Research online Publishing
www.ronpub.com

Open Access

Open Journal of Internet of Things (OJIOT)
Volume 7, Issue 1, 2021
http://www.ronpub.com/ojiot
ISSN 2364-7108

Building Next Generation IoT Infrastructure for Enabling M2M Crypto Economy

Suat Mercan, Kemal Akkaya

Department of Electrical and Computer Engineering, Florida International University,
10555 W Flagler St., Miami, FL, USA, {smercan, kakkaya}@fiu.edu

Abstract

As Bitcoin and other cryptocurrencies are becoming part of our lives, there is a growing interest to enable using them in our daily lives even for micropayments. This interest stems from many factors including privacy, convenience and overhead/fraud that comes with credit cards. In this regard, Internet of Things (IoT) devices can also benefit from this feature for enabling touchless payments for users. However, there is even a bigger opportunity there considering the nature and diversity of very large-scale unattended IoT devices. The integration of any IoT device with blockchain including cryptocurrencies and smart contracts can trigger a machine-to-machine (M2M) economy revolution by streamlining business among IoT devices. Under such a future business model, IoT devices can autonomously request a service and make a payment in return. Such a large-scale ecosystem should rely on various components thus requiring a paradigm shift on the current design and understanding of the IoT systems. In particular, decentralized architecture of blockchain with cryptocurrency and smart contract capability can be a key enabler. In this vision paper, we advocate the need and necessary elements of a M2M crypto economy infrastructure and investigate the role of blockchain in realizing this vision. We specifically focus on the advantages and challenges of blockchain-based systems along with the existing proposed solutions. We then offer several future directions in creating such a M2M economy.

Type of Paper and Keywords

Visionary paper: *Internet of Things, M2M economy, cryptocurrency, smart contract*

1 Introduction

Internet of Things (IoT) has been penetrating into our lives increasingly in the last decade in various domains from agriculture to tourism [7, 13, 14]. Currently, the estimation for the number of IoT devices already deployed in different applications is around 20 billion [2]. There is already many standards related to IoT to regulate their operations, security and reliability. The diverse set of IoT devices made it possible to bring their capabilities to layman (smart home technologies) while the resources for some of them are increasingly enriched to run more sophisticated applications that may rely on AI/ML and crypto technologies.

This paper is accepted at the *International Workshop on Very Large Internet of Things (VLIoT 2021)* in conjunction with the VLDB 2021 conference in Copenhagen, Denmark. The proceedings of VLIoT@VLDB 2021 are published in the Open Journal of Internet of Things (OJIOT) as special issue.

Thanks to such sophistication and prevalence, we are about to witness a new phase where IoT devices can autonomously exchange payment in return of service such as parking, vehicle charging, utility billing, tolling, sensor data sale as shown in Fig. 1, which is called machine-to-machine (M2M) economy [12]. This requires an ecosystem that supports service discovery, seamless interaction among heterogeneous devices, reliable service delivery and micro financial transactions among potentially millions of IoT devices. In such an economy, *decentralization* will be a key characteristic to have a self-managed system without relying or trusting on third parties (such as banks) and dealing with their management. In this sense, *blockchain* offers great potential as it relies on distributed ledger technologies providing decentralized management of cash without trusting any third parties [15]. Therefore, rather than relying on digital cash [5], cryptocurrencies offer a great potential as the underlying money type which can also handle the scalability issue with the decentralized approach. Consequently, the vision is to build a new large-scale overlay infrastructure on top of the existing IoT infrastructure that will smoothly offer cryptocurrency micro-payments as shown in Fig. 1.

Nevertheless, pursuing such a direction will bring back a well-known debate on large-scale IoT or sensor networks on the identification of the IoT devices. When sensor networks were first introduced in the early 2000s [4], majority of the research was following the TCP/IP-based paradigm where each source (e.g., sensors or IoT devices) would have a unique address (i.e., IP address or similar). In this way, these devices can become part of a network and communicate with other devices using these logical addresses to exchange data. However, the limited resources available on IoT devices posed a lot of challenges on using IPv4 and later IPv6 addresses which led to a lot of research on how best integrate them with IoT protocols for scalability purposes [10]. Later, however, there has been a growing interest on a *data-centric* paradigm where applications are only interested in the data generated by IoT devices rather than their addresses. This led to creation of a new paradigm called *named data networking (NDN)* that utilizes queries looking for specific IoT data content [22]. In particular, this approach was promising in dealing with very large scale sensor databases or IoT networks. Nevetheless, realization of M2M economy vision will require a paradigm shift in this context to uniquely identify objects since payments should be directed to specific accounts. In other words, when transactions come into play, our understanding of IoT infrastructure will need to change significantly to offer addressability, reliability, accountability, security, privacy and quality of services (QoS).

We recognize that these features will be dictated by transactions among IoT devices that will be mostly micro-payments. As they will be a crucial part of this ecosystem, it is important to start working on the creation of an efficient and convenient payment model. First of all, a very large-scale IoT network that consists of millions/billions of devices will generate a huge number of data points and payment requests, which is difficult to handle with centralized architectures. Current infrastructures and payment methods may not respond to the requirements of such large-scale network. Specifically, existing digital payment systems suffer from several challenges when considered in this context: Transaction fees are relatively high for micro payments, centralized management violates user anonymity and privacy, and the systems are very susceptible to fraud. Therefore, we advocate blockchain as an alternative with its decentralized architecture along with cryptocurrency and smart contract features to help create a M2M economy by addressing the aforementioned problems. Nevertheless, popular blockchain-based cryptocurrencies and smart contracts, such as Bitcoin and Ethereum, are not directly applicable to the IoT domain. First of all, they are not compatible with resource-constrained IoT devices as their computation and storage requirements are typically high. Second, throughput (transaction per second) and latency are not satisfactory to meet the requirements for business. Nevertheless, with continuing research efforts to solve these problems, a successful integration seems possible and promising.

Therefore, in this vision paper, we would like to bring this promising topic to attention of the community. We first discuss various aspects of the envisioned M2M crypto economy in high level to enable further discussions and try to shed light on its potential applications. Blockchain based cryptocurrency and smart contract are emphasized as emerging concepts to address some of the challenges facing the realization of an overlay network on top of IoT infrastructure to support this M2M ecosystem. We discuss some of the existing preliminary efforts but mainly we turn our attention to numerous open issues that need to be further investigated in line with the challenges of IoT devices and networks.

The remainder of this paper is organized as follows: Section II gives preliminaries. In Section III, we explains practical challenges while Section IV discusses existing efforts. Section V presents open issues and future directions and Section VI concludes the paper.

2 Background

Before getting in to the components of an IoT infrastructure to support M2M crypto economy, we provide some background for understanding the concepts.

2.1 Blockchain

Blockchain is the underlying concept of cyrptocurrency, which is a list of records called blocks linked together

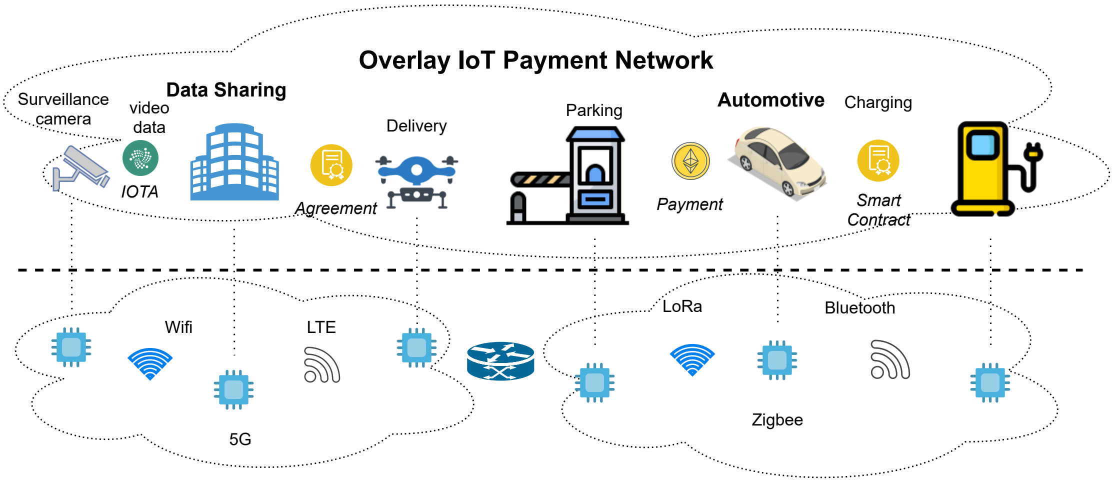


Figure 1: Devices communicate for service agreement and payment on top of existing infrastructure

with the hash of the previous block [15]. The list of blocks continues to grow with the addition of new ones as it is not possible to delete existing blocks. It provides a transparent and public ledger hosted jointly by the participants. A block is simply comprised of transactions (data), timestamp, nonce, the hash of the current block and the hash of the preceding block as shown in Fig. 2. All the blocks in chain structure are distributed among the nodes which have to agree on the state of the blockchain by using a consensus protocol for the approval of a block. This makes it nearly impossible to modify any data that has been written. This working scheme of blockchain carries unique properties such as elimination of central authority trust, immutability of record. Blockchain is classified as public and private based on user participation policy. While public blockchains are open to anyone, private (permissioned) blockchains are established by a group of stakeholders who are only allowed to make transactions. Two important applications of blockchain are cryptocurrency and smart contract as explained next.

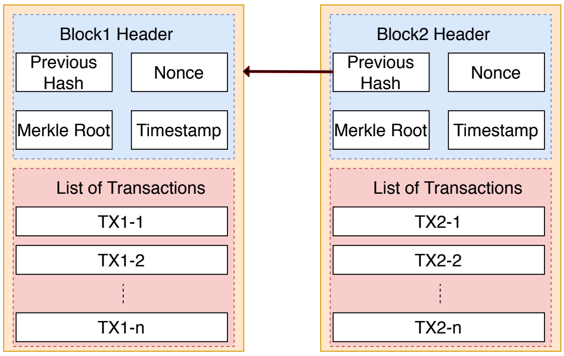


Figure 2: Blockchain representation

2.2 Cryptocurrency

The most common application of blockchain is cryptocurrency which is a cryptographically secure and verifiable currency. This makes it nearly impossible to counterfeit and double spend. The cryptocurrencies are generated by their corresponding blockchains. It can be transferred from one person to another to purchase a service or good as well as to pay for the transaction fee to the miners who are responsible for producing and verifying the blocks. Basically, they receive fees from users to include their transactions in the blockchain. This is an incentive for miners to perform the mining task. The main difference from fiat currency is that there is no authority such as central banks that manages the issuance and value. This lures people as it makes value transfer easy although it raises concerns from the government perspective for accountability purposes. The global cryptocurrency market cap is around $2.4T as of writing this paper [1]. Bitcoin is the first blockchain-based cyrptocurrency and its current market cap as exceeded $1T. It is followed by Ethereum with $350B valuation. Since the emergence of Bitcoin in 2011, many other coins followed the trend with various features and capabilities. There are currently around 4K different cryptocurrencies in the market.

2.3 Smart Contract

A smart contract enables participant to define rules which will be enforced by the network participants collectively [8]. The joining parties will interact under the defined rules to execute the protocol. It provides mechanisms to embed governance rules in verifiable way that can be audited by the consensus algorithm. The smart contract will be executed if/when preconditions are met without any third party involvement which makes the process fast and reliable. They can be used in peer-to-peer transactions such voting, legal testament etc. For instance, the fund is released from escrow account when a service is provided or ownership of an asset is transferred. Blockchains allow developing complex contracts with their programming environment to define conditions and exceptions in detail. Discrepancies in regular bookkeeping methods may take weeks to resolve; smart contract with its transparent and distributed structure can help for dispute resolution.

2.4 Applications for IoT Micro-Payments

In the last decade, IoT devices started to become standard consumer electronics in homes such as thermostats, smart TVs, electric plug-ins [23] in addition to urban IoT applications in cities and other areas [9]. While they are typically used to collect data or serve for some specific purposes, there is also increasing interest for them to request from or provide services to other similar devices in return for cash. For example, imagine a scenario where a printer can order its supplies by itself when the cartridge is nearing its life. Similarly, a fridge may request refill for some items or order them from the grocery store without any human intervention. An electric autonomous vehicle may pay for charging and tolls automatically. Self-driving trucks can communicate to infrastructure or other vehicles to form a platoon which will reduce the energy consumption and labor cost. A smart meter in a home can pay the utility bill automatically at the end of each month.

There may be mixed scenarios where humans can be in the loop too. For instance, people can share their smart phones' resources such as computation power, data, charge, Internet with a payment incentive that is exchanged among the phones automatically. Smart city applications may also benefit from this integration. For instance, drones can play a significant role in delivery, which can be rented by people through their on-board payment reception system and smart contracts. Their video recording can be sold to users/businesses, who are interested in this service.

All these examples point out to a future where we will witness many use-cases of IoT involvement for payments that will eventually form the backbone of a M2M economy. Preferring cryptocurrencies as the payment method will provide a lot of flexibility and automation. Therefore, a successful integration of IoT and cryptocurrencies will be a crucial element of this envisioned M2M economy.

3 Challenges of Enabling a M2M Crypto Economy

The vision for M2M Crypto Economy requires building an underlying infrastructure to support its services. This infrastructure will need to be built on top of existing TCP/IP IoT infrastructure as an *overlay network* that will provide communication and payment services as was shown in Fig. 1. However, building such a large-scale overlay network will pose many challenges exacerbated with the limitations of current blockchain solutions. In the balance of this section, we elaborate on these challenges.

3.1 Interoperability

Realization of a reliable system with necessary functionalities will require new approaches in terms of connectivity in addition to implementing new features. IoT devices are heterogeneous that are using different types of protocols for communication. While this problem is not new within the IoT context, the challenge is to address it with non-invasive solutions so that the existing IoT protocols and solutions are preserved. As such, interoperability will still become one of the implementation issues to be solved.

In addition, there is also interoperability among coins not just protocols. Specifically, different types of cryptocurrencies might be owned by these devices. This raises cross-chain and compatibility issues among blockchains as their consensus and security levels are different. This necessitates a framework to enable them working together.

3.2 Scalability

Considering variety and density of IoT devices interacting in M2M system, this will generate incredibly high number of transactions to handle. Moreover, it is very difficult for traditional payment systems to process in timely manner as it has to check sender balance each time. On the other hand, current popular blockchains, Bitcoin and Ethereum, are much less efficient in terms of transaction per second (tps) and confirmation time. For example, Bitcoin has around 60 minutes of waiting time for finalizing a transaction and can process 7-9 transaction per second. This makes it necessary to come up with scaling architectures in terms of tps. Designing a new coin from scratch that is scalable is not helpful since the market is already dominated with other established coins so solutions should instead address integrating both options.

3.3 Micro-Payment vs. Transaction Fee

Service exchange among IoT devices may require micro-payments which is generally considered to be less than $10. In this case, transaction fee may become bigger than actual payment amount. This makes infeasible to accommodate micro-payments especially if it goes to level of pennies. With the recent increase in Bitcoin value, transaction fee exceeded $20 as of writing. To make the system attractive with respect to credit card based solution, these fees need to be cut down to almost zero.

3.4 Resource Constraints for IoT Devices

Although IoT devices are heterogeneous, most of them are typically characterized with limited resources. This renders running traditional security protocols and blockchain systems on these devices impractical. For instance, in order to be part of a blockchain system, its software needs to run on a device. For instance, 250 GB storage is required for running a full Bitcoin node. IoT devices are not be capable of running a full Bitcoin node. Although there are various solutions to create lightweight versions and simplified payment verification (SPV) [15], it is still difficult to run on many IoT devices.

3.5 Physical IoT Security

Computer systems are physically secured in a data center, however, IoT devices might be unattended and they might be easily captured/damaged by malicious actors. This might endanger the data security in the system. Blockchain presumably ensures data integrity once the data has been inserted into the system. However, the data acquisition method, its hardware and software are vulnerable to various errors and attacks. False data may be injected if the private key used by a user is compromised by a malicious entity.

3.6 Legal and Business Issues

Blockchain based smart-contracts and cryptocurrencies are not regulated by the law. Although the system supposed to eliminate third party and be the trusted source for dispute resolution, it is not certain how to address if any discrepancy appears. For instance, a payment is made based on the input that the service is provided. Since the payment is irreversible, it is not possible to claim refund. Moreover, smart contracts on blockchain are not legally binding and enforceable by law. Another major issue is the taxation. Currently, there is no tracing capability of cryptocurrency flow between people and thus it is not possible to charge sales tax. How to deal with the taxation when an IoT device makes a transaction that will be automatically reported to a central location as well as not lost. This will raise many issues that may significantly impact the design.

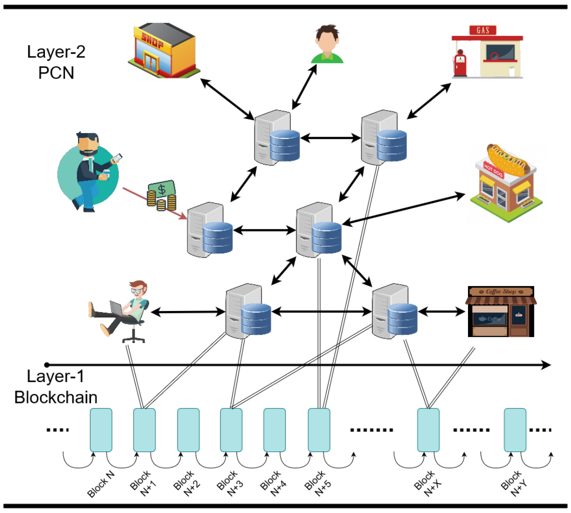


Figure 3: Payment Channel Network concept

4 Preliminary Efforts

There has been intensive efforts and out-of-box ideas to address some of the challenges listed in the previous section in the context of several applications. As they might be useful for the envisoned M2M ecosystem, we briefly summarize these efforts below.

4.1 Offchain Concept for Scalability

The main issue with major blockchain systems is scalability as the number of transactions to be processed is limited. To this end, *offchain* concept has been proposed. It basically enables execution of transactions without writing to the main blockchain with near instant delay and limitless number of transactions. An offline channel established among two users is extended to Payment Channel Networks (PCN) by forming a network of many users as seen in Fig. 3. Any two nodes can exchange fund through intermediate nodes without having a direct offchain channel. The idea has been found promising as it addresses the major issues, which are latency, throughput and high transaction fee. Lightning Network (LN) [17] is a prominent example to this concept and it has received great attention recently. However, running LN still requires hosting Bitcoin node and LN software, which is not feasible for an IoT device.

4.2 IoT Integration with Trusted Gateways and Light Clients

Limited resource on IoT devices restricts the use of blockchain as it requires high computation and storage. One solution to this problem is using a gateway to connect lightweight devices to the rest of the blockchain. IoT device basically relies on a gateway which broadcasts transactions to blockchain on its behalf [16]. The communication between these two entities can be provided using a wireless connection in a secure manner. For instance, Bitcoin client API is utilized to establish this scheme. Hyperledger [6], a popular private blockchain supported by IBM, employs similar approach to collect information from IoT devices. Light client [19] is an alternative method to embrace resource constrained devices. They host the only the block header instead of full block and they use Simplified Payment Verification (SPV) for transaction verification. Electrum and Bitpay are some popular examples. However, full nodes still need to exist to maintain the system. Direct integration scheme either through a gateway or using light client solely does not solve blockchain's existing challenges. Nevertheless, it facilitates the IoT device to take place in the ecosystem. Although there is no silver bullet to solve all the challenges mentioned previously, this scenario might be viable for many applications.

4.3 New Blockchains for Resource Constrained IoT

Various blockchain designs have been proposed with alternative Proof-of-Work (PoW) and architecture to relax heavy resource requirements. For instance, Ethereum is switching to Proof-of-Stake (PoS) [3] from PoW to increase scalability and make it less resource demanding. Similar approaches have been adopted to replace energy consuming mining with validation based on reputation or stake. This type of shift is criticized as it may degrade the security level in the *blockchain trilemma*. DAG-based (Directed Acyclic Graph) structures, called *Tangle*, led by IOTA proposes parallel confirmation of transactions instead of single chain [18]. A transaction must be confirmed by a certain number of succeeding transactions (Fig. 4). Since the structure grows as a tree, it is supposed to provide better scalability with higher number of transactions. Moreover, *side-chain* idea is introduced to enable transaction execution outside of the main-chain. It is basically a separate blockchain with its own consensus algorithm and security level. Two blockchains are linked with *two-way peg* using a lock mechanism which can be used to transfer an asset in both ways. As opposed to the state channels (offline channels), transactions are broadcast to the rest of the side-chain network. A compromise in the side-chain will be confined to it.

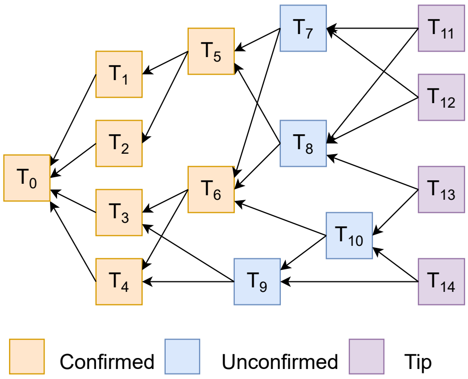


Figure 4: Directed Acyclic Graph

5 Future Research Issues

As can be seen from the above discussions, the vision for an M2M crypto economy still requires a lot of new research to address the shortcomings and introduce the needed features. In this section, we discuss some future research issues that need to be tackled to realize the M2M crypto economy vision.

5.1 Device Identification

Existence of financial transactions among objects/devices requires clear identification of devices to direct the payment to the correct service provider. This means that implementing M2M economy would require us re-think data-centric approaches (i.e., NDN) in IoT and perhaps go back to original address-based approaches, which means paying attention to address management and scalability issues. This is because, now we need to be able to identify every source and hold them accountable whenever needed due to execution of financial transactions. In particular, with the transitioning to IPv6, the address space is becoming even bigger to bear by the IoT devices with limited storage. Another direction could be to explore approaches to co-exist with data-centric approaches. Obviously, this will bring a lot of new challenges within the M2M economy context.

5.2 Networkless Payment

Current cashless payment systems depend on Internet connectivity where the intermediary such as Visa verifies the balance and transfer occurs between accounts. Blockchain-based payment also requires to be online for transaction execution. However, devices may have intermittent connectivity or no connection in some regions or cases such as after a disaster. In such situations, it is important to be able to resume the payment system execution among IoT devices. Cryptographic token based coins using trusted execution environment is among the studies to address this problem [21]. Signing smart contract and payment in offline mode to be executed later with available Internet connection can be another direction to be investigated.

5.3 Cross-Chain Operations

Although many existing coins will disappear, it is foreseen that multiple coins will survive. As each of them has different features and requirements, they may serve for different uses cases. When it comes to interaction between different types of currencies, it is needed to do conversion and data exchange. A broker-like system may be an intermediate digital asset exchange operation between end-user accounts. However, this scheme depends on a trusted third party to hold funds. Atomic swaps are one of the proposed solutions that utilizes Hash Time Lock Contracts to perform exchange between some specific cryptocurrencies [11]. Handling cross-chain operation efficiently and securely under different consensus algorithms and architectures is an open issue to further investigate. This will also impact the scalability of the M2M ecosystem since there are many coins designed for scalability that can be integrated with Bitcoin in a hierarchical manner.

5.4 Alternative Approaches

As scalability remains as the main obstacle for adoption of cryptocurrency for micropayments, new designs and alternative approaches will be investigated further. PCN is a promising approach attracting more attention from community. For instance, LN of Bitcoin can handle near real-time transactions and it grew to more than 10,000 users in two years. Nevertheless, it still has issues regarding its scalability, reliability and fees. Therefore, more studies are likely to emerge targeting more efficient, secure, privacy preserving and sustainable systems. In this respect, DAG with its tree alike structure seems another strong alternative to block-based single chain.

5.5 Low-Cost Trusted Execution Environments

Solutions for secure execution and protection against key compromise within a device already exist in the industry, which are known as trusted execution environments (TEE) [20]. However, they are not feasible to adopt in all devices since they are not cost-effective and sometimes come with additional hardware. Efforts to provide cheaper methods for hardware security will be one direction to be explored in order to realize reliable and secure infrastructure.

5.6 Accountability vs Privacy

Interest in blockchain and cryptocurrency from public and institutions such as banks, retailers etc. proves the confidence in its potential. It also indicates that they will be part of the future. Thus, governments will be interested in regulating this area to hold people accountable in the case of needs. While the decentralized nature is the main attractive point especially for cryptocurrency, the desire and need to put them under control to prevent tax evasion and funding of criminal activities by tracing money flow will be clashing points in the future.

6 Conclusion

In this paper, we drew attention to an emerging and promising concept that motivates the need for building a new large-scale overlay payment network among IoT devices. With wide adoption of IoT devices and improvement in crypto technologies, such an overlay payment network is unavoidable where the IoT devices can act as autonomous entities and get involved in financial transactions, eventually forming an M2M economy. We highlighted the importance and advantages of blockchain and cryptocurrency ideas as well as their challenges for implementing this M2M vision. We envision that intense research efforts in addressing existing problems will lead to a successful realization of M2M crypto economy.

References

[1] "Coin marketcap," https://coinmarketcap.com/all/views/all/, accessed: 2021-05-06.

[2] "Internet of things (iot) and non-iot active device connections worldwide," https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/, accessed: 2021-05-05.

[3] "Proof-of-stake," https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/, accessed: 2021-05-06.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE*

Communications magazine, vol. 40, no. 8, pp. 102–114, 2002.

[5] M. D. Bordo and A. T. Levin, "Digital cash: Principles & practical steps," National Bureau of Economic Research, Tech. Rep., 2019.

[6] C. Cachin *et al.*, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, 2016, p. 4.

[7] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things journal*, vol. 1, no. 4, pp. 349–359, 2014.

[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[9] A. Gaur, B. Scotney, G. Parr, and S. McClean, "Smart city architecture and its applications based on iot," *Procedia computer science*, vol. 52, pp. 1089–1094, 2015.

[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[11] M. Herlihy, "Atomic cross-chain swaps," in *Proceedings of the 2018 ACM symposium on principles of distributed computing*, 2018, pp. 245–254.

[12] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia computer science*, vol. 98, pp. 461–466, 2016.

[13] K. Lakhwani, H. Gianey, N. Agarwal, and S. Gupta, "Development of iot for smart agriculture a review," in *Emerging trends in expert applications and security*. Springer, 2019, pp. 425–432.

[14] S. Mercan, L. Cain, K. Akkaya, M. Cebe, S. Uluagac, M. Alonso, and C. Cobanoglu, "Improving the service industry with hyper-connectivity: Iot in hospitality," *International Journal of Contemporary Hospitality Management*, 2020.

[15] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, 2008.

[16] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based iot with ethereum, swarm, and lora: the software solution to create high availability with minimal security risks," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 28–34, 2019.

[17] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[18] S. Popov, "The tangle," *cit. on*, p. 131, 2016.

[19] E. Reilly, M. Maloney, M. Siegel, and G. Falco, "An iot integrity-first communication protocol via an ethereum blockchain light client," in *2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT)*. IEEE, 2019, pp. 53–56.

[20] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: what it is, and what it is not," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 57–64.

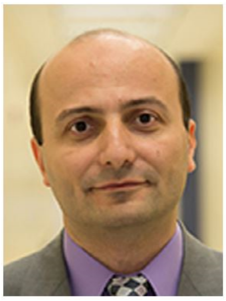
[21] P. D. B. A. G. P. S. H. Samudrala, Arun and W. Drewry, "Networkless mobile payments with minimal changes in trusted execution environments," *Technical Disclosure Commons*, 2021.

[22] W. Shang, A. Bannis, T. Liang, Z. Wang, Y. Yu, A. Afanasyev, J. Thompson, J. Burke, B. Zhang, and L. Zhang, "Named data networking of things," in *2016 IEEE first international conference on internet-of-things design and implementation (IoTDI)*. IEEE, 2016, pp. 117–128.

[23] H. Thapliyal, "Internet of things-based consumer electronics: Reviewing existing consumer electronic devices, systems, and platforms and exploring new research paradigms," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 66–67, 2017.

Author Biographies

Suat Mercan is postdoctoral researcher at Florida International University. He received Ph.D. degree in Computer Science at University of Nevada-Reno (UNR), Reno, NV in 2011 and M.S degree in Electrical and Computer Engineering from University of South Alabama (USA), Mobile, AL in 2007. His main research interests are blockchain, payment channel networks, cybersecurity and internet of things. He serves on the TPC of networking and blockchain conferences including ICBC and LCN.



Dr. Kemal Akkaya is a full professor in the Department of Electrical and Computer Engineering at Florida International University. He received his PhD in Computer Science from University of Maryland Baltimore County in 2005 and joined the department of Computer Science at Southern Illinois University (SIU) as an assistant professor. Dr. Akkaya was an associate professor at SIU from 2011 to 2014. Dr. Akkaya leads the Advanced Wireless and Security Lab (ADWISE) in the ECE Dept. His current research interests include security and privacy, IoT, and cyber-physical systems. Dr. Akkaya is a senior member of IEEE. He is the area editor of Elsevier Ad Hoc Network Journal and serves on the editorial board of IEEE Communication Surveys and Tutorials. Dr. Akkaya was the General Chair of IEEE LCN 2018 and TPC Chair for IEEE ICC Smart Grid Communications. He has served as the guest editor for many journals and in the OC/TPC of many leading network/security conferences. He has published over 230 papers in peer reviewed journal and conferences. He has received “Top Cited” article award from Elsevier in 2010.