Convergence of IoT and Blockchain technologies, for securing human life

Authors

Arshak Babayan
Samsung IoT Academy (Moscow)
Moscow Technological University(MIREA)
National Polytechnic University of Armenia
National Instruments (NI)
5G Research Group (Yerevan)
Moscow/Yerevan 2018
Email: arshbabayan@mail.ru

Tigran Hakhunts
Russian Presidential Academy of National Economy and Public Administration
Yerevan State University
Moscow/ Yerevan 2018
Email: tigran.hakhunts@gmail.com

Abstract - In the Internet of Things (IoT), the blockchain and, in general, Peer-to-Peer approaches could play an important role in the development of decentralized and data intensive applications running on billion of devices, preserving the privacy of the users. Our work whether the blockchain and Peer-to-Peer approaches can be employed to foster a decentralized and private-by-design IoT.

In this paper we present the result of symbiosis between two leading technologies nowadays - IoT and blockchain. We will present an existing problem and make an offer to resolve it. There will be a new software that will help to ensure people's lives. The essence of the program is the following. People who use smart phones, that have the ability to capture photo or video anywhere, at any time, and having our software installed on the phone, in any complicated or dangerous situation, only by joining the program, the current status of the user will be immediately shared among the users of the system, even with law enforcement authorities. The system will provide the opportunity to show immediate assistance to the ambulance services, and if there is necessity for police intervention, the overall information about the accident will be quickly sent to them accordingly. Project users will be individuals and they will have an opportunity to create a smart contract with any service and agency that will be included in the project database. Having partnerships with ambulance, police authorities, security agencies, law centers, human rights defenders and other services, the project will also have a variety of usage. The crashed driver will be immediately provided with assistance, and insurance agencies will have the ability to analyze all the necessary preliminary data and make an immediate decision.

The use of blockchain technology will help to secure data storage and transfer, identification and transfer of IoT technology data.

Project benefits and highlights

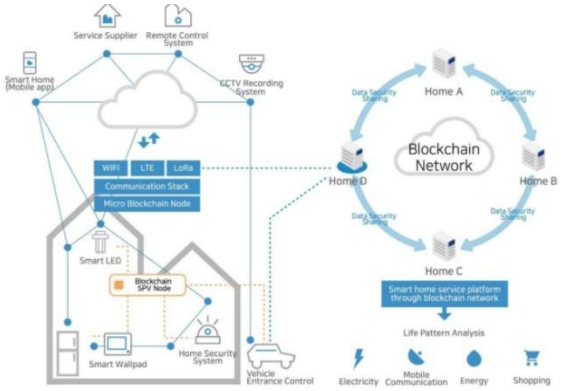
1. Ensuring the safety of people's life,
2. Avoiding data fraud,
3. Reduction of corruption Risks,
4. Ensuring immediate intervention by law enforcement agencies;
5. Making the exact decision,
6. Human rights protection anywhere in the world,
7. System usage will help to disclose terror threats

We review how this mechanism works and also look into smart contracts—scripts that reside on the blockchain that allow for the automation of multi-step processes. We then move into the IoT domain, and describe how a blockchain-IoT combination, facilitates the sharing of services and resources leading to the creation of a marketplace of services between devices.

Keywords - Blockchain, smart contracts, internet of things,

INTRODUCTION

As defined by ITU [1], the Internet of Things (IoT) refers to the network of numerous physical objects (20 billion by 2020, according to Gartner [2]) which are provided with Internet connection. Such devices acquire information about the surrounding environment, and they communicate with each other and with software systems through the Internet. As a consequence of such rich interaction, they also produce a large amount of data, in turn usable to enable dependent The blockchain is a P2P ledger, firstly used in the Bitcoin cryptocurrency [4] for economic transactions. It is tamper-proof and contains only authentic information; in addition, since it is P2P, it is not controlled by any single centralized entity. For these reasons, cryptocurrencies are just one of the possible applications of this technology. The blockchain is a P2P ledger for transactions. To issue transactions, public key cryptography is employed. A user isprovided with a public and a secret key: the secret key is used for signing transactions, while the public one is used as address in the system. So, no real-world identity is needed for transactions: this is a form of pseudonymity. Transactions are relayed in the P2P network and some peers, called miners, collect them together into a data structure, called block.



1.Pic. IoT and Blockchain combination

Once a new block is assembled, it is relayed in the P2P network and, if valid, is chained to the current last block of the blockchain. Each block contains a reference to the previous block. After some time a block is stored the blockchain, the transactions of the block are considered confirmed. A block is valid if it contains valid transactions and if miners have performed a computationally-hard puzzle, which consists in finding an hash of the block lower than a predefined target. The miner which adds the next block to the blockchain is the first which has assembled a valid block and has found a valid solution to the puzzle. This specific mining technique is called Proof-of-Work (PoW). The PoW allows to achieve distributed

consensus, which means that all nodes agree on the same version of the blockchain and this blockchain contains valid transactions. Forks could happen in this chain of blocks, that is, there could be two contrasting branches of the chain. However, thanks to PoW, eventually one of the branches should be discarded and all nodes should agree on the same blockchain. In case of forks, the rule is that miners extend the longest branch or the one that has the most difficult PoW. Moreover,
thanks to PoW, the blockchain is hard to be tampered.
Blockchains have recently attracted the interest of stakeholders across a wide span of industries: from finance [1] and healthcare [2], [3], to utilities [4], real estate [5], [6], and the government sector [7]. The reason for this explosion of interest: With a blockchain in place, applications that could previously run only through a trusted intermediary, can now operate in a decentralized fashion, without the need for a central authority, and achieve the same functionality with the same amount of certainty. This was simply not possible before. We say that the blockchain enables trustless networks, because the parties can transact even though they do not trust each other. The absence of a trusted intermediary means faster reconciliation between transacting parties. The heavy use of cryptography, a key characteristic of blockchain networks, brings authoritativeness behind all the interactions in the network.



Pic.2 Smart Contracts technology using IoT and Blockchain

Smart contracts –self-executing scripts that reside on the blockchain– integrate these concepts and allowfor proper, distributed, heavily automated workflows. This should make blockchains enticing to researchers and developers working in the Internet of Things (IoT) domain. Of course the transition to a decentralized network may not always make sense. On top of that, even if such a transition is desirable, the application's requirements may be such that a blockchain-based network cannot fulfil them. Blockchains and smart contracts bring a slewof advantages to the table, but as we will see, they also come with a bag of disadvantages. The goal of this work is to provide a detailed description
of how blockchains and smart contracts work, to identify the pros and cons that their introduction brings to a system, and highlight the ways the blockchains and IoT can be used together. This will allow the reader to identify potentially new use cases for their IoT work, and also make educated decisions when integrating a blockchain in their project. The paper is structured as follows. In Section II we examine what a blockchain is, how a blockchain network operates, and how smart contracts allow us to radically redefine how interactions between transacting parties on a network can be set up and automated[6].

Integrating the block chain technology with IoT gives us various benefits such as:

- A decentralized system where the ledger will be distributed to every entity on the network
- A trust system which does not require the entities to know each other on the platform
- The ability to provide micro transaction services at considerable speeds due to the elimination of the "middle-man". The collected data can be solved to companies.
- The ability to backtrack previous activities with guaranteed validity thus making it easier to make smart contracts.
- A higher difficulty of data being tampered due to the big number of nodes present on the network and the Proof of Work (POW) requiring high computational resources for someone to do so.
- Tracking activities and certifications to their genesis phase, such as a supply chain over its whole process so that any physical outcome is accompanied by a 'digital passport' that proves its authenticity and origin (IBM Watson IoT block chain)[7].
- Sharing of indelible records with regulatory bodies and insurers Can be scaled down to make 'smart home IoT ecosystems', with cryptographic hashes of device firmware stored in a bock chain to reduce verification time

The constructed program allows the following:

This work is based on the IoT and Blockchain technologies. Each year we have numerous losses and injuries because of accidents and quick assistance is urgent to save people. Program named "AR1" registered and starts to work when a hazardous situation is initiates. It will be necessary to connect program and keep camera capturing and recording the accident/situation and the data will be immediately shared and saved by the people registered in the system. In the case of accident when the, first steps of safety are done. During this time the information will be sent to GPS and IoT modules with the help of Blockchain system, after which the coordinates of GPS system through IoT module will send the coordinates of accident in a form of message (picture, video, audio) to rescue services. In rescue centers the coordinates of damaged vehicles will appear on Google map.

CONCLUSIONS AND FUTURE WORK

Regarding the integrity and the adaptability, we found that large blockchain systems like Bitcoin are the most secure, but at the same time Bitcoin scalability issues make it little suitable for the IoT. Regarding the anonymity, we found that in the blockchain only pseudonymity is guaranteed. To address the integrity and the adaptability issues, our future work will consist in testing existing secure and scalable blockchains and in designing a layered architecture for IoT applications on top of the most suitable of them. Moreover, we will investigate mixing protocols and other solutions to achieve anonymity and further protect people's privacy. Data transfer of any kind are usually faster and cheaper for the user when completed via a blockchain, and they also benefit from the protocol's security.
Program code using Blockchain technologies:

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
        begin
        byte state[4,Nb]
```

```
state = in
AddRoundKey(state, w[0, Nb-1])
for round = 1 step 1 to Nr–1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
out = state
                end:
```

The algorithm for decrypting / decrypting has been tested on the LabView (Figure 7) program.

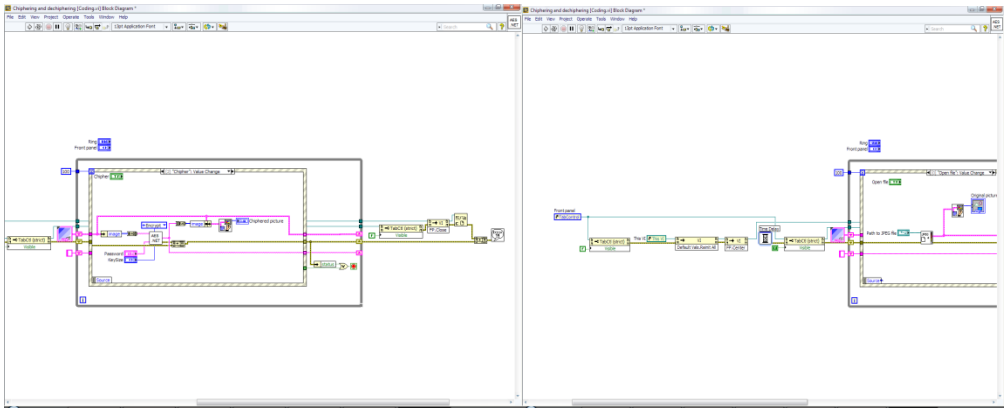


Figure 7. Program code (Block Diagram), [Developed by the author].

```
input:
                cipher input
start:          state at start of round[r]
s_box:          state after SubBytes()
s_row:          state after ShiftRows()
m_col:          state after MixColumns()
k_sch:          key schedule value for round[r]
output:         cipher output:
input:          inverse cipher input
istart:         state at start of round[r]
is_box:         state after InvSubBytes()
is_row:         state after InvShiftRows()
```

ik_sch: key schedule value for round[r]

ik_add: state after AddRoundKey()

ioutput: inverse cipher output:

Process chipping: 128 бит (Nk=4, Nr=10),

iinput = 00112233445566778899aabbccddeeff,

K = 000102030405060708090a0b0c0d0e0f,

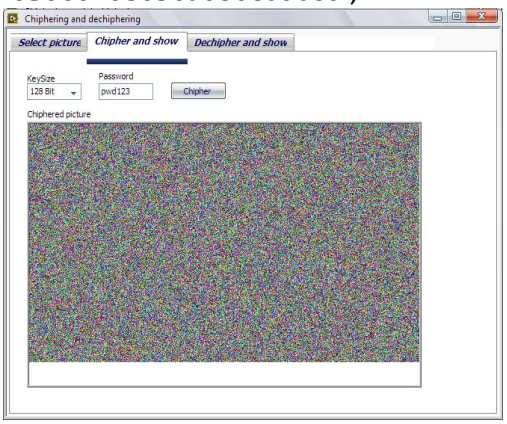


Fig. 8. Process chipping, [Developed by the author].

round[0].input 00112233445566778899aabbccddeeff
round[0].k_sch 000102030405060708090a0b0c0d0e0f
round[1].start 00102030405060708090a0b0c0d0e0f0
round[1].m_col 5f72641557f5bc92f7be3b291db9f91a
round[1].k_sch d6aa74fdd2af72fadaa678f1d6ab76fe
round[2].start 89d810e8855ace682d1843d8cb128fe4
round[2].m_col ff87968431d86a51645151fa773ad009
round[2].k_sch b692cf0b643dbdf1be9bc5006830b3fe
round[3].start 4915598f55e5d7a0daca94fa1f0a63f7
round[3].m_col 4c9c1e66f771f0762c3f868e534df256
round[3].k_sch b6ff744ed2c2c9bf6c590cbf0469bf41
round[4].start fa636a2825b339c940668a3157244d17
round[4].s_box 2dfb02343f6d12dd09337ec75b36e3f0
round[5].start 247240236966b3fa6ed2753288425b6c
round[5].k_sch 3caaa3e8a99f9deb50f3af57adf622aa
round[6].k_sch 5e390f7df7a69296a7553dc10aa31f6b
round[7].start c62fe109f75eedc3cc79395d84f9cf5d
round[7].m_col c57e1c159a9bd286f05f4be098c63439
round[7].k_sch 14f9701ae35fe28c440adf4d4ea9c026
round[8].start d1876c0f79c4300ab45594add66ff41f
round[8].s_box 3e175076b61c04678dfc2295f6a8bfc0
round[9].start fde3bad205e5d0d73547964ef1fe37f1
round[9].s_box 5411f4b56bd9700e96a0902fa1bb9aa1
round[9].k_sch 549932d1f08557681093ed9cbe2c974e
round[10].start bd6e7c3df2b5779e0b61216e8b10b689
round[10].s_row 7ad5fda789ef4e272bca100b3d9ff59f
round[10].k_sch 13111d7fe3944a17f307a78b4d2b30c5

round[10].output 69c4e0d86a7b0430d8cdb78070b4c55a

Reverse decryption process:

round[0].iinput 69c4e0d86a7b0430d8cdb78070b4c55a
round[0].ik_sch 13111d7fe3944a17f307a78b4d2b30c5
round[1].is_row 7a9f102789d5f50b2beffd9f3dca4ea7
round[1].ik_add e9f74eec023020f61bf2ccf2353c21c7
round[2].istart 54d990a16ba09ab596bbf40ea111702f
round[2].ik_sch 47438735a41c65b9e016baf4aebf7ad2
round[2].ik_add baa03de7a1f9b56ed5512cba5f414d23
round[3].is_row 3e175076b61c04678dfc2295f6a8bfc0
round[3].ik_add c57e1c159a9bd286f05f4be098c63439
round[4].is_box c62fe109f75eedc3cc79395d84f9cf5d
round[4].ik_sch 5e390f7df7a69296a7553dc10aa31f6b
round[4].ik_add 9816ee7400f87f556b2c049c8e5ad036
round[5].istart e8dab6901477d4653ff7f5e2e747dd4f
round[5].is_row e847f56514dadde23f77b64fe7f7d490
round[5].is_box c81677bc9b7ac93b25027992b0261996
round[5].ik_sch 3caaa3e8a99f9deb50f3af57adf622aa
round[5].ik_add f4bcd45432e554d075f1d6c51dd03b3c
round[6].istart 36339d50f9b539269f2c092dc4406d23
round[6].ik_add 6385b79ffc538df997be478e7547d691
round[7].istart 2d6d7ef03f33e334093602dd5bfb12c7
round[7].ik_add 4c9c1e66f771f0762c3f868e534df256
round[8].istart 3bd92268fc74fb735767cbe0c0590e2d
round[8].is_row 3b59cb73fcd90ee05774222dc067fb68
round[8].is_box 4915598f55e5d7a0daca94fa1f0a63f7
round[8].ik_sch b692cf0b643dbdf1be9bc5006830b3fe
round[8].ik_add ff87968431d86a51645151fa773ad009
round[9].istart a7be1a6997ad739bd8c9ca451f618b61
round[9].is_row a761ca9b97be8b45d8ad1a611fc97369
round[10].istart 6353e08c0960e104cd70b751bacad0e7
round[10].ioutput 00112233445566778899aabbccddeeff

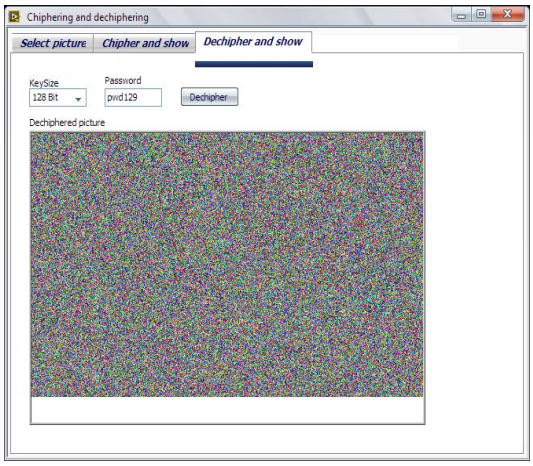


Fig.9. decoding, [Developed by the author].



Fig. 10. Running the program, [Developed by the author].

Through this program every person have opportunity to chipping data (picture, video, audio) and share with emergency services, for helping and for making a true decision.

list of literature

[1] International Telecommunication Union, “Measuring the Information Society Report,” International Telecommunication Union (ITU), Report, 2015. [Online 02.02.2018].

[2] “Gartner Says 6.4 Billion Connected ”Things” Will Be in Use in 2016, Up 30 Percent From 2015,” http://www.gartner.com/newsroom/id/3165317 [Online 02.02.2018].

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf [Online 02.02.2018].

[4]Y. Zhang and J. Wen, “An IoT electric business model based on the protocol of bitcoin,” in ICIN. IEEE, 2015, pp. 184–191.

[5] D. W¨orner and T. von Bomhard, “When your sensor earns money: exchanging data for cash with Bitcoin,” in UbiComp Adjunct. ACM, 2014, pp. 295–298.

[6] Boldyreva, A. Order-Preserving Symmetric Encryption / A. Boldyreva, N. Chenette, Y. Lee, A. O'Neill // EUROCRYPT '09 Proceedings of the 28th Annual International Conference on Advances in Cryptology. -2012. -С. 224-241.

[7] L. Axon, “Privacy-awareness in Blockchain-based PKI,” 2015. [Online 09.02.2018]. Available: http://goo.gl/3Nv2oK

[8] O. Dandash, Y. Wang, P. D. Le, and B. Srinivasan, "Fraudulent Internet Banking Payments Prevention using Dynamic Key," JNW, vol. 3, pp. 25-34, 2008.

Здравствуйте, я 2016 году поступил магистратуру Мирэа, на данный момент учусь на втором курсе на отлично. хочу продолжать обучение в аспирантуре , я договорился с руководителем и выбрали тему кандидатской работы . ниже отправлю документы для получения квоты, пожалуйста посмотрите и ответьте смогу ли я учавствовать в конкурсе без моего присутствия, соглашение от вуза и согласование с руководителем отправлю на этой неделе.