# Novel Architecture for Internet of Things and Blockchain Technologies

**Chetna Dabas and Aniket Dabas**

**Abstract** Diverse companies and platforms are falling madly in love with the blockchain technology in the present scenario. So, it is of due importance that the relations among the different types of blockchains are established. Further, the extraction of capabilities of strengths of diverse blockchains catering to different kind of micro-services is a crucial step toward the realistic blockchain. This issue even became of utmost significance when specifically the researchers are dealing with Internet of things (IoT) purposes. The IoT in general is composed of a wide spectrum of technologies varying from soft real time to hard real time, from stateless through state full, and from unconstrained to constrained. Therefore, for all definite implementations, no definite blueprint of the IoT architecture may be referenced. When it comes to blockchain technology melded with IoT, the existing literature seems to lack a hybrid architecture which contains the best of both these worlds. This research paper proposes a hybrid architecture for IoT and blockchain along with the evaluation of this architecture by implementing an application for the same. The application is for a common user using these technologies which enable the user to select among diverse cryptocurrencies efficiently. The evaluation of the proposed architecture is carried out by implementing blockchain on IoT devices. The results retrieved as a part of this work are encouraging in terms of execution times.

**Keywords** Internet of things · Blockchain · Radio frequency identification
IoT architecture

C. Dabas (✉)
Department of CSE, Jaypee Institute of Information Technology, Noida, India
e-mail: chetna.dabas@jiit.ac.in

A. Dabas
Erricson India Global Services Pvt. Ltd., Noida, India
e-mail: aniket.dabas@erricson.com



L. C. Jain et al. (eds.), *Data and Communication Networks*, Advances in Intelligent Systems and Computing 847, https://doi.org/10.1007/978-981-13-2254-9_18

## 1 Introduction

In almost all the information industries across the globe, the concept of Internet of things is prevalent in its wider most form. It has deeply impacted the life of a common man and has caught the attention of academia, industries, and the governments worldwide. An Internet of things (IoT) [1] is an advanced and extending technology having its basis grounded on the well-known Internet technology. There lie immense possibilities of expansion and scalability with IoT. The IoT includes any kind of objects or things connected through wired or wireless technologies involving orientation tracing, intelligent recognition, equipments like Radio Frequency Identification (RFID) [2, 3] tags and readers, numerous kinds of sensors, GPS, laser scanners to name a few. Further, the IoT can be well connected to cloud computing [4–9] technology to make the matter more complicated to address [10].

There are various initial developments in the direction of the Internet of things which have paid special attention to the product life cycle applications and RFID infrastructures in Business-to-Business (B2B) logistics but still the IoT is farther to go and make even a common man capable to effectively access as well as contribute rich, secure, and cost-effective information about locations and things.

Due to the heterogeneous environment of the IoT scenarios, there is a lack of precise and generic architecture which can govern the majority of applications in diverse scenarios. Apart from this, there exist lots of constraints in such an environment which hampers the performance of applications and increases the cost involved in developing methods to assist fast and reliable transactions across the network. Further, there come security issues embedded with such heterogeneous and scalable environments where IoT is connected to the cloud as well.

Blockchain [11–13] can perform a crucial role in such a scenario to suggest reliable and secure solutions with the Internet of things [1].

Specifically, the blockchain is considered as a distributed and public ledger. The transactions in blockchain are kept in a linked list consisting of blocks. This chain expands upon the addition of new blocks which are added continuously on the Internet. Various cryptography and distributed algorithms have been utilized for maintaining the security and consistency of the ledger. Blockchain comes with advantages of persistence, decentralization, auditability, and anonymity which enable the improvement of the efficiency and saves time.

Specifically, mentioned in [13] paper, the blockchain holds great potential in constructing the future Internet systems to come in due years.

In this work, a hybrid IoT architecture is proposed, the possible applications of the proposed architecture are suggested, and the architectural elements of the proposed IoT architecture are discussed. Further, the integrated view of the proposed hybrid IoT architecture composed of technologies like RFID, cloud computing, and blockchain is presented. Apart from this, IoT data analytics is performed along with result assessment.

The rest of the research paper is ordered in the way mentioned ahead. The related work is presented in Sect. 2. Section 3 presents the proposed Internet of things hybrid architecture. This section also contains subsections which contain the possible applications for the proposed architecture, the architectural elements of the proposed IoT architecture, and the integrated view of the proposed architecture. In Sect. 4, authors give a detailed explanation of our proposed work. Section 4 presents the IoT data analytics along with result assessment. Section 5 presents open challenges and future vision. The research paper concludes with Sect. 5 which presents the conclusions of the work and summary is discussed as well.

## 2 Related Work

This related work section describes the existing literature on various existing architectures of IoT-based systems along with the possibilities of the existing technologies like cloud computing, Radio Frequency Identification, and blockchain along with IoT.

In [10], authors have discussed architectural aspects of integrating cloud and RFID for the scalability. The authors have also talked about the possibilities of kinds of applications that can be running on this integrated architecture. The authors of this paper have revealed the blending possibilities of the two important technologies, namely cloud and RFID.

The authors of paper [14] have given a cloud-centric vision for IoT scenarios. This paper also makes a point that with the present existence of a variety of numerous RFID tags and other wireless sensor technologies and sensor equipments, IoT is believed to be the forthcoming revolutionary technology which is supposed to transform the present Internet to future Internet which is fully integrated.

In the paper [15], the authors present a basic architecture of IoT with three layers, namely perception layer, network layer, and application layer. This paper lacks the workflow of these layers in detail.

The authors of research work [16] have tabulated the security issues in IoT. Further, they have presented the role of blockchain in solving a huge number of security issues associated with IoT and hence revealing the significance of blockchain in IoT scenarios.

In [17], the research work by the authors discussed the future architecture for the IoT. This paper discusses the definitions and existing developments in the area, along with key requirements. This paper also discusses a proposal for the future IoT. Apart from this, in both user-centric and business-centric environments, this paper examines the usability by stakeholders.

The authors of the paper [18] discuss the significance of IoT in day-to-day life, present the architecture of IoT, the protocols for IoT, and further discuss possible IoT applications.

The research work in [19] presents a framework for IoT architectures. The framework proposed by the authors is designed for the applications which are service-based and in smart cities. The data input for this framework is retrieved from data sources which form data cloud.

In [20], the authors have proposed the classification along with a comparison of the blockchains and the blockchain-based systems. This paper claims that the presented work helps in assisting the assessment and design procedure of blockchains on the existing architectures.

The authors of [21] highlight the existing trends and generic architecture of IoT composed up of application layer, middleware layer, perception layer, business layer along with the future application. The authors of this paper specifically stress on the fact that IoT is gaining popularity across diverse fields like industry, academia to name a few. Further to this, the authors convey that IoT bears the capability to bring benefits to professionals and even to individuals.

In [22], the authors of this paper have proposed specific media-aware traffic security architecture. This architecture depends on the given traffic classification for catering various multimedia services.

In the existing literature, so far no work has been noted on the integration of all these technologies like blockchain, RFID, cloud computing in a single architecture melded with IoT.

The authors of this paper took this step further in the proposed research work as follows.

The research aim of this proposed work is to offer fusion architectures with Internet of things and blockchain technologies, while utilizing Radio Frequency Identification and cloud computing perception altogether. The vision of this proposed research work is to provide data security, management, analytics, and implications to a common man while keeping low cost and optimum performance.

## 3 The Proposed Internet of Things Hybrid Architecture

System blockchains are the inventions of the present era that have revolutionized the way one distributes personal information over the cloud and Internet in secured manner. Blockchain has been of great importance to the daily personal (both textual and image) data playing its crucial role on social Web sites, etc., and hence in the commercial aspect. RFID has on the other hand revolutionized the association of unique identities and tracking to things, places, animals, and even human beings. The hybrid use of RFID and blockchain leverages a benefit of distributed ledger which fortifies both security and transparency.

Aryanvika is a self-improved RFID and blockchain system and method which has the ability to boost the performance and decline the cost of the data analyzed in optimum ways in which data can be handled.

The idea was first conceived by the authors when they were busy observing their surroundings to seek an innovative design architecture on how to use their creativity for the enhancement of the society. As a consequence, the attention of the authors fell on the day-to-day problem of storing the magnanimous amount of data generated by photographs taken by people every day all over the world and not being able to store them properly due to issues like lack of security. Then the authors thought why not to think of some innovative way of solving this problem.

This idea is not sold; neither has it gone through any official process. No prototypes have been made. Authors do have a hard copy of our calculations and workouts and researches that made us finalize the features for the system and method.

## 3.1 Example Scenarios of Applications of the Proposed IOT Architecture

In this section, the authors explain with the help of a few examples the possible applications that may be used on the proposed architecture.

- For instance, suppose a person in India was working on a technology 'X' and had his personal photograph album for it stored on his personal cloud at his home. He also wants to associate a unique identification to his photographs for security reasons. Suppose he now moves to a different country, let's say Australia, for a job and wants to show his secure photographs to his new colleagues. This can be easily accomplished with the proposed hybrid IoT architecture which he might have constructed in his home back in India.
- Another interesting example of this scenario is related to mining of user choice-based cryptocurrencies pertaining to scalable, efficient, and cost-effective way in a heterogeneous IoT environment. The proposed architecture delivers a significant performance in a cost-effective manner in such a scenario.

## 3.2 Elements of the Proposed IoT Architecture

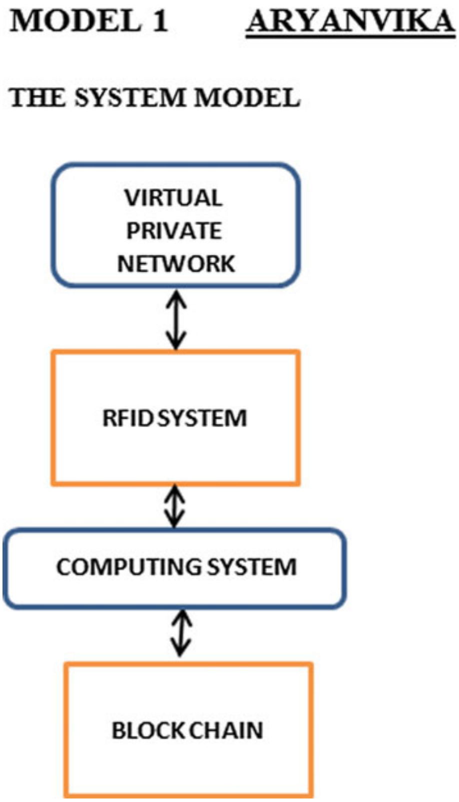
The proposed architecture in the present research work is described in Fig. 1 in abstract as a system model. It makes use of blockchain, Radio Frequency Identification, and cloud technologies. This system model is primarily composed of four layers as is self-explanatory in Fig. 1. The authors have named it as Aryanvika.

The detailed workflows of the proposed hybrid IoT architecture are presented in the subsections ahead.

### 3.2.1 Workflow of Layer 1

Layer 1 corresponds to the virtual private network on the cloud. It is composed of three heterogeneous devices, namely EndUser Device 1 (laptop), EndUser Device 2 (smartphone), and EndUser Device 3 (raspberry pi 3). These heterogeneous devices may be scaled up or down according to the requirements. Further, these devices have their own respective user interfaces (may be same or different). With the help of these

**Fig. 1** System model




user interfaces, the user can see or update the data on these devices. These end user devices form a virtual private network. This layer 1 is further connected to layer 2 of the proposed hybrid IoT architecture which is explained in the next subsection. The system model of layer 1 is presented in Fig. 2.

#### 3.2.2 Workflow of Layer 2

Layer 2 as depicted in Fig. 3 takes its input from layer 1. The interface of this layer interacts with the layer 1 as well as the RFID reader. There exists a sound possibility of using more than one RFID reader in this layer of the architecture. The RFID reader offers a unique identification of the asset linked to another interface which is linked to layer 3 of this architecture. The output of layer 2 is fed as an input to layer 3.

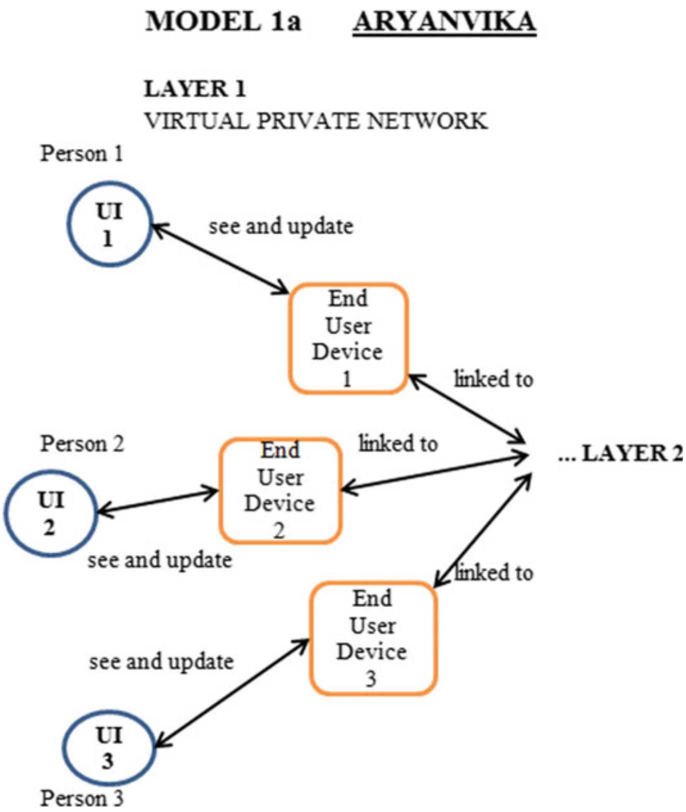



**Fig. 2** System model: layer 1

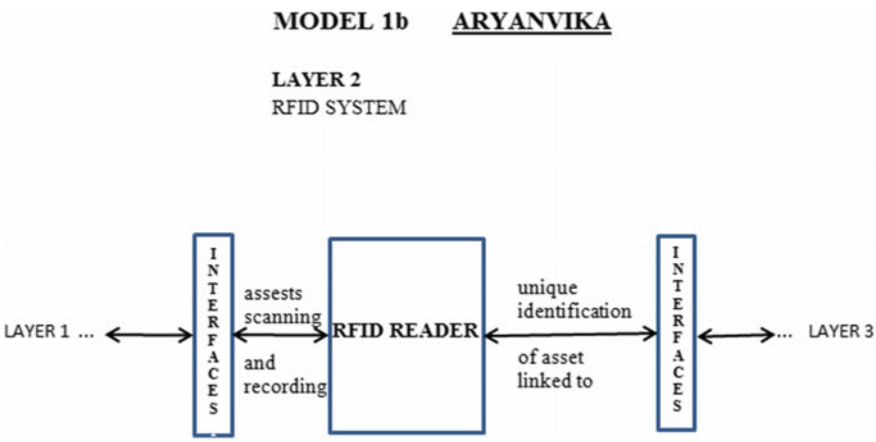



**Fig. 3** System model: layer 2

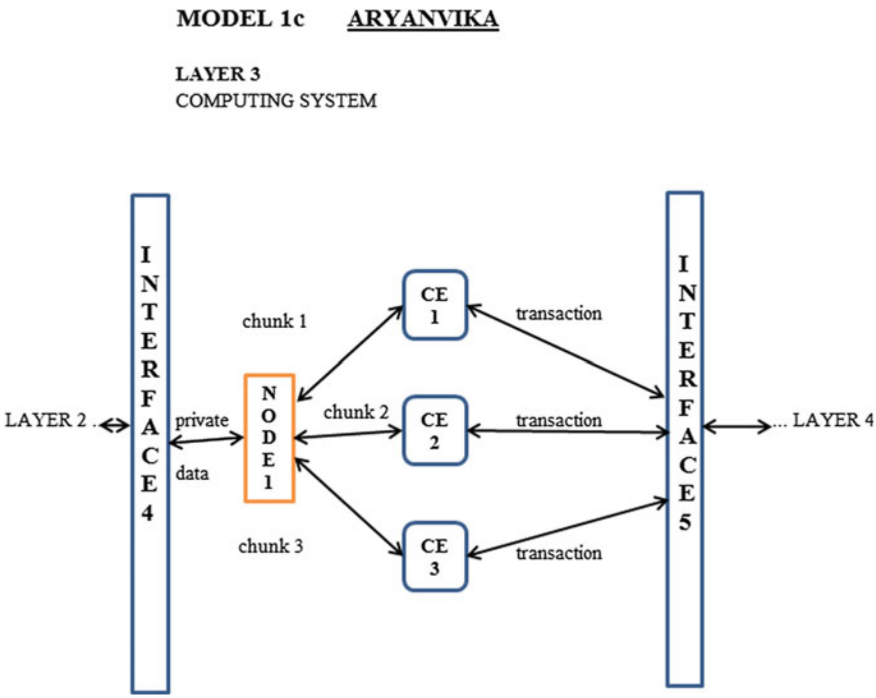



**Fig. 4** System model: layer 3

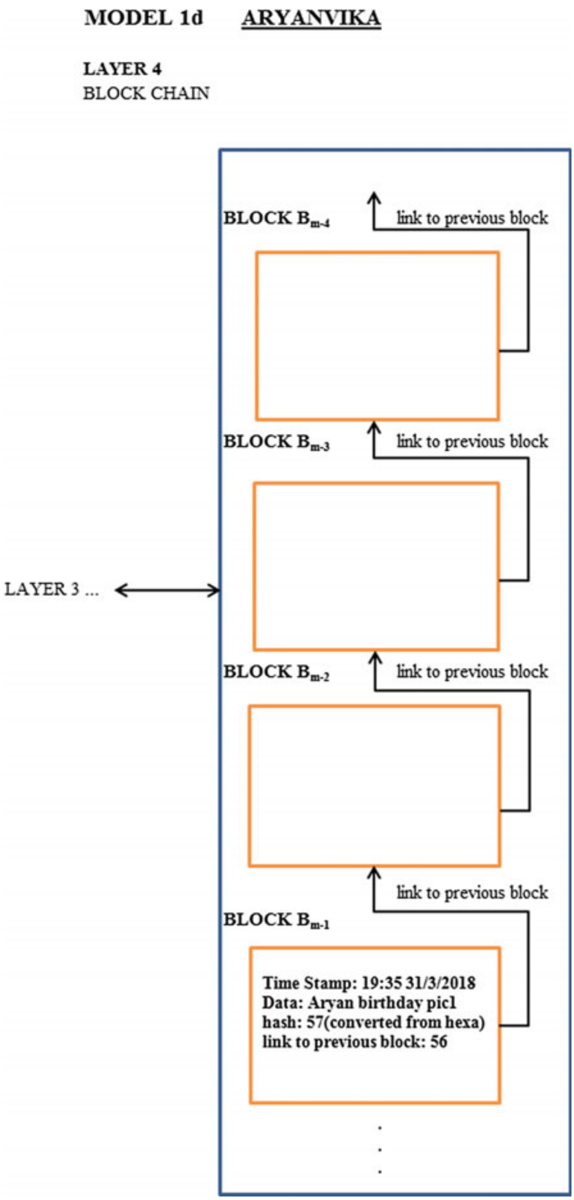
### 3.2.3 Workflow of Layer 3

Layer 3 of the proposed novel architecture is shown in Fig. 4. This layer takes its input from layer 2 and passes on its output to layer 4. In layer 3, there exists a single node (to save cost) although there exists a strong possibility to scale it to multiple nodes depending on the requirements. There exist three computational elements in the present architecture (which may be extended to n in numbers). By this layer of the architecture, a transaction is initiated and layer 4 is invoked.

### 3.2.4 Workflow of Layer 4

Layer 4 corresponding to the proposed hybrid IoT architecture is presented in Fig. 5. This layer is composed of the blockchain. The data in the block of the chain may be like the time stamp, date hash, and link as is clearly indicated in the figure. The data block is added securely and uniquely with tracking details.

**Fig. 5** System model: layer 4



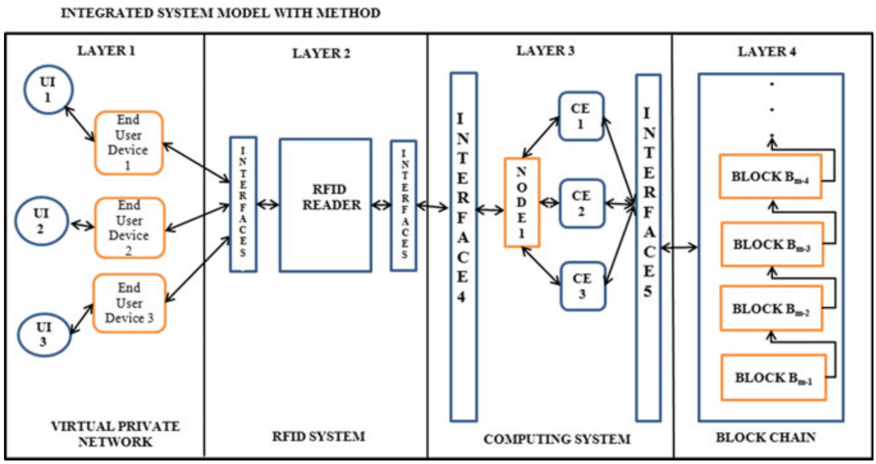



**Fig. 6** Proposed hybrid Internet of things architecture (with blockchain and RFID technologies)

## *3.3 Integrated View of Hybrid Internet of Things Architecture*

Here, the authors describe the integrated functioning of the proposed hybrid architecture of the Internet of things. The pictorial view of the proposed novel IoT architecture is presented in Fig. 6.

The functioning of the proposed IoT architecture is described by the following four major components or layers:

(1) *Virtual Private Network (VPN): Accessing Data*
Whenever a request from the user comes, a data file is generated locally on the virtual private network (local cloud) from one of the heterogeneous devices, for example, from EndUser Device 1 (laptop) or EndUser Device 2 (smartphone) or EndUser Device 3 (raspberry pi 3). These devices may be further generalized to n numbers. The data file may be in a different format depending on the source. There exists a Python script to convert the requested file in the desired format.
(2) *RFID System: Reading Data*
The RFID reader is connected to the VPN and reads data from the same. The Python script is used to connect the RFID reader to the VPN and reading the data and associating a unique identification to the data. This ensures the uniqueness of the desired data. There can be a single RFID system or a collection of RFID devices. In case of more than one RFID reader, there will be a necessity of incorporation of the RFID anti-collision protocols [23].
(3) *Computing system: Processing Data*
This data from the RFID reader is further fed to a cluster of small fast processing computers at a single node (there is a possibility of multiple nodes connected at

this point consisting of *n* number of computational elements depending on the horizontal scalability parameters) which contains execution of Python scripts.

(4) *Blockchain: Managing Data*
The concepts of proofs are written according to the requirements, the specific or generic algorithms are up and running on the computational nodes, and the data is appended as a block in the chain in the most reliable and cost-effective manner.

## 4 Proposed Architecture Assessment and Results

This section discusses the experimental setup and assumptions made while executing the designed architecture, and then, results are displayed corresponding to the successful execution of the proposed hybrid IoT architecture. The application under consideration is written in Python and aims to offer a user the best-rated cryptocurrency among the four considered in the present scenario. The four cryptocurrencies considered in this work are BTC, Etherum, Ripple, and Zcash.

### *4.1 Environment of Execution*

The environment under consideration is as discussed in the proposed hybrid architecture for IoT under Sect. 3 of this research paper.

### *4.2 The Scenario and Application Under Consideration*

A user of the proposed architecture has migrated to some other location, and his IoT architecture setup exists at his home in India. The user who is temporarily migrated to some other location now wishes to offer a new business proposal to his new organization where he wishes to seek the old mined data kept on his cloud at his home. He wishes to offer an application which makes use of all the technologies like RFID, cloud, blockchain, and IoT to make secure transaction and offer his new organization a secure, unique, and reliable solution.

### *4.3 Execution of the Application*

The data in layer of the architecture was successfully mined with the help of designed Python scripts. Each of the data center storage had one of the four different types of files, namely low priority type-1, high priority type-1, low priority type-2, and

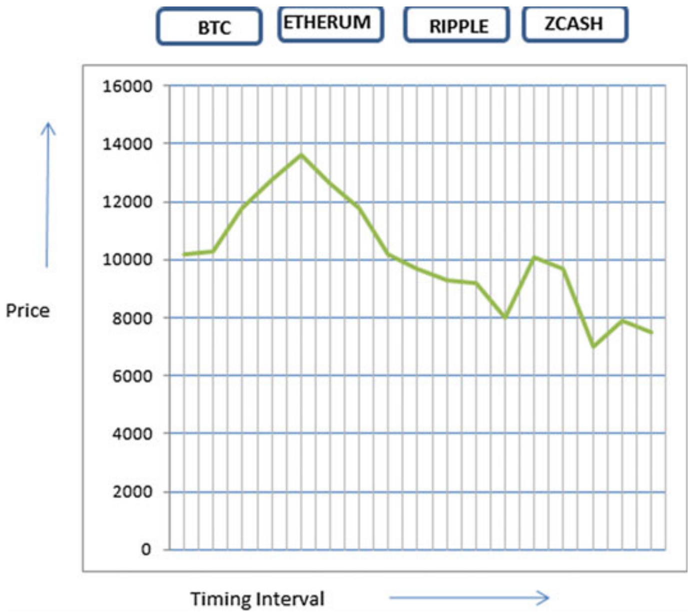



**Fig. 7** Timing interval versus price of various cryptocurrencies

high priority type-2. For simulating the configuration, the authors used three end user devices, a cluster of three graphical processing units, one RC522 RFID reader, specially designed user interfaces, one raspberry pi 3 module with Wi-Fi module, one Samsung smartphone, and one HP laptop (core i3). The results were successfully obtained at the user interface of a different node as depicted in Fig. 7.

## 5 Open Challenges and Future Visions

The challenges associated with the proposed work are to bring the instances of the proposed architectures to life for amplification of the performance of the hybrid IoT system and also to reduce the cost of data handled to a prime level while keeping into consideration the heterogeneous devices utilized in Internet of things. More challenges associated with the proposed research work are multi-technologies awareness and integration capabilities along with the blockchain vulnerabilities. The future vision for the proposed work imbibes the possibilities of implementation of the proposed architectures with polyglot programming and polyglot approaches.

## 6 Summary and Conclusions

The prime idea of this research work is that the proposed IoT architecture would require no external characteristics to govern the cost or the performance of the hybrid system. Further, the instances resulting from implications of the proposed architecture would possess the self-capability for analyzing the performance of the private data which is in the system and hence set the cost, timing to list a few among crucial parameters. Further, there lie intensive market opportunities for the proposed research work. This is due to the fact that one can make discrete Aryanvika kind of system and methods for diverse stretches across the globe, catering to their own needs of preserving data from heterogeneous sources in a secure and cost-effective manner. Aryanvika is a huge research, business, and expansion opportunity.

## References

1. Huckle, S., Bhattacharya, R., White, M., Beloff, N.: Internet of things, blockchain and shared economy applications. Procedia Comput. Sci. **98**, 461–466 (2016)
2. Molnar, D., Wagner, D.: Privacy and security in library RFID: issues, practices, and architectures. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 210–219. ACM, Oct 2004
3. Bolic, M., Simplot-Ryl, D., Stojmenovic, I. (eds.): RFID systems: research trends and challenges. Wiley, New York (2010)
4. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Gener. Comput. Syst. **25**(6), 599–616 (2009)
5. Moreno-Vozmediano, R., Montero, R.S., Llorente, I.M.: IaaS cloud architecture: from virtualized datacenters to federated cloud infrastructures. Computer **45**(12), 65–72 (2012)
6. Zhu, J.: Cloud computing technologies and applications. In: Handbook of Cloud Computing, pp. 21–45. Springer, Boston (2010)
7. Al-Dhuraibi, Y., Paraiso, F., Djarallah, N., Merle, P.: Elasticity in cloud computing: state of the art and research challenges. IEEE Trans. Serv. Comput. **11**(2), 430–447 (2018)
8. Malik, S.U.R., Khan, S.U., Ewen, S.J., Tziritas, N., Kolodziej, J., Zomaya, A.Y., Malluhi, Q.M.: Performance analysis of data intensive cloud systems based on data management and replication: a survey. Distrib. Parallel Databases **34**(2), 179–215 (2016)
9. Kapoor, S., Dabas, C.: Cluster based load balancing in cloud computing. In: Eighth International Conference on Contemporary Computing (IC3), pp. 76–81. IEEE, Aug 2015
10. Dabas, C., Gupta, J.P.: A cloud computing architecture framework for scalable RFID. In: Proceedings of the International MultiConference of Engineers and Computer Scientists, vol. 1, Mar 2010
11. Zheng, Z., Xie, S., Dai, H.N., Wang, H.: Blockchain challenges and opportunities: a survey. Work Paper (2016)
12. Cachin, C.: Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310, July 2016
13. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: IEEE International Congress on Big Data (BigData Congress), pp. 557–564. IEEE, June 2017
14. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)

15. Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., Liu, W.: Study and application on the architecture and key technologies for IOT. In: International Conference on Multimedia Technology (ICMT), pp. 747–751. IEEE, July 2011
16. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. **82**, 395–411 (2018)
17. Uckelmann, D., Harrison, M., Michahelles, F.: An architectural approach towards the future internet of things. In: Architecting the Internet of Things, pp. 1–24. Springer, Berlin (2011)
18. Kraijak, S., Tuwanut, P.: A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends (2015)
19. Al-Fagih, A.E., Al-Turjman, F.M., Alsalih, W.M., Hassanein, H.S.: A priced public sensing framework for heterogeneous IoT architectures. IEEE Trans. Emerg. Top. Comput. **1**(1), 133–147 (2013)
20. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A taxonomy of blockchain-based systems for architecture design. In: IEEE International Conference on Software Architecture (ICSA), pp. 243–252. IEEE, Apr 2017
21. Khan, R., Khan, S.U., Zaheer, R., & Khan, S.: Future internet: the internet of things architecture, possible applications and key challenges. In: 10th International Conference on Frontiers of Information Technology (FIT), pp. 257–260. IEEE, Dec, 2012
22. Zhou, L., Chao, H.C. Multimedia traffic security architecture for the internet of things. IEEE Netw. **25**(3) (2011)
23. Dabas, A.C., Balhara, B.M., Gupta, C.J.P.: CDMA based anti-collision deterministic algorithm for RFID tags. Int. J. Recent Trends Eng. **1**(1), 603 (2009)