Title

Blockchain Radio Access Network (B-RAN): Towards Decentralized Secure Radio Access Paradigm

Authors

Ling, Xintong
Wang, Jiaheng
Bouchoucha, Taha
et al.

Publication Date

2019

DOI

10.1109/access.2018.2890557

Peer reviewed

Date of current version Nov. 27, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.DOI

Blockchain in the Air: Establishing Trust for a Decentralized Radio Access Network

XINTONG LING[1], (Member, IEEE), JIAHENG WANG[1], (Senior Member, IEEE), TAHA BOUCHOUCHA[2], BERNARD C. LEVY[2], (Life Fellow, IEEE), ZHI DING[2], (Fellow, IEEE)

[1]National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: {xtling, jhwang}@seu.edu.cn)
[2]Department of Electrical and Computer Engineering, University of California, Davis, CA 95616 USA (e-mail: {tbouchoucha, bclevy, zding}@ucdavis.edu)

Corresponding author: Jiaheng Wang (e-mail: jhwang@seu.edu.cn).

ABSTRACT The relentless growth of wireless applications and data traffic continues to accentuate the long felt need for decentralized, self-managed, and cooperative network architecture. In this article, we describe a new mechanism to leverage the power of blockchain to manage network transactions among inherently trustless network entities and identify promising applications made possible by adopting blockchain concepts for open access wireless networks. We propose novel distributed protocols for effective and dynamic network resource management based on blockchain and smart contract. Our test results demonstrate the benefits of blockchain-based networking strategies. We further present a number of challenges and future research directions.

INDEX TERMS Blockchain, B-RAN, Decentralization, Smart contract, Trustless trust, Wireless network

I. INTRODUCTION

THE surge and breakneck expansion of wireless services in terms of scale, speed, and breadth continue to strain the existing network infrastructure and pose a number of challenges to network access and quality assurance for the next generation wireless networks. Increasingly, it becomes difficult for traditional wireless networks to keep up with the tremendous growth of wireless users and their desire for ubiquitous connectivity [1], [2]. One well known solution is to leverage decentralized, crowd-sourced multi-layer network coverage [2], [3]. Such coverage not only provides low cost practical network access, but also overcomes the many shortcomings of centralized control that can be vulnerable to malicious hacking attacks on security and privacy.

Blockchain has recently taken both the financial sector and the society at large by storm. Originally made popular by its role in cryptocurrencies including the famous Bitcoin, blockchain can establish transactional faith among peer entities on decentralized, peer-to-peer (P2P) platforms while overcoming the shortcomings (e.g. vulnerability to hacking) of centralized ledger host [4]. Blockchain has also emerged as a potential tool in designing a self-managed and scalable decentralized network [5]–[8].

The integration of blockchain in network access and resource management provides several important benefits. First, blockchain-based network management, characterized by a fully decentralized control mechanism, enables communication links to be directly established among network users at P2P level without relying on intermediary agents, which leads to lower communication cost and better security. Second, the blockchain mechanism possesses important characteristics with respect to trust and privacy, two essential features for a successful and large-scale network deployment without centralized management [9], [10]. Third, blockchain can allow independent operators to integrate the individually developed systems and to provide access/authentication settings to enable roaming user access across networks and operators. Another inherent advantage of blockchain mechanism is its flexibility for dynamic network deployment and operational environment.

Blockchain represents a highly promising tool against the challenges posed by the exponentially growing wireless network users and services. However, the development of blockchain based technologies for wireless network control and management is still in its infancy [11]–[15]. In [15], a wireless mesh network was built via deploying the Hyperledger Fabric (HLF), which is a permissioned blockchain implementation. In [16], a blockchain-based anonymous ac-

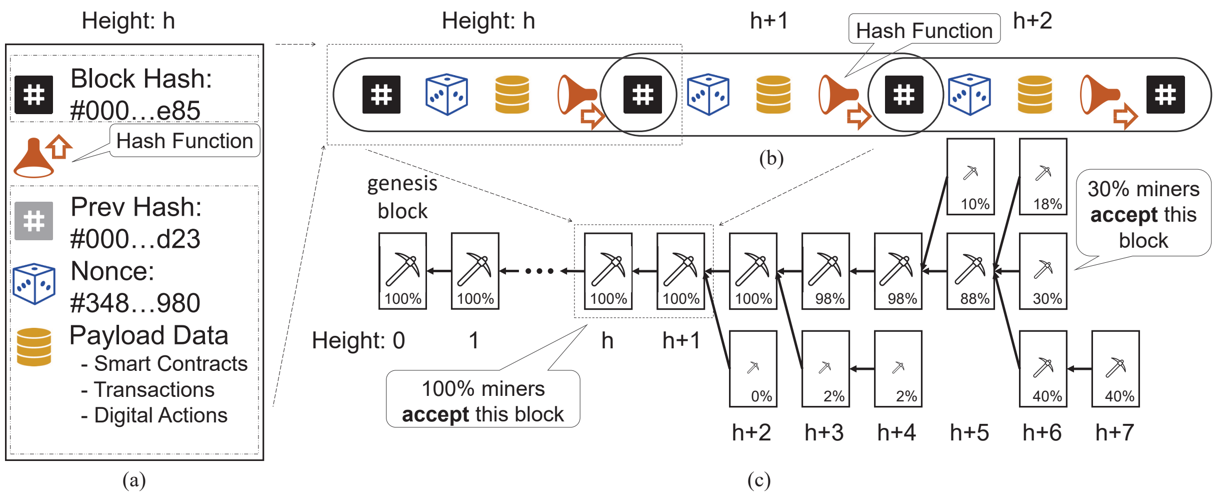

FIGURE 1. An overview and details of a proof-of-work (PoW)-based Blockchain. a) Block structure. The current block hash generated from the hash of the previous block, the nonce (see Section III-B), and the payload data. b) Links between blocks. The hash function builds an unbreakable link between every two successive blocks. c) Blockchain and forks. Each block is labeled by the percentage of miners that accept the block at a particular time. Generally, the miners have an agreement (consensus) on the early blocks in the chain (e.g., at heights h), but may follow different candidate blocks (i.e., forks) near the end of the blockchain (e.g., at height $h+6$).

cess (BAA) was proposed for cloud radio over fiber network. A large number of open issues remain with respect to the design of practical and commercially viable platforms[1] that can manage decentralized networks and establish efficient communication protocols to guarantee trustworthy network operations and transactions. Several exploratory research works have already attempted to leverage frameworks from economics such as auction and contract-based markets [9], [10]. These and related works considered open telecommunication markets by allowing the networked nodes to play the roles of network access providers and access requesters interchangeably. Nevertheless, one often must rely on a trusted central entity to facilitate the auction or contract process and to establish trust among players. With the help of properly designed blockchain technologies, the increasingly complex problems of such schemes in terms of trust, decentralization, and security, due to the exponential network growth, can be mitigated.

The goal of this article is to investigate the utility of blockchain in wireless networks by designing a decentralized, scalable, and self-organized network. First, we present a general background about the concept and the fundamentals of blockchain. Next, we introduce the concept of blockchain radio access network (B-RAN) and highlight the advantages inherited from the basic blockchain. We further discuss more advanced functions based on the B-RAN framework. We also provide numerical results to validate the proposed protocol. Lastly, we outline some key challenges and potential future research directions in this area.

II. BRIEF INTRODUCTION ON BLOCKCHAIN

Blockchain is a chain of interconnected information blocks forming a public ledger file for recording a list of digital actions (e.g., transactions). Digital actions are enforced by scripts that reside in the blockchain, known as smart contracts, via two steps. First, smart contracts that convey the digital actions are organized into blocks and broadcast to the network. Second, network nodes that help maintain the consensus, often known as miners, approve the transactions by inspecting the digital signature and confirming its validity through, e.g., verifying that the payer has sufficient funds in his account for transactions. The miners organize a bundle of valid digital actions into a new block for attachment to the end of the blockchain via a puzzle solving procedure known as mining.

As shown in Fig. 1(a), a typical block contains the following basic fields:

- Block ID: the hash value of the current block, which is generated from the parent's block hash and the other fields in the payload.
- Parent's block hash: the hash value of the previous block, which leads to the generation of a chain of blocks from the genesis block[2] to the current block.
- Payload Data: the digital actions and the information that need to be announced and spread among networked users.

Blocks may also contain some other fields depending on the specific protocols and the mining schemes, such as nonce (introduced in Section III-B), height[3], etc.

[1] For example, SMARTMESH: http://smartmesh.io/(accessed Novmember, 2018).

[2] A genesis block is the first block in a blockchain.

[3] Height is the number of blocks within the current chain between the current block from the genesis block.

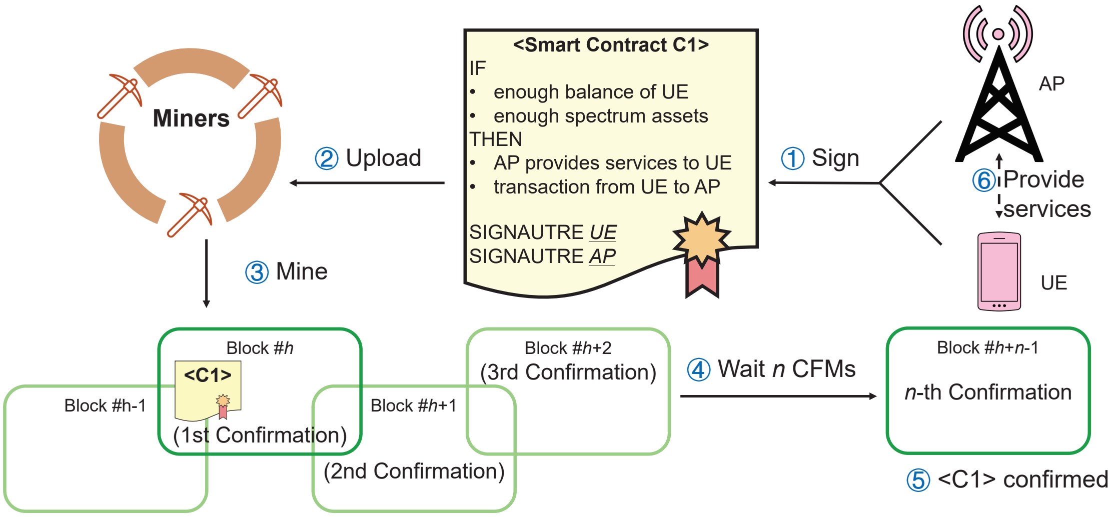

FIGURE 2. Typical processing stages in B-RAN for a UE requesting data access from an AP.

Each block is linked to the previous one (parent) by referencing the parent block's hash, as shown in Fig. 1(b). Hash is a function that uses a cryptographic algorithm to generate a short digest from data of an arbitrary size. Protected by this mathematical property, it is difficult to tamper with any information in a block further back in a blockchain. Any change to a block will influence its descendant blocks. From this perspective, each newly generated block can be regarded as a confirmation of its parent block, thereby contributing to maintaining the consensus and trust of the publicly distributed database. This process implies that the blocks (including the digital actions) in the earlier part of a blockchain are more secure, whereas more recent blocks near the end of a chain are more vulnerable due to insufficient number of confirmations.

Any digital actions that have not been recorded in the blockchain, are called unconfirmed actions. The miners in the network can collect a set of unconfirmed digital actions, locally validate them, assemble them into a candidate block, which is broadcast to the rest of the network. The next block is more likely to be found by the miner with more mining resources[4]. Due to the decentralized network structure, two or more versions of a blockchain may occur near the end, leading to a blockchain fork[5], as shown at height $h + 6$ in Fig. 1(c). Because of potentially malicious actions and/or propagation delays, the nodes in the network may generate different versions of the blockchain, especially near the end of the chain. A rational miner always switches to the longest branch. This mechanism implies that a blockchain may not reach an immediate convergence but an eventual convergence [5], [8]. Hence, mining can be seen as a vote by the miners with rich mining resources to favor the majority-preferred version of the blockchain in a fork.

Digital actions in a blockchain-based system are carried by smart contracts, which are scripts in each block allowing for the automation of multi-step processes. When pre-defined conditions are met, the contract terms are enforced and executed automatically among the participating entities by executing the open source scripts of the blockchain without relying on a third party or central nodes. The flexibility and variety of smart contracts empower a blockchain to form a distributed virtual machine (e.g., Ethereum[6]) beyond a simple cryptocurrency transaction system. Authorized by digital signatures, a smart contract is a reinforcer representing the deployment of an agreement among participating entities. Utilizing the mechanism of blockchain and the flexibility of smart contracts, we can build transactional trust among the initially trustless participants.

III. FRAMEWORK OF B-RAN

A. B-RAN SETUP

We design the framework of "B-RAN" by leveraging the principle of blockchain. In B-RAN, there is a population of Internet users (businesses or individuals) who are willing to provide controlled public wireless access to other similar well-behaving users. These B-RAN participants allow other participants to access their own WiFi networks to receive a payment or a credit for reciprocal services. B-RAN relies on a blockchain to confirm each smart contract and uses the digital actions in the smart contracts for payment (or reciprocal service credit). Therefore, the blockchain in B-RAN can organize a large cooperative network and protect participants' benefits.

To illustrate the concept of B-RAN, we consider an example in which the proposed protocol is based on software-

[4] Mining resources refer to different capabilities in different mining schemes, e.g., computational power in Bitcoin.

[5] Sometimes a fork is defined as a change in protocol.

[6] Ethereum: http://ethereum.org/, accessed Novmember, 2018.

defined radio[7]. Specifically, the basic relationship between users and hosts in B-RAN is shown in Fig. 2. In the proposed protocol, user equipments (UEs) and host access points (APs) reach an agreement on the contract terms, such as payment and spectrum assets[8]. These terms will be explicitly recorded in a smart contract authorized by the digital signatures of the clients (step 1 in Fig. 2). The smart contract is uploaded (step 2) to the mining network, and verified by miners to determine if the UE has a sufficient credit balance to pay the AP and the requested spectrum assets have not already been allocated to, or used by, others. The verified contracts are aggregated to create a new block, which is then added to the existing blockchain (step 3). After several verifying blocks built on top of it (step 4), the new pending block will be accepted into the main chain (step 5). If the contract conditions are satisfied (e.g., enough balance and spectrum assets), the UE will be granted a time-limited access to the specific spectrum assets, and the AP will automatically receive the payment for the access from the UE (step 6). The UEs' interests and the APs' rights are enforced by the smart contracts, thereby establishing the trust between unrelated APs and UEs. .

Through the introduction of the blockchain, we can provide sufficient economic incentives, avoid unnecessary overhead cost associated with centralized schemes, and establish the necessary trust among participating users. Compared to the current thread of spectrum trading for network cooperation, B-RAN participants both as access users and access providers can self-organize into a powerful network by removing intermediate brokers and their inherent security risk. Blockchain can enable roaming data exchange across multiple parties and networks, as shown in Fig. 3, with faster identification of visiting subscribers. The nature of B-RAN as a virtual public network that is secure and self-organizing leads to an open market. The competition and cooperation among participants can lower the cost of large-scale data access services without the need for additional radio infrastructure deployment.

B. CONSENSUS MECHANISM

The consensus algorithm is one key component in the B-RAN system. As a publicly accessible network, B-RAN requires a proper consensus mechanism to safeguard security. Proof-of-Work (PoW) proposed in Bitcoin [4] is one option, which has been proven to be secure by the widespread use of cryptocurrencies. In the PoW scheme, each valid block contains a nonce, which is a random number that answers a particular numerical puzzle. The hash-based PoW is to find a suitable nonce such that the hash value of the generated block satisfies

$$\text{Hash}\left(\text{Prev Hash} + \text{Data} + \text{Nonce}\right) \leq \text{Given value}. \quad (1)$$

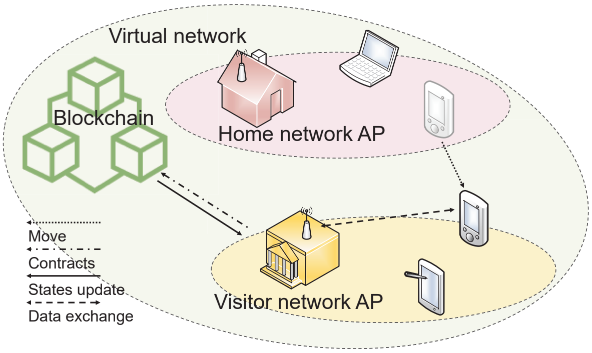

FIGURE 3. Illustration of cross-network roaming in B-RAN. Blockchain can enable roaming data exchange for visiting subscribers across multiple networks, and establish a virtual network among initially trustless parties.

Due to the non-invertibility of the hash function, the only way to find a solution is to make multiple random attempts on the nonce. A miner with more computational resources may find a successful hash solution faster, thereby generating its next block candidate faster.

Despite its popularity, PoW expends a considerable amount of computing power. Hence, less costly consensus mechanisms may provide efficient alternatives. There is a remarkable feature of B-RAN—it is built on numerous hardware devices (e.g., smart phones, WiFi routers, etc.) that offer access for data transmission. These devices can be utilized to design consensus algorithms. Compared to cryptocurrencies, forging the identity of a device, which is often required to be unique, is much more costly in data transmission systems. (Conversely, to forge an identity is almost costless in cryptocurrency where users can create multiple identities.) The unique hardware identifiers, e.g., the international mobile equipment identity (IMEI) in cellular phones, can be used to distinguish different devices. The identity-based consensus mechanism, namely Proof-of-Device (PoD) [17], allows the devices to vote on the new generated blocks based on their unique identifiers. Instead of solving complex cryptographic problems in (1), PoD selects a suitable device as the winner of the next block satisfying

$$\text{Hash}\left(\text{Prev Hash} + \text{Data} + \text{ID} + \text{Timestamp}\right) \leq \text{Given value}. \quad (2)$$

Each device will have the same probability to win the race according to their unique identifier, similar to lottery. PoD requires less computational cost than PoW, because the miners in PoD only need to evaluate the hash function once for each timestamp. It is possible that a user owns several devices, but it is almost impossible for a single user (or party) to own more than half of devices in a network in order to control the whole blockchain. Additional regulations should be added to the prototype of PoD for further improvement.

C. SAFEGUARD MECHANISM

The alternative history attack, or referred to as "the double spending attack" in cryptocurrency, is one major security

[7] The full code of the sample smart contract can be found online in the repository referenced in https://github.com/xtling/BRANContract/ (accessed Novmember 2018)

[8] A spectrum asset represents the short-term right to exclusively transmit or receive with a fixed power mask over a given frequency band within a given geographic area [3].

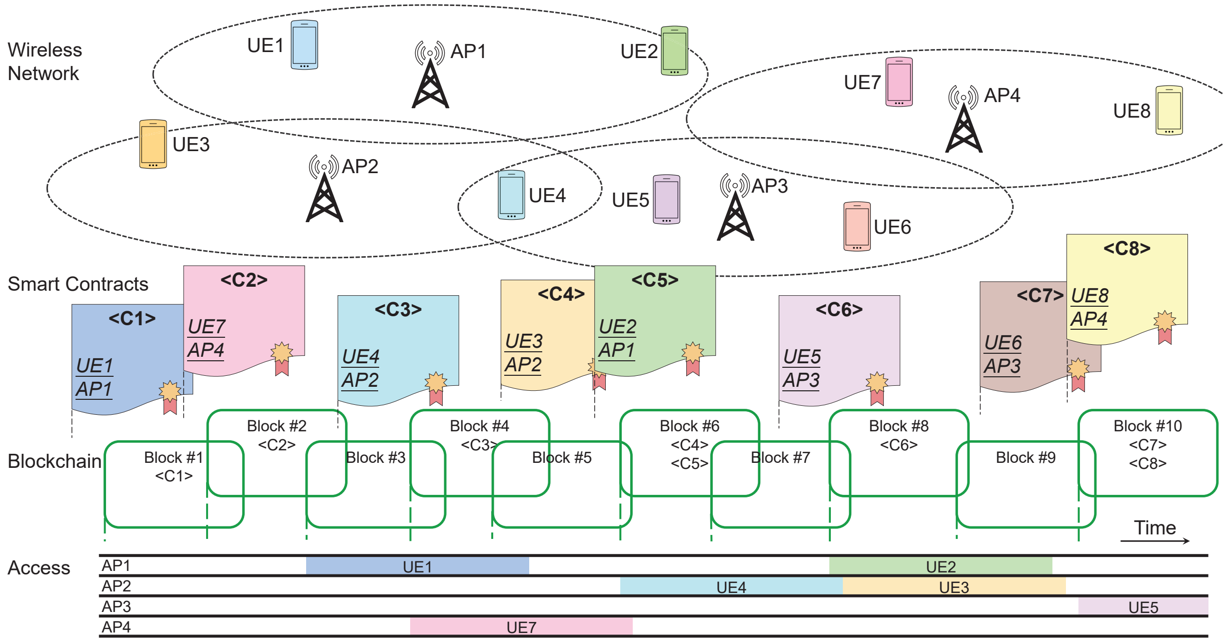

FIGURE 4. Demonstration of the blockchain-based B-RAN. The network is built on an open market following the first-come-first-serve rule via a blockchain, where UEs purchase spectrum assets from APs. We will take the smart contract <C2> as an example. The smart contract <C2> captures the agreement between the buyer (UE 7) and the vendor (AP 4), and records it in Block #2. Block #2 including the contract <C2> is confirmed to be in the main chain after three confirmations (Blocks #2, #3 and #4). Then, AP 4 will provide the access service to UE 7, and the transaction from UE 7 to AP 4 will be executed automatically by the contract <C2>.

loophole in most of distributed systems. The attacker privately mines an alternative blockchain fork in which a fraudulent double-spending transaction is included. After waiting for several confirmations for the network to accept the current main chain, the attacker releases the fraudulent fork. If the fraudulent fork is longer than the benign one, the attacker can successfully alter a confirmed history, which can be catastrophic for the whole blockchain. In B-RAN, altering a confirmed chain may let two UEs use the same spectral asset at the same time, causing serious interferences.

This security issue is due to the inconsistency of an asynchronous distributed network. The blockchain is designed to produce a history of transactions that is computationally impractical to modify. The consensus mechanisms, such as PoW, guarantee an eventual convergence instead of an immediate convergence. The cost is to wait for several confirmations until the network "almost" converges. Clearly, more confirmations can reduce the risk of fraud.

Yet, waiting for more confirmations generally leads to longer latency. Usually, in cryptocurrency systems, six confirmations (almost 60 minutes in Bitcoin) may be desirable. This delay, however, may be too long for wireless access services. As a protocol of wireless access, it is possible to use a less number of confirmations for security in B-RAN than that in cryptocurrencies. Fewer confirmations for a new block results in a shorter delay, although it might increase risk of alternative history attack. Also, the wireless access services in this work are not just packet-level connection requests but connections from minutes to hours. Thus, the delay in tens of seconds to register a new service is acceptable. We will show the trade-off between latency and security in Section V-C.

D. PENALTY MECHANISM

The alternative history attack is always be possible [6]. As a further secure step, blacklisting can be introduced to recognize double spendings and identify the tainted credits in B-RAN. The victim should monitor these credits and track their flow. Other APs might not be willing to accept tainted credits, since they are likely associated with a fraud.

Particularly, if PoD is adopted as the consensus algorithm, it may not prevent malicious users mining several forks simultaneously since the mining cost is much lower compared to PoW. Hence, an extra penalty need be introduced to discourage miners from trying to create a new branch by increasing the opportunity cost of mining.

Moreover, interference control in B-RAN can be realized conveniently among participating nodes. Through prepayment (credit) or deposit, an AP can be fined a penalty if it is found to have caused interference to other contracted services, or to be transmitting at very high radio power that degrades other participants' QoS.

IV. BEYOND SIMPLE ACCESS

A. COOPERATIVE TRANSMISSION

More advanced interactive and cooperative relationships beyond the scheme in Section III can be flexibly defined by smart contracts, e.g., multi-AP cooperative transmission. The proposed smart contracts can lead to an agreement among multiple trustless clients to establish more intricate cooperative relationship. If a UE is within the range of several APs, these APs can cooperatively provide a common data service in the same spectrum band such that the UE service is enhanced by leveraging spatial channel diversity. The terms, such as the required spectrum assets, the total payment, and the payment proportions for serving APs, can be established in smart contracts of a blockchain, and enforced automatically.

B. MULTI-HOP DATA BROKERS

Stimulated by blockchain technologies, it is possible to develop an incentive-driven protocol in mobile ad-hoc networks (MANETs) among even selfish and possibly dishonest peers. Mobile devices, namely brokers, dynamically form a self-organized network and forward data to destination nodes within MANET. The UEs indicate their requests in smart contracts for information sharing with another node or for network access to a gateway. A multi-hop route to a destination node, instead of a direct AP-UE link, can be established according to an agreement among the UEs and the data brokers via the consensus achieved by blockchain. Once a smart contract is admitted into the main chain, The predefined delivery fee will be transferred, and the contracted data brokers will help forward data streams showing the digital signature of the source node. Such a network can be established in a trustless environment without any existing infrastructure.

More complex protocols can be designed to improve the efficiency of such an self-organized network. For example, a UE can announce in the smart contract that only data brokers in the shortest or quickest route receive payment. Payment will be declared in the smart contract according to the urgency or the expected resource consumption. In this way, each broker, acting independently in its self interest, attempts to maximize its gain by computing its expected reward, its delivery cost, and its position and connections within the network. Consequently, overall efficiency of network resource usage is optimized through the competition among brokers in a decentralized manner.

C. PRIVACY PROTECTION

Blockchain can serve in cases beyond an open market for data services. It can play an important role in privacy protection in data sharing without revealing sensitive information of content originators. There are several common privacy issues. First, content originators shall own and fully control their data. Second, each user shall have complete authority and awareness on what data to share and how they are accessed. In principle, personal and sensitive information, though stored or delivered by third party, shall be kept confidential to them for preventing possible misuse. Herein, blockchain provides a decentralized solution for data sharing with privacy protection.

TABLE 1. Simulation parameters for B-RAN.

Parameter	Value
Average Block Time	12 sec
Noise Power Spectral Density	-174dB
Noise Figure	3dB
Maximum Power per Spectrum Assets	1.8mW
AP to UE Pathloss with Distance r	15.3 +37.6$\log_{10}(r)$
Antenna Gain	0 dBi
Maximum Rate per UE	20Mbps
Number of Spectrum Asset	25
Bandwidth of each Spectrum Asset	180kHz
AP Coverage Radius	400m
Length of Service	600 sec
Simulation Range	5000m×5000m
Number of APs	125
Number of UEs	5000

In the proposed B-RAN, privacy protection can be an additional term in the smart contracts. Users are granted the usage of spectrum assets, but they may not want the APs to access the content of the transmitted data. The smart contracts in a blockchain can act as content access controllers in addition to managing transmission services. With the help of a blockchain, only authorized nodes (e.g., the legitimate receivers) are allowed to read encrypted transmitted data using access keys issued by the data owner via a smart contract, while the data owner is identified by its digital signature. In this scenario, users are able to operate data transmission and manage content access simultaneously.

Another privacy related scenario arises in cloud operations such as data sharing, remote software updating, cloud computing and storage. In reality, fully trusted cloud service providers, albeit often claimed, may not actually exist. Cloud servers are expected to access personal data with explicit permissions. Blockchain-based cloud can authenticate data owners via their digital signatures and identify shared services via delegated permissions. Only those authorized by the owner are allowed to read/write the encrypted data, while the owner controls its data accessibility. In future extensions, secure multi-party computation can be further incorporated to avoid unauthorized access of sensitive data but can instead still provide distributed computing directly.

V. CASE STUDY

To further demonstrate the concept and efficacy of B-RAN, we shall provide a series of numerical examples. The simulation parameters are listed in Table 1 according to [7], [10]. The APs and UEs are randomly located in a given range. UEs generate data requests of different rate requirements, while the APs receive payment for providing the requested services. We employ the B-RAN framework described in Section III to build an open access market following the first-come-first-serve rule via a PoW-based blockchain, where UEs purchase spectrum assets from APs. Smart contracts capture the agreement between buyers and vendors, which will be executed automatically after it is recorded in the blockchain (requiring a minimum of three confirmations), as

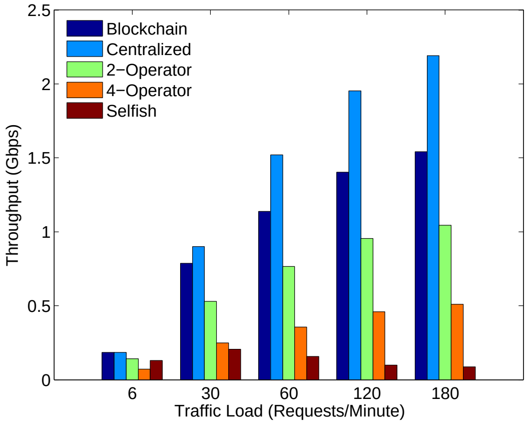

FIGURE 5. Network throughput versus traffic load among different schemes.

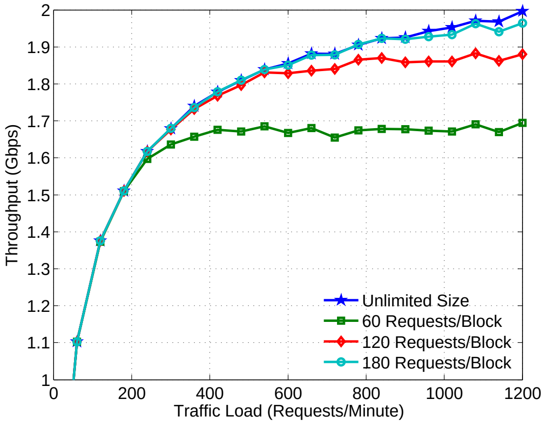

FIGURE 6. Network throughput versus traffic load among different schemes.

illustrated in Fig. 4.

A. THROUGHPUT VS TRAFFIC LOAD

In Fig. 5, we show the achieved throughput of the overall network for different traffic load (i.e., request frequency). In the centralized scheme, all requests are collected by a trusted center that controls spectrum allocation by maximizing the throughput to avoid any possible interference (formulated as an integer linear program). It requires a center with large computation power that is costly and often unavailable, though achieving the highest throughput. In the multi-operator network, there are several independent operators in the network, each with its own spectrum assets and APs. For its UEs, such network is only partially trusted via the operator it accesses. This type of partial trust may cause spectral underutilization, which explains why the 4-operator scheme is outperformed by the 2-operator one. In the selfish scheme, each UE tries to access the AP showing the best link quality without considering mutual interference. The selfish scheme, despite fully decentralized, represents the extreme case of no trust, making it impossible to coordinate the usage of limited spectral resources. Consequently, a great deal of mutual interference arises and degrades the system performance. The blockchain-based B-RAN outperforms both multi-operator and selfish schemes, leveraging its advantages of both decentralization and network-level trust.

B. THROUGHPUT VS BLOCK SIZE

In a blockchain, each block generally has a limited size (i.e., the maximum digital action number). Figure 6 illustrates the impact of the block size on the network throughput in B-RAN. The larger the block size, the more data requests can be dealt within unit time and hence, and the higher the throughput. Such an impact becomes notable if the traffic load is higher than 300 requests per minute. This is because in this case the number of requests generated in an average block time (12 seconds) is likely to be more than the maximum digital action number (e.g., 60). When the block size reaches 180 requests per block, the network throughput is marginally affected. Hence, the block size should be properly chosen according to traffic load and network size. This blockchain scalability problem is a topic for future investigation (see Section VI-C).

C. LATENCY VS SECURITY

The average latency of completing a data request is displayed in Fig. 7 for different number of confirmations n. One can see that, more required confirmations n naturally lead to larger latency. A higher request frequency will increase waiting time due to network congestion. Usually, the wireless access services will be longer than a dozen minutes, or even hours. Hence, the latency within one minute is acceptable for a mobile device's first attempt to access in the B-RAN scenario.

On the other hand, we find that there is a trade-off between latency and security. Fig. 8 shows that, given the attacker's hash rate, more confirmations will decrease the probability of an alternative history attack, but lead to a higher latency. The latency-security tradeoff implies that an appropriate number of confirmations should be selected according to the network safety level. For example, two confirmations can reduce the risk to all under 0.1%, if the attacker has 1% hash rate compared to the whole network. Meanwhile more confirmations are required if the attacker is more powerful. Latency can be regarded as the cost to build the trust in a trustless environment.

VI. FUTURE INVESTIGATIVE DIRECTIONS

Our investigation shows that blockchain clearly offers many practical benefits. However, the integration of the blockchain technology within communication networks also poses several challenges and opens new interesting future research directions.

A. MINING BY POWER-LIMITED NODE DEVICES

Green mining mechanisms instead of PoW should be designed for power-limited devices in B-RAN network. PoD is a good attempt to utilize the feature of wireless networks,

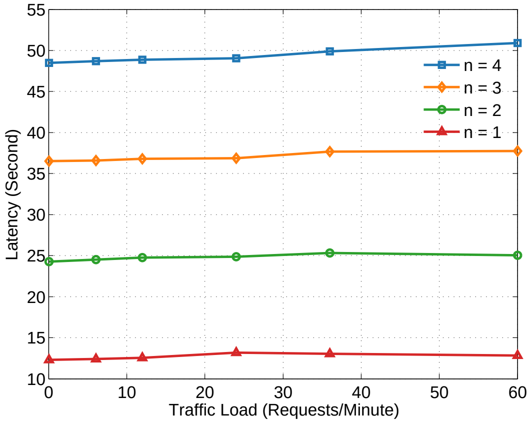

FIGURE 7. Network throughput versus traffic load among different schemes.

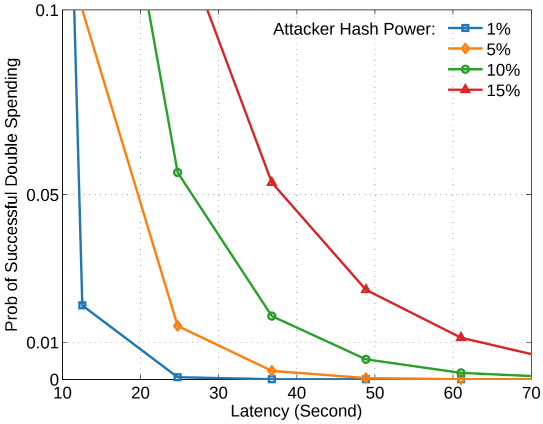

FIGURE 8. Network throughput versus traffic load among different schemes.

but still needs more refinement and further development. Note that mining requires setting up puzzles that are hard-to-solve but easy-to-verify. Such problems naturally exist in a communication process, such as decoding of long error correction codeword and optimizing resource allocation. Integrating these useful communication tasks into mining can avoid wasteful power consumption expected on meaningless puzzle solving.

B. BLOCKCHAIN IN COST-SENSITIVE TRANSMISSION NETWORKS

Conventional blockchains are built on Internet, where block spreading thus far uses wired networks and is often considered to be of little cost. However, in wireless networks, especially in MANETs, wireless data transmission can be resource-costly, thereby posing a substantially different challenge for wireless blockchain. Important research issues include: how a blockchain may survive in such an environment and how to introduce more incentives for block spreading. Seeking answers to these questions not only can be important to the specific self-organized networks based on blockchain, but also provides avenues for potentially improving blockchain technologies of the future.

C. BLOCKCHAIN SCALABILITY

The current blockchain technologies suffer from high processing and packet overhead as well as limited scalability. The blockchain scalability can be a bottleneck that limits the performance of blockchain-based decentralized networks (see, e.g., Fig. 6). It is estimated [7] that, using the current blockchain technology, the processing rate is at most 27 digital actions per second, which would be too slow for operating highly dynamic wireless networks. More advanced blockchain technologies, such as Hyperledger[9], Lightning[10], and Raiden[11], are expected to help address dynamic networking problems.

D. LATENCY REDUCTION

Latency has been a critical issue that restricts blockchain applications in delay-sensitive scenarios. In the blockchain-based networking services, the procedures of generating and confirming blocks are the main causes of latency. This is essentially the cost of establishing trust in a trustless network. One key research challenge is to reduce latency by reducing the block confirmation time, while satisfying the requisite system security and trust required by the users.

E. QUALITY ASSURANCE

Performance enhancement is expected by incorporating feedback from end users when deciding the final payment. One interesting idea is to make payment correlated with the amount of data served. However, a major obstacle lies in the difficulty of guaranteeing the authenticity of user feedbacks, given that the network is trustless to begin with. There is a strong incentive to investigate ways to improve the efficiency and reliability of blockchain-based decentralized networking.

VII. CONCLUSION

In this article, we propose to exploit the blockchain concept to develop a large self-organized network coverage by virtually combining multiple distributed networks without relying on a highly powerful, resource-rich, and information-aware network center. The advantages of blockchain such as decentralization, self-organizing, trust-building, and privacy protection make it a highly promising mechanism to overcome many challenges posed by the two conflicting forces of the rapid expansion on one hand and the rising users demand for quality of service assurance on the other.

REFERENCES

[1] C. V. N. Index, "Cisco visual networking index: global mobile data traffic forecast update, 2016–2021," Tech. Report, Feb. 2017.

[2] R. Bruno, M. Conti, and E. Gregori, "Mesh networks: commodity multihop ad hoc networks," IEEE Commun. Mag., vol. 43, no. 3, pp. 123–131, Mar. 2005.

[9] Hyperledger: https://www.hyperledger.org/, accessed Novmember, 2018.

[10] Lightning: https://lightning.network/, accessed Novmember, 2018.

[11] Raiden: https://raiden.network/, accessed Novmember, 2018.

[3] R. Berry, M. L. Honig, and R. Vohra, “Spectrum markets: Motivation, challenges, and implications,” IEEE Commun. Mag., vol. 48, no. 11, pp. 146–155, Nov. 2010.

[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Tech. Report, Oct. 2008.

[5] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio, 2016.

[6] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Commun. Surv. Tutorials, vol. 18, no. 3, pp. 2084–2123, thirdquarter 2016.

[7] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer et al., “On scaling decentralized blockchains,” in Proc. 19th Int. Conf. Financial Cryptogr. Data Secur. (FC’15). San Juan, PR: Springer, Jan. 2016, pp. 106–125.

[8] C. Decker and R. Wattenhofer, “Information propagation in the bitcoin network,” in Proc. 13th IEEE Int. Conf. Peer-to-Peer Comput. (P2P’13), Cambridge, MA, USA, Sep. 2013, pp. 1–10.

[9] L. Gao, J. Huang, Y. J. Chen, and B. Shou, “An integrated contract and auction design for secondary spectrum trading,” IEEE J. Sel. Areas Commun., vol. 31, no. 3, pp. 581–592, Mar. 2013.

[10] H. Wang, J. Wang, and Z. Ding, “Distributed power control in a two-tier heterogeneous network,” IEEE Trans. Wireless Commun., vol. 14, no. 12, pp. 6509–6523, Dec. 2015.

[11] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When mobile blockchain meets edge computing,” IEEE Commun. Mag., vol. 56, no. 8, pp. 33–39, Aug. 2018.

[12] K. Kotobi and S. G. Bilen, “Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access,” IEEE Veh. Technol. Mag., vol. 13, no. 1, pp. 32–39, Mar. 2018.

[13] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “BlockChain: A distributed solution to automotive security and privacy,” IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, Dec. 2017.

[14] N. Herbaut and N. Negru, “A model for collaborative Blockchain-based video delivery relying on advanced network services chains,” IEEE Commun. Mag., vol. 55, no. 9, pp. 70–76, Sep. 2017.

[15] M. Selimi, A. R. Kabbinale, A. Ali, L. Navarro, and A. Sathiaseelan, “Towards blockchain-enabled wireless mesh networks,” in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. ACM Press, 2018.

[16] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, “Blockchain-based trusted authentication in cloud radio over fiber network for 5g,” in 2017 16th International Conference on Optical Communications and Networks (ICOCN), Aug 2017, pp. 1–3.

[17] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, “Designing microgrid energy markets: A case study: The Brooklyn microgrid,” Appl. Energy, vol. 210, pp. 870–880, Jun. 2018.