# Proof of Position: A Lightweight Concenses Mechanism for IoT Oriented Blockchain

Zhitao Wan [1] , Minqiang Cai [2], Jinqing Yang [2] , Heng Zhang [3], Xiuping Hua * [4]

[1] University of Nottingham Ningbo China and Ningbo Free Trade Zone Blockchain Laboratory, Ningbo, China.
[2] Institute of Advanced Technology Research, Ge Lian Corporation, Hangzhou, China.
[3] Quality Department, State Information Center, Beijing, China
[4] Nottingham University Business School China, University of Nottingham Ningbo China, Ningbo, China.

Email: [1]wan@pku.edu.cn; [2]cai@ge-lian.com; [3]heng_zhang@126.com; [4]xiuping.hua@nottingham.edu.cn

***Abstract* - The accurate position information of the Things plays a more important role in many scenarios such as healthcare, smart grids, spot guidance, supply chain, and, the anticipated evolution of IoT for more security, credibility, authenticity, reliability, and scalability automated systems. However, there are still some challenges especially for accurate and trustable position information acquirement. To enhance the accuracy of the Global Navigation Satellite Systems technologies such as differential GPS, Real Time Kinematic, and Continuously Operating Reference Stations are adopted. Basically, the concept of mentioned technologies is to use two way data to eliminate the jitter and bias with expensive hardware or infrastructure. This research proposes a proof of position mechanism for blockchain based two way positioning data sharing and position information endorsement. The mechanism enables peers in blockchain to exchange, verify position information without the expensive hardware and infrastructure. The proof of concept demonstrates this mechanism provides a robust, cost effective and trustable high accuracy positioning service.**

***Keywords - Proof of Position; IoT; High Accuracy Positioning; Blockchain; Concesus***

## I. INTRODUCTION

Positioning services are basic services, common provided by Global Navigation Satellite System (GNSS), mobile network based positioning system [1], Lora-based metro positioning system [2], Wi-Fi based indoor positioning system [3], Bluetooth based positioning system [4], Ultra Wide Band (UWB) based positioning system [5]. Among them, GNSS can provide relatively complete outdoor coverage capabilities, while other positioning systems can only provide coverage capabilities for a certain area.

The demand of position accuracy increases rapidly and the positioning accuracy of a single GNSS terminal cannot satisfy. Differential GPS[6], especially RTK [7] and similar technologies utilize reference station or Continuously Operating Reference Stations (CORS) [8] service to eliminate deviation for higher positioning accuracy. The hardware cost and CORS service fee are relatively high.

In fact, high accuracy positioning mobile terminal can also provide similar receiving capacity of satellite positioning raw data (hereinafter referred to as raw data) like the reference station. if a raw data sharing and verification network can be built, mobile stations can achieve high accuracy positioning by sharing satellite positioning raw data with each other without expensive hardware or additional CORS service cost anymore.

Blockchain is a collaborative, tamper-resistant ledger that maintains transactional records. The ledger can be used to record and share the data generated by Things, the identity and contribution of the Things. The IoT and blockchain integration are widely adopted. This research designs a blockchain consensus mechanism to enable high accuracy positioning for peer IoT systems basing on blockchain. The proposed approach is to construct a blockchain network based on the original data of satellite positioning, by distributing, verifying, recording the contribution of each node and an appropriate incentive mechanism to maintain the network system, providing a low cost high accuracy positioning infrastructure based on raw data sharing.

## II. RELATED WORK

Public blockchain is an application mode of computer technology such as distributed data storage, peer-to-peer transmission, consensus mechanism, and encryption algorithm to ensure the security of data transmission and access, and uses smart contracts composed of automation script code to program and operate data.

In the traditional blockchain system, the Proof of Work (PoW) through hash requires a large amount of computing power investment and energy consumption, and the proof-of-work method through storage requires a large amount of storage space. The other consensus mechanisms such as Proof of Stake (PoS) [9], Practical Byzantine Fault (PBF)[10] and variations are overhead for the blockchain system, i.e., the consensus mechanisms consume large volume of resources for the agreement [11].

The basic feature of consensus algorithm of the blockchain is that the results of the consensus are easy to verify. Hash computing, hard disk storage proof, and other consensus mechanisms have this feature. The accuracy positioning of GNSS usually use the raw data of a node in a known position to eliminate the bias incurred by the satellite system and space environment. Fig. 1 depicts the basic scenarios of current accuracy positioning implementation. Scenario 1 uses fix land reference station and scenario 2 uses a base station near a rover. The terminal and rover perform almost the same behavior.

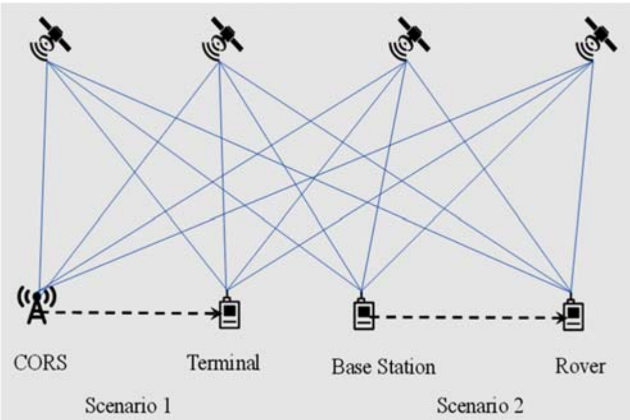


Figure 1. The two basic scenarios of high accuracy GNSS positioning.

## III. PROOF OF POSITION

In this section, we elaborate on the design of the consensus protocol in detail. Fig. 2. depicts the concept of our approach. A blockchain network replaces the dedicated channels in the scenarios mentioned in section II. And the peer nodes support each other using raw data and there is no dedicated land reference station or base station any more.

### *A. The Basic Concepts*

Raw data, the binary observation message of satellites, is used for high accuracy positioning and converted to RINEX, in ASCII, as the common format. The raw data of satellite positioning is time and space related, and the results can be quickly verified through solving and comparison as the basis for consensus. High accurate positioning usually needs two way raw data that come from two different chipsets respectively.

GPS, GLONASS, Galileo, QZSS, BeiDou and SBAS are supported and multi-constellation, multi-frequency chipset is recommended. GPS time is used for GNSS data handling and positioning algorithms rather than Universal Time Coordinated (UTC) to avoid leap seconds handling.

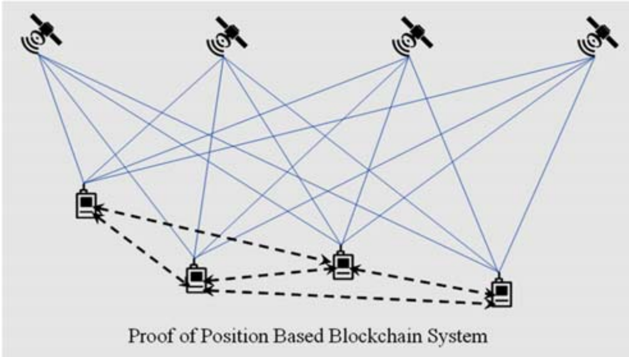


Figure 2. The concept of blockchain based high accuracy GNSS positioning.

### *B. Components of Peer*

A peer should include at least a processor, GNSS chipset, storage, and internet access. GNSS chipset receives raw data from satellites and the raw data can be send to another peer by processor via internet and receive raw data from other peers via internet. A peer can perform positioning and store, synchronize data with other peers.

### *C. Contribution and Incentive*

The main contribution of a peer is to share raw data stream with peers. The raw data steam should keep a while to make sure other peers can get their high accurate position. The incentive in this context is the endorsement of data sharing quality $q$ that indicates the number of satellites in the raw data stream, duration $d$, and share copy $n$. The contribution $C$ can be calculated as following formula:

$$C = \sum_{k=1}^{n} qd \tag{1}$$

The incentive is the accumulation of the contribution. To encourage the peers to contribute all the time that keeps the system running smoothly, the incentive $I_j$ is calculated as the share of all contribution during a given period, say, one hour. An alternative approach is random incentive assignment.

$$I_j = \frac{C_j}{\sum_{k=1}^{n} C_k} \tag{2}$$

### *D. Consensus Algorithm*

The public blockchain system in this paper have the characteristics of distribution, autonomy, openness, and free access. Peer-to-peer networks is used to organize nodes involved in data validation and accounting. All nodes in the network are equal and interact with each other in a flat topology, there is no centralized nodes and hierarchies, and each node can verify block data, propagate block data, and vote to accept/reject new nodes. The basic concept of the consensus algorithm is that the results of the consensus are easy to verify but hard to tampered. The GNSS satellite signal can be received anywhere and can be verified easily.

1) *Initial the Joining Process:* A new peer (requesting node) issues a blockchain network access request while GNSS chipset is ready for satble raw data receiving.

2) *Estibilsh connection:* An online peer (verification node) verifies the identity of the requesting node and establishes a connection.

3) *Forward Verification of the New Peer:* The requesting node sends out the raw data stream, which can effectively improve the positioning accuracy of the verification node. If the result meets the accuracy requirements, verificaiton node endorses the requesting node conditionally.

4) *Reverse Verification of the New Peer:* The verification node sends raw data of the satellite positioning to the requesting node and requires the return of high accuray positioning resolution, and if the result meets the accuracy requirements, it fully endorses the application node. Full endorsement is made immediately after validation, the list of local neighbor nodes is updated, and neighbor nodes are broadcasted to neighbors. After being verified and fully endorsed by neighboring nodes, the requesting node completes the joining of the blockchain network.

5) *Exchange Raw Data and Generate Blocks:* Peers support each other to perform single node high accuracy positioning by sharing raw data. The positioning request node issues a raw data request containing the private key signature, timestamp and identification to the neighboring node, receives the corresponding raw data shared with the private key signature from the neighboring node, records the request, and issues an endorsement request to the neighboring node. If more than half of the neighboring nodes (more than 50%) give the endorsement the request will be recorded in the blockchain.

## IV. EXPERIMENTAL METHODOLOGY, HARDWARE AND SOFTWARE

We setup testbed basing on raspberry Pi 4B, Cortex M4 board, X86 Atom board. The GPS chipset include high end Ublox ZED-F9P and legacy Ublox LEA-6T, a cheap chip mainly for GNSS timing with raw data support. The implementation of the Proof of Position algorithm is following the steps in section III.

### *A. Hardware Platfrom*

We use the following hardware Platform for the testbed and the combinations are listed in Table I and Table II:

GPS chipset: Ublox ZED-F9P, Ublox LEA-6T
Processor: Cortex M4, BCM2711, X86 Atom
Storage: SD card, eMMC
Network: WiFi, 100M/1000M Ethernet

### *B. Accuracy Positioning Software Stack*

RTKLIB [7] is an open source package supporting high accuracy positioning with GNSS such as GPS, GLONASS, Galileo, QZSS, BeiDou and SBAS. It provides Windows and Linux based releases and can be ported to embedded platforms such as Cortex M4. We use Cortex M4 to utilize the DGPS mode of Ublox ZED-F9P chipset and use Linux based software for both Ublox ZED-F9P and legacy Ublox LEA-6T. The topology is depicted in Fig. 3. Four different nodes compose the minimum system.

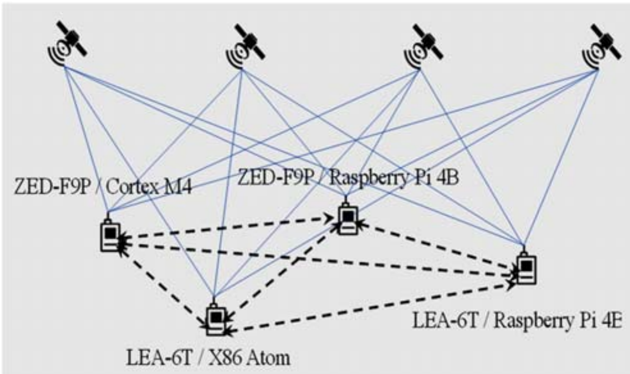


Figure 3. The proof of concept testbed with four nodes.

We setup base station and rover station [12] based testbed as groups of comparison. There are four combinations listed in Table I.

TABLE I. TESTCASES OF BASE STATION AND ROVER STATION

| Testcase# | Base Station | Rover Station |
|---|---|---|
| 1 | Ublox ZED-F9P | Ublox ZED-F9P |
| 2 | Ublox ZED-F9P | Ublox LEA-6T |
| 3 | Ublox LEA-6T | Ublox ZED-F9P |
| 4 | Ublox LEA-6T | Ublox LEA-6T |

The proof of position based blockchain test cases are list in Table II. The peers provide raw data to each other respectively, the test results will be doubled from 6 to 12.

TABLE II. TESTCASES OF BASE STATION AND ROVER STATION

| Testcase# | Peer A | Peer B |
|---|---|---|
| 5 | ZED-F9P / Cortex 4 | LEA-6T / X86 Atom |
| 6 | ZED-F9P / Cortex 4 | LEA-6T / Raspberry Pi |
| 7 | ZED-F9P / Cortex 4 | ZED-F9P / Raspberry Pi |
| 8 | ZED-F9P / Raspberry Pi | LEA-6T / X86 Atom |
| 9 | ZED-F9P / Raspberry Pi | LEA-6T / Raspberry Pi |
| 10 | ZED-F9P / Raspberry Pi | ZED-F9P / Cortex 4 |

## V. RESULTS AND DISCUSSIONS

The test results in field test show that testcase 1 can reach centimeter level accuracy in means about 21 seconds for cold start and 6 seconds for warm start. For testcase 2, 3, 4 the convergence times is around 35 minutes to reach 0.3~0.5meter level accuracy. The positioning accuracy and convergence times are GNSS chipset related, and Ublox ZED-F9P has significant performance improvement comparing with legacy Ublox LEA-6T. Two way test results of testcase 5 and testcase 10 can reach centimeter level accuracy about 21 seconds in mean for cold start and 7 seconds for warm start. For testcase 6, testcase 7, testcase 8 and testcase 9 it will cost around 35 minutes to reach 0.3~0.5meter level accuracy. The convergence times are similar to testcase 1 to 4.

Generally, the Ublox ZED-F9P chipset has much better sensitivity and multi-band support. The convergence times is much faster and reliable. Ublox LEA-6T is a much cheaper legacy chipset with slower convergence times. To start the blockchain system in short time the convergence times is critical for peer joining and high accuracy positioning experience. So current main stream chipsets such as ZED-F9P are applicable for our proposed consensus approach. The overhead of blockchain system is not significant. And there is no observable accuracy down grade.

The highest accuracy level can be reached of the system is also environment related. The atmosphere, cloud, surrounding building etc. impact the satellite observation and signal receiving. And, according to different pseudo-range measurement, DGPS can be classified as code differential positioning and carrier-phase differential positioning. The positioning accuracy of Carrier Phase Differential Positioning RTK [7] is much higher than code differential GPS once the ambiguity has been determined [13].

The proof of concept system demonstrates that the proof of position consensus we proposed can reach agreement by the intrinsic ability of GNSS chipset. The computation demands of the system is relatively low. It saves the total cost of high accuracy positioning system significantly especially for massive IoT systems.

## VI. CONCLUSION AND FUTURE WORK

The IoT systems widely adopt and the high accuracy positioning is a very important in many scenarios. The current high accuracy positioning system is costly base/rover station pair or reference infrastructure based. This paper proposed a proof of position consensus mechanism to construct trustable low cost IoT infrastructure. The proof of position based blockchain system can provide a flat data exchange platform that no dedicated reference station needs anymore, and low cost global or regional trustable IoT system supporting.

The proposed IoT blockchain system basing on proof of position consensus mechanism has not been deployed in massive node environment yet. We are currently working on developing a cross platform system supporting more chipset and software platform. We aim to deploy a wide coverage massive peer system, and further introduce more things and advanced IoT capabilities into the system, such as Inertial Measurement Unit, indoor positioning and other sensing and enforcing components. We also aim to improve incentive mechanism within the system to reward peers for introducing fast convergence times chipsets and, delivering more accurate positioning.

The approach is applicable for those location related application scenario such as financial service, travel service, smart agriculture, and many other application scenarios.

## ACKNOWLEDGMENT

This research was supported by Ningbo Science and Technology Innovation 2025 Major and Special Program "Research and Application of Reliable Financial Service Platform Based on Blockchain E-Invoice" (Grant No: 2019B10029), “Research and Application of Regional Culture-Gene Decoding and Precise Disseminating Technology” (Grant No: 2021Z017), and State Information Center special program on General Cross Blockchain Platform.

## REFERENCES

[1] J. A. del Peral-Rosado, R. Raulefs, J. A. López-Salcedo, and G. Seco-Granados, “Survey of Cellular Mobile Radio Localization Methods: From 1G to 5G,” IEEE Communications Surveys and Tutorials, vol. 20, no. 2. 2018. doi: 10.1109/COMST.2017.2785181.

[2] I. S. B. M. Isa and A. Hanani, “Development of real-time indoor human tracking system using LoRa technology,” International Journal of Electrical and Computer Engineering, vol. 12, no. 1, 2022, doi: 10.11591/ijece.v12i1.pp845-852.

[3] A. Noble Mary Juliet, N. Suba Rani, S. R. Dheepiga, and R. Sam Rishi, “Wi-Fi-Based Indoor Patient Location Identifier for COVID-19,” in Lecture Notes on Data Engineering and Communications Technologies, vol. 75, 2022. doi: 10.1007/978-981-16-3728-5_38.

[4] M. Z. Chaari, R. Al-Rahimi, and A. Aljaberi, “Real-Time Monitoring of Indoor Healthcare Tracking Using the Internet of Things Based IBeacon,” in Lecture Notes in Networks and Systems, 2022, vol. 298. doi: 10.1007/978-3-030-82529-4_32.

[5] R. J. Fontana, “Recent system applications of short-pulse ultra-wideband (UWB) technology,” in IEEE Transactions on Microwave

Theory and Techniques, 2004, vol. 52, no. 9 I. doi: 10.1109/TMTT.2004.834186.

[6] A. Patel, S. K. Katiyar, and V. Prasad, “Performances evaluation of different open source DEM using Differential Global Positioning System (DGPS),” Egyptian Journal of Remote Sensing and Space Science, vol. 19, no. 1, 2016, doi: 10.1016/j.ejrs.2015.12.004.

[7] T. Takasu and A. Yasuda, “Development of the low-cost RTK-GPS receiver with an open source program package RTKLIB,” International Symposium on GPS/GNSS, 2009.

[8] R. A. Snay and T. Soler, “Continuously Operating Reference Station (CORS): History, Applications, and Future Enhancements,” Journal of Surveying Engineering, vol. 134, no. 4, 2008, doi: 10.1061/(asce)0733-9453(2008)134:4(95).

[9] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017, vol. 10401 LNCS. doi: 10.1007/978-3-319-63688-7_12.

[10] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance and Proactive Recovery,” ACM Transactions on Computer Systems, vol. 20, no. 4, 2002, doi: 10.1145/571637.571640.

[11] G. T. Nguyen and K. Kim, “A survey about consensus algorithms used in Blockchain,” Journal of Information Processing Systems, vol. 14, no. 1, 2018, doi: 10.3745/JIPS.01.0024.

[12] R. Leandro et al., “RTX positioning: The next generation of cm-accurate real-time GNSS positioning,” in 24th International Technical Meeting of the Satellite Division of the Institute of Navigation 2011, ION GNSS 2011, 2011, vol. 2.

[13] S. Chen, Y. Wang, and F. Chen, “A study of differential GPS positioning accuracy,” 2002. doi: 10.1109/ICMMT.2002.1187711.R. J. Fontana, “Recent system applications of short-pulse ultra-wideband (UWB) technology,” in IEEE Transactions on Microwave Theory and Techniques, 2004, vol. 52, no. 9 I. doi: 10.1109/TMTT.2004.834186.

.