engineering) from Banasthali University, Rajsthan. Her expertise is in the area of computer science and engineering, particularly software engineering, enterprise application integration, cloud computing, internet of things and cyber physical systems. She has taught these subjects for nearly 17 years at universities such as Jaypee University, Northcap University, and GD Goenka University.
Contribution in the current study, she helped in the interpretation of simulated results, reviewed and provided suggestions to improve quality of work. The research work has been deemed possible owing to her guidance and supervision.