Towards Large-Scale and Privacy-Preserving Contact Tracing in COVID-19 pandemic: A Blockchain Perspective

Wenzhe Lv, *Student Member, IEEE*, Sheng Wu, *Member, IEEE*, Chunxiao Jiang, *Senior Member, IEEE*, Yuanhao Cui, *Member, IEEE*, Xuesong Qiu, Yan Zhang, *Fellow, IEEE*

Abstract—Activity-tracking applications and location-based services using short-range communication (SRC) techniques have been abruptly demanded in the COVID-19 pandemic, especially for automated contact tracing. The attention from both public and policy keeps raising on related practical problems, including *1) how to protect data security and location privacy? 2) how to efficiently and dynamically deploy SRC Internet of Thing (IoT) witnesses to monitor large areas?* To answer these questions, in this paper, we propose a decentralized and permissionless blockchain protocol, named *Bychain*. Specifically, 1) a privacy-preserving SRC protocol for activity-tracking and corresponding generalized block structure is developed, by connecting an interactive zero-knowledge proof protocol and the key escrow mechanism. As a result, connections between personal identity and the ownership of on-chain location information are decoupled. Meanwhile, the owner of the on-chain location data can still claim its ownership without revealing the private key to anyone else. 2) An artificial potential field-based incentive allocation mechanism is proposed to incentivize IoT witnesses to pursue the maximum monitoring coverage deployment. We implemented and evaluated the proposed blockchain protocol in the real-world using the Bluetooth 5.0. The storage, CPU utilization, power consumption, time delay, and security of each procedure and performance of activities are analyzed. The experiment and security analysis is shown to provide a real-world performance evaluation.

Index Terms—Blockchain, Potential Field, Contact Tracking, COVID-19

I. Introduction

A. COVID-19 Requirement

The COVID-19 pandemic has been a global health emergency, spreading to more than 18 countries of the world and infecting more than 8,359,869 population. As an essential tool for public health officials and local communities to fight the rapidly spreading, contact tracing methods draw attention across the world. Early in the outbreak, when there were only a few cases, contact tracing can be done manually with a slight impact on society. Nevertheless, with the skyrocketing of the infections in the vast majority of countries, manual contact tracing tends to be unrealizable on both economy and policy considerations.

Location-Based Services (LBS) provided by Short-Range Communication (SRC) techniques are considered a viable solution to perform contact tracing. Due to the intensive penetration of mobile smartphones, wearable devices, and ubiquitous sensors, residents can opt-in contact tracing service via an over-the-air mobile application installation, whenever Internet access is available. The Singaporean government released a mobile phone app, TraceTogether, that is designed to assist health officials in tracking down exposures after an infected individual is identified.

In general, a recorded SRC interaction with timestamp and location info can certify that, at a given moment and position, two radio terminals have been closer than the maximum transmission distance. If one of the two terminal owners is tested positive for COVID-19, the SRC record can be strong evidence of epidemiological exposure for the other owner. Therefore, the contact identification can be automatically made by analyzing the infected person's SRC records.

On the other hand, the chosen of SRC standard and storage methods would significantly impact the performance of SRC-based contract tracking. Shorter communication distance increases identity accuracy. An overlong communication range may result in excessive identified contactees whose physical exposure may do not actually occur. As an example, the South Korea government analyzes Call Detail Record (CDR) collected from telecommunication operators. When a COVID-19 patient is detected, the entire building should be quarantined, which results in a significant impact on the company business. Therefore, benefit from easy to deployment and stone-cast data transmission, Bluetooth Low Energy (BLE) has been considered as a possible contact tracing approach.

B. Daily Requirement

If we take a longer-term and world-wide perspective, increasingly more people rely on LBS apps to track, monitor, manage, and plan their daily life. These mobile apps have profoundly impacted and even initialized various industries, such as Uber [2] and DiDi in transportation sharing, Ele in food delivery, Fitbit and Nike+ in fitness, and Pokergo in augmented reality games. The key features of these apps are

to collect location information in a certain time period and to perform path generation to share the personal location/activity path/summary with other users/service providers on a social network. For example, activity-tracking programs are developed in United Health and Aetna to modify insurance rates according to an activity analysis [3].

However, these activity-tracking services assume users are trusted and honest to report their location and time information, which is generally impractical and unrealistic. Indeed, the fashion of self-reporting location information using global positioning system (GPS) coordinates, cell triangulation and IP address tracking are all susceptible to manipulation such that users can handily claim a mendacious location [19], which may cause serious cheating issues, especially to financial and critical service providers. To address these issues, SRC records also consider being an applicable method to improve their location reliability.

C. Challenges and Motivations

Although LBS provided by SRC (especially BLE) techniques are highly demanded in the contact tracing of COVID-19 pandemic and many more daily demands, much uncertainty still exists on data security, privacy, and deployment efficiency.

- Security: Traditional security services such as authentication, integrity, and provenance provided by third-party brokers. However, the third-party brokers maybe not trustable.
- Privacy: User privacy may be violated when service providers collect, store, and analyze customer's locations using a centralized database. The service providers can even sell customer data by taking a little advantage of the fine print in the service agreements. Although Europe's General Data Protection Regulation (GDPR) has been implemented, the unintended data leakage of service providers still call for technical privacy concerns.
- Deployment Efficiency: A phone-to-phone SRC record demonstrates the spatial connection between two individuals. However, long-term monitoring of a high-risk hotspot area is still critical in contact tracing. Governments or philanthropic organizations are willing to deploy several IoT witnesses, e.g., BLE beacons, to achieve an all-weather day-and-night low-cost area surveillance. These organizations may not cooperate. Therefore, an efficient deployment strategy is desired in the blockchain system.

In this paper, we propose a permissionless blockchain for automated contact tracing and activity-proofing, named *Bychain*. An interactive zero-knowledge proof based protocol is designed to provide transaction security and identity privacy while taking advantage of cryptographic techniques instead of employing a trusted third party. The deployment problem is addressed by proposing an incentive allocation mechanism based on a visual potential field algorithm; a participant would be distributed the maximum reward when it is on the position of force equilibrium. Ideally, the blockchain network archives maximized monitoring area when the IoT witnesses in the blockchain are static equilibrium.

This protocol relies on the cryptography technique to create SRC proofs for its nearby mobile users. The proposed protocol consists of three stages: First, users obtain secure and privacy-preserving proofs of location during their activities, by relying on an over-the-air lightweight message exchange between their mobile device and the witness point. Proof of Location (PoL) commitments are generated, digitally signed, and verified by their nearby witness nodes through BLE techniques. Second, the activity proofs are uploaded on a decentralized ledger that is transparently and distributively stored on the Internet. Finally, the trusted activity summary can be generated by using a zero-knowledge proof based authentication based on a smart contract after an ownership verification. The blockchain could compute an accurate and trusted activity summary of an authenticated user to fulfill the requirement of COVID-19 contact tracing, without revealing activity information to anyone else.

To empower Bychain with the ability of witness deployment, an incentive allocation algorithm is proposed based on the virtual potential field. Each witness node is treated as a charged particle, such that artificial electric fields are constructed in a way that each node is repelled by repulsive force from other nodes. As a result, the witnesses in blockchain could spread itself throughout the environment. Finally, the monitoring area of the blockchain system tends to maximize the monitoring area when the IoT witnesses in blockchain tend to static equilibrium.

Additionally, in the blockchain system, a semi-trusted decentralized activity-proofing system and zero-knowledge based authentication techniques could provide security from cheating and protect identity privacy. The public essential cryptography technique is naturally merged to provide an ownership certification of personal location information. As a benefit from the zero-knowledge proof technique, a user could claim data ownership without revealing the private key to anyone else. However, the decentralized ledger is transparent such that the public can verify the location information. Hence, we introduce a crucial escrow technique to alternate the traditional one-key-per-user with a one-key-per-proof scheme. The on-chain data traceability becomes almost impossible, and the identity information is pseudonymous. Thus, data security and identity privacy requirements are met in our system. Consequently, the attack of controlling the certificate authority and the central database can be avoided. Furthermore, plenty of attacks can be avoided, such as the reply attack and the dust attack. We will discuss them in detail later in this paper.

The contributions of this paper can be summarized as follows:

- A proof-of-activities generation and verification protocol is introduced to achieve trusted activities proof for contact tracing and related SRC usage. Bychain protocol addresses the activity-proofing problem without a trusted third party while considering privacy and anonymity. Bychain can be rapidly applied to against COVID-19 with a low economic cost.
- By jointly design of crucial escrow and zero-knowledge proof method, the proposed protocol is able to obtain location identity privacy and security. It can resist various

attacks and collusion. A generalized block structure is proposed to fulfil the requirement of new on-chain operations. Furthermore, to address the efficient deployment of IoT witnesses, an incentive allocation mechanism using virtual potential field is proposed to maximizing the monitoring area.

- A prototype implementation is realized and verified on the Android platform. The performance analysis shows that our protocol requires preferably low computational time, energy, and storage. Experiments show that the proposed protocol is practical and can be applied in many scenarios, even in a highly dynamic environment.

The rest of the paper is organized as follows. Section II discusses related work. Section III describes the overview of the proposed blockchain system. In Section IV, we discuss our proposed proof of activity protocol and incentive allocation mechanism. A security analysis of our proposed protocol against different types of attacks is provided in Section V. In Section VI, we describe our implementation and simulation and present our experimental results on the performance evaluation. Finally, Section VII concludes the paper.

II. RELATED WORK

Digital contact tracing has been recognized as a powerful tool that are able to reduce the reputation number R_0 to less than 1 [4] (R_0 is the expected number of cases directly generated by single infected case), therefore spread of the COVID-19 can be significantly controlled. However, the security and privacy of current contact tracing strategies may have serious implications on individual's safety and civil rights. The authors in [5] have presented and identified privacy lapses of different contact tracing applications and protocols around the world. Short-range communication technologies, such as Bluetooth, have been proposed to generate location evidence from its neighbours. The mutual verification protocol of a set of users is proposed based on users' spatiotemporal correlation in [6]. The privacy is performed by deciding whether to accept location proof requests and is decided by user themselves. Furthermore, various privacy aspects of QR codes, WiFi and Bluetooth has also been discussed in [7] to form a compressive survey.

Indeed, SRC based contact tracing is developing by Google and Apple [8] in a privacy-preserving fashion. However, the SRC records are stored in mobile terminals facing storage shortage problems. The deployment of IoT witnesses is not supported as well. With the benefit of more trustable data collection, blockchain technology and its applications have drawn enormous attention from various researchers in IoT era. A reputation-based model is proposed in IoT blockchain systems to spread reliable and certified information of distributed devices [9]. The potential trust relationships of cloud-of-thing partners are exploited in [10] to improve the mutual trust and helpfulness between individual and group devices. In order to address open issues and challenges in smart city applications, a novel blockchain as a service framework, named BlockSDN, is proposed under software defined network-enabled architecture [12]. BlockSDN is considered to be an efficient solution which is able to contain various service attacks, including malware

attack and distributed denial of service attack on compromised switch.

Furthermore, the blockchain technology is widely developed in the area of unmanned aerial vehicles. The security and privacy challenges of spectrum sharing between aerial and terrestrial communication systems are addressed by a spectrum blockchain framework in [11]. In [14]–[17], highly reliable communication is supported by blockchain and neural networks for unmanned aerial vehicles. A blockchain protocol is also proposed to manage data for the vehicular network in [18]. Last but not least, a blockchain-based secure data processing framework, named BloCkEd [13], is proposed to minimize the link breakage and reducing latency. The implementation and evaluation demonstrated the proposed BloCkEd is able to achieve more effective resource allocation policy.

However, the existing contract tracing and blockchain based applications can not straightforwardly address the privacy, security and deploy-efficiency problems considered in this article.

III. AN OVERVIEW OF LOCATION-BASED BLOCKCHAIN ARCHITECTURE

The proposed blockchain protocol is a peer-to-peer system, which provides users with anonymous and trusted location proofing, transparent data storage, and zero-knowledge proof based data ownership authorization. Fig. 1 illustrates the proposed blockchain architecture, in which the network is summarized as three layers :

- **The service layer** contains honestly witnesses that afford location-proofing service to passing-by provers via near-field communication techniques, and verifiers that finally generate activity certifications in the form of tabular activation summary. In a given time period, T_n, a prover collects witness-signed PoL commitments and then uploads them on blockchain as the cornerstone of trust evaluation. A straightforward trust level evaluation via the cumulative method is marked as green labels in Fig.1.
- **The network layer** enables the peer-to-peer (P2P) transmission mechanism to exchange collected PoL commitments of each prover and virtual force of each witness. This information are carried by the Transactions (Tx) field in the proposed generalized data structure and received by chain nodes.
- **The blockchain layer** is comprised of a distributed database recording immutable and continuously growing transactions and a location-based consensus mechanism maximizing total coverage of witness nodes, which is detailed in Sec. IV. The blockchain system disburses a budget coverage package per 24 hours to stimulate witness movement to form maximum coverage of the sensing area. During each round of consensus procedure, a *miner* calculates the incentive allocation scheme and then sticks it into the next block. The miner is pseudo-randomly determined from a node sequence in the order of owned stock value. The proposed block is broadcasted and finally confirmed by an elected consensus committee according to the value of mortgaged stocks.
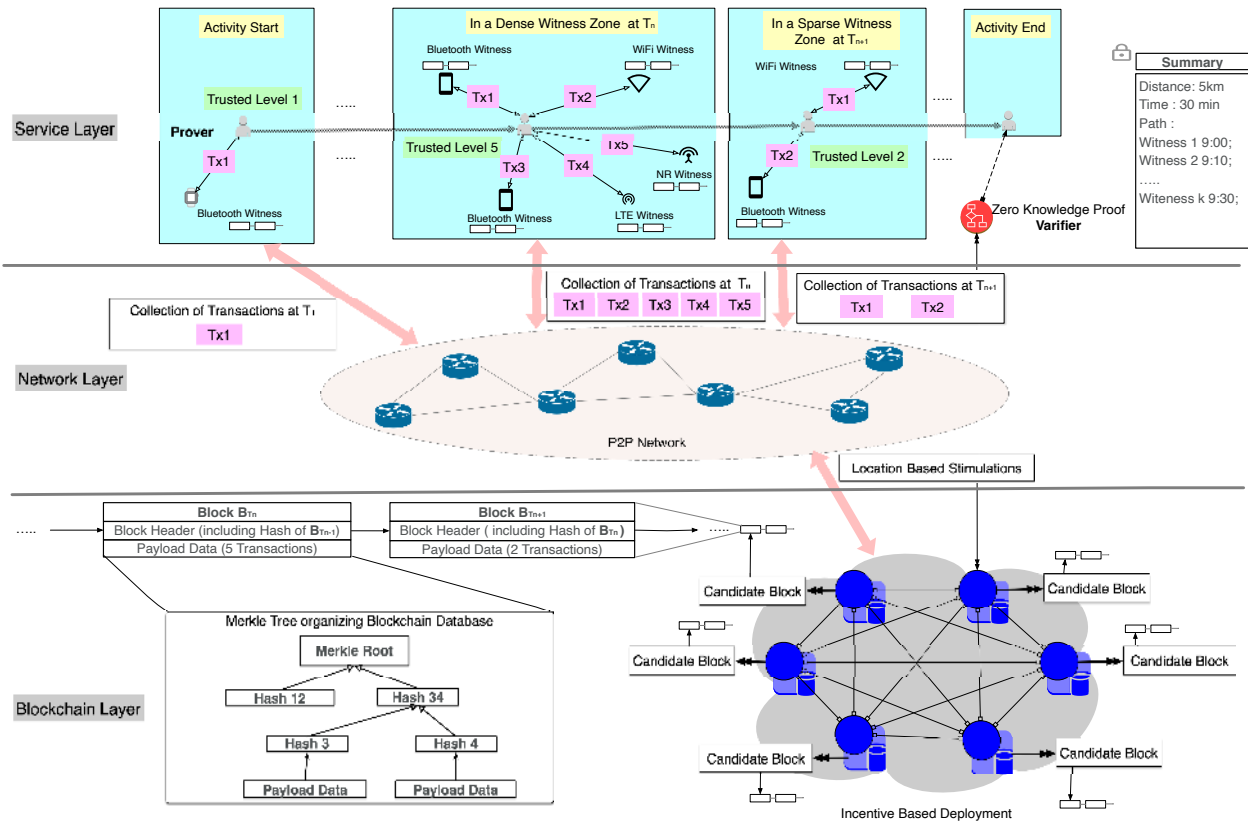
Fig. 1: Overview of proposed blockchain architecture.

The key entities and mechanisms in each layer would be detailed in the following subsections.

A. The Service Layer

Individuals can access the blockchain with unified application software, which ensures data integrity by forcing a data consistency check when initializing. The service layer establishes a set of available application operations and coordinates the application's response in each operation. Although all IoT nodes with application installation are fully functional, the three logical roles involved in those operations need to be elaborated for a better understanding of readers.

1) Prover: In the proposed blockchain architecture, the prover acquires anonymous and trusted location proofing, transparent data storage, and zero-knowledge proof based data authorization. Provers indeed are a set of wireless nodes that desires location-based proof-of-activities. Each prover is equipped with a GPS module as well as Bluetooth, WiFi, or LTE antennas has Internet activity to the blockchain and moves in a given region that is covered by our wireless access point (AP) networks. It's worth noting that the precision of GPS module does not impact the credibility of SRC records, because SRC records are generated if and only if the distance of two terminals is less than communication radius of short distance communication. These provers can communicate with AP nodes involved in our system only if their distance is lower than the communication distance R, where R is determined by the near-field communication technology, which means

Bluetooth, WiFi or LTE will provide three kinds of distances, defined as R_B, R_W, and R_L, respectively. Both prover and witnesses has the characteristic of mobility. The sum of communication durations between provers and AP nodes can be completed before the prover leaves the coverage area of AP, which is verified in our experiment.

Each prover i is equipped with a memory as a critical escrow agent to stock pairs of cryptology keys. The stocked vital pairs are generated when service initializes and randomly sign each near-field communication message, which means the kth proof-of-location commitment is uniquely identified by public key $pk_{p_i}^k$ and a private key $sk_{p_i}^k$. Without loss of generality, we assume provers will never hand or even reveal their private keys to anyone else.

2) Witness: Witnesses are wireless nodes that provide location-based proofs to provers. These witnesses may be fixed WiFi APs, Bluetooth low power equipment (BLE) or an LTE base station owned by an ISP provider, deployed in the area where provers pursue their proofs. More importantly, a witness could discover another if their distance is lower than its coverage radius. Hence, witnesses are aware of the locations of their neighbors.

All the witnesses and provers have synchronized clocks and are equipped with a GPS device that is aware of the location of itself. This WiFi AP localization technique can be realized by the analysis of communication channel state information. Different from provers, each witness i can be uniquely identified by a pair of cryptology keys, known as a public key pk_{w_i} and a private key sk_{w_i}. Without loss of

generality, we also assume the witness will never hand or even reveal their private key or digital signature to anyone else. The witness can access the Internet and communicate with the blockchain.

In our system, we assume each witness is semi-trusted and privacy-honest, which means it does not reveal the prover's information to any nodes, but cheating such as collusion may occur. Practically, a witness is probably willing to collude with other witnesses or provers cheating for blockchain awards.

3) Verifier: A verifier is an entity that a prover wants to request an activity certification from, such that a prover's claim appears in a certain location at a particular time. The verifier is completed by interactive zero-knowledge proof based on the smart contract, such that it is self-running and able to protect the identity privacy of a specific user.

When the prover intends to request certification, a verification request including the on-chain index of PoL commitment, public keys of the prover, and witness are submitted to the blockchain system. The verifier smart contract is triggered when the particular verification request appears in a new block. Consequently, the ownership of the PoL commitment is verified by a zero-knowledge proof algorithm without revealing private keys to anyone else. Hence, the prover can be verified and certified as the owner of the particular PoL commitment, i.e., the prover is witnessed at a certain timestamp.

B. The Network Layer

The network layer takes responsibility for routing data packages between blockchain nodes. Considering lacking retransmission and reordering in User Datagram Protocol (UDP), transmission reliability of large package (block size up to 4 MB) could not meet the network requirement. Bychain uses an unstructured peer-to-peer network with TCP connections as its foundational communication protocol.

Bychain introduces several novel operations in the service layer such that traditional blockchain data structure [34] could not be straightforwardly applied. Take several new operations as an example, 1) the prover intermittently broadcasts a package including multiple PoL commitments collected in a time window. 2) The witness reports its location and virtual forces during every round of consensus procedure. 3) In the blockchain layer, the miner publishes the *incentive allocation* into the next block, which will be detailed in the next section.

Hence, for efficient and confidential data transmission, Bychain reconstructs the transaction structure and then develops a general block format, as shown in Fig.2. More precisely, **Expiration** and **Signature** fields are applied to indicate the producer and timeslot of one transaction. Hence, there would be multiple **Operations** happening over the specified identity and time duration. The broadcasted transactions are stored in a buffer pool to be serially packaged into **Blocks**. The buffer pool is maintained and checked by the consensus committee.

C. The Blockchain Layer

In contrast to existing location-proof methods, the proposed system does not require a trusted centralized third-party. Furthermore, aiming to endow the blockchain with maximizing

the monitoring area, Bychain proposes a new location consensus based on the virtual electric field to maximizing the sum coverage of the location-proofing service. Furthermore, Bychain adopts an interactive zero-knowledge proof method to ensure data confidentiality and anonymity. We will describe the necessary entities and mechanisms in the following.

Blockchain [23] is composed of a distributed database and a peer-to-peer node network. The blockchain database is a secured, shared, fault-tolerant, distributed, and append-only database that facilitates consensus-based recording and tracking information without a centralized, trusted third party. The blockchain network is based on the peer-to-peer communication protocol and untrusted nodes.

All the data processes on the blockchain are decided by the majority users in the blockchain network, and the decision-making procedure is called *consensus generation* or *mining a block*. All the network nodes attend a mining competition in each turn to decide which node can produce and broadcast the new block to the other nodes. The new blocks are composed of new unpacked data in the distributed database. There are several existing *consensus generation* algorithms, including Proof-of-Work (PoW) [27], Proof-of-Stake (PoS) [28], [29], Proof-of-Space (PoSpace) [30] and practical Byzantine fault tolerance (PBFT) [31].

The blockchain system produces cryptocurrency to incentivize miners to take part in competitions for block recording rights in each turn. Due to the majority decision and resource-consuming competition, the blockchain does not rely on a traditional trusted third party when recording data if the majority of network nodes are honest. It is because a successful attack can only occur when the attacker wins enough mining competitions; however, the cost of this *51% attack* would go beyond expectation. According to an analysis in 2018 December [32], it will cost 1.4 billion dollars to realize the *51% attack* in the Bitcoin blockchain.

Although a blockchain is composed of a database and a node network, the decentralized system is able to process some proper, on-chain, and heavily automated workflows by using the concept of the *smart contract* [33]. *Smart contracts* are self-executing scripts stored in the blockchain database and independently executed on each network node in a sandboxed virtual machine. The Turing-complete virtual machine allows us to implement complicated logic smart contracts with deterministic outputs and on-chain data interactions. The smart contract can be regarded as a predetermined on-chain rule triggered by particular on-chain data, such as a specific transaction.

1) Signature and Key Escrow: To validate the authenticity of PoL commitments and on-chain transactions, our blockchain employs the elliptic curve digital signature algorithm (ECDSA) asymmetric cryptography technique. The ECDSA cryptography is implemented by using the secp256k1-based Koblitz curve for the ECDSA key-pair in the open-source project OpenSSL. The generated private witness key is able to sign the PoL messages to authorize that the prover appears in a particular location and at particular timestamps. Furthermore, the on-chain transaction data also need to be signed such that the transaction is traceable and verifiable.
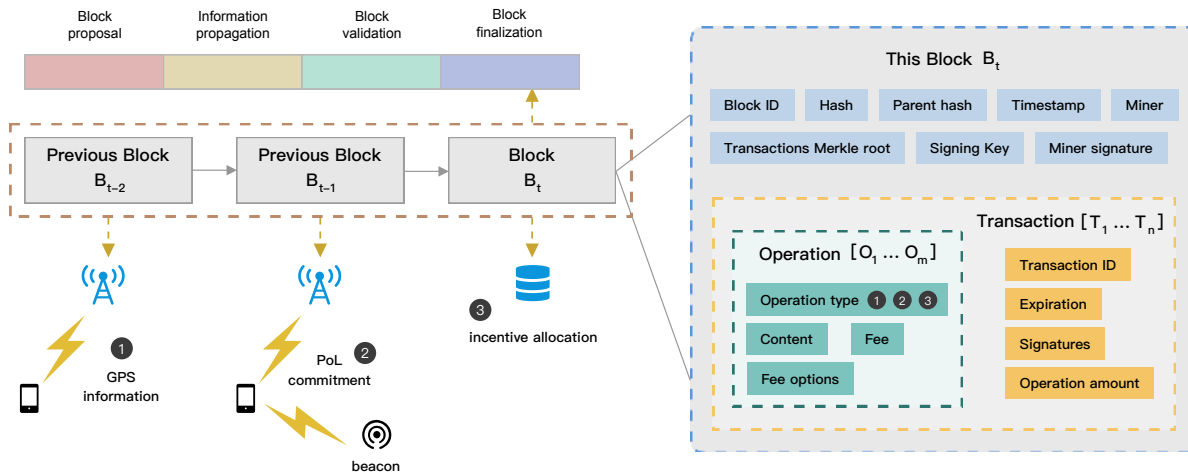
Fig. 2: The proposed generalized block structure, the transaction field is extended to support multiple new operations.

Due to the on-chain data transparency, anyone can access and analyze the on-chain data freely. In this case, identity privacy becomes a critical problem introduced from the blockchain technique because the prover's activity information can be easily tracked on the blockchain. In our protocol, a key escrow is employed for the prover to achieve the separation of identity information and location information. A primary private key and several generated key pairs are initialized and stored in the memory when the system initializes. The generated vital pairs are iteratively employed for each PoL message interaction procedure, and consequently, the generated public key is uploaded into the blockchain database for verification. Because it is almost impossible to calculate the main private key based on the generated public key, we consider that the identity privacy is achieved.

2) Zero-Knowledge Proof Based Authorization: Because the key escrow is applied in our protocol, the only way to verify the identity information of the on-chain PoL commitment is by checking the private key. However, there is no third party that can be trusted to verify the private key on a blockchain system. Otherwise, location privacy may be 'stolen' by copying the private key.

zero-knowledge proof technique tries to help a verifier trust a prover without leaking any secret information to anyone else during the verification procedure. In this paper, we employ an interactive proof scheme in which the prover demonstrates its authorization information (private key) to the verifier by several interactive rounds. During the interactive procedure, the prover answers a randomly generated challenge from the verifier. However, most of the recent zero-knowledge proof based authorization to reply to a trusted third party, which is not always practical in the real world.

In our system, zero-knowledge proof based authorization procedure is considered part of our blockchain so that the information leakage risky from a third party is avoided. Hence, the private key is not required when verifying the clear on-chain proof-of-location commitments.

Furthermore, the blockchain itself can generate and dis-tribute and update sets of pseudonyms (the pairs of the public key and private key as mentioned above) for every prover and witness.

IV. PROPOSED PROTOCOL AND LOCATION-BASED CONSENSUS

In contrast to existing contact tracing and proof-of-location methods, the proposed system does not require a trusted centralized third-party. Furthermore, Bychain proposes a new DPoS consensus based on the virtual electric field to maximize the sum coverage of the location-proofing service. We will describe the necessary entities and mechanisms in the following.

A. Proposed Protocol

Our goal is to establish a contact tracing and location-proofing system that guarantees the authenticity of the user location and activity data with respect to cheating nodes, the underlying untrusted centralized supernode, and malicious nodes, and provide almost complete privacy protection with respect to on-chain nodes that are trying to track provers. In this section, we detail our blockchain-based proof-of-location system. The system is shown in Fig. 1, and the scheme is shown in Fig. 5. In general, there are two kinds of technology that utilizes SRC records for contract tracing in COVID-19. The instant notification to close contacts and the trustable verification for uninfected people. In this paper, we focus on the verification methods. Therefore, two stages are involved in our contact tracing protocol: the proof-of-location stage, and the activity generation stage.

Stage 1: Proof of Location for SRC Record Generation

1) Broadcasting: The broadcasted PoL request can be de-scried by multiple witness nodes as shown in Fig. 3. Suppose a prover p_i at location $L_{i,t}$ wants to start an activity proof collection event at sampling time t, so it periodically generated a location proof request P_i^k using the kth pair of cryptology keys $\{pk_{p_i}^k, sk_{p_i}^k\}$ and broadcasts P_i^k to nearby devices. Note
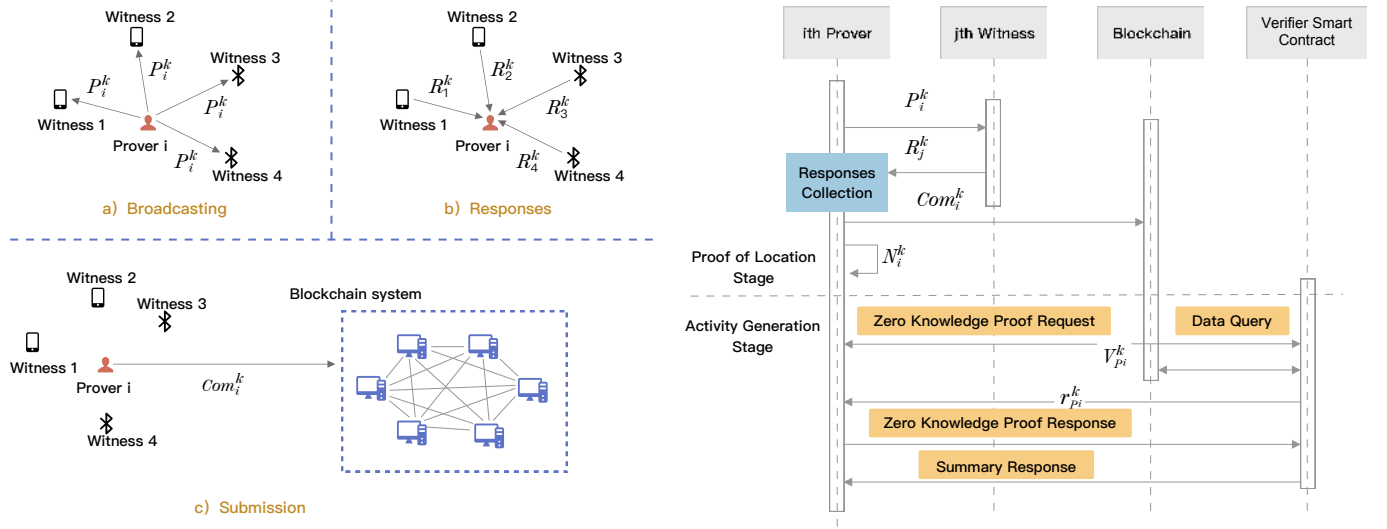
Fig. 3: The proposed protocol consists of two stages, including PoL stage and activity generation stage.

that $\{pk_{p_i}^k, sk_{p_i}^k\}$ will be updated as $\{pk_{p_i}^{k+1}, sk_{p_i}^{k+1}\}$ when this PoL stage is completed. The PoL request is constructed as follows,

$$P_i^k = C\{pk_{p_i}^k, \text{nonce}_{p_i}(t), L_{p_i,t}, t, S_{sk_{p_i}^k}\}, \qquad (1)$$

where $\text{nonce}_{p_i}(t)$ is a random number with respect to prover p_i and timestamp t and $L_{p_i,t}$ represents the current location information at time t. The payload data is compressed by the SHA256 function $\mathcal{H}()$ to reduce the communication complexity in the signature. $S_{sk_{p_i}^k} = \text{Sign}_{sk_{p_i}}\{\mathcal{H}(pk_{p_i}^k, \text{nonce}_{p_i}(t), L_{p_i,t}, t)\}$ denotes the signature of $sk_{p_i}^k$ agrees with the PoL request. The request is specified with respect to wireless protocols that are denoted as $C\{\}$.

2) Response: Each witness in its communication range decides whether to respond to the request. The witness node may reject the PoL request due to fake parameters, for example, the location information in P_i^k shows that distance between the prover and current witness is significantly larger than the communication range. Request rejection also happens if crypto-verification fails, i.e., $S_{sk_{p_i}^k} \neq \text{Sign}_{sk_{p_i}}\{\mathcal{H}(pk_{p_i}^k, \text{nonce}_{p_i}(t), L_{i,t}, t)\}$ or is not paired with the public key pk_{p^k} in P_i^k. If the request is accepted by the witness j, the witness sends back a response message R_j^k at timestamp t'. Without loss of generality, the time difference $t' - t$ is not enough for the prover to move out of witness j's communication range. R_j^k can be constructed as follows,

$$R_j^k = C\{pk_{p_i}^k, \text{nonce}_{p_i}(t), L_{i,t}, t, S_{sk_{p_i}^k}, \text{nonce}_{w_j}, S_{sk_{p_i}^k, sk_{w_j}^k}\}, \qquad (2)$$

where $\text{nonce}_{w_j} = \{pk_j||n\}$ is a combination of public key pk_j of witness j and an unrepeatable built-in counter as n. It is worth noting that pk_j is specific and unique to j-user, and nonce_{w_j} functions as an on-chain index of the PoL commitments.

$$S_{sk_{p_i}^k, sk_{w_j}^k} = \text{Sign}_{sk_{w_j}}\{\mathcal{H}(pk_{p_i}^k, \text{nonce}_{p_i}(t), L_{i,t}, t, S_{sk_{p_i}^k}, \text{nonce}_{w_j})\}, \qquad (3)$$

denotes that a signature of $sk_{p_i}^k$ agrees with this response. This response is sent back to the prover as a witness location proof.

3) Submission: Consequently, a dozen of responses with diverse witness signatures are collected at the prover's antenna in a short time window. If the responses originate from M receivers, then the PoL commitment can be constructed by combining all the PoL responses,

$$\text{Com}_i^k = \{R_1^k||R_2^k||\cdots||R_M^k\}. \qquad (4)$$

Com_i^k is uploaded on the blockchain such that the PoL commitment for kth PoL request at the ith prover is immutable. A trusted level of Com_i^k can be generated at the activation summary depending on number of combined PoL responses. The prover-witness collusion attack can be avoided when M is large enough and the honest witnesses are more than $\frac{M}{2}$. These steps are illustrated in Fig. 3.

For each submitting procedure k, a PoL note is stocked for a further zero-knowledge proof. The PoL note is a combination of private key $sk_{p_i}^k$ in the broadcasted request, the random number $\text{nonce}_{p_i}(t)$ and the collected witness indices $\text{nonce}_{w_1}, \ldots, \text{nonce}_{w_M}$ and can be written as,

$$N_i^k = \{sk_{p_i}^k||\text{nonce}_{p_i}(t)||t||\text{nonce}_{w_1}||\cdots||\text{nonce}_{w_M}\} \qquad (5)$$

PoL notes the function as an identifier of its corresponding on-chain commitment, prover always can precisely locate the on-chain commitment and proofs of the ownership to anyone else by a zero-knowledge proof smart contract verifier without revealing the private key $sk_{p_i}^k$.

Algorithm 1 The Proposed Bychain Protocol

Input: Key pair $\{pk_{p_i}^k, sk_{p_i}^k\}$, Responsed Witeness Set $w_1, w_2, ..., w_M$, Maximum Response Duration T_{max}.

Output: Activity Summary

1 **Stage 1 : Proof of Location**
2 **for** *Prover p_i* **do**
3   Generate and Broadcast PoL request P_i^k according to (1). A clock is initialized as T.
4   **foreach** *witness i in $w_1, w_2, ..., w_M$* **do**
5   PoL response R_j^k is generated according to (2)
6   **end**
7   **while** $T \leq T_{max}$ **do**
8   Responses collection and combination according to (4).
9   **end**
10   Local storage for private key and nonces storage according to (5).
11 **end**
12 **Stage 2 : Activity Generation**
13 **for** *Prover p_i* **do**
14   Generate and transmit verification request according to (6).
15     $r_{p_i}^k$ is returned from contract.
16   Generate and transmit Proof according to (7).
17   **for** *Verifier* **do**
18   **if** $Verify_{pk_i}(Proof) == Sign_{sk_{p_i}}\{\mathcal{H}(nonce_{p_i}(t), r_{p_i}^k)\}$ **then**
19   **if** $Verify_{pk_i}(S_{sk_{p_i}^k})$ equals to $Sign_{sk_{p_i}}\{\mathcal{H}(pk_{p_i}^k, nonce_{p_i}(t), L_{i,t}, t)\}$ **then**
20   Activity Summary transmission starts.
21   **else**
22   The verification is failed.
23   **end**
24   **else**
25   The verification is failed.
26   **end**
27   **end**
28 **end**

Stage 2: Activity Generation for Uninfected Verification In our system, the activity summary is generated by two steps: location verification and summary generation.

1) Location Verification: To verify the kth commitment, a single-round interaction zero-knowledge proof is applied. Firstly, prover p_i produces a verification request,

$$V_{p_i}^k = \{nonce_{w_1} || \cdots || nonce_{w_M}\}. \quad (6)$$

The smart contract verifier searches on-chain data according to index $nonce_{w_1} || \cdots || nonce_{w_M}$. The outcome is the kth PoL broadcasting request, shown as $\{L_{i,t}, nonce_{p_i}(t), pk_i, t, S_{sk_{p_i}^k}\}$. Consequently, the verifier generates a pseudorandom number $r_{p_i}^k$ as response to prepare zero-knowledge verification.

Secondly, the prover signs a proof by using $sk_{p_i}^k$, as

$$Proof = Sign_{sk_{p_i}}\{\mathcal{H}(nonce_{p_i}(t), r_{p_i}^k)\}. \quad (7)$$

The verifier can identify the ownership of the commitment by comparing $\mathcal{H}(nonce_{p_i}(t), r_{p_i}^k)$ with on-chain $nonce_{p_i}(t)$ and local $r_{p_i}^k$, which is according to the randomness of $r_{p_i}^k$ and $nonce_{p_i}(t)$. The private key $sk_{p_i}^k$ will not be revealed to the verifier such that no one can complete the ownership verification in the future except prover i.

Finally, the verifier returns true or false as a result of PoL verification. It implies whether or not the PoL commitment belongs to the specific prover i.

2) Summary generation: After each PoL is verified, the smart contract produces an activation summary, including the trusted level generated from the number of witnesses M and the activation path.

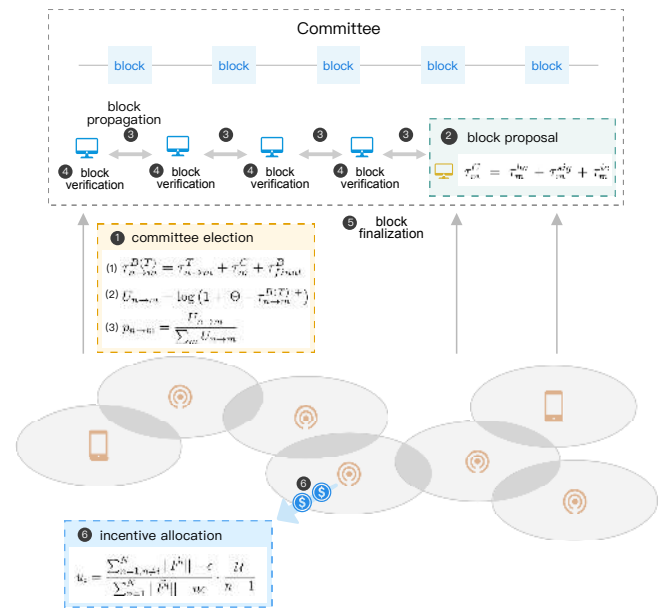### B. Location-based Consensus

Fig. 4: The overview of location based consensus.

In this subsection, we present the details of the location-based consensus algorithm. Inspired from DPoS and aiming to maximize the monitoring area, the proposed consensus algorithm consists of six parts: 1) committee election, 2) block proposal, 3) block propagation, 4) block validation, 5) block finalization and 6) incentive mechanism. Different from DPoS or another consensus, the participants of Bychain are given a different number of votes according to its last location reward. The reward allocation (or incentive allocation) scheme is one of the vital consensus procedures for permissionless blockchain [35], especially to encourage the profit-oriented blockchain participants to act in the way Bychain expect them to. The details about the proposed consensus are introduced in the following.

1) Committee Election: Although every participant in Bychain can be elected as a committee member, the computation capacity limited by hardware should meet the minimum requirement of the block and consensus computation. On the other hand, instead of DPoS, where stockholders vote

for a committee candidate according to personal willingness, the IoT devices in Bychain prefer the candidate with high utility, i.e., the higher network quality and higher computation capacity, the higher probability to be voted.

From the viewpoint of IoT node n, the timestamps of transaction generation, block proposal and block finalization can be observed in the finalized blocks. Therefore, for given Tth transaction that collected by mth committee member in block B, the delay of transaction and block procedure can be written as,

$$\tau_{n \to m}^{B(T)} = \tau_{n \to m}^{T} + \tau_{m}^{C} + \tau_{final}^{B}, \tag{8}$$

where $\tau_{n \to m}^{T}$ denotes the delay of transaction propagation from node n to committee member m. The block computation delay τ_{m}^{C} consists of three parts: a) the hash time consumption τ_{m}^{ha}, b) the signature generation delay τ_{m}^{sig}, and c) the incentive computation delay τ_{m}^{ic}, $\tau_{m}^{C} = \tau_{m}^{ha} + \tau_{m}^{sig} + \tau_{m}^{ic}$. τ_{m}^{ic} will be described in next subsection IV-C. τ_{final}^{B} is the block finalization delay, which is determined according to the overall network quality. For the permissionless blockchain that may be world-widely deployed, τ_{final}^{B} is set to be 3s or 0.5s in Bitshares or EOSIO, respectively.

In general, $\tau_{n \to m}^{B(T)}$ implies the network quality and computation capacity of committee member m that observed by IoT node n. Consider the maximum block processing delay of being a committee member is Θ, we define an utility function to indicate the election,

$$U_{n \to m} = \log \left(1 + [\Theta - \tau_{n \to m}^{B(T)}]^+ \right), \tag{9}$$

where $[a]^+ = \max\{a, 0\}$. $U_{n \to m}$ is set to be 0 when the block processing delay observed by n is more than the given threshold Θ. Otherwise, $U_{n \to m}$ would achieve a logarithmic increment. Therefore, the probability of n voting for m can be written as,

$$p_{n \to m} = \frac{U_{n \to m}}{\sum_m U_{n \to m}}, \tag{10}$$

which means the higher utility of m, the higher chance to be voted. Then the committee $\mathcal{M} = \{1, .., M_c\}$ is elected as the top M_c winners, where M_c is the maximum number of committee members.

2) Block Proposal, Block Propagation and Block Validation: When the committee is elected to take part in a consensus algorithm, at each block generation slot, the committee members take turns to act as a block miner proposing a block in a round-robin fashion.

In a specific block proposal process, the miner packages collected PoL transactions into an unverified block. The incentive allocation is also performed in this procedure. It is elaborated in the next subsection in IV-C. Then the unverified block is propagated to other committee members for block validation. The delay of information propagation highly depends on committee members' geographical distribution and the block size. The other committee members verify the signatures of the block proposer and transaction generator. If the verification is successful, the block is appended into the local block database. Otherwise, the appended procedure would be forbidden.

3) Block Finalization and Incentive Mechanisms: In Bychain, the block finalization follows the Longest-chain rule. Due to network uncertainty and possible malicious participant, the blockchain may be forked into the longest chain and several shorter chains. In this case, the block miner should always propose a block that extends the longest chain. Otherwise, a local database update should be performed ahead of the block proposal.

There are two kinds of incentive mechanisms involved in Bychain: 1) the first incentive is the reward of block generation can claim a certain amount of token reward, 2) the second incentive is allocated to IoT devices for pursuing maximizing monitoring area, which can be rewarded according to certain amount of votes. 1) is commonly applied to encourage more participants to join in the permissionless blockchain systems, e.g., Bitshares, Bitcoins, etc. We will describe 2) in detail.

C. Incentive Allocation for Maximizing Monitoring Area

In this subsection, we detail the incentive allocation mechanism to maximizing the total coverage area. For every 24 hours, or every 28800 blocks at 3s block production interval [1], Bychain issues a fixed-value budget as total incentive of maximizing network communication coverage usage. With omnidirectional mobility, each IoT node is willing to find and deploy itself to where maximizes the next round reward. We define it as an *Incentive Allocation for Maximizing Monitoring Area* problem.

Problem: *Given a coverage budget worth $\mathcal{U}$, and N incentive-pursuing noncooperative nodes with isotropic communication module of available radius R, how should the budget be allocated so that the resulting configuration is tending to maximize the network communication coverage?*.

Before going further, some underlying constraints need to be clarified:

- Global-class computing may not be feasible due to limited computation and power consumption of IoT devices. Furthermore, localization of devices is not globally available because, as mentioned in the last subsection, location ciphertext $L_{p_i, t}$ cannot be publicly understood.
- Bychain opens for anyone to access, read, send, or receive transactions and blocks. Hence, the problem-solution requires high scalability and adaptivity to contain abrupt attendance or absence.
- The connectivity between Bluetooth devices highly depending on the electromagnetic propagation characteristics of the natural environment. In certain scenarios with high path loss and shadow fading, the signal from sources in different directions is necessary to avoid the "dead" coverage zone.

Motivated by potential virtual field in robotic navigation and obstacle avoidance [36], Bychain applies artificial virtual potential field to address above incentive allocation for maximizing monitoring area problem. Each witness node in the blockchain system is treated as a charged particle, such that artificial electric fields are constructed in a way that each

---

[1] Due to fixed block broadcast interval, the number of blocks is a widely used dimension to measure time difference in blockchain system.

node is repelled by repulsive force $\vec{F}_r^{(i,j)}$ from other nodes, thereby forcing the blockchain to spread itself throughout the environment. Bychain then introduces an attractive force $\vec{F}_a^{(i,j)}$ to gather nearby witness nodes, and keep the repetitive coverage area.

1) Potential Field of Single Node: According to the relationship between potential field and force, given ith witness node and jth near-by witness node, the repulsive force with respect to the scalar potential field P_j can be written as,

$$\vec{F}_r^{(i,j)} = -\nabla P_j = \begin{cases} -k_{rep} \cdot \dfrac{1}{r_j^2} \cdot \dfrac{\vec{x}_j - \vec{x}_i}{r_j}, & r_j \leq R_r, \\ 0, & r_j > R_r. \end{cases} \tag{11}$$

where k_{rep} denotes the strength constant of the repulsive field, r_j is the Euclidean distance between node j and node i, where $r_j = ||\vec{x}_j - \vec{x}_i||_2$, $\vec{x}_j$ and $\vec{x}_i$ denote the absolute position of node j and node i, respectively. In general, $\vec{F}_r^{(i,j)}$ is a conservative force that subjects to the gradient of potential field. The piecewise function indicates that each node out of the disc of radius R_r would not affected by its repulsive potential field.

Let us focus on the potential field of ith witness node. As illustrated in Fig.4(a), regardless of the attractive force $\vec{F}_a^{(i,j)}$, $\vec{F}_r^{(i,j)}$ could result in non-overlapping network coverage with uncovered gaps. Indeed, the repulsive-only field could perform well as an initial deployment solution of densely placed nodes. However, it probably conduces a discrete dot-like coverage in urban scene. Therefore, a larger range of attractive field is necessary to gether nearby nodes out of the repulsive field.
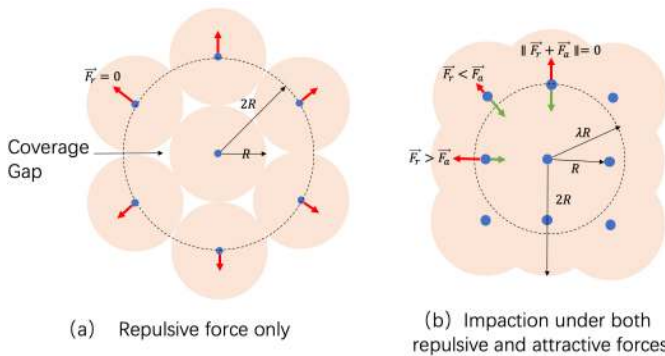

Fig. 5: Illustrations of final coverage caused by potential field. In subfigure (a), we set $R_r = 2R$ and remove the effects of attractive force $\vec{F}_a^{(i,j)}$, where dotted circle denotes the range of repulsive field. At this moment the coverage is maximized, however, resulting in several coverage gaps that lifts the interruption probability of Bluetooth connections. After taking attractive force $\vec{F}_a^{(i,j)}$ into account, subfigure (b) showns a node reaches the force equilibrium at λR.

As illustrated in Fig.4(b), an attractive field of $\vec{F}_a^{(i,j)}$ is constructed subjects to $||\vec{F}_a^{(i,j)} + \vec{F}_r^{(i,j)}|| = 0$ on the circle of radius λR. Furthermore, for nearby node j, we wish $\vec{F}_a^{(i,j)}$ growth exponentially with r_j, such that node i is able to

pull far-distant node back. Hence, $\vec{F}_a^{(i,j)}$ is constructed as following,

$$\vec{F}_a^{(i,j)} = \begin{cases} -k_{att} \cdot \dfrac{1}{(r_j - R_r)^2} \cdot \dfrac{\vec{x}_j - \vec{x}_i}{r_j}, & r_j \geq R_r, \\ 0, & r_j < R_r. \end{cases} \tag{12}$$

where k_{att} denotes the strength constant of the attractive field. The resultant force between node i and node j is

$$\vec{F}^{(i,j)} = \vec{F}_a^{(i,j)} + \vec{F}_r^{(i,j)}. \tag{13}$$

Meanwhile, the combined attractive and repulsive potential field construct a zero potential ring at radius λR such that $||\vec{F}_a^{(i,j)} + \vec{F}_r^{(i,j)}|| = 0$, shown as the red circle in Fig.5. By substituting (11), (12) and $r_j = \lambda R$ into constraint $||\vec{F}_a^{(i,j)} + \vec{F}_r^{(i,j)}|| = 0$, the relationship between strengths of potential fields k_{rep} and k_{att} could be written as following,

$$k_{att} \cdot \frac{1}{(\lambda - 1)^2 R_r} - k_{rep} \cdot \frac{1}{\lambda^2 R^2} = 0. \tag{14}$$

Hence,

$$\lambda^2 k_{att} = (\lambda - 1)^2 k_{rep}. \tag{15}$$
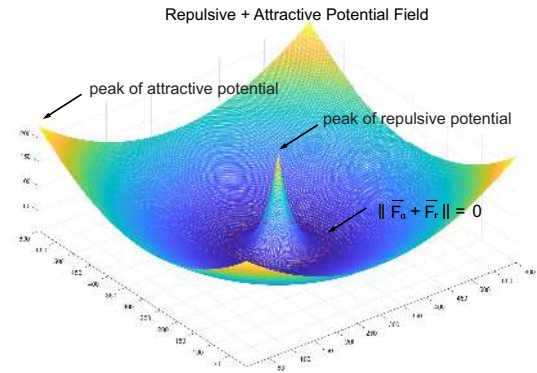

Fig. 6: Illustration of the combined potential field, where a witness node locates at (200,200).

2) Potential Field and Intensive of Multiple Nodes: Let's extend the perspective to the relationship between multiple nearby nodes, denote as a node set $\mathcal{K}$. The total force of node i can be given by,

$$\vec{F}^i = \sum_{j \in \mathcal{K}} \vec{F}_a^{(i,j)} + \sum_{j \in \mathcal{K}} \vec{F}_r^{(i,j)} \tag{16}$$

The total force of node i results in an acceleration that adjust its velocity according to the well-known *Equation of Motion*. Therefore, given consensus round k, node i with velocity $\vec{v}_k$, the new velocity $\vec{v}_{k+1}$ can be written as:

$$\vec{v}_{k+1} = \vec{v}_k + \frac{\vec{F}^i - \alpha \vec{v}_k}{m}, \tag{17}$$

where $\alpha < 1$ denotes viscosity factor and m is the virtual mass of this node.

Network Static Equilibrium and Intensive: It is obvious that the network could asymptotically approach a static

equilibrium because the viscous friction term results in monotonically decreasing system energy over time. Hence, one can see a necessary condition for the maximum coverage of the network is the equilibrium on each node.

Therefore, if blockchain aims to encourage nodes to participate in above coverage maximization, such objective should design proper budget allocation strategy to incentive motion of each node. Hence, Bychain allocates the coverage intensive to node i as follow,

$$u_i = \frac{\sum_{n=1,n\neq i}^{N} ||\vec{F}^n|| + \epsilon}{\sum_{n=1}^{N} ||\vec{F}^n|| + n\epsilon} \cdot \frac{\mathcal{U}}{n-1} \quad (18)$$

where ϵ is a perturbation factor that sufficiently small preventing denominator to be 0. (18) performs three key characters: 1) the incentive of node i would decrease as $||\vec{F}^i||$ increase. 2) When the network static equilibrium, each node would be distributed $\frac{1}{n}\mathcal{U}$ budget. 3) The sum of network budget still approximately equal to $\mathcal{U}$.

V. Security Analysis

In this section, we analyze our proposed blockchain's security properties and prove that the protocol can achieve our security goals.

1) A prover cannot generate a location proof without a witness.

Since witnesses do not give away their private keys, a prover cannot claim the activities information by signing it using the private key of the witness. If this situation occurs, the blockchain key cryptography system can detect it.

2) If the witness does not reveal the private key, a prover cannot generate a legitimate location proof at the claimed location and claimed time without colliding with more than half of the witnesses.

If a witness does not provide its private key, the digital signature cannot be produced by any node except by the witness itself. In this case, there may be two kinds of attack: (1) the prover may provide a false location claim, or (2) the prover may perform *signature relaying attack*, that is, store the digital signature in the last location and transmit it in the current location.

The attack (1) can be detected easily since the communication between the witness and prover is always near-range communication. The witness will always calculate the distance between the prover and the witness. If the distance calculated from the physical layer is significantly different from the claimed location information, this attack can be easily detected by the witness. (2) There is an auto-increment field $nonce_{w_j}$ corresponding to the jth witness w_j. Consequently, the $nonce_{w_j}$ is different in each PoL. If the attack (2) occurs, the signature could not be the same due to $nonce_{w_j}$. Therefore, attack (2) can be easily detected by verifying the content.

In the proof-of-location stage, the prover may receive more than one proof-of-location response. Since the witness is semi-trusted and majority-honest, the attack can be conveniently detected by analyzing the proof-of-location responses if the prover does not collude with more than half of the witness nodes.

3) The prover, witness and verifier are not able to modify generated activity proofs.

In the second stage, the proof-of-location information is uploaded on the blockchain, and the data on the blockchain is transparent and tamper-resistant. It is almost impossible to modify the generated activity proofs.

4) This protocol is able to avoid the PoL replaying attack on the blockchain.

Due to the consistency of the blockchain database, the on-chain storage space is precious. A malicious user may resubmit the PoL commitment to occupy the storage space, named the *PoL replaying attack*. Since each peer of the blockchain network checks, if the current PoL is contained in the blockchain database before submitting, it is not possible to successfully complete the replaying attack.

5) A verifier can verify the activity information without the private key of the proof.

The zero-knowledge proof is applied in our protocol. The private key will not be revealed to the service provider. The signature of the activity information is verified by providing the verifier, a signed verifier-specified nonce, and this kind of attack can be avoided.

6) Only the prover and verifier can access the location information in this protocol, such that the privacy is maximized.

While these activity proofs are uploaded on the blockchain such that they are transparent to all the other users, the public key and private key are managed by key escrow and changed in each k proof-of-location stage. No one can connect this information with an uniform identity. At the same time, the user does not need to reveal its private key to anyone else when verifying ownership, such that the risk of revealing the private key is avoided. Hence, privacy is maximized.

VI. Implementation and Evaluation

To verify our system in a real-world setting, we implement production-grade software by using Bluetooth 5.0. The implemented system is shown in Fig.7. In this section, we study the performance and constraints of our proposed protocol, such as the message interaction latency, power consumption, computation and storage limitations. The main software components and data structures are shown as follows.

- Programming Language: The client is implemented using Java and Kotlin while the blockchain server and smart contract are implemented using C++. Kotlin is a statically typed language with a type inference suggested as an alternative to Java on the Android platform. We use Kotlin to reduce the programming complexity on the client interface. Due to the low computation cost, C++ is considered to be one of the best choices of our blockchain system.
- Bluetooth 5.0: This is latest version of the Bluetooth wireless communication protocol. We adopt Bluetooth 5.0 in our protocol to study the feasibility of our protocol under the latest wireless standards. The PoL message exchange can also benefit from the extended advertising data length such that the signal Bluetooth frame is able to carry our PoL requests and PoL responses. In our

software, the Bluetooth 5 advertising extension mode is employed. The primary physical layer parameter is LE 1M and the secondary physical layer is LE 2M.

- OpenSSL: This is a general-purpose cryptography library for the transport layer security (TLS) and secure sockets layer (SSL) protocols. The OpenSSL library is a successor of commercial-grade and full-featured cryptography implementations. OpenSSL is required in our protocol to provide signing, signature verification, key pairs generation and key escrow operations.
- Bitcoinj-core: This is a Java implementation of the Bitcoin protocol for building blockchain applications. Peer-to-peer communication, network nodes organization and the blockchain object database are implemented and applied in our protocol.
- nRF-connect: This is wireless performance analysis software that is produced by Nordic Semiconductor, including Bluetooth, WiFi and cellular signals. The received signal strength indication (RSSI), packet history, packet changes, Bluetooth advertising intervals, etc., can be analyzed using nRF-connect in real time and in real-world applications.
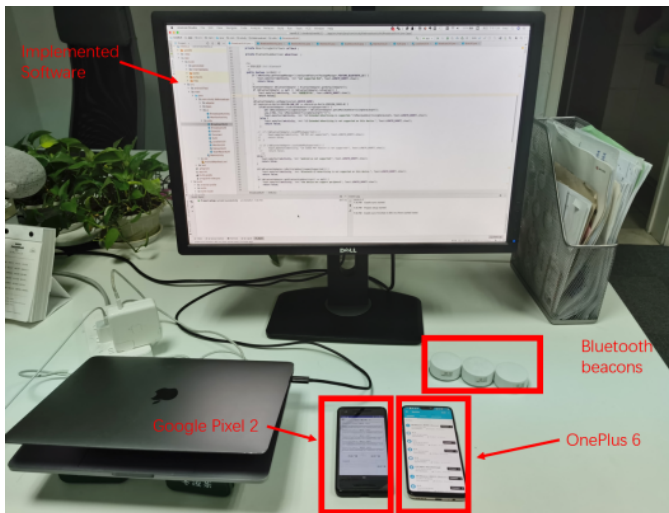

Fig. 7: Implemented System which is composed of a Google Pixel2, an One Plus 6, several Bluetooth beacons and the blockchain nodes running on Alibaba Cloud.

Blockchain network and nodes: We realize our protocol on Alibaba Cloud. On the blockchain, we generate the genesis block (known as the first block of blockchain) using the unique Merkle hash root at 2017-09-05 12:15:00. After two years of running, it is proved that our DPoS blockchain is stable in practice. We then modified its incentive mechanism from March 2020. Because the on-chain data transaction is not heavy, the current size of our private blockchain database is approximately 2.4 GB and the number of network nodes is approximately 65. Note the number of nodes varies from 60–68 during the experiment. To simulate the real world, our blockchain is implemented on an Intel(R) Xeon(R) CPU E5-2650 v3 platform with 2 GB RAM and 10 Mbps bandwidth for each node is provided by Alibaba Cloud and Amazon Cloud.

Nodes in the blockchain network are virtual private servers such that they broadcast and receive block messages via a physical communication link. The mining interval is set as 3 s.

The provers and witnesses: To mimic real-world user activities, we developed a client to realize the functions required by the prover and witness. The client is implemented by Java and Kotlin on One Plus 6 and Google Pixel 2 (all with Android 9.0). One plus 6 equips Qualcomm SDM845 Snapdragon 845 (10 nm) with 4x2.8 GHz CPU cores and 4×1.7 GHz CPU cores, 6 GB RAM, WiFi 802.11 a/b/g/n/ac, Bluetooth 5.0 and a GPS module. Google pixel 2 equips Qualcomm MSM8998 Snapdragon 835 (10 nm) with 4×2.35 GHz CPU cores and 4×1.9 GHz CPU cores, 4 GB RAM, WiFi 802.11 a/b/g/n/ac, Bluetooth 5.0 and a GPS module. Both One Plus 6 and Pixel 2 can communicate with blockchain via the WiFi or 4G signal provided by China Mobile.

Data structure: The interacted message involved in our protocol includes the following: the PoL request P^k, the PoL response R^k, the PoL commitment Com^k and the verification information N^k. In our protocol, the length of P^k advertising data is approximately 320 bytes including a 128-bit service UUID and payload data shown in (2). The message length is heavily dependent on the key length of the cryptosystem. There always exists a trade-off between the performance and security level when deciding the public key length. Our public key is a 160-bit hash of the SHA256 hashed ECDSA public key and the private key is abstract syntax notation one (ASN.1) coded strings. The signature of the PoL commitment is a 65-bit ECDSA formed signature. As a comparison, the length of R^k is approximately 540 bytes, and the PoL commitment under a single witness is approximately 520 bytes. The location information is required from the GPS module with 14 bit data and 10^{-7} accuracy, i.e., centimeter-level location information.

A. System Performance

In this subsection, we study the performance and cost of deploying our protocol including the storage, CPU, power consumption, and the latency in each procedure. We also measure the system performances under various relative velocities and number of witnesses.

1) Storage, CPU and Power Consumption: The running of the client code costs approximately 120 MB of data memory, while the blockchain system takes approximately 3.5 GB of data memory. With 62 blockchain network nodes mining the block, the blocks of uploaded location information generate each 6 seconds. Considering that the peer-to-peer network propagation delay is unstable, we monitor the *arrived time interval of each block* indicating the timestamp differences of the current arrived block and the last arrived block. The result shows that the minimum time interval is 6532 milliseconds and the maximum time interval is 13245 milliseconds. The arrived time interval depends on the network condition, such as the retransmission rate and the verification delay of the PoS algorithm. Therefore, we believe that a powerful CPU and the adjoining blockchain network node may have a positive effect on the blockchain propagation time.

TABLE I: CPU and power consumption of each entity

Property	Distance d_{p-w}(m)	CPU utilization(%)			Power Consumption P_E (mW)		
		minimum	maximum	mean	minimum	maximum	mean
Prover	3 m	2	7	4	356	552	456
	15 m	3	7	4.5	468	636	534
Witness	3 m	0.2	0.9	0.5	296	350	323
	15 m	0.4	1.1	0.6	394	538	432
Blockchain Miner		15	43	30			

We monitor the CPU utilization of each prover, the witness nodes and the blockchain nodes. When the prover node is broadcasting and the witness node is monitoring, the CPU consumption is approximately 4 percent and 0.5 percent, respectively. This may be due to the listening Bluetooth signal employing less computation than the emitting Bluetooth signals. Another possible reason is that the cryptosystem involved in the prover processing flow costs more in terms of computation. The CPU utilization of blockchain mining nodes is always above 30 percent. We also realize that the CPU utilization of the network mining node reaches a peak when it is mining the block, in which heavy computations such as authentication and encryption/decryption are involved.

The power consumption of the prover, witness and blockchain is studied as well. We monitor the device power consumption before and after the program launched as P_{before} and P_{after}, respectively. Hence the power consumption of each entity can be computed as $P_E = P_{after} - P_{before}$. The experiment is evaluated 50 times for each entity to study its statistical properties, which is shown in Table I. For each experiment and each entity, we measure the CPU utilization and power consumption with distances $d_{p-w} = 3\,m$ and $15\,m$ between the prover and witness. It is shown that farther Bluetooth signal interaction causes higher power consumption while computation varies little.

2) Delay Evaluation: We evaluate the time delay of each procedure in a relative static environment, where the prover and witness are immobile. The system parameters are shown in Table II. During the evaluation, the PoS blockchain system is maintained by 65 mining nodes. The Pixel 2 is in witness mode and One Plus 6 phone is set in the prover mode with the advertising interval $t_{adv} = 100\,ms$, which is the minimum advertising interval provided in the Android Bluetooth Low Energy API . We set the maximum advertising duration $t_{adv} = 1000\,ms$ in the implementation.

The reason for this setting is to try to minimize the detection delay that is caused by random access methods in the Bluetooth protocol. Ideally, the prover's Bluetooth module broadcasts an advertising frame in each advertising event, while the duration of advertising event is controlled by the advertising interval. However, the scanning window of the witness's Bluetooth module is independent of the prover's advertising event, such that the Bluetooth message interaction succeeds if and only if the witness's scanning window coincides with the prover's advertising event. Because

TABLE II: Parameters used in the delay evaluation.

Parameters	Description	Value	Unit
N	Number of Blockchain Mining Nodes	65	
d_{p-w}	Distance between Prover and Witness	1	m
t_{adv}	Advertising Interval	100	ms
P_{tx}	Prover and Witness Transmit Power Level	−11	dBm
	Primary Physical Layer Parameters	LE 1M	
	Secondary Physical Layer Parameters	LE 2M	
t_{adv}^{MAX}	Maximum Advertising Duration	1000	ms
S_{block}^{MAX}	Maximum Block Size	2	MB
S_{COMM}^{MAX}	Maximum Commitment Size	9	KB

the prover does not share its information with witnesses, the message interaction of the prover and witness is considered to be a random access event. We set the minimum advertising interval to improve the possibility of successive Bluetooth message interactions. Hence, the communication delay of the PoL message interaction will be minimized.
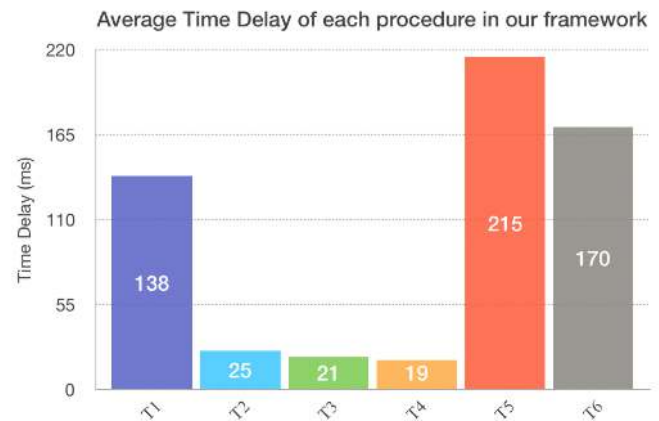

Fig. 8: Average time delay of each procedure. T1 is the key escrow generation (key-pair generation for 100 times), T2 denotes the PoL request generation, T3 represents the delay of the PoL request emission task, T4 is the time cost of signature generation, T5 is the time cost of PoL commitment uploading, T6 is the signal propagation delay between the prover and witness.

We also constrain the blockchain parameters' maximum block size S_{block}^{MAX} and maximum commitment size S_{COMM}^{MAX} as 2 MB and 9 KB to mimic real-world network conditions, respectively. In our experiment, the adoption of Alibaba Cloud

and Amazon Cloud may cause unrealistic network conditions because the blockchain miner is considered to be worldwide and under various network conditions. The network condition of our miner nodes are much better than the average blockchain miners such as Bitcoin miners, including the average packet loss probability, the network bandwidth and average latency. A large block size (>2 MB) and commitment size (>9 KB) increase the computation complexity and bandwidth requirement such that it is much more difficult to maintain the data consistency of the distributed blockchain database. According to the running parameters of the Bitcoin blockchain, we adopt $S_{\text{block}}^{\text{MAX}} = 2\,\text{MB}$ and $S_{\text{COMM}}^{\text{MAX}} = 9\,\text{KB}$ to mimic a world-wide deployed blockchain system.
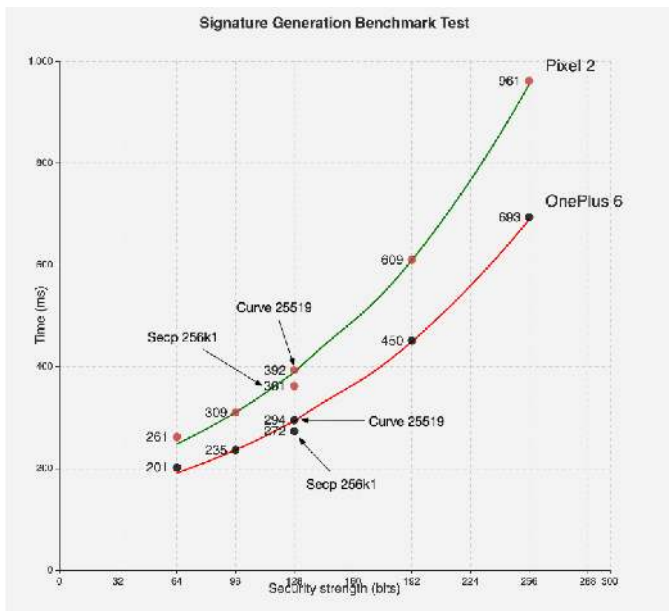

Fig. 9: Time comparison under different security strengths.

To study the sensitivity of our protocol to the time delay of each procedure, we evaluate the time durations of key escrow generation, PoL request generation, PoL request emission, signature generation, PoL commitment uploading and the over-the-air signal propagation delay. After a 50-turn test, the average time delay of each procedure is illustrated in Fig. 8. Among these procedures, the key escrow generation, PoL commitment uploading and the over-the-air signal propagation delay are significantly higher than the others. The PoL commitment uploading is limited by the propagation delay and churn of the peer-to-peer blockchain network; thus it is observed to have high volatility that increases to 421 ms and decreases to 121 ms. The signal propagation delay is determined by the channel states of Bluetooth with respect to the relative velocity and activity between the prover and witness. We will further study the influence of key escrow generation and activity in next paragraph.

The generation of key pairs and signature is studied to evaluate the authentication performance and security. The delay of the key and signature generation and verification is highly dependent on the device performance. We run key pair generation and signature verification 10,000 times regarding secp256k1

(with 128 bits of security strength), secp128r1 (with 64 bits security strength), secp192k1 (with 96 bits security strength), secp384r1 ((with 192 bits security strength)), secp521r1 (with 256 bits security strength), and curve25519 (with 128 bits security strength) on One Plus 6 and Pixel 2. The performances of key generation under different security strengths are shown in Fig. 9. The performance evaluation shows that the time cost increase exponentially with the security strength. However, the curve 25519 algorithm performs with more complexity than secp256k1 even in same security strength. Hence, secp256k1 is implemented in our blockchain system.

3) Activities Evaluation: We further evaluate the sensitivity of over-the-air signal propagation to the received signal strength indication (RSSI) and various activity conditions. We adopt Pixel 2 as the prover, all witnesses are static, the experimental tests are conducted in an urban area, and the initial activity condition is shown in Fig. 10(a). It is shown that the RSSI decreases with the more significant initial distance d_{p-w} and the tremendous accelerated velocity of a; this confirms our intuition and suggestions. When a barrier wall appears in the experiment, the Bluetooth signal faces significant fading such that there appears a 2-second gap in subfigure (h). The PoL message interactions are impossible in this signal gap. A prover walking through multiple witness nodes is evaluated in (j), (k), and (l): the witnesses are placed around the prover in (j), and one-by-one in (k) and (l). The signals that originate from different witnesses are painted with different colors. The result confirms that our protocol works well to collect multiple witness messages in an urban area. Although the PoL message interaction could not coincide, the time interval between each PoL message interaction event is still acceptable at 0.4–2 s, such that a running user could not run out of the coverage area of Bluetooth 5.0 equipment.

VII. CONCLUSION

In this paper, we proposed and implemented a decentralized blockchain system to address the security, privacy and deploy efficiency issues for digital contact tracing to against the COVID-19 pandemic. In the proposed protocol, data security of contact tracing and location-proof is addressed by a combination of cryptographic techniques and a decentralized blockchain system without reliance on trusted third parties. The identity privacy problem is protected by proposing a combination technique of zero-knowledge proof and key escrow. The connection of unique cryptographic identity and on-chain proof-of-location commitment is decoupled such that it is almost impossible to track and identify the owner of transparent on-chain data. Hence, data security and identity privacy in contract tracing is protected. An virtual potential field based incentive allocation method is proposed and applied in the consensus procedure of blockchain, aims to maximize the monitoring area. Several implement results show that the proposed contact tracing and location-proofing technology works well even in the real world. The power consumption, time delay of each procedure and BLE performance of the proposed contract tracing protocol has been analyzed to confirm the availability of real-world digital contact tracing.
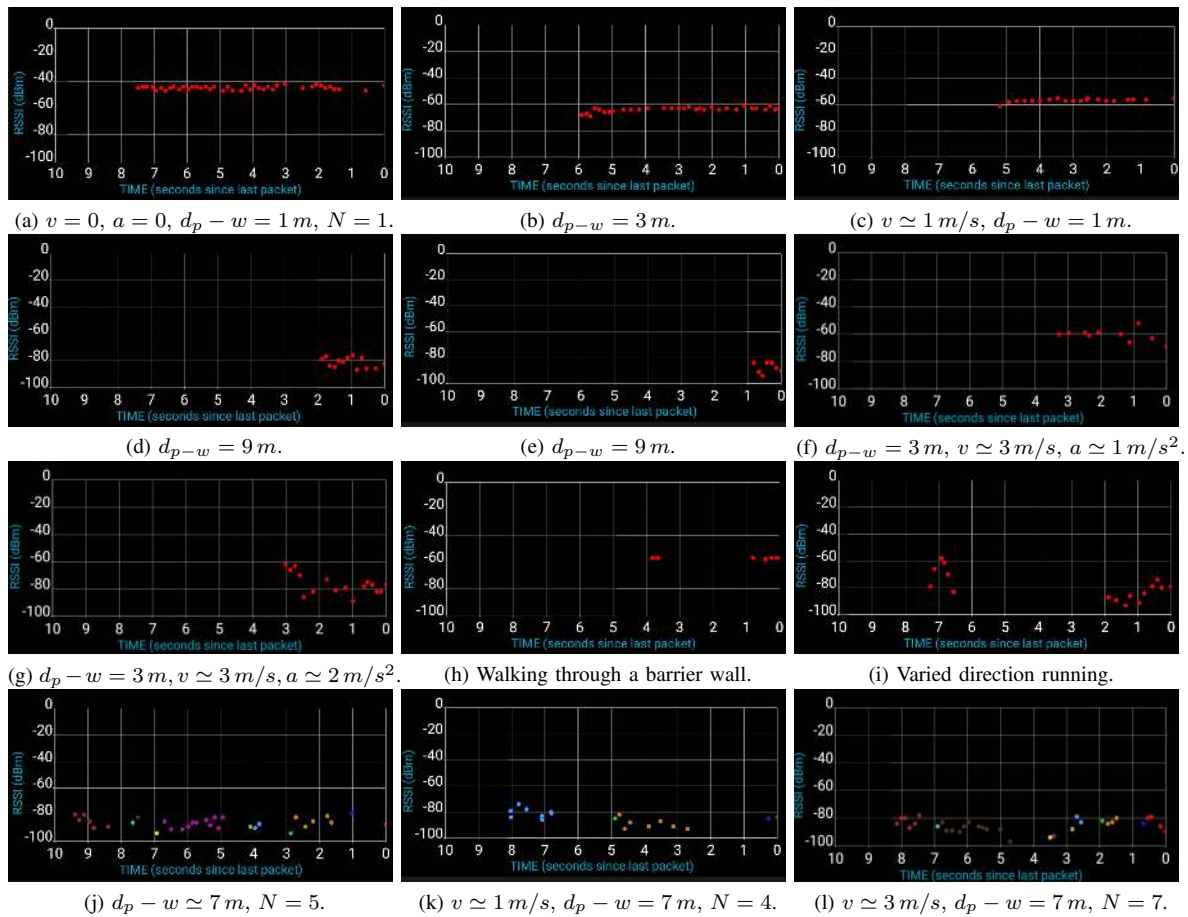
(a) $v = 0$, $a = 0$, $d_p - w = 1\,m$, $N = 1$.

(b) $d_{p-w} = 3\,m$.

(c) $v \simeq 1\,m/s$, $d_p - w = 1\,m$.

(d) $d_{p-w} = 9\,m$.

(e) $d_{p-w} = 9\,m$.

(f) $d_{p-w} = 3\,m$, $v \simeq 3\,m/s$, $a \simeq 1\,m/s^2$.

(g) $d_p - w = 3\,m$, $v \simeq 3\,m/s$, $a \simeq 2\,m/s^2$.

(h) Walking through a barrier wall.

(i) Varied direction running.

(j) $d_p - w \simeq 7\,m$, $N = 5$.

(k) $v \simeq 1\,m/s$, $d_p - w = 7\,m$, $N = 4$.

(l) $v \simeq 3\,m/s$, $d_p - w = 7\,m$, $N = 7$.

Fig. 10: Prover Activities Experiment under different velocity v, accelerated velocity a, initial distance d_{p-w}, environment and witness number N.

VIII. FUTURE WORK

As analysed in previous sections, data security, identity privacy and deploy efficiency issues are three of the most important issues of the digital contract tracing approaches. They are all under investigation although the contact tracing applications have been deployed around the world. There are also some engineering aspects related to our proposed work, e.g. the data storage of user devices may be fulfilled rapidly when the witnesses are densely deployed; the witnesses may be not always semi-honest while there is an economic incentive in practice. Last but not the least, federal leaning, blockchain and edge computation have been considered to be powerful enabling technologies in contract tracing method to perform on-line and secure data analysis and sharing, respectively.

REFERENCES

[1] Aruba, *Location Service with Aruba Bluetooth Beacons*, Aruba, June 10, 2019. Accessed on: Feb 13, 2020. [Online]. Available: https://www.arubanetworks.com/products/location-services/aruba-beacons/

[2] J. D. Angrist, S. Caldwell, and J. V. Hall, *Uber vs. Taxi: A Driver's Eye View*, Tech. report, National Bureau of Economic Research, 2017.

[3] S. Bertoni, *Oscar Health Using Misfit Wearables to Reward Fit Customers*, *Forbes*, Dec. 8, 2014. Accessed on: Sept. 22, 2019. [Online]. Avalialbe: https://www.forbes.com/sites/stevenbertoni/2014/12/08/oscar-health-using-misfit-wearables-to-reward-fit-customers

[4] F. Luca, et al. "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science*, vol. 368, pp. 6491, May 2020.

[5] C. Hyunghoon, I. Daphne and Yu. Yun William, "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs," *arXiv preprint arXiv:2003.11511*. ArXiv, Mar. 2020.

[6] M. Talasila, R. Curtmola, and C. Borcea, "Link: Location verification through immediate neighbors knowledge," in *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*. Springer, 2010, pp. 210–223.

[7] J. Li and X. Guo, "COVID-19 Contact-tracing Apps: A Survey on the Global Deployment and Challenges," *arXiv preprint arXiv:2005.03599*. ArXiv, Mar. 2020.

[8] Apple Inc., *Privacy-Preserving Contact Tracing*, Apple Inc., Dec. 31, 2019. Accessed on: Feb 20, 2020. [Online]. Available: https://www.apple.com/covid19/contacttracing

[9] G. Fortino, F. Messina, D. Rosaci and G. M. L. Sarne, "Using Blockchain in a Reputation-Based Model for Grouping Agents in the Internet of Things," *IEEE Transactions on Engineering Management*. IEEE, June 2019.

[10] G. Fortino, F. Messina, D. Rosaci and G. M. L. Sarne, "Using trust and local reputation for group formation in the cloud of things," *Future Generation Computer Systems*. Elsevier, vol. 89, pp. 804-815, Dec. 2018.

[11] J. Qiu, D. Grace, G. Ding, J. Yao and Q. Wu,"Blockchain-Based Secure Spectrum Trading for Unmanned-Aerial-Vehicle-Assisted Cellular Networks: An Operator's Perspective," *IEEE Internet of Things Journal*. IEEE, vol.7, pp 451-466, Sept. 2019.

[12] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han and R. Buyya,"BlockSDN: Blockchain-as-a-Service for Software Defined Networking in Smart City Applications," *IEEE Network*. IEEE, vol.34, pp 83-91, June 2020.

[13] G. S. Aujla, A. Singh, M. Singh, S. Sharma, N. Kumar and K. R. Choo,"BloCkEd: Blockchain-Based Secure Data Processing Framework

in Edge Envisioned V2X Environment," *IEEE Transactions on Vehicular Technology*. IEEE, Feb. 2020.

[14] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K. R. Choo, "Neural-blockchain-based ultrareliable caching for edgeenabled UAV networks," *IEEE Transactions on Information Theory*, IEEE, vol. 15, pp. 5723-5736, Oct. 2019.

[15] J. Wang and C. Jiang and H. Zhang and Y. Ren and K. Chen and L. Hanzo, "Thirty Years of Machine Learning: The Road to Pareto-Optimal Wireless Networks," *IEEE Communications Surveys & Tutorials*, IEEE, vol. 22, no. 3, pp. 1472-1514, 2020.

[16] C. Jiang and H. Zhang and Y. Ren and Z. Han and K. Chen and L. Hanzo,"Machine Learning Paradigms for Next-Generation Wireless Networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 98-105, 2020.

[17] C. Jiang and X. Zhu,"Reinforcement Learning Based Capacity Management in Multi-Layer Satellite Networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 7, pp. 4685-4699, 2020.

[18] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things Journal*, vol. 6, no. 2, pp.1495–1505, Apr. 2019.

[19] D. Doolittle et al., *UT students use fake GPS signals to take over superyacht,* July 2013. Accessed on: Mar 10,2020. [Online]. Available: www.HispanicBusiness.com

[20] B. Carbunar and R. Potharaju, "You unlocked the Mt. Everest badge on foursquare! Countering location fraud in Geosocial Networks," in *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*. Las Vegas, 2012, pp. 182-190.

[21] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *European Workshop on Security in Ad-hoc and Sensor Networks*. Berlin, 2007, pp. 129-141.

[22] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: Applications, challenges and implementations," in *Proceedings of the 9th Workshop on Mobile Computing Systems and Applications*. New York, 2008, pp. 60-64.

[23] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *IEEE P2P 2013 Proceedings*. Italy, 2013, pp. 1-10.

[24] A. Pham, K. Huguenin, I. Bilogrevic, I. Dacosta, and J.-P. Hubaux, "Securerun: Cheat-proof and private summaries for location-based activities," *IEEE Transactions on Mobile Computing*, IEEE, vol. 15, pp. 2109-2123, Aug. 2015.

[25] Z. Zhu and G. Cao, "Toward privacy preserving and collusion resistance in a location proof updating system," *IEEE Transactions on Mobile Computing*, IEEE, vol. 15, pp. 51-64, Nov. 2011.

[26] X. Wang, A. Pande, J. Zhu, and P. Mohapatra, "STAMP: Enabling privacy-preserving location proofs for mobile users," *IEEE/ACM Transactions on Networking*, IEEE, vol.24, pp. 3276-3289, Dec. 2016.

[27] S. Nakamoto et al., *Bitcoin: A Peer-to-Peer Electronic Cash System*, Working Paper, 2008.

[28] F. Saleh, *Blockchain without waste: Proof-of-stake,* May 2019. Accessed on: Oct. 2019. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3183935

[29] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual International Cryptology Conference*. Berlin, 2017, pp. 357–388.

[30] G.-T., Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain." *Journal of Information Processing System.*, vol. 14, no. 1, pp. 101-128, Jan. 2018.

[31] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, Chicago, Illinois, 2016, vol. 310.

[32] M. Moos, *Analysis: Bitcoin costs $1.4 billion to 51% attack, consumes as much electricity as Morocco*, Cryptoslate, Nov. 29 2018. Accessed on: Feb. 20,2020. [Online]. Availalbe: https://cryptoslate.com/analysis-bitcoin-costs-1-4-billion-to-51-attack-consumes-as/

[33] V. Buterin et al., *A Next-Generation Smart Contract and Decentralized Application Platform*, White Paper, vol. 3, 2014.

[34] L. Zhou, L. Wang, Y. Sun and P. Lv, "BeeKeeper: A Blockchain-Based IoT System With Secure Storage and Homomorphic Computation." *IEEE Access*, IEEE, vol. 6, pp. 43472-43488, 2018.

[35] X. Yang and Z. Ning and L. Wenjing and H. Y Thomas, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, IEEE, vol. 22, pp. 1432-1465, Jan. 2020.

[36] F. E. Scheider, D. Wildermuth, and H.-L. Wolf, "Motion coordination in formations of multiple mobile robots using a potential field approach," *Distributed Autonomous Robotics Systems*, Springer, pp. 305-314, 2000.
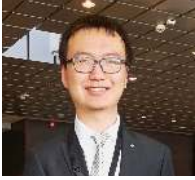
Wenzhe Lv received his B.S degree in Harbin Institute of Technology in 2012. He is currently working toward the Ph.D degree at Beijing University of Posts and Telecommunications. His research interest focuses on blockchain technology and distributed system.

Sheng Wu (S'13-M'14) received the B.S. and M.S. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2004 and 2007, respectively, and the Ph.D. degree in electronic engineering from Tsinghua University, Beijing, in 2014. He was a post-doctoral researcher in the Tsinghua Space Center at Tsinghua University, Beijing, China. He is currently an Associate Professor with the Beijing University of Posts and Telecommunications. He has published over 60 journal and conference papers. He also holds over 30 granted patents. His research interests are mainly in iterative detection and decoding, channel estimation, massive MIMO, and satellite communications. He has received the first prize from the Science and Technology Award of Chinese Institute of Electronics in 2017, the silver medal from the 46th Geneva International Exhibition of Inventions in 2018, the second prize from the National Technological Invention Award of China in 2018, and the Natural Science Foundation of China Excellent Young Scientists Fund Award in 2020.

Chunxiao Jiang (S'09-M'13-SM'15) is an associate professor in School of Information Science and Technology, Tsinghua University. He received the B.S. degree in information engineering from Beihang University, Beijing in 2008 and the Ph.D. degree in electronic engineering from Tsinghua University, Beijing in 2013, both with the highest honors. His research interests include application of game theory, optimization, and statistical theories to communication, networking, and resource allocation problems, in particular space networks and heterogeneous networks. Dr. Jiang has served as an Editor of IEEE Internet of Things Journal, IEEE Network, IEEE Communications Letters, and a Guest Editor of IEEE Communications Magazine, IEEE Transactions on Network Science and Engineering and IEEE Transactions on Cognitive Communications and Networking. He has also served as a member of the technical program committee as well as the Symposium Chair for a number of international conferences, including IEEE CNS 2020 Publication Chair, IEEE WCSP 2019 Symposium Chair, IEEE ICC 2018 Symposium Co-Chair, IWCMC 2020/19/18 Symposium Chair, WiMob 2018 Publicity Chair, ICCC 2018 Workshop Co-Chair, and ICC 2017 Workshop Co-Chair. Dr. Jiang is the recipient of the Best Paper Award from IEEE GLOBECOM in 2013, the Best Student Paper Award from IEEE GlobalSIP in 2015, IEEE Communications Society Young Author Best Paper Award in 2017, the Best Paper Award IWCMC in 2017, IEEE ComSoc TC Best Journal Paper Award of the IEEE ComSoc TC on Green Communications & Computing 2018, IEEE ComSoc TC Best Journal Paper Award of the IEEE ComSoc TC on Communications Systems Integration and Modeling 2018, the Best Paper Award from ICC 2019, IEEE VTS Early Career Award 2020. He received the Chinese National Second Prize in Technical Inventions Award in 2018 and Natural Science Foundation of China Excellent Young Scientists Fund Award in 2019.

Yuanhao Cui received his B.S. degree in Henan University in 2012. From 2016 until 2018, he was working as a Ph.D visitor of Aalto University in Helsinki, Finland. He is currently working toward the Ph.D. degree in signal processing at Beijing University of Posts and Telecommunications. His research interests include blockchain application in Internet of Things, coexistence of radar and communication and machine learning application in wireless communication.

Xuesong Qiu received the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2000. He is currently a Professor, a doctoral supervisor, and the deputy director of the State Key Laboratory of networking and switching technology, and vice president of Network Technology Research Institute of Beijing University of Posts and Telecommunications, China. He was editor of the two ITU-T standards and 4 industry standards of China. He has published more than 200 academic papers. He won twice the national scientific and technological progress prize of china. His major research interests include network and service management, information and communication technology of smart grid.

Yan Zhang (Fellow, IEEE) is currently a Full Professor with the Department of Informatics, University of Oslo, Norway. He received the Ph.D. degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. His research interests include next-generation wireless networks leading to 5G beyond/6G, green and secure cyber-physical systems (e.g., smart grid and transport). Dr. Zhang is an Editor (or Area Editor, Senior Editor, Associate Editor) for several IEEE transactions/magazine, including IEEE Communications Magazine, IEEE Network Magazine, IEEE Transactions on Network Science and Engineering, IEEE Transactions on Vehicular Technology, IEEE Transactions on Industrial Informatics, IEEE Transactions on Green Communications and Networking, IEEE Communications Survey and Tutorials, IEEE Internet of Things Journal, IEEE Systems Journal, IEEE Vehicular Technology Magazine, and IEEE Blockchain Technical Briefs. He is a symposium/track chair in a number of conferences, including IEEE ICC 2021, IEEE Globecom 2017, IEEE PIMRC 2016, IEEE SmartGridComm 2015. He is an IEEE Vehicular Technology Society Distinguished Lecturer during 2016-2020 and he is named as CCF 2019 Distinguished Speaker. He is the Chair of IEEE Communications Society Technical Committee on Green Communications and Computing (TCGCC). He is an elected member of CCF Technical Committee of Blockchain. Since 2018, Prof. Zhang was a recipient of the global "Highly Cited Researcher" Award (Web of Science top 1% most cited worldwide). He is Fellow of IEEE, Fellow of IET, elected member of Academia Europaea (MAE), and elected member of Norwegian Academy of Technological Sciences (NTVA).