Blockchain for an Alternative GPS

Davut Çulha,
ASELSAN
culha@aselsan.com.tr

***Abstract*—Global Positioning System is very critical for many applications. If it is out of service, there may be chaotic situations for the applications. For this reason, there should be other types of sources for location information. In this work, a blockchain is proposed for location information. Blockchain provides a resilient system, and it can also provide reliable location information. Reliability of location information is also supported by short-range communication. Short-range communication eliminates location information errors outside the communication range. Therefore, it helps to minimize location information errors. In the blockchain, there are special devices to provide location information. The proposed blockchain is a market for location trade with its own cryptocurrency, which is used mostly to incentivize the devices to share location information among themselves. Moreover, the proposed blockchain respect location privacy using encryption mechanism.**

Keywords—blockchain, location information, GPS, internet of things, cryptocurrency, short-range communication, location privacy

I. INTRODUCTION

Many applications have complicated features which are based on location information. These applications consume location information from Global Positioning System (GPS). The features like navigation are indispensable now. Therefore, GPS is very critical for those applications. This increases the risks based on GPS malfunctioning. For this reason, there should be other sources for GPS location information. In this work, a blockchain is proposed for GPS location information. Blockchain can provide reliable data. Also, it is resilient to security attacks.

The proposed blockchain depends on special devices and interactions among them via short-range communication like Wi-Fi. Any system which requests location information will use short-range communication instead of GPS satellites. For this reason, the blockchain should be as widespread as possible. In other words, there should be many devices for the blockchain. In this point, Internet of Things (IoT) overlaps with the proposed blockchain. There should be many IoT devices, which will serve GPS service, and they should cover nearly all the geological surfaces of the World for a widespread utilization.

Short-range communication is important for resilience, and it is also important for reliability of location information. The IoT devices which will serve GPS service will communicate with the other IoT devices using short-range communication channel. The range of the communication will be used to guarantee location information. In other words, the two IoT devices can deceive themselves at most within the range of the communication. In the blockchain, the IoT devices can register to the blockchain after mutually approving their location information. In short, each IoT registration will approve parent IoT devices also, so it will empower the reliability of location information.

The proposed blockchain requires many IoT devices for widespread utilization. Those IoT devices should be active in data sharing and collaboration. For this reason, there should be incentive mechanisms. In this work, the proposed blockchain has its own cryptocurrency, and IoT devices which share information are rewarded with cryptocurrency.

Location information is very critical. Likewise, its privacy is also critical. The proposed blockchain regards location privacy. In the blockchain, location of IoT devices are not revealed. Only the IoT devices will share location information between themselves. Blockchain will keep only encrypted data about location information.

The rest of the paper is structured into sections. In the next section, related work is presented. Then, the proposed blockchain is explained. In the following sections, the main transaction of the blockchain and experimental results are given. In the last section, conclusion is made after discussion.

II. RELATED WORK

Locations of objects are important for many applications. Especially navigation systems depend on location information. GPS provides location information to requesting devices and applications. Therefore, GPS is very critical for numerous applications, and will be very critical for others in the future. If GPS does not function properly or stops services, there should be other sources for location information. Certainly, these sources should provide reliable location information. A special blockchain can be constructed, which can provide a decentralized network for reliable location information without needed GPS satellites. Blockchain was animated firstly with the implementation of Bitcoin [1]. Bitcoin is a monetary system and provides reliable money transfer and reliable accounts in a decentralized manner. Likewise, the GPS blockchain can provide reliable location information.

IoT arouses as number of IoT devices increases. For IoT, there is a special blockchain named IOTA [2]. IOTA is designed for IoT devices which have light computing resources mostly. In this work, some IoT devices request location information from the blockchain, and some special IoT devices answer the requests. The proposed blockchain considers light computing resources of IoT devices. IoT devices interact with the environment directly, which exposes them to security attacks. Communication among IoT devices should be secure and reliable. In [3], a reliable authentication scheme is proposed for IoT devices which are resource constrained. In this work, IoT devices communicate each other directly, and they agree on location information. The agreement is broadcasted to the blockchain, and miners of the blockchain finalize the agreement. In the blockchain,

miners are different from IoT devices to regard light computing resources of the IoT devices.

In [4], reliability of location information is considered. Against fake location information, blockchain is proposed. IoT devices post their location information and location information of their neighbor IoT devices to the blockchain. The blockchain eliminates false location information using location of neighbors and obtains reliable location information. In this work, a tree of neighbors is used for the reliability of location information. In [5], Byzantine fault tolerance (BFT) mechanism is used to eliminate and exclude attackers from the IoT communication network to provide reliable location information.

Data sharing among IoT devices is a must for many applications. However, IoT devices are not willing in sharing data even if a secure system is established. In [6], it is showed that monetary reward mechanisms provide enough data sharing required for proper working of applications. In [7], methods of data sharing among IoT devices are presented. A special part of IoT is Internet of Vehicles (IoV). In [8], security of IoV data is ensured using a blockchain and a special consensus algorithm. In [9], a blockchain with a reward system is proposed for reliable and secure IoV communication. In IoV, data sharing is also a must for efficient working. In [10], a secure blockchain is proposed for data sharing. Reward mechanism gives some cryptocurrency to vehicles according to the participation in data sharing. In this paper, some cryptocurrency is used to incentivize IoT devices which provide location information for data sharing.

IoV data can be used to enable traffic safety and efficiency. Intelligent Transportation Systems (ITS) also require shared IoV data to assure road safety, fast traffic, and minimized traffic jams. In [11], blockchain is used to guarantee correct location information of vehicles, which also assists to detect and prevent security attacks.

Vehicular networks with dynamic networking properties are called Vehicular Ad Hoc Networks (VANETs). Current VANET is centralized. In [12], blockchain-based VANET is proposed to decentralize VANET. The proposed VANET protects identity of vehicles and provides location privacy of vehicles.

In [13], a blockchain-based system is presented for producing proofs of location. Proof of location ensures that location information is correct. A decentralized peer-to-peer blockchain system guarantees correct location information for IoT devices, and it preserves location privacy. In the method, short-range communication like Wi-Fi helps in the verification process of location information. If two IoT devices are able to communicate via short-range communication channel, they guarantee their locations within the range of the communication. In this paper, short-range communication is employed to assure reliable location information.

In [14], location information is used for second factor for authentication. The implementation is done using smart contracts [15]. Smart contracts are expensive for execution and storage. Therefore, the data kept in smart contracts should be small. Enough precision of Virtual Earth's Tiling System [16] can be used to keep location information. Location-based Services (LBSs) becomes more popular day after day. Vehicular networks are good examples of LBSs. Users can benefit from LBSs according to their locations. Therefore, location privacy is very important for these services. Location information should be protected. In [17], location privacy in vehicular networks is analyzed, and technologies are covered to enhance location privacy. In [18], challenges of data integrity are investigated, and a blockchain-based solution is proposed. The solution is implemented using smart contracts. In [19], locations are verified in a peer-to-peer fashion for LBSs. In [20], geofences are used to guarantee correct location information needed for LBSs.

III. THE PROPOSED BLOCKCHAIN

The proposed blockchain is a single-chain blockchain with Proof-of-Work (PoW) consensus mechanism like Bitcoin. The blockchain has its own cryptocurrency called GpsCoin. The blockchain keeps the following types of transactions:

- GpsCoin transfer between accounts
- GPS location ID registration
- GPS location trade

GpsCoin transfer between accounts is common in blockchain systems, which transfers cryptocurrencies between blockchain accounts like in the Bitcoin blockchain.

The proposed blockchain is especially a market for trading location information. IoT devices which want to sell their GPS location information are registered using GPS location ID registration transaction. These type of IoT devices are called GPS IoT devices afterwards. These transactions build a tree of GPS location IDs. The root element of the tree is virtual, and its GPS location ID is 0. Each transaction can be a request to connect to the root element or to an existing GPS location ID as follows:

- Connection request to the root
- Connection request to an existing GPS location ID

For the first type of request, the GPS IoT device creates a request transaction with enough reward GpsCoin. The miners take the request and write it to the blockchain in return for reward GpsCoin. The details of the transaction are as follows:

GPS IoT device named Provider creates a request to connect to the root:

$<G\ L_W\ 0\ N\ K_1\ K_2>$

where

G is the public key of the GPS location ID of Provider,

L_W = Fake GPS location; a random GPS location near Provider,

L_C = Correct GPS location of Provider,

$|L_W - L_C| < 100$ m; distance should be less than 100 m (1)

0 depicts the root element,

N is the amount of reward GpsCoin,

$K_1 = H(G\ L_W\ 0\ N)$,

H(x) is the SHA256 hash of x,
$K_2 = S_G(K_1)$,
$S_y(x)$ is the signature of y on x.

Miners add the transaction to the blockchain:
<G L_W 0 N K_1 K_2 K_3 K_4>
where
M is the public key of the miner,
(2)
T(x,y,n) is a transfer of n GpsCoin from x to y,
$K_3 = T(P, M, N)$,
$K_4 = S_M(K_1\ K_3)$.

For the second type of request, the GPS IoT device creates a request to an existing GPS location ID. In this case, the existing GPS IoT device registered before should approve the request by signing. First, the requester GPS IoT device and the existing GPS IoT device should be close enough to each other. In other words, their distance should be within the short-range communication distance, and it is limited, e.g., at most 100 m. The parent GPS IoT devices approve child GPS IoT devices because their reliabilities will increase by building a big sub-tree. The child GPS IoT device will offer some GpsCoin to the miners for writing the transaction. The details of the transactions are the following:

GPS IoT device named Provider creates a request to an existing GPS location ID:

<G L_W A N K_1 K_2 K_3>
where
G is the public key of the GPS location ID of Provider,
L_W = Fake GPS location; a random GPS location near Provider
L_C = Correct GPS location of Provider
$|L_W - L_C| < 100$ m; distance should be less than 100 m
A is the public key of the GPS location ID of the parent GPS IoT device, (3)
N is the amount of reward GpsCoin,

$K_1 = H(G\ L_W\ A\ N)$,
H(x) is the SHA256 hash of x,
$K_2 = S_A(K_1)$,
$S_y(x)$ is the signature of y on x,
$K_3 = S_P(K_1)$.

Miners add the transaction to the blockchain:
<G L_W A N K_1 K_2 K_3 K_4 K_5>
where
M is the public key of the miner,
(4)
T(x,y,n) is a transfer of n GpsCoin from x to y,
$K_4 = T(P, M, N)$,
$K_5 = S_M(K_1\ K_4)$.

A GPS IoT device can have at most one parent GPS IoT device. Therefore, the resulting graph of GPS IoT devices is a tree-like structure. Miners check whether the requesting GPS IoT device had registered before. If so, the requesting transaction is discarded. Miners also check fake location information for consistency. The distance between fake locations of Provider and its parent should be less than 300 m. Because the real distance between the two locations should be less than 100 m, and there can be at most 100 m fake distance for each of them. This check increases consistency of location information.

These GPS location ID transactions build a tree in the blockchain. This tree is called GPS Location ID Tree which will be used for consulting by the requesters of location information.

IV. THE MAIN BLOCKCHAIN TRANSACTION

GPS location trade transactions are main transactions for the proposed GPS blockchain. GPS requesting devices broadcast GPS requests to the environment via short-range communication. A GPS request can reach to GPS IoT devices which are in a circular area centered at the GPS requesting device. The GPS IoT devices which take the GPS request reply with their GPS location IDs. GPS requesting device take these GPS location IDs and checks them in the blockchain. If they are in the blockchain and they seem to be reliable, then the GPS requesting device starts the GPS location trade transaction. Then the transaction is mined in the blockchain. After mining, GPS requesting device can learn the GPS location information from the blockchain.

Location information can be simplified using Virtual Earth's Tiling System [16]. If 16 levels in the tiling system are used, it indicates nearly 2-meter precision. Therefore, location information can be expressed with 16 level latitude and longitude values. Each level is kept with 1 bit. Therefore, in the blockchain each location information can be kept in 4 bytes.

GPS location trade transactions are created in the following steps:

- A GPS request is created by an IoT device which will be called Requester.
- A GPS providing IoT device responses the GPS request, which will be called Provider.
- Requester starts the transaction.
- Provider adds location information and broadcast it to the blockchain.
- Miners check the transaction and write it to the blockchain.
- Requester learns the GPS location information from the blockchain.

The details of the GPS location trade transaction is explained as following:

Requester broadcasts for location information. Appropriate providers send their IDs to Requester:

<G V>
where
(5)
G is the public key of the GPS location ID of Provider,
V is the public key of a random pair of public-private key of Provider,

If Requester finds that G is reliable, Requester starts the transaction:

<Z>

where

$Z = E_V(R\ N\ V\ K_1\ K_2)$,

$E_y(x)$ is the encryption of x by public key of y,

R is the public key of the requester,

N is the amount of reward GpsCoin for each actor, (6)

V is the public key of a random pair of public-private key of Provider,

$K_1 = H(R\ N\ V)$,

H(x) is the SHA256 hash of x,

$K_2 = S_R(K_1)$,

$S_y(x)$ is the signature of y on x.

Only Provider can decrypt Z with the private key of V, adds location information, and broadcast the transaction:

$<R\ N\ V\ K_1\ K_2\ L_C\ K_3>$

where

(7)

L_C = Correct GPS location of the provider,

$K_3 = S_P(K_1\ L_C)$.

Miner checks and writes:

$<R\ N\ V\ K_1\ K_2\ L_C\ K_3\ K_4\ K_5\ K_6>$

where

M is the public key of the miner,

T(x,y,n) is a transfer of n GpsCoin from x to y, (8)

$K_4 = T(R, P, N)$,

$K_5 = T(R, M, N)$,

$K_6 = S_M(K_3\ K_4\ K_5)$.

GPS Location ID Tree is kept inside the blockchain. Requester R decides whether GPS location id G is reliable using GPS Location ID Tree. If G is a big enough sub-tree, R assumes G is reliable.

Miner checks whether R has 2*N GpsCoin in its account. Miner also checks that R V pair is unique in the blockchain transactions. If there is a main transaction containing R V, then miner discards the transaction. Therefore, the same location information request cannot be executed again. Requester finds the result of its request using the pair R V in the blockchain.

Location information provider has at least two IDs. First ID is G, which is used in the GPS Location ID Tree. The second ID is P, which is used as an account in the blockchain transactions. No one can understand the relation between P and G IDs except the requester of the location information. Therefore, location privacy is preserved.

V. EXPRERIMENTAL RESULTS

The proposed blockchain is implemented using programming language python. The implemented blockchain is a single-chain blockchain with PoW consensus mechanism. The blockchain has its own cryptocurrency named GpsCoin. The smallest denomination of GpsCoin is nanoGpsCoin, which is one billionth of GpsCoin. The blocks in the blockchain are limited with up to 1000 transactions. Miners ern nearly 100 nanoGpsCoin from each transaction.

In the implementation, there are 10 miners and 100 providers as threads. There are 1000 virtual requesters who request location information from providers. The program was executed up to 1000 blocks. Table 1 shows the total market at the end of the execution. In the execution, 895016 transactions were realized. Requesters spent 178,986,706 nanoGpsCoin for location requests. Providers earned 89,483,404 nanoGpsCoin, and miners earned 89,503,302 nanoGpsCoin. At average, each requester spent 0.00018 GpsCoin, each provider earned 0.00089 GpsCoin, and each miner earned 0.00895 GpsCoin.

TABLE I. TOTAL GPSCOIN MARKET

	Requester	**Provider**	**Miner**
Number of objects	1000	100	10
Market (nanoGpsCoin)	178986706	89483404	89503302
Average market (nanoGpsCoin)	178987	894834	8950330
Average market (GpsCoin)	0.00018	0.00089	0.00895

VI. DISCUSSION

In the GPS Location ID Tree, fake locations are used because location information requesters should not learn the exact location of the provider without paying its price. Providers can share the correct location information in return for some cryptocurrency. The payment of location information is realized via a blockchain transaction. The transaction guarantees the money transfer and there is also correct location information in the transaction. The requester can learn the correct location information from the blockchain transaction. In the transaction, there is no data about the GPS Location ID of Provider. Therefore, except the requester no one can learn the location information as well as miners.

Fake location information also helps to minimize errors. Providers cannot share extremely wrong location information because their correct location information should be near their fake location.

VII. CONCLUSION

GPS is an indispensable system for our lives. Therefore, there should be redundant and reliable alternatives. In this work, a blockchain is proposed as an alternative to GPS. Blockchain provides a decentralized peer-to-peer network, which can work even in case of severe situations. Blockchain is very resilient to physical and cyber security attacks.

The proposed blockchain depends on short-range communication like Wi-Fi. Moreover, there are IoT devices to provide location information using short-range communication. Therefore, there should be many IoT devices to cover all the geographical surfaces of the World for efficient location information service. Usually, IoT devices have light computing resources. The proposed blockchain system regards the light computing resources of IoT devices by separating IoT devices from the blockchain miners. IoT devices only create transactions, the rest of the blockchain tasks are realized by the miners.

The proposed blockchain is a single-chain blockchain with Proof-of-Work (PoW) consensus mechanism. The blockchain has its own cryptocurrency. Since there should be many IoT devices for widespread utilization, participation of IoT devices to the blockchain is empowered with incentivization mechanism. IoT devices are rewarded with some cryptocurrency for collaboration.

Short-range communication constitutes reliability of location information. Errors in location information is minimized within the range of communication channel.

The proposed blockchain keeps a tree of GPS IoT devices. The tree is built after mutual approvals of GPS IoT devices. If a GPS IoT device in the tree has a big sub-tree of GPS IoT devices, it means that the location of the GPS IoT device is approved by the GPS IoT devices of the sub-tree. In brief, the reliability of the location information increases by adding GPS IoT devices to the related sub-tree.

The proposed blockchain provides location information to requesting devices. However, it does not reveal their location information to respect their location privacy. Location privacy is protected by separating location IDs from account IDs. Only requesting IoT devices can get correct location information from the blockchain.

REFERENCES

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

[2] Popov, S. (2017). The tangle

[3] Fu, C., Kezmane, T., Du, X., Fu, Y., & Morrisseau, C. (2018, March). An location-aware authentication scheme for cross-domain internet of thing systems. In 2018 International Conference on Computing, Networking and Communications (ICNC) (pp. 452-456). IEEE.

[4] Cheikhrouhou, O., & Koubaa, A. (2019). BlockLoc: Secure Localization in the Internet-of-Things using Blockchain. arXiv preprint arXiv:1904.13138.

[5] Bornholdt, L., Reher, J., & Skwarek, V. (2019, May). Proof-of-Location: A method for securing sensor-data-communication in a Byzantine fault tolerant way. In Mobile Communication-Technologies and Applications; 24. ITG-Symposium (pp. 1-6). VDE.

[6] Dahlinger, A., Ryder, B., & Wortmann, F. (2015). Car as a Sensor. Paying people for providing their car data. In Proceedings of the 5th International Conference on Internet of Things, Seoul, South Korea. 5th International Conference on Internet of Things.

[7] Lamtzidis, O., & Gialelis, J. (2018, December). An IOTA Based Distributed Sensor Node System. In 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[8] Joy, J. (2017, November). Vehicular blocktrees. In 2017 IEEE Vehicular Networking Conference (VNC) (pp. 147-150). IEEE.

[9] Singh, M., & Kim, S. (2018, February). Trust Bit: Reward-based intelligent vehicle commination using blockchain paper. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 62-67). IEEE.

[10] Zhang, L., Luo, M., Li, J., Au, M. H., Choo, K. K. R., Chen, T., & Tian, S. (2019). Blockchain based secure data sharing system for Internet of vehicles: A position paper. Vehicular Communications.

[11] Baza, M., Nabil, M., Bewermeier, N., Fidan, K., Mahmoud, M., & Abdallah, M. (2019). Detecting sybil attacks using proofs of work and location in vanets. arXiv preprint arXiv:1904.05845.

[12] Li, H., Pei, L., Liao, D., Sun, G., & Xu, D. (2019). Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET. Peer-to-Peer Networking and Applications, 12(5), 1178-1193.

[13] Brambilla, G., Amoretti, M., & Zanichelli, F. (2016). Using blockchain for peer-to-peer proof-of-location. arXiv preprint arXiv:1607.00174.

[14] Noble, M., & Wang, Z. (2019, March). Securing critical infrastructures with location based authentication blockchain. In Sensors and Smart Structures Technologies for Civil, Mechanical, and Aerospace Systems 2019 (Vol. 10970, p. 109700S). International Society for Optics and Photonics.

[15] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151, 1-32.

[16] Bing Maps Tile System. [Online]. Available: http://msdn.microsoft.com/en-us/library/bb259689.aspx, accessed 29.08.2019

[17] Asuquo, P., Cruickshank, H., Morley, J., Ogah, C. P. A., Lei, A., Hathal, W., & Sun, Z. (2018). Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. IEEE Internet of Things Journal, 5(6), 4778-4802.

[18] Kumar, K. M., & Sunitha, N. R. (2017, December). Preserving Location Data Integrity in Location Based Servers using Blockchain Technology. In 2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT) (pp. 1-6). IEEE.

[19] Zhanikeev, M. (2019). The Last Man Standing Technique for Proof-of-Location in IoT Infrastructures at Network Edge. Wireless Communications and Mobile Computing, 2019.

[20] Victor, F., & Zickau, S. (2018, November). Geofences on the Blockchain: Enabling Decentralized Location-based Services. In 2018 IEEE International Conference on Data Mining Workshops (ICDMW) (pp. 97-104). IEEE.