IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON BLOCKCHAIN-ENABLED TRUSTWORTHY SYSTEMS

Received May 4, 2020, accepted May 26, 2020, date of publication June 1, 2020, date of current version June 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2998951

An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends

ALEKSANDR OMETOV[1], (Member, IEEE), YULIA BARDINOVA[1,2], ALEXANDRA AFANASYEVA[3], PAVEL MASEK[4], (Member, IEEE), KONSTANTIN ZHIDANOV[2], SERGEY VANURIN[2], MIKHAIL SAYFULLIN[2], VIKTORIIA SHUBINA[1], (Graduate Student Member, IEEE), MIKHAIL KOMAROV[5], (Senior Member, IEEE), AND SERGEY BEZZATEEV[3], (Member, IEEE)

[1]Tampere University, FI-33720 Tampere, Finland
[2]Enecuum HK Limited, Hong Kong
[3]ITMO University, Saint Petersburg 197101, Russia
[4]Brno University of Technology, 616 00 Brno, Czech Republic
[5]National Research University Higher School of Economics, Moscow 119049, Russia

Corresponding author: Aleksandr Ometov (aleksandr.ometov@tuni.fi)

This work was supported in part by the Technology Agency of the Czech Republic (TACR) under Grant TJ02000332, in part by the European Union's Horizon 2020 Research and Innovation Programme through the Marie Sklodowska Curie Grant through Project A-WEAR under Grant 813278, and in part by the Government of the Russian Federation, under Grant 08-08.

ABSTRACT The blockchain technology is currently penetrating different areas of the modern Information and Communications Technology community. Most of the devices involved in blockchain-related processes are specially designed targeting only the mining aspect, i.e., solving the computational puzzle task. At the same time, the use of wearable and mobile devices may also become a part of eCommerce blockchain operation, especially during the on-charge time. The paper considers the possibility of using a large number of constrained devices to support the operation of the blockchain with a low impact on battery consumption. The utilization of such devices is expected to improve the system efficiency as well as to attract a more substantial number of users. This paper contributes to the body of knowledge with a survey of the main applications of blockchain for smartphones along with existing mobile blockchain projects. It also proposes a novel consensus protocol based on a combination of Proof-of-Work (PoW), Proof-of-Activity (PoA), and Proof-of-Stake (PoS) algorithms for efficient and on-the-fly utilization on resource-constrained devices. The system was deployed in a worldwide testnet with more than two thousand smartphones and compared with other projects from the user-experienced metrics perspective. The results prove that the utilization of PoA systems on a smartphone does not significantly affect the lifetime of the smartphone battery while existing methods based on PoW have a tremendous negative impact. Finally, the main open challenges and future investigation directions are outlined.

INDEX TERMS Communication system security, cryptographic protocols, distributed information systems, mobile computing, prototypes, cellular phones.

I. INTRODUCTION AND MOTIVATION

Today, the number of mobile devices is growing tremendously. According to CISCO, there were more than 0.7 billion wearable devices in 2017, with almost 44% being smartphones [1]. This number is expected to reach 12.3 billion mobile-connected devices by 2022, which will exceed the world's projected population at that time (8 billion) by one and a half times. This rapid growth is largely forming a standalone niche of Internet of Wearable Things (IoWT) [2] as part of the enormous Internet of Things (IoT) paradigm [3]. The mobile devices present on the market today already have the computational power of 5 years old computer [4], allowing for broader utilization of those not only for calls and human-based data exchange but also for much more complex computational tasks opening a broad way for various emerging applications [5]. One of those tasks is related to the operation of the distributed solutions, as part of future

The associate editor coordinating the review of this manuscript and approving it for publication was Patrick Hung.

Cyber-Physical Systems (CPS), relying on *blockchain technology*, which is expected to affect the society at large by storm.

Historically, blockchain systems known today are made on the basis of the system proposed by Ralph C. Merkle in 1979 [6]. In recent times, the applications that could previously work only through trusted centralized entities achieved an opportunity to operate without any constant connection to the authority while maintaining the same security level and improving the overall system functionality [7]. The main idea behind blockchain itself lies in the concept of *trust* [8], [9]. This idea is based on the fact that parties interacting within the system do not necessarily know or trust each other but still have an opportunity to transact securely. By these means, the use of blockchain eliminates the need for the involvement and continuous maintenance by the centralized 'trusted' authority, thus, enabling the network to operate in a completely distributed manner.

At the same time, the possibility to customize and style along with technological enhancements towards small-scale electronics and modern applications make handheld and wearable devices a strong contender in the IoT technological race [10]. This fascinating development is a driving force behind the convergence of the physical and digital worlds that promises to create an unprecedented IoT market of $52 billion during the oncoming years [11]. Moreover, it is expected that a significant percentage of those devices will be smartphones, tablets, and wearables. Currently, there are about 3.2 billion smartphones in the world [12], and the average one can process 2 billion floating-point operations per second (FLOPS) [13], thus, leaving us with constantly underused 5 EFLOPS. If needed, this power can be applied for the transaction publication and validation processes, smart contracts [14], incentivization by cellular operators [15], trusted data crowdsensing [16], or distributed storage [17].

However, deploying blockchain applications to mobile and resource-constrained devices acting as actual miners, i.e., nodes solving a highly-complex computational puzzle or Proof-of-Work (PoW), faces many critical challenges [18], [19]. The PoW mining process habits requires not only computing power but also energy from interacting mobile devices. There are, however, several miner implementations of blockchain applications for smartphones, but it has been shown that the income of a single mobile device acting as a miner in the blockchain network is nonprofitable [20].

It is worth pointing out, the use of constrained devices is generally underestimated in the context of blockchain. The mining feature is ultimately not the most efficient utilization of this class due to the computational and power limitations, but the concept known as Proof-of-Stake (PoS) provided the first opportunity for such constrained devices utilization [21]. Here, PoS nodes do not act as miners to solve complex tasks but rather as temporary authorities [22] to confirm transactions and blocks based on their ''stake'' in the system, and the use of the resource-constrained device, for this reason, is a natural step forward. The role of PoSs is to pay only the transaction fees of the network without involvement in actual mining.

Nonetheless, almost every modern smartphone already has the power to act the part of not computationally hungry Proof-of-Activity (PoA) operation [23] and calculate related cryptographic primitives [24]. Broadly, PoA aims at validating the transaction instead of signing or mining the blocks. To throw some oil on the fire, vendors are already providing blockchain-enabled smartphones for public use, foreseeing the inevitable future of distributed applications on handheld devices. Some devices already have native support for decentralized applications, including, as of May 2020, Samsung Galaxy S10, HTC Exodus, Sirin Labs Finney, Pundi Xphone, and Electroneum M1.

Based on the above, the evolution of blockchain towards mobile electronics in the state of the technology nature. Therefore, this paper aims to (1) *analyze the state-of-the-art in mobile blockchain systems* and (2) *to propose a hybrid consensus protocol with low impact on smartphone operation*. The main contributions of this work[1] are:

- Overview of existing trends in blockchain applications related to resource-constrained and wearable devices. *Goal 1*
- Comparison of existing 'living' projects involved in smartphones-based blockchain processes. *Goal 1*
- Development of a protocols' family and its implementation allowing for efficient blockchain integration on modern smartphones and its security analysis. *Goal 2*
- Performance evaluation of publicly available smartphone-based blockchain solutions along with the developed one and the corresponding impact on the user experience of the device owner. *Goals 1 and 2*
- Outline of the main challenges and future perspectives of the blockchain adoption by both users and industry. *Goal 1*

A. LITERATURE REVIEW METHODOLOGY

This survey summarizes recent industrial activities and research breakthroughs on blockchain and blockchain-based applications and open challenges for smartphones and resource-constrained devices. In order to identify key publications on the analysis of the blockchain technology, a literature search in scientific databases was performed covering leading computer science journals and conferences: *IEEE Xplore*, *ACM Digital Library*, *ScienceDirect*, *SAGE Journals Online*, and *Springer Link*. To find relevant articles and papers for our research, the following search string was compiled and used: *(Blockchain OR "Distributed Ledger") AND ("State-of-the-Art" OR Challenges OR "Performance Evaluation" OR Attack OR Implementation OR Prototype OR "White Paper")*. Industrial blogs and project White Papers were also analyzed, covering the present phase of technology development and integration. In total, a set of 1312 potentially

[1] This paper is a significantly extended version of published work [25].

relevant publications was completed, excluding grey literature and pre-prints.

During the reviewing process, the titles, keywords, and abstracts of the publications were analyzed to identify papers and articles that were relevant to the problematics of the blockchain applications for mobile devices. As a result, a total of 60 publications were selected. To further extend the literature sample, a more in-depth analysis of the selected publications references was executed, aiming at additional papers or articles relevant to the research action. Accordingly, this process resulted in a total of 79 publications.

Once the literature selection process was completed, the selected publications were carefully read, and an open coding approach was applied to identify the described applications and challenges. Next, the extracted applications were classified into four general groups. The results of the analysis are presented in the next section.

B. PAPER STRUCTURE

The rest of the paper is organized as follows.

In the first place, this paper outlines the main applications of blockchain technology for smartphones and wearable devices stepping aside from conventional cryptocurrency perspective in Section II. The overview covers such areas as infrastructure and resource sharing, security and access control, trust, and user involvement aspects.

Next, the study surveys various market-available blockchain-based systems and related consensus algorithms in Section III. It elaborates on the actual involvement of resource-constrained devices in the blockchain ecosystem operation.

Based on the analysis, this paper contributes with a hybrid algorithm, coupling together Proof-of-Work, Proof-of-Stake, and Proof-of-Activity, which allows involving mobile devices in the new block generation process, as detailed in Sections IV. Section V provides a detailed description of the developed cryptographic protocols.

Section VI provides the performance evaluation of existing solutions from Section III and the developed system as well as its qualitative security and privacy analysis.

Section VII sheds some light on several open challenges that should be considered by the blockchain system developers. Finally, this section highlights future perspectives of the utilization of blockchain on smartphones. The last section concludes the paper and summarizes the main findings.

II. STATE-OF-THE-ART OF BLOCKCHAIN APPLICATIONS FOR MOBILE DEVICES

Despite conventional applications such as cryptocurrency [26], governance, Distributed Ledger Technology (DLT) operation [27], and supply management [28], smartphones and resource-constrained wearables are naturally involved in a plethora of networking activities driven both by humans and devices themselves. This section outlines the applications mostly related to smartphones and other resource-constrained devices.

A. INFRASTRUCTURE AND RESOURCE SHARING

One of the constantly evolving markets of today is related to cellular communications driven by the 3rd Generation Partnership Project (3GPP) organization actively developing Long Term Evolution (LTE)-related standards. The number of directions for the application of blockchain in LTE is vast and accomplished with Wireless Local Area Network (WLAN) services, broadly deployed worldwide. Moreover, the Federal Communications Commission (FCC) shared tentative thoughts to deploy blockchain as an enabler for 6G in 2018 Mobile World Congress (MWC) [29].

Today, both vendors and operators have access only to limited resources from energy, computing, and spectrum perspectives [30]. From the operator's point of view, the radio resource is the biggest bottleneck due to the growing demand for various applications, including Virtual and Augmented Reality (VR/AR) applications, high definition video streaming, and Tactile Internet paradigm [31]. Spatial and spectral resources of different operators may be unequally used due to various reasons and, thus, such systems as Licensed Shared Access (LSA) [32] and Licensed Assisted Access (LAA) [33] were proposed by 3GPP. Blockchain technology may become one of the enablers for making the manipulation with those resources more flexible, especially in the IoT context [34].

In particular, the work [35] proposes the adoption of blockchain technology as a virtualized intermediary for the shared use of network resources in a sovereign, autonomous, safe, and reliable mode. The authors highlight the possibilities of the infrastructure and network resources sharing through Peer-to-Peer (P2P) self-executing transactions in a distributed manner.

The authors of [36] also focus more on the Network Functions Virtualization (NFV) in 5^{th} generation networks (5G). In particular, this work proposes to utilize blockchain for intelligent network slicing in Software-defined Network (SDN) by introducing Blockchain Slice Leasing Ledger Concept for a 5G network. Here, the mobile network service provider has the ability to compromise with external tenants' network slice requests quickly and automatically relying on the accessibility of infrastructure provider resources.

The topic of content-centric data sharing form privacy perspective is discussed in work [37]. The authors propose to combine blockchain and encrypted cloud storage in a content-oriented network in order to maintain the users' confidentiality and secure data exchange flexibly. The authors of [38] facilitate the use of blockchain for incentivization in terms of distributed data storage. The data stored by each node is considered to be a block in the chain. The reward will be received by the node that stored the data, and the reward for the sale of the node increases with the volume growth of stored data. The study in [39] provides a profound overview of the Cloud Exchange (CloudEX) storage empowered by blockchain technology aiming to avoid the additional need for an intermediary and empowering trust at the same time.

The potential of offloading the resource-intensive mining tasks to neighboring computing nodes with blockchain is discussed in [40] concerning data caching. The paper analyzes the computational offloading and content caching in wireless blockchains with Mobile Edge Computing (MEC). The authors focus on the offloading strategies selection, i.e., offloading to the nearest Access Point (AP) or a group of users in device-to-device (D2D) proximity, and the caching strategy regardless of whether to cache the requested content and computing or not. Those approaches are jointly studied and formulated. The study [41] describes a similar edge computing problem, and the work [42] focuses on Cloud and Fog operation aspects. The authors of [43] also propose the secure data sharing framework based on blockchain in combination with D2D applicable for Delegated PoS operation. The results have shown that the use of an AP-based relaying strategy may significantly improve the utility of Edge nodes by means of computational offloading while mobile devices were acting as PoS nodes.

B. SECURITY AND ACCESS CONTROL

Another large segment of blockchain applications on mobile smartphones is related to access procedures and tracking from different perspectives.

The works [44] and [45] highlight accessing the Internet via blockchain-powered access control, which allows keeping records of transactions that track the device actions (access nodes, channels, gateways, services, etc.). It allows for flexible economic compensation for used resources in a transparent, decentralized, and reliable way. The authors of [46] also puropose a protocol to apply blockchain for access management in public Wi-Fi APs. The method is based on virtual credentials instead of actual user information.

The authors of [47] develop and implement an authentication scheme to concurrently and efficiently ensure anonymity and accountability without dependence on any trusted third party. The system uses the unmodified Bitcoin blockchain as a platform for managing and determining access credentials in a peer-to-peer way. The method suggests associating the user's access right with their bitcoin address, which can be used as credentials to access public Wi-Fi APs.

Another work [48] proposes a blockchain-based cross-domain authentication scheme for Wi-Fi networks. The designed solution authenticates users and servers in a distributed and anonymous way, avoiding a single point of failure and privacy leakage.

The identity management aspect is also in the focus of the study [49]. The authors suggest a privacy-enhancing user identity management system based on blockchain technology that gives due importance to both anonymity and attribution and also supports end-to-end management from user approval to billing for use. The setting provides access to the network using aliases, preventing the restoration of subscriber identity.

An exciting niche of the blockchain application falls in the area of Self-Sovereign Identity (SSI) [50], [51]. With the term not being fully defined, it generally corresponds to an identity management system allowing individuals to own and manage their digital identity fully. From a broad adoption perspective, there is a very active scene creating ''wallet apps'' for storing Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs). An example or a real-life implementation is the application called ''Bloom – Secure Identity'' providing a protocol for SSI on modern smartphones [52].

The authors of [53] propose to utilize private blockchain for detecting malicious applications in application stores. The idea behind is to enable third parties to execute independence security scans of the application after it is published and add the result to the chain aiming to decrease the false positive rate of detection systems.

In the medical domain, the research work [54] proposes to apply blockchain technology for the insider attack mitigation in the Internet of Medical Things (IoMT). The authors focused on Medical Smartphone Network (MSN) environment and developed a trust management scheme. The proposed approach allows the users to quickly update the blacklist of nodes to analyze the information about the status of traffic from suspicious ones better.

C. DATA EXCHANGE IN (UN-)TRUSTED ENVIRONMENTS

The decentralized trust management scheme based on the blockchain technology is proposed in [55]. It enables mobile nodes to evaluate the trustworthiness of neighbors based on the Bayesian Inference Model and assess the credibility of received messages. Another trust management scheme is proposed in [56], where the authors have introduced a token-sharing scheme that motivates users to share information securely.

The authors of [57] focus on the aspects of trust in Wireless Sensor Networks (WSNs). This article proposes a new application for the blockchain as a secure decentralized storage for cryptographic keys, as well as for exchanging of trust information in the context of autonomous wireless sensor networks. The proposed mechanisms depict how to apply the blockchain immutability to solve problems in the field of decentralized ad-hoc networks, i.e., how to build a complete solution that provides authentication mechanisms as well as an assessment of trust in a self-organizing network.

In contrast to many anonymization-targeted works, paper [58] proposes the system that aims to map personnel information to the blockchain-based transaction system by creating digital identities based on identifiers issued by the government. This digital identifier is associated with a mobile device. The system is based on the biometric parameters and trust computing technology to ensure that the information stored in the blockchain correctly reflects reality. The work [59] also provides an overview of the blockchain potential from a biometrics perspective.

Blockchain could also be used for data crowdsourcing, as it is examined in [60]. This work aims to preserve the privacy of the participants and keep the integrity of the service request and provision. The authors of [61] also propose to utilize

the blockchain to avoid third party involvement during the crowdsourcing process.

D. USER INVOLVEMENT

Since the roots of publicly-known blockchain technology lie in the financial field, some researchers propose to utilize blockchain as a user incentivization mechanism, which was already discussed in [56], [62], [63]. Interestingly, the authors of [64] propose a blockchain-based incentivization schema for Public Protection and Disaster Relief (PPDR) scenarios. The approach uses a smartphone with a delay-tolerant network (DTN) support, which relies on Bitcoin to encourage nodes to collaborate. The scheme is entirely decentralized and independent of any central trusted authority.

Another standalone niche based on the cryptocurrency concept is related to online- and P2P based gaming [65], [66]. The application of blockchain for both in-game cryptocurrencies and/or centralization of gaming events would allow creating a secure and fully decentralized architecture to transform a game towards becoming community-sustainable. It is foreseen that blockchain would bring completely new paradigms to the gaming industry, including more exciting and parallel gaming universes, better-regulated gaming economies, faster micro-transactions, fraud resistance, and general fairness to players [67]. Overall, blockchain-based gaming already benefits from the features of decentralized applications (DApps) [68].

Generally, the blockchain potential in applying it to communications and related aspects as a specific niche is still in its infancy. Most of the presently developed solutions for smartphone-related scenarios focus on resource sharing, access control, user involvement, and incentivization. The main driver behind the broad adoption of blockchain in the wireless environment would still be hardware providers and operators due to their tight connection to mobile devices evolution.

III. MOBILE BLOCKCHAIN ACTIVE PROJECTS AND CORRESPONDING CONSENSUS

Indeed, the blockchain development towards smartphones is still in the infancy. On the other hand, there are some ongoing public projects actively working in this direction. This section highlights the main concepts and related paradigms in the current mobile blockchain area.

Due to the blockchain property of immutability, it can be abstracted as a transactional system that enables a consensus to form within its participants [69]. The consensus holds unique probabilistic properties and can thus be leveraged as a fundamental building block for adaptive middleware that offers both deterministic and probabilistic consensus.

Most of the public blockchain operation known today is based on specially designed devices – miners, i.e., nodes that attempt to solve the computational puzzles, in other words, to achieve the PoW [70], [71] for new block creation, and profit from the monetary compensation associated with it. The first node to solve the computational puzzle receives a reward. In order for the system to stay operational, the complexity adjustment (often known as ''number of leading zeros'') is utilized, i.e., in fact, it aims at minimization of the number of nonces which need to be tried before a match is found. The difficulty of mining should be adjusted dynamically throughout the lifetime of the system [72].

A. PROOF-OF-WORK SYSTEMS

This subsection lists living PoW-based blockchain systems available on smartphones.

1) MIB COIN

The first system is the Mobile SmartX Blockchain platform based on Mobile Integrated Blockchain (MIB) coin. MIB public network was launched on November 12, 2018, reaching more than a thousand active users just two weeks after release [73]. A year after the release, the number of active users has almost reached two thousand.

MIB is branded as environmentally friendly, inexpensive PoW mining for mobile devices based on Bitcoin. The main difference is that MIB's Mobile Proof-of-Work (MPoW) utilizes the CPU resources of mobile devices to mine blocks. The application is designed to take into account the capabilities of the device; users can choose the desired mining complexity to protect the smartphone from overheating, allowing budget devices of any processing power to be part of the network. Low-power PoW is another MIB feature. MIB states that the smartphone application spends 150 times less power than an application-specific integrated circuit (ASIC) mining [74].

It is essential to point out that the MIB network is centralized. Network servers assigned by the project owners distribute cryptographic tasks between nodes, and then they publish blocks. Thus, mobile devices do not support a distributed network, but the servers they are connected to. The control over the network remains with MIB executives. Having created a centralized network, the project is deprived of one of the distinguishing features of blockchain technology, i.e., a distribution that allows one to send transactions without a generally trusted third party but a selected one.

To finalize, MIB application is not able to be executed in the background mode, making every-day use of smartphone inconvenient. The need to keep the application constantly open makes MIB mining possible only on spare devices of specifically designed farms, which makes MIB operation costly not only from hardware but also from energy consumption perspectives.

2) uPlexa

uPlexa's main goal is to form a platform for IoT devices to create an anonymous blockchain-based payment system. The beta version was released in 2018. At the beginning of 2019, the uPlexa team developed an Android application for the public domain. As of now, users can also use it on their PC CPU, Android device CPU, AMD GPU Devices, and Nvidia devices.

uPlexa also relies on the PoW concept, i.e., IoT devices' CPU or GPU resources are used to add transaction records to the ledger. It creates an anonymous payment system with the support of interlinking IoT devices, which can be used for telecom and internet service providers for e-commerce.

uPlexa aims at overcoming Bitcoin's issues, specifically, slow transaction time and hefty fees, by introducing a model where micropayment fees increase when the network is overloaded. This method helps decrease the amount of these micropayment transactions and, consequentially, lower the load on the network. At the same time, in order to sustain the balance, any other payments still have low fees.

The project allows operation on different types of hardware, including phones, tablets, PCs, TVs, TV Boxes, Raspberry Pi's, and the team is planning to scale the list by supporting as many IoT devices as possible while keeping the mining ASIC-resistant.

Since IoT devices vary significantly, the uPlexa application offers a choice between different settings to fit each device's resources. So, the users can adjust the level of CPU usage and the number of threads to be utilized to prevent over-use and overheating.

B. PROOF-OF-TRANSACTION SYSTEMS

Smartphone-based blockchain applications may rely not only on computational resources but also on transporting the value between involved instances. Here, devices are competing on accumulating transactions to generate new blocks and get transaction fees. An example of this activity is a TAU Coin, which Android application was released in May 2019, though its users were active since 2018. Currently, there are more than 440,000 registered accounts but less than a thousand active ones as of May 2020.

The project's algorithm, Proof-of-Transaction (PoT), determines a new block generation address based on accumulated transaction history [75]. For every address, there is a linear proportion between the new block generation probability and the address' transaction history, and this proportion is called mining power, which is an equivalent to Bitcoin's hash power. The more transactions the user has made, the higher the chance of receiving rewards, which come in the form of a transaction fee. The algorithm incentivizes users to make transactions actively and thus increase coin's circulation.

Unlike other projects that use PoW and PoS algorithms, TAU has its entire coin supply already minted in the genesis block. The reason for that is to fight the hoarding (stockpiling) mentality that is present in the cryptocurrency market. The platform rewards active participants of the network who make transactions and the currency circulates freely.

TAU has security measures against the majority or 51% attack; the attacker would need to have more transactions than the rest of the network combined for a year, which makes the attack highly challenging to perform.

C. CLOUD SYSTEMS

Cloud mining, a process of token mining using a remote datacenter, is a new concept that is utilized in Electroneum and Phoneum projects. Cloud mining is provided for free and delivers an easily understandable experience, allowing users to participate regardless of their hardware and knowledge of cryptocurrency economy and mining algorithms.

1) ELECTRONEUM

Electroneum is one of the most popular smartphone-based mining projects [76]. Following the start of the development in 2017, Electroneum held a successful ICO sale, and by the beginning of 2018, the beta version on an Android application was launched. By Q3 2018, the project reached two million registered users. As of May 2020, there are around 2.5 million registered users and 200,000 active miners.

Electroneum is resistant to 51% attack; the security is achieved by the addition of a moderation layer, which becomes active when there is a possibility of an attack. The layer establishes the attack's origin and shuts it down.

Electroneum is compliant with a Know Your Customer (KYC) process; the platform requires users to fill out their legal name and surname, country, telephone number, and upload their photo to verify their identity and to minimize the risk of illegal use of the app. This, however, may compromise the user's privacy, since the entered information is shared with third parties according to the project's policy.

2) PHONEUM

Phoneum is another project that utilizes cloud mining [77]. After almost two years of development, the Phoneum mining application, as well as a gamified platform, had been released in May 2019.

The project is designed to function on multiple platforms and has been implemented in a gamified experience as a game called Crypto Treasures, where users can earn Phoneum's currency by playing games. The project is expected to have an easy to integrate API to allow other developers to utilize cryptocurrency in their projects.

Cloud mining utilized in both Electroneum and Phoneum is activated through the corresponding applications without any prerequisites and requires reactivation every week. The rewards are distributed for free once mining is started. The smartphones, however, do not perform any activity and do not help confirm new blocks, and as a result, they do not bring blockchain utility. Since the apps and the cloud mining services are free and do not require an entry fee, it makes the rewards easy to gain and, eventually, decreases token's value.

Based on the analysis of the existing projects, the majority of those were found either relying on computationally expensive mechanisms or not involved in block generation at all, which may result in the need to pregenerated the blocks anyway, i.e., to have the empty blocks already prepared for utilization. In the next section, we propose our approach that

FIGURE 1. Smartphones as part of the blockchain ecosystem.

may be potentially used for mobile blockchain operation and compare it with the listed solutions.

IV. PROPOSED UTILIZATION OF BLOCKCHAIN

This section provides a brief overview of the main system components used during protocols development.

An intelligent combination of PoA, PoS, and PoW is proposed aiming at the involvement of mobile devices for blockchain operation (see Fig. 1). As a baseline, the system utilizes *ID-based cryptography* initially discussed in [78] during the times when blockchain itself was brought to the research community's attention. After 20 years, the first realization of this strategy took place in work [79] by C. Cocks *et al.* They proposed a new approach of obtaining the sender's secret key to generate a signed message using a private key generator (PKG) and a unique sender ID. However, there are several challenges related to PKG utilization: (i) PKG can sign and decrypt all the messages; (ii) key revoking is not implemented; (iii) safe channel is required for the key dissemination; and (iv) encryption and decryption mechanisms are computationally different. Most of those could be mitigated by utilizing Shamir Secret Sharing (SSS) [80], allowing for the PKG secret key dissemination and reconstruction based on only a portion of previously distributed shares, which is used in the developed algorithm.

A. DESIGNED CONSENSUS 'TRINITY'

In particular, a hybrid multi-level architecture is proposed to achieve better fairness and flexibility of the system operation. Here, the first level consists of a large number of devices with limited computing and communication capabilities (i.e., PoAs), while the second level devices have significantly greater capabilities (i.e., PoSs), carries greater responsibility and greater risks for the functioning of the system due to distributed decision making. The third level consists of the devices responsible for solving the computational puzzle (i.e., PoWs). The involvement of the devices from all three levels is required in order to add a new block to the blockchain, which is detailed further in this section.

The system defines four types of major components that would be explained before proceeding to the actual operation (see Fig. 2):

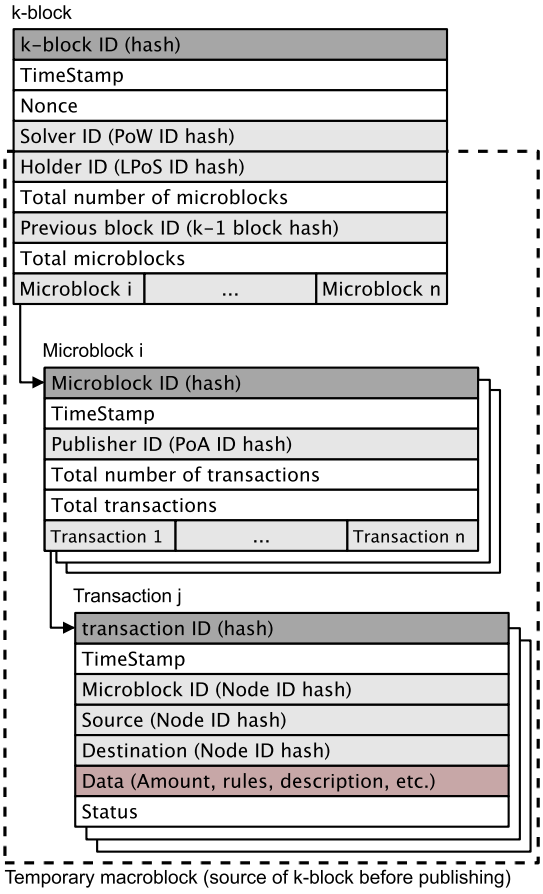


FIGURE 2. Proposed block structure.

1) k-block – is the actual block added to the blockchain, which is a result of a computation puzzle solution by PoW, which is based on macroblock signed by a trusted PoS node with high stake along with a group of PoAs acting as verifiers. The generation of k-block requires significant computing and energy resources, as well as an online presence.
2) Macroblock – is a temporary block signed by currently selected Leading PoS node.[2] Its header is generated prior to sending it to a group of PoA nodes for actual transaction verification (via microblocks, see the next item). After the verification phase is complete, the LPoS signs a set of verified microblocks (macroblock) and broadcasts it to PoW nodes for adding to the blockchain. Macroblock generation requires a significant stake of tokens and the online presence of the current LPoS node.
3) Microblock – is a set of transactions signed by currently selected LPoS node and verified by a single PoA node together with the macroblock header. Not a computationally hungry task and does not require constant online presence – PoA may participate in the

[2]The Leading PoS (LPoS) is one of PoS nodes selected by pseudorandom procedure or the voting of other PoS nodes, i.e., a portion of PoS nodes should approve the announced potential LPoS to take its role for this block.

verification process voluntarily since the number of PoA nodes is typically high.

4) Transaction – the peculiar data to be added to the blockchain. It is originated from nodes outside the consensus. It may contain certain rules or smart contract-related information (encrypted to assure the data privacy if required).

Overall, k-block is the top-level result of the interaction by all nodes with different roles listed further.

1) HOLDER (PROOF-OF-STAKE)

PoS nodes are holding a significant amount of tokens, thus, becoming a more trustworthy part of the system operation (similarly to banks and trusted authorities). Any node can prove the eligibility to become a holder by staking the highest number of tokens (currently set to 10% of all available tokens). Key SK_{HK} is a shared key distributed between a set of holders based on the Lagrange interpolation formula [81]. The corresponding PK_{HK} is known to any node. The *resident* node is responsible for SK_{HK} generation, and a group of holders forms a PKG.

The resident's functions are: (i) to store SK_{HK}; (ii) to distribute it to other PoSs; and (iii) to estimate the Lagrange polynomial properties. After the resident is stopped, the key shares will be distributed to PoS according to protocols described in subsections V-G and V-H. The Lagrange polynomial characteristics would not be possible after the resident leaves the system and, thus, they should be adjusted after the initial period of the system operation.

Holders are systematically executing the protocol described in subsections V-A to verify who has the right to distribute the publication keys during this system operation state. The corresponding time interval is set to 100 k-blocks in the simulation environment. The Leading PoS (LPoS) selection result is then stored as statistic blocks and may be verified by any node. Selection is based on the pseudo-random procedure or the voting of other PoS nodes, i.e., a portion of PoS nodes should approve the announced potential LPoS to take its role for this block.

Next, the required number of PoSs are involved in the session secret key for LPoS generation after the k-block retrieval. The publication public key is calculated based on the k-block ID (hash sum) and LPoS ID. The secret key and the corresponding shares are calculated based on the protocol described in subsection V-B. The holder gets a reward for participation in the voting and PKG-related procedures. Therefore, current LPoS recovers a version of the secret key from other PoS miners. A session key is required to sign microblocks. Only LPoS with all necessary key shares of the secret key can accept and sign blocks from PoA nodes.

LPoS announces the possibility to verify current transactions to be added to the block to a set of pseudo-randomly selected PoA nodes and the ones who replied receive the transaction(s) signed by the session key to be verified and further combined into the macroblock, see subsection IV-A2.

After PoAs have successfully verified the transactions, the macroblock is broadcasted to available PoW nodes, according to subsection IV-A3.

2) VERIFIER (PROOF-OF-ACTIVITY)

PoA nodes are involved in the microblock publication process. The main task of the PoA nodes is to listen to the network continuously. Each PoA in the group of selected PoAs verifies the signature of the delivered microblock payload (array of transactions) and forwards the signed version back to the LPoS in case of the verification success. After the LPoS received all microblocks verified by PoAs, i.e., all data becomes validated by PoAs and LPoS node in the system, their participation may be verified later.

Microblocks must be verified and signed by PoA nodes using their own secret keys. The participation of PoA nodes is ensured by their binding to the specified k-block. PoAs are resource-constrained devices and are not involved in the 'mining' process. In brief, PoA nodes are limited in terms of computing and communications and, accordingly, are dedicated to the operation on smartphones. PoSs – could be stationary power- and storage-independent nodes. The number of PoS nodes is expected to be smaller (by orders of magnitude) than PoAs'.

3) SOLVER (PROOF-OF-WORK)

PoW nodes are responsible for the generation of new k-blocks from macroblocks delivered from current LPoS. The main requirements for this type of nodes are (i) reliable access to the Internet; (ii) storage (required to store the blockchain structure); and (iii) computational power for hashing. The solver is recursively calculating nonces for new k-block generation according to the set of predefined rules – difficulty, batch number, hash links validity. Each k-block is distributed through the network in a broadcast way after its generation to PoS and, potentially, PoA nodes. Each node checks its validity based on locally stored data and adds it to local blockchain storage if valid.

As a baseline, widely known Nakamoto protocol [82] is used for the blockchain construction. PoW's main aim is to generate the block and obtain the resulting award for the computational expenses. The k-block contains its public key. The selection of the hashing function does not affect the overall system operation directly. RandomX function, developed by Monero [83], is currently adopted on the PoW side in order to increase the fairness of the system.

4) EXAMPLE OPERATION

For example, at the i^{th} time instant of the blockchain operation, k_{i-1} k-block from $i-1^{th}$ interval is already present in the blockchain and new transactions begin to appear. LPoS is selected by active PoS nodes by advertising itself along with its stake. PoSs that agreed on LPoS selection (based on the advertised stake probabilistically), provide it with 'salted' secret shares and, if the number of shares is higher than

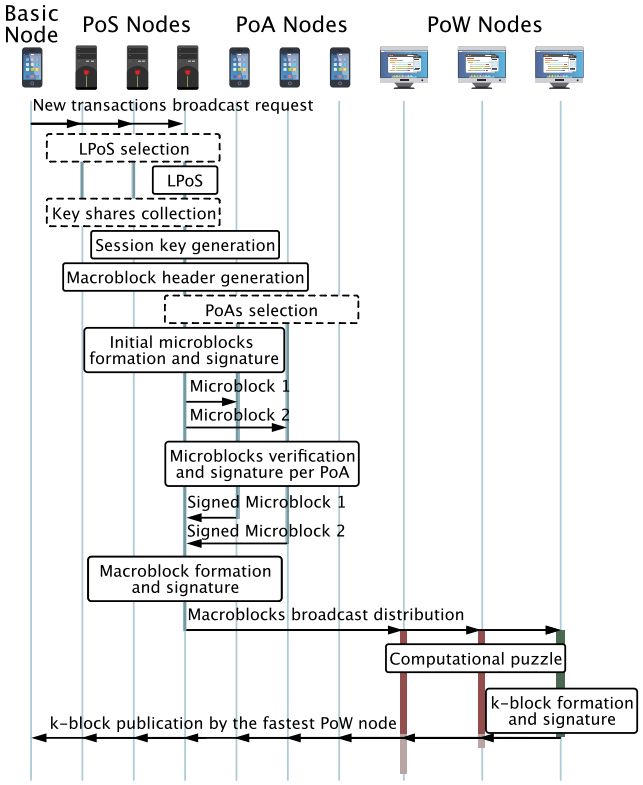


FIGURE 3. Proposed system block publishing process.

required by SSS threshold, LPoS constructs the session secret key used for signing microblocks and current macroblock.

Next, LPoS announces the possibility of verifying the transactions for future k-block for all online PoAs. A group of PoAs from the replied ones is selected by LPoS based on the pseudorandom procedure. If at least one of the selected PoAs will interrupt the communications during the oncoming phases – the group of PoAs selection procedure should be restarted by LPoS.

LPoS then signs each set of transactions with the session key and sends those to different PoAs from the group. PoAs verify the signature and sign the own microblocks with a personal secret key. Finally, each PoA returns the signed microblock to LPoS, which further combines those in the Merkle tree and signs by its own secret key.

By this means, a new macroblock is generated based on the previous k-block from $i - 1^{th}$ interval, the root hash of the Merkle tree of the collected and signed microblocks, and its signature created by LPoS selected during the i^{th} interval. LPoS is sending the generated macroblock to PoW nodes in a broadcast way, and the fist PoW to solve the computational puzzle adds it to the blockchain. Simply, the proposed process of the block publication is explained in Fig. 3. The following subsections describe the relationship between the blockchain nodes.

The proposed blockchain construction algorithm belongs to the permissioned category since PoA nodes sign the microblocks they form with own secret keys, public keys are known, and all PoS are known, and the procedure for entering a node into the PoS category is public.

5) ADDITIONAL DETAILS

Bitcoin-NG protocol is selected to handle macroblocks [84] to reduce the latency between the creation of blocks so that each microblock inside a macroblock is created in real-time and adds transactions to the blockchain immediately upon their arrival. So, there is no need to wait until an entire macroblock is completed, its hash is found, and it is synced between all nodes in the network – small microblocks can be generated concurrently inside it. The main reason behind the utilization of this protocol lies in its possibility to increase the mining speed in the system, i.e., to increase the number of blocks generated by the system within the selected time frame. The fundamental limit here is the distribution time of the newly generated block between all the nodes in the system. In case the generation time is shorter, the probability of forking in two distant sections of the network may arise tremendously. Direct Acyclic Graph (DAG) [85] allows the addition of new blocks in different network segments handling the forking.

The goal of DAG is to deterministically rearrange the k-blocks for the ledger recalculation based on the following set of requirements:

- Graph construction and graph walk procedures are developed minding the *consensus* between the nodes, i.e., there is a need for defining the minimal number of nodes to guarantee the validity of current system state at any time of execution;
- New k-block is validated (added to consensus) during a specific time frame;
- New k-block should be inserted in the chain according to its publishing time;
- Addition of a new k-block should not require the traversal of the entire graph;
- Long-time forks should be avoided.

Generally, PoWs form k-blocks according to the standard rule, providing the specified properties of the hash, thereby confirming the work done. The primary purpose of the work is to streamline the general chain of events. The main drawback is that they cannot build blocks too often, while they cannot provide sufficient transaction transfer speed.

B. PROPOSED UTILIZATION OF DAG

First, the graph walk procedure is defined, starting with inverting the DAG. Next, the Queue-based topological order algorithm is applied to the graph as by iterative removing of the nodes and storing the logs of this process, see [85]. The system utilizes a deterministic algorithm allowing to calculate the difficulty for each k-block during the graph traversal. Therefore, every new k-block is considered valid if its hash is equal to its difficulty. This algorithm allows to calculate the value *branch_max* during the graph traversal based on the k-block *number*, *brunch* ($0 < branch < branch_{max}$).

Each k-block s has two links to previous and next k-blocks t_1 and t_2 such that $t_1.branch == s.branch$ and $t_1.branch != s.branch$ despite the case when $branch_{max} = 1$.

New k-block generation procedure is described as follows. First k-block has $branch = 0$, $number = 0$. It is valid if:

1) $\{number, branch\}$ pair is unique;
2) k-block has links to t_1 and t_2, $t_1.branch == s.branch$, $t_1.branch != s.branch$, $s.number > t_1.number$. In case there are more than one s, the one with higher $t_2.number$ will be accepted;
3) k-block's hash is equal to *difficulty*.

C. LEDGER OPERATION

The following parameters are considered during the ledger calculation: k-block mining, a reward for microblock publishing, and transaction fee. The rewards are dynamic and are based on the blockchain operation history. The transactions inside the microblock are stored in a sorted array. Therefore, all k-blocks, microblocks, and transactions could also be arranged for any DAG size. As a result, the entire history of events could be linearly retrieved allowing to calculate the states of the account balance.

At the beginning of the execution, the ledger is empty. During the block rewarding process, the balance of the existing account will be changed, or a new record will be found. The states of nodes are updated during the transactions accordingly. The transaction is treated as invalid if there is no information about the account in the ledger, or it has not enough tokens in the wallet. Invalid transactions are discarded.

D. REWARDING AND DIFFICULTY ESTIMATION POLICIES

The estimation of the reward is based on the deterministic algorithm for each system state relying on history and the current block. The estimation of rewards depends on the emission curve and current emission distribution. Initially, the distributions are as follows: PoW – 10%; PoS – 25%; and PoA – 65% of the emission. The emission distribution balance is a dynamic system property and could be used as a tool to mitigate malicious activity between different nodes based on a specifically selected emission curve. Generally, the values of rewards are estimated in such a way that it is inexpedient to run PoA emulators on the hardware suitable for PoW or PoS.

The authors have designed a reward and difficulty assignment system, Neuro, current neural network, inspired by [86]. Neuro utilizes historical blockchain data to predict the required rewards and difficulties for each new cycle. As soon as a cycle is completed, the statistics of that cycle are used to improve the network's next predictions. In order to make these predictions, a variation on a type of neural network that has a selective long-term memory was applied: a recurrent neural network. For the non-recurrent neural network, each forward cycle starts with a clean state, and neurons have values that originate only from weighed connections to neurons in the previous layers (or inputs). A recurrent neural network is a network where the result of a neuron activation, the state, affects the next forward cycle of the network.

V. DEVELOPED CRYPTOGRAPHIC PROTOCOLS

This section provides a brief overview of the developed protocols. More details on the implementation could be found in [87], more recent versions of protocols (if any changes) would also be available via the link.

Each k-block has its unique ID_k estimated according to correct execution of function $H(*)$ as

$$ID_k = H(block_{k-1}), \tag{1}$$

where H is the desired hashing function.

A. PROTOCOL OF THE "LEADING" PoS MINER SELECTION DURING THE SESSION (VOTING)

The main requirement of the protocol is resistance against the repetitive selection of the same miner during a series of sessions, i.e., improved randomization, and protocol should be executed either by a group of PoS nodes or all the available ones but the selection rule is different for each execution.

To exclude the possibility of restarting elections by disgruntled PoS miners, the result should be pseudo-random but directly related to the number of current k-block and list of voters. A series of assumptions are thus introduced:

1) All PoS miners in the current system state can compile a list of all PoSs. In this case, all sets of identifiers will be obtained identically and ordered lexicographically.
2) In the course of the routing procedures, each PoS miner compiles a list of currently active PoS. At the same time, the lists of participants differ by no more than 10%. The list is stored as a binary vector: $V_{PoS} = (0, 1, 1, 1, 0, \ldots, 1)$, where the number of positions coincides with the size of the list from item 1, where 0 means that the participant with the given identifier is inactive, and 1 that it is active.

With this list and its associated vector, each node can vote.

- *Stage A*: After the list is constructed, each participant (PoS miner) calculates the hashing function

$$r = \frac{H(ID_k|PoS_1|\ldots PoS_N)}{H_{max}} \in (0, 1), \tag{2}$$

where $H_{max} = max\ H(ID_k|PoS_1|\ldots|PoS_N)$ and PoS_i is PoS ID from the list.

Therefore, the voting is further based on r and on comparing it to a newly generated discrete random variable in the same bound. Thus, each PoS_i receives a probabilistic value based on its public rating. The sum of all PoS probabilities should be equal to 1. After that, the probabilities are logically interpreted into intervals on the section from 0 to 1, and the tagged PoS node is selected if r is located in its interval.

- *Stage B*: After the tagged PoS was selected (LPoS status), the voter calculates the corresponding publication public key and transmits the 'salted' secret key share to selected LPoS. After one PoS receives at least k of shares (basically, those have the same list on their side), the secret key is generated as described in Algorithm V-B.

- *Stage C*: LPoS forms a header of the future block after the session key is received according to Algorithm V-B. The entry is formed from the k-block number and voting list signed with the session key. Thus, it becomes possible to validate LPoS rights and distribute rewards.

B. LEADING PoS SESSION KEY GENERATION

The main requirements are: keys could only be used once; keys should be distributed securely; any user could not generate keys; and keys do not contain any information related to PoS miner secret keys.

The protocol is executed for $LPoS = PoS_i$ accordingly. Each PoS has its pair of keys PK_{PoS_i}, SK_{PoS_i} directly related to its wallet.

Next, the session key PK_{LPoS} is generated for leading PoS. It will be further utilized for the microblocks signature and, thus, would be split into shares and distributed between PoAs. PK_{LPoS} is defined by k block present in current session and ID_{LPoS}. ID_{LPoS} is selected as PK_{LPoS} or a function of this key. PK_{LPoS} and SK_{LPoS} would be thus selected as

$$PK_{LPoS} = H1(block_k||ID_{LPoS}) = Q, \quad (3)$$

$$SK_{LPoS} = ss_i\, Q, \quad (4)$$

where $H1$ – is a mapping function described in Algorithm 1, Q is an element of $G1$, and ss_i, is obtained by Algorithm 2.

SK_{LPoS} is generated by PoS nodes according to the distributed ID-based cryptographic PKG method [88] by k of n schema, which considers the collision resolution for cases when more that one leader is selected. After the key is generated PoS can group and sign the transactions and distributed those to applicable PoAs.

Algorithm 1 Initialization of ID-Based Schema With Distributed PKG

1: Define groups:
2: Define $G1$ as a cyclic group of order q (group of points on elliptic curve);
3: Define multiplicative group $G2$;
4: Define functions:
5: $H1 : (0, 1)^* \rightarrow G1$;
6: $H2 : G2 \rightarrow (0, 1)^*$;
7: $H3 : (0, 1)^* \rightarrow Zq$;
8: $e : G1 \times G1 \rightarrow G2$ (bilinear mapping);
9: Define Master Secret Key (MSK) as $s \in Zq$;
10: Define P: generator of $G1$;
11: Define Master Public Key (MPK) as sP.

Algorithm 2 PKG (k, n) Master Secret Key Splitting

1: Generate random polynomial in residue field q: $deg(\phi(x)) = k - 1,\ \phi(0) = s$;
2: Each participant (PoS) receives its key share of Master Secret Key $ss_i = \phi(ID_i)\ mod\ q$.

Algorithm 3 Session Key SK_{LPoS} Generation for $LPoS$

1: Each of k participants calculates equation 3.
2: Transmits its $ss_i \cdot PK_{LPoS}$ and ID_i to LPoS.

Algorithm 4 Secret Key Recovery

1: LPoS is calculating SL_{LPoS} based on the received from Algorithm 3 data as
2: $SK_{LPoS} = \sum_{i=1}^{k} \lambda(ID_i, 0)(ss_i\ PK_{LPoS}) = sQ$, where $\lambda(ID_i, 0)$ is a Lagrange coefficient generated per coalition for each user ID_i and 0.

C. PROTOCOL OF THE PoA APPLICABILITY FOR MICROBLOCK GENERATION PROCEDURE

The coalition of PoAs is selected after a new set of transactions is collected is published. It is selected based on constant N_{PoA} per node and the corresponding ID such that $H(PoA_{ID}) = H(k - block||i), i = 1, \ldots, N_{PoA}$. Therefore, each node has an opportunity to verify if its ID is in the group fast, while brute-force attack on the ID is a computationally complex task.

D. VERIFICATION OF MICROBLOCK BY PoA FOR CURRENT K-BLOCK

The main requirements for the protocol are simultaneous and independent execution of the coalition members; data exchange minimization; in-block additional data minimization; and confirmation of the participation in the verification.

Each PoA verifies if it is applicable for new microblock verification V-C after new k-block header is published. In case applicable, it verifies the assigned microblock M based on the selected transaction with a predefined size. After M is verified, PoA adds the following data to it: PoA_{ID}, k-block number. Next, it is signed by its' SK_{PoA} and immediately published (returned to LPoS).

E. LPoS MICROBLOCK ASSURANCE PROTOCOL

After Algorithm V-A was executed, and the new session key was generated with Algorithm V-B, LPoS starts to assure the microblocks.

- *Stage A*: After PoAs have signed the corresponding microblocks, LPoS is collecting those from the network. LPoS is verifying the k-block number and verifies if PoAs are in the coalition of this block.
- *Stage B*: LPoS verifies the validity of transactions in the microblock based on the ledger.
- *Stage C*: In case the verification succeeds, each microblock is signed with the session kety SK_{LPoS} from Algorithm V-B according to Algorithm 5.

Meanwhile, PoS miners are in standby mode until the required number of transactions is collected, and generate final macroblock from all the obtained microblocks to be distributed to PoWs for the actual addition to the blockchain.

Algorithm 5 Microblock Signature Protocol

1: LPoS generates r from Zq;
2: Calculates $R = rP$ and

$$S = SK_{LPoS} + r\ H1(M||ID_{LPoS}), \tag{5}$$

where $SK_{LPoS} = sQ$ is obtained with Algorithm 4, $H1$ with Algorithm 1, and M is selected microblock.
3: Adds (R, S) to the macroblock.

F. CRYPTOGRAPHIC MICROBLOCK VERIFICATION PROTOCOL

The main goal of the protocol is to verify any microblock at any time, and the requirements are: it should be executable at any node; it should be based only on publicly available information. Two signatures verify each microblock: the first one is the signature of PoA node, that verified the corresponding microblock, and the second one is the signature of related LPoS miner. The verification procedure is made according to Algorithm 6.

Algorithm 6 Cryptographic Microblock Verification Protocol

1: The verifying node check the k-block number, and then that the PoA-miner is a member of the group of selected PoAs for this session and its signature.
2: It calculates PK_{LPoS} according to equation (3).
3: The verifying node checks the signature of the microblock R and S by

$$e(P, S) = e(MPK, PK_{LPoS} = Q) \cdot e(R, H1(M||ID_{LPoS})), \tag{6}$$

where P is a generator of G1, MPK is a Master Public Key and M is a microblock.

The microblock is assumed as verified if both signatures are checked successfully.

G. DISTRIBUTED PKG SECRET UPDATE

This phase is executed either whenever the set of PoS miners changes, or during the ledger recalculation, i.e., when any of the PoS nodes loses the PoS status. The resident node distributes new key shares. It is also responsible for the (k, n) relations during the initial system operation stage. After the system operation is stable, its role is distributed between PoSs.

H. DISTRIBUTED PKG NEW SECRET SHARE TRANSMISSION PROTOCOL

When a new PoS node arrives, the new node requests its share of PKG master secret key. If it has the right, the resident node responds. Keys to new participants are built and given out by the resident node, while the system developer or owner acts in its role. When the parameters are settled, the resident role can be dissolved in PoS miners. For a new participant node, its polynomial point is calculated as

$$ss_{new} = \phi(ID_{new})\ mod\ q, \tag{7}$$

where q is the order of the group of points G1.

By efficient integration of the previously developed protocols, it becomes possible to involve a high number of recourse-constrained devices in the blockchain operation.

In the next section, the proposed system is compared with existing ones and analyze it from user experience metrics.

VI. EVALUATION OF SMARTPHONE-BASED BLOCKCHAIN SOLUTIONS

This section briefly outlines the performance evaluation setup from the hardware perspective and provides the technical specification of the devices, followed by the description of the performance campaign.

A. COMPARISON OF EXISTING SYSTEMS

Various aspects of presently available solutions were taken into consideration during the development phase. The results of the analysis are given in Table 1. Overall, most of the existing projects utilize either PoW or Cloud-like techniques, and, in the latter case, smartphones are not participating in the blockchain operation process rather than delegating it to some other instance in the network. Systems like uPlexa and MIB actually involve the devices, which is the reason behind our numerical evaluation targeting those systems.

After the protocols are appropriately described, the next subsection provides the detailed performance evaluation of MIB and uPlexa on modern smartphones and tablets along with the developed system.

B. PERFORMANCE EVALUATION ENVIRONMENT

For the purpose of this work, we have selected multiple devices from two categories in order to have a broader overview of the blockchain integration potential: (i) smartphones and (ii) tablets. Both flagship and old models of devices and operating systems were analyzed, and the corresponding specification is given in Table 2. Note, Apple devices are not analyzed within this work since power-hungry applications by design are prohibited by subsection 2.4.2 of App Store Review Guidelines. Most of the devices in each class have very similar characteristics except for the flagship models. This paper mainly focuses on user-oriented metrics since smartphones and tablets aim to provide the best user experience as the most significant personal device of today.

All measurements were carried out under the same conditions and the corresponding dataset is available at [89]. The device had a display on to simulate user interaction, as it has the highest power consumption compared to other smartphone modules [90]. Overall, we analyzed the following scenarios:

1) Self-discharge with turned on display.
2) Operation with different smartphone-oriented blockchain techniques.

TABLE 1. Comparison of existing mobile blockchain projects.

Project	Technology	Features	Background mode	Identification
MIB Coin	Mobile Proof-of-Work: Bitcoin-like mechanism with lowered mining cost	Claims to be the first mobile-only mining project; has three difficulty settings to protect smartphones from overheating; eco-friendly PoW mining achieved with low energy consumption	Not available	E-mail required
uPlexa	Proof-of-Work: IoT, PC, and Smartphone CPU mining with fast transactions	IoT mining & eCommerce; open-sourced; has numerous difficulty settings to protect smartphones from overheating; has a near-zero network congestion model for fast transactions	Available	Not required
TAU Coin	Proof-of-Transaction: block generation probability is determined based on address' accumulated transaction history	Fixed total token supply; open-source	Available	Not required
Electroneum	Cloud Mining: rewarding users with free tokens; mining period extension is required every week	The first cryptocurrency compliant with KYC; resistant to 51% attack	Cloud mining continues with a closed application, but no blocks are actually mined or verified	E-mail for participation; identification required for withdrawal
Phoneum		Offers gamified experience		Not required
Hybrid solution	A combination of PoW, PoS, and PoA (PoA is applied for block validation on resource constrained devices)	PCs and mobile devices form one blockchain; smartphones perform simple verification instead of solving complicated tasks, resulting in low energy consumption	Available	Not required

TABLE 2. Selected devices with their corresponding specifications.

Device model	Android version	Type	SoC	Processor	RAM	Battery
Samsung Galaxy S9	9.0	Smartphone	Exynos 9810	2.7 GHz Quad-Core Mongoose M3, 1.7 GHz Quad-Core Cortex-A55	4 GB	Li-Ion 3,000 mAh
Huawei P8	6.0	Smartphone	HiSilicon Kirin 930	2.0 GHz Quad-Core Cortex-A53, 1.5 GHz Quad-Core Cortex-A53	3 GB	Li-Ion 3,400 mAh
Meizu M5c	6.0	Smartphone	Mediatek MT6737	1.3 GHz Quad-Core Cortex-A53	2 GB	Li-Ion 3,000 mAh
Xiaomi Redmi 4A	7.1.2	Smartphone	Qualcomm MSM8917 Snapdragon 425	1.4 GHz Quad-Core Cortex-A53	2 GB	Li-Ion 3,120 mAh
Xiaomi Redmi 5A	7.1.2	Smartphone	Qualcomm MSM8917 Snapdragon 425	1.4 GHz Quad-Core Cortex-A53	2 GB	Li-Ion 3,000 mAh
Lenovo YOGA Tablet 2 8.0	5.1.0	Tablet	Intel Atom Z3745	1.33 GHz Quad-Core	2 GB	Li-Ion 6,400 mAh

3) Different connectivity options:
   a) Connected over cellular link (LTE).
   b) Connected over WLAN (IEEE 802.11n/2.4GHz).

By selecting this set of scenarios, we cover most of the smartphone operational states.

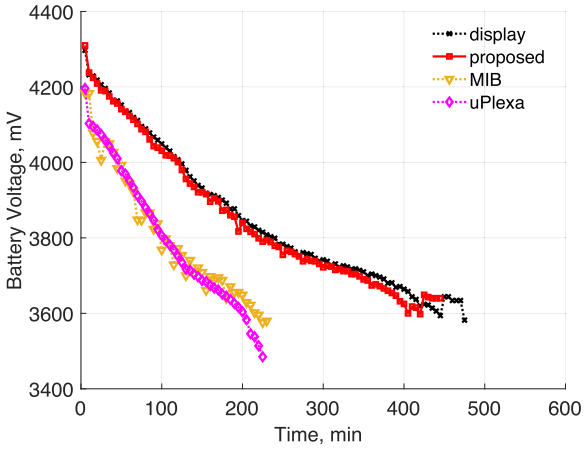
C. NUMERICAL RESULTS

This subsection provides the main results obtained during the performance evaluation campaign.

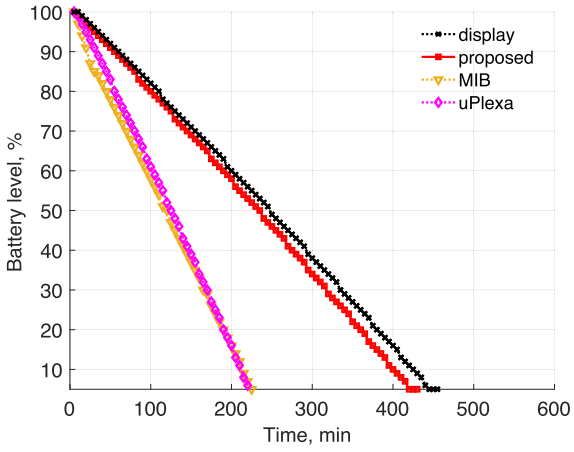
In the first set of experiments, the main focus is given to the flagship smartphone Samsung Galaxy S9 as the best representative for handling the potential negative impact of blockchain operation. First, currently available mobile blockchain-related applications and related concepts are overviewed as described in Section III.

Note, only concepts utilizing the computational power of the smartphone instead of delegated Cloud computing are analyzed. Cloud mining has been excluded from the evaluation due to the fact that mobile devices running Electroneum or Phoneum do not mine neither validate blocks nor perform any tasks. Additionally, with cloud mining, the application is not required to stay open, making battery monitoring unnecessary.

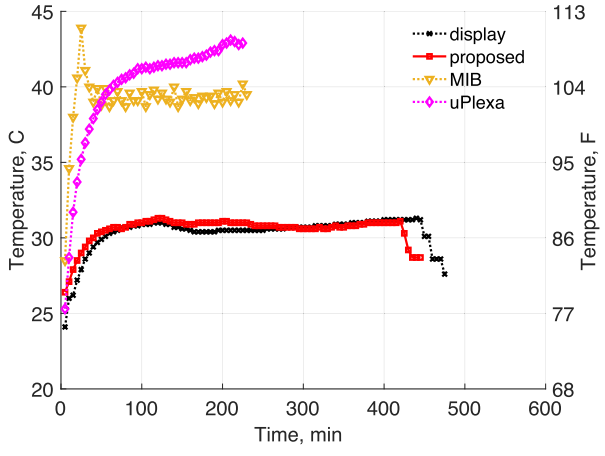
According to the results depicted in Fig. 4, the PoA-based solution proposed in this work contributes only approximately an additional 5% to the device's discharge rate caused by the display utilization. At the same time, the negative impact of PoW-based strategies (MIB and uPlexa) can reach up to 45%, i.e., the smartphone's battery will drain twice as fast (see Fig. 4b) causing a negative impact on user



(a) Battery output voltage

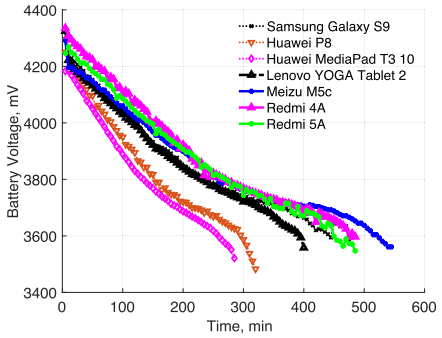


(b) Battery level

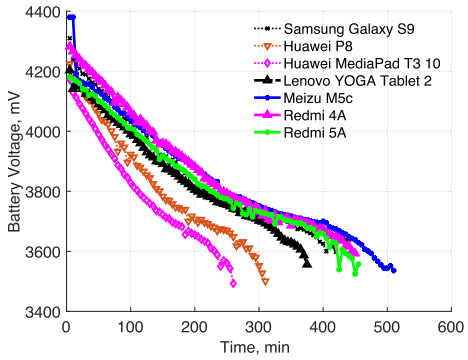


(c) Battery temperature

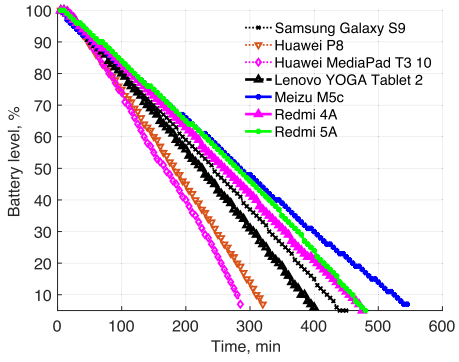
FIGURE 4. **Impact of different blockchain techniques on Samsung Galaxy S9 battery.**



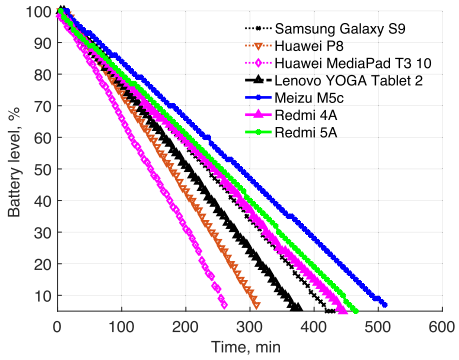
(a) Battery output voltage: Display only



(b) Battery output voltage: PoA and display



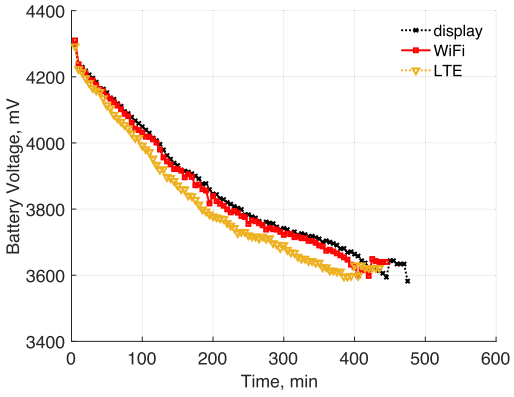
(c) Battery percentage: Display only



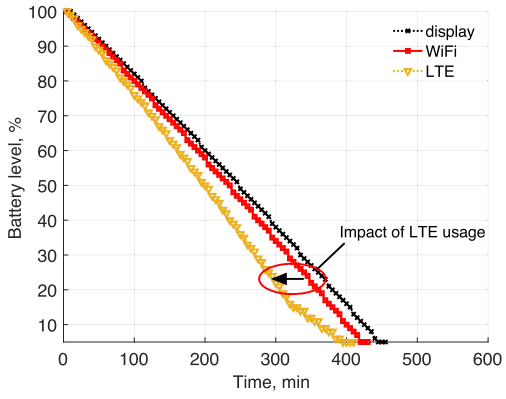
(d) Battery percentage: PoA and display

FIGURE 5. **Comparison of the devices from Table 2.**

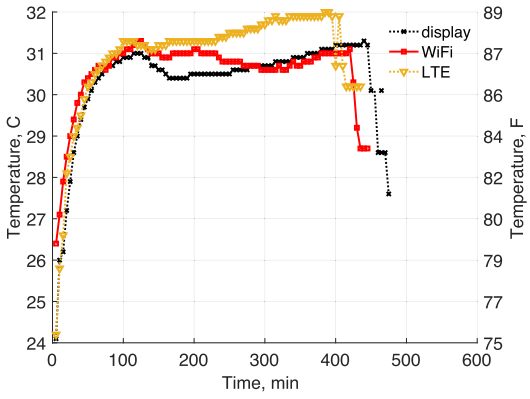
experience. In addition to this observation, the temperature of the battery was measured, and the results are given in Fig. 4c. According to our measurements, the use of PoW on a mobile phone will not only negatively affect the discharge rate of the battery but also will increase its temperature to 112^oF (44^oC), which makes the device practically unusable and potentially dangerous. The same tests were executed ten times per concept, and the results fall within the same range for stable operation (battery level >10%).



(a) Battery output voltage



(b) Battery level



(c) Battery temperature

FIGURE 6. Impact of wireless technology selection on Samsung Galaxy S9 battery.

While the developed solution proved itself as a promising one from a user experience perspective, we kept the evaluation towards its impact on different devices listed in Table 2. All the studied devices show similar behavior as Samsung Galaxy S9 in terms of battery output voltage (see comparison in Figs. 5a and 5b) and discharge rate (Figs. 5c and 5d), i.e., less then 5% of negative impact. Interestingly, the plots also provide an observation on the battery saving mode presence either in the battery controller around 400 mins interval, i.e., after the output voltage drops beyond the threshold value, see Fig. 4a self-discharge and the

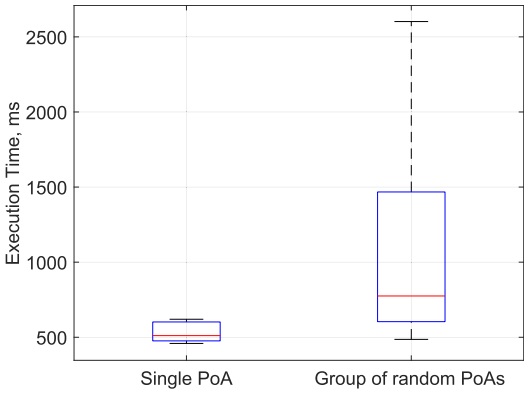


FIGURE 7. PoA verification time.

proposed system operation scenarios. However, the utilization of PoW has such a tremendous impact on the battery state that this behavior is not visible at all due to a rapid discharged rate.

Notably, previous tests were executed utilizing the WLAN interface, i.e., IEEE 802.11n operating at 2.4GHz. Because handheld smartphone devices are mobile nodes by definition, the analysis of the cellular utilization impact compared to WLAN is also provided in this paper. For these measurements, the Samsung Galaxy S9 smartphone was chosen since the results from other devices, see Fig. 5, prove similar behavior in terms of battery impact.

The second scenario is focused on the comparison of LTE versus WLAN utilization, the measurements are shown in Fig. 6. Interestingly, utilization of cellular connection is less energy efficient compared to WLAN, see Fig. 6b. As was observed in Fig. 5, joint power consumption PoA operation over WLAN has an impact of only 5% while switching to LTE may increase it up to 20%. Interestingly, the selection of wireless interface does not have any significant impact on the battery temperature, see Fig. 6c, but only on the battery lifetime, which allows to execute in on the smartphone without noticeable impact on the user experience. Moreover, the proposed system shown itself as a promising instrument with the battery consumption of the instant messenger level.

Execution time-wise, the involvement of resource-constrained PoA node in the microblock verification process is transparent for the user, see Fig. 7. The plot shows two cases, the left one corresponds for the execution time of a single PoA node from the moment it receives the transactions from LPoS until the acknowledgment is sent back (measured on Galaxy S9). The right one provides measurements related to the overall PoA involvement process measured from the LPoS side, i.e., the time from the first message to the first PoA in the group until the acknowledgment reception from the last one. The execution was observed 1,000 times, and there were five random PoA nodes selected for each execution in the second scenario. According to the measurements, a single verification requires only 500 ms, excluding the communications overhead. This pattern is highly visible in

the second scenario. Unpredictable network state, as well as differences in hardware, has an impact on variance while the impact on the mean is not significant.

Based on the executed trial, the utilization of PoA-based solutions on the smartphone itself shows a better perspective compared to PoW-based ones in terms of user experience metrics.

D. QUALITATIVE SECURITY AND PRIVACY ANALYSIS

After evaluating the ability to execute the designed primitives on real devices, this subsection provides the analysis of primary security and privacy aspects of the designed system. While providing a quantitative analysis of such a complex system would require a separate publication, this subsection provides the following overview.

Security risk assessment can be made qualitatively or quantitatively, there are some techniques that assist in the threats analysis. To define whether existing threats relevant to the system, the penetration testing approach was performed. By applying this methodology to the top-down system analysis, it becomes evident how the system would react in coping with emerging threats. The analysis includes specific information on vulnerabilities and possible approaches taken to mitigate each risk.

Utilization of a multi-level structure allows obtaining greater flexibility and reliability of the blockchain system. As for general countermeasure, all nodes utilize asymmetric cryptography for encrypting their communications in order to avoid Man-in-the-Middle Attacks (MITM), each node generates a key pair (public and secret key) thus providing the authentication. In particular, the information provided by each PoA node of the first and lowest level is authenticated and simultaneously protected from spoofing by using the digital signature and secret key. The same applies to LPoS and PoW node.

The appearance of a *malicious PoA node* in the system can be detected by the second-level PoS nodes in the process of forming the macroblock, which consists of the microblocks verification executed by PoAs. Proposed voting and selecting of current LPoS for each successive macroblock prevents a particular malicious PoS from ''colluding'' with one or more PoAs.

The Algorithm V-E for microblocks assurance performed by PoS nodes provides protection against *Double Spending Attack* [91]. Since LPoS verifies the validity of transactions in the microblock during stage B, any node's signature verification can be achieved based on the ledger later on. Any node will receive a confirmation of a false transaction since the signature is easy to verify using only the information about the current block number and the LPoS ID, i.e., no additional blockchain information is required. An incorrect signature formation is not possible without the participation of the LPoS, as well as collusion of almost all PoS (the key issuance threshold provides this) cannot forge a transaction. It is also impossible to reuse the transaction and change its location inside the chain since LPoS is linked only to its k-block (confirmed by the voting results). The lifetime of each LPoS keys are limited to one k-block, after which new elections should be held, and a new key will be issued, i.e., it will not be possible to use the session key to fake microblocks in the future.

According to [92], the *Majority Attack* could be defined as ''The attacker submits to the merchant/network a transaction which pays the merchant, while privately mining a blockchain fork in which a double-spending transaction is included instead''. In the proposed system, the attacker, even with 100% of PoW miners, does not have a chance to generate the fork by design. Moreover, the utilization of RandomX ensures random code execution, together with several memory-hard techniques to minimize the efficiency advantage of specialized hardware. Each transaction must be signed by a PoA linked to the k-block number, macroblocks with a set of transactions must be signed by the elected LPoS using a unique session key, which is generated based on a significant number of PoS nodes. Thus, the attack becomes exceptionally complex compared to the conventional power-wise approach. To form such a hidden fork, it is necessary to completely capture all three levels of the network being geographically and logically separated.

Selfish Miner Attack is used to reverse a transaction by ''forking'' the blockchain one block behind the block the transaction was included in [93], [94]. In the proposed system, the length of a branch is determined by the number of transactions included in it, and therefore it is not possible to eliminate out transactions by creating empty branches without the participation of all three security levels.

From the network perspective, the nodes are highly distributed not only spatially but also between the logical layers. That includes public keys for verifying PoS and PoA signatures and rules for forming nodes associated with each k-block. This feature makes it difficult to execute *Routing attacks*, e.g., to isolate a node or network segment and fake the traffic by emulating the operation of a large number of malicious nodes. Moreover, PoS nodes involved in voting require significant stake, thus making the execution of the attack not only computational- but also token-wise consuming. So, the *Eclipse Attack* [95] can only be applied in the short-term to the weakest PoA clients that can be attracted to work by creating blocks with a false number, while their work will not be paid for, but it would not result in a *DDoS attack* since their packages will be filtered out without processing by design.

Sybil Attacks [96] aim at providing multiple identities to other nodes mainly for data crawling, are not critical in the proposed system, on the one hand, since transactions are supposed to be stored in the blockchain by regardlessly and, on the other hand, high dynamics of the proposed architecture only provide a temporary view on the network. One of the countermeasures for future implementation may be a temporary additional node ID based on public IP address, thus, requiring a massive pool of public addresses to execute the attack. To highlight, current PoS nodes are publicly listed but

could also lose the status over time due to variations in stake. Similarly to Sybil attack, *NodeID attack* could be described as multiple nodes trying to obtain a specific NodeID for false information distribution. The attack may be crucial for PoS operation but is mitigated through the distribution of PKG between active PoS nodes after the genesis period. Therefore, a group of PoS nodes is required to provide a new one with its secret key similarly to voting procedure and session key generation.

Timejacking attack [97] targets at interaction with the system counter. In the proposed system, it could be targeted at slowing down the system operation by either malicious LPoS or PoA nodes. In the case of LPoS, the system operation may be affected if the node is reporting to the system that transactions are discarded, but it will result in the loss of credibility and a lower probability to receive new transactions for distribution between PoAs, i.e., decreasing the impact in the future. In the PoA case, the operation would be affected by precisely one cycle of the PoA verification since LPoS would re-select a group of PoAs if even one of them failed the verification.

Rare *Poison Block Attack* [98] is aimed at generating a false block with a timestamp ahead of time along with malicious miner, which should accept the block. The attack is mitigated by multi-layer architecture involving more nodes in the verification process, which includes the timestamp checks.

From the data privacy perspective, the system is designed to provide full transparency of the operation, i.e., k-block data contains the details about all involved nodes, their actions and transactions. The node ID (essentially, the node's public key) is not based on any real-world identifiable data. However, the field ''Data'' in each transaction (see already discusses k-block structure in Fig. 2) could be encrypted based on the application needs assuring the data privacy of the selected transaction, e.g., for smart contracts. Moreover, it provides an additional overlay layer, which is kept outside the scope of the basic system operation description.

Overall, the system was designed taking into consideration the majority of known attacks on similar blockchain systems while keeping the data transparency and cross-verification in mind.

VII. OPEN CHALLENGES AND FUTURE INVESTIGATIVE DIRECTIONS

Indeed, blockchain systems are incredibly complex compared to the centralized ones. However, our research reveals that many practical advantages can be yield with blockchain. Nevertheless, there are several challenges related to the integration of blockchain technology within smartphones and communication networks. Still, engaging future research and investigation directions remain to be analyzed. This section aims to bring the reader's attention to potential challenges that should be taken into consideration during the development of future distributed systems and redesigning currently existing ones.

A. BLOCKCHAIN SCALABILITY

Naturally, distributed systems tend to support a continually increasing number of devices. However, many existing projects faced numerous scalability issues, starting with the pioneering example of Bitcoin [82]. Overall, many modern blockchains suffer from high processing, storage, and transmission overheads, as well as limited scalability [99], [100]. Therefore, the possibility to avoid this bottleneck should be carefully taken into consideration during future steps of the blockchain evolution.

B. INTEROPERABILITY ASPECTS

One of the most important goals of blockchain from the smartphone utilization perspective is enabling interoperability between different device vendors. Presently, there may be at least two ways of said integration since straightforwards possibility is still far from possible.

The first option is interest from a big smartphone vendor (or OS system developer). Therefore, related protocols could be integrated as part of the market-available device significantly reducing the overheads coming from the integration phase.

The second option is related to additional pressure brought by the cellular operators willing to offload their expensive licensed resources. The software could be distributed automatically either with the SIM cards or directly through the operator's cloud. This, however, does not eliminate the need to convince OS developers to provide the essential functionality support.

C. POWER AND RESOURCE LIMITATIONS

Blockchain developers should carefully consider the limitations of the devices. Even though the devices are already capable of executing blockchain-related computations, they still may be developed in a very inefficient way, as shown in Section VI. Some works have already investigated the possibility of creating a specifically designed overlay network suitable for IoT blockchain-based networks [101] and proposing custom DLTs fulfilling the storage and computational limitations of said constrained devices [102].

Moreover, there are research works being actively developed in the field of Green Mining, focusing on resource-constrained devices in terms of more efficient resource allocation [29]. Another perspective direction for assisting smartphone-based systems by means of Edge Computing, especially for PoW concepts [41], e.g., by allowing for intelligent computational and storage offloading. Therefore, the devices would face a need for transmission vs. computational trade-off. Smartphones and other wearables thus would abandon meaningless puzzle solving by either effectively selecting to delegate the computation or use lighter solutions, like PoA.

D. SENSITIVE TRANSMISSION NETWORKS

Indeed, current networks utilized by smartphones could not be described as specifically designed for low latency

operation ones mainly due to the high level of heterogeneity of short- and long-range wireless technologies and standards. There is no option to analyze such complex and unpredictable networks in terms of packet propagation delay, which directly affects the fairness of the blockchain network operation. Many activities are presently happening in the field of Ultra-Reliable Low Latency Communications (URLLC), which is expected to be widely deployed as part of LTE release 14 [103].

Latency is a severe challenge that restricts blockchain applications in delay-sensitive scenarios [63]. In the blockchain-based networking services, the processes of generating and validating blocks are the primary sources of latency. Essentially, this is the cost of forming trust in an untrusted network. One key research challenge is to reduce latency by lowering the block confirmation time while satisfying the requisite system security and trust required by the users.

Nonetheless, the operation of the blockchain itself creates additional load on the communication networks [104], [105], which should also be carefully considered by both blockchain systems' developers and communication operators.

Conventional blockchains are built on the Internet, where block spreading is executed via wired networks and is often considered to be of little cost. However, in case operators would plan to integrate custom blockchain solution operation on the smartphones/Edge, the latency could be significantly reduced by keeping the traffic inside the LTE core whenever possible.

E. GENERAL SECURITY

Mostly, blockchain systems are designed with security, privacy, and anonymity in mind. However, the evolution of various blockchain systems has shown the community a variety of attacks that were growing with the development of the monetary component of market-available systems.

The number of attacks is vast, including but not limited to the following. Sybil attacks are depicted as a node presenting itself with multiple identities to other nodes [106], [107]. When the amount of identities is high enough, the attacker will become capable of taking over the network. Well known Distributed Denial of Service (DDoS) attack may be performed on critical nodes [108], e.g., PoSs in order to disrupt the network operation. Time-related attacks aim at manipulation with the blockchain internal counter values [109]. Those include poisoning [110] and time jacking attacks [111]. In the majority attack [112], [113], the intruder submits a transaction to the network which pays the merchant, while privately mining a blockchain fork where a double-spending transaction is included instead.

Communication-related attacks include Eclipse attack [93], which aims to take control of the communications of a single node and force it to accept false data. Partitioning attack splits the network into two or more disjoint groups. It can be done by taking control of particular points within the network that acts as the linking point between two groups followed by the delay attack, i.e., packet capture and push the packets to an isolated network segment.

F. GENERAL PRIVACY

Despite resisting to security threats, assurance of the data privacy plays a vital role in storing and transmitting the data without revealing sensitive information of the content originators [114], [115]. There are several common privacy issues. First, personal and sensitive information should remain confidential to prevent possible misuse even if stored or delivered by third parties [116]. The second privacy-related scenario arises in cloud operations such as data sharing, remote software updating, cloud computing, and storage [117]. In reality, it may not be possible for cloud services providers to be fully trusted, as cloud servers are expected to access personal data with explicit permission [118]. Herein, blockchain may provide a decentralized solution for exchanging data while ensuring privacy and integrity protection.

G. LEGAL ASPECTS

Despite various challenges arising from the financial segment [119], the utilization of blockchain and any resource-hungry applications on smartphones and wearable devices are bounded by two main legal aspects. On the one hand, some regions prohibit the operation with any cryptotokens [120], which may potentially slow down the integration of blockchain.

On the other hand, smartphone operating systems are commonly not open-source and aim at increasing the battery lifetime. It results in the policies that prohibit running any computationally hungry applications/services on their devices. The adoption by vendors is very far from being resolved, and this may significantly decrease the possibility for easy and on the fly integration.

H. USER ADOPTION

Besides technological, security, and legal aspects, the developers should carefully consider the user adoption side of the coin [121]. In particular, a significant portion of humanity does not yet trust virtual tokens as carrying any actual value. The need for proper education in terms of incentives and user involvement may still be very challenging. On the bright side, the ICT community is deeply correlated with distributed systems, and adding one more natural driver for the corresponding development may be met positively from their side.

VIII. CONCLUSION

The number of mobile devices is continuously growing, however, the computational power of those devices is vastly underused, mainly due to battery constraints. Numerous applications could use those FLOPs, and one of them is blockchain. The design of modern blockchain systems mainly relies on Proof-of-Work consent aiming to solve the computa-

tional puzzle, which is not suitable for smartphones but there are a few exceptions.

This paper outlined the main applications of blockchain technology for smartphones and wearable devices stepping aside from conventional cryptocurrency perspective comparing existing market-available systems. Next, a set of protocols coupling together Proof-of-Work, Proof-of-Stake, and Proof-of-Activity blockchain strategies was proposed aiming to involve mobile devices in the new block generation process. The protocol is already implemented in a real-life distributed test network involving more than 2,500 mobile nodes around the globe.

The developed system operation was compared with other similar approaches and concluded that it has a shallow impact (5%) on user experienced battery consumption compared to regular device operation and other systems (up to 40%) keeping the system secure and transparent privacy-wise. After that, the main challenges of blockchain adoption from both user and regulatory perspectives were highlighted.

The future directions and the main mobile blockchain challenges related to the integration of blockchain-based solutions on smartphones conclude the paper.

ACKNOWLEDGMENT

The authors would like to acknowledge Enecuum community support in the testing of the developed system. For the research, the infrastructure of the SIX Center was used.

This paper is an extended version of work by Zhidanov, K., Bezzateev, S., Afanasyeva, A., Sayfullin, M., Vanurin, S., Bardinova, Y. and Ometov, A. ''Blockchain Technology for Smartphones and Constrained IoT Devices: A Future Perspective and Implementation.'' In Proceedings of the 21st Conference on Business Informatics (CBI), Vol. 2, pp. 20-27, 2019. IEEE.

REFERENCES

[1] Cisco, ''Global mobile data traffic forecast 2017–2022,'' Cisco, San Jose, CA, USA, White Paper, 2019.

[2] S. Hiremath, G. Yang, and K. Mankodiya, ''Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare,'' in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare (MOBIHEALTH)*, 2014, pp. 304–307.

[3] X. Wang, Xuan Zha, Wei Ni, Ren Ping Liu, Y Jay Guo, Xinxin Niu, and Kangfeng Zheng, ''Survey on blockchain for Internet of Things,'' *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.

[4] A. Ometov, ''Social, private, and trusted wearable technology under Cloud-aided intermittent wireless connectivity,'' Ph.D. dissertation, Dept. Electron. Commun. Eng., Tampere Univ. Technol., Tampere, Finland, 2018.

[5] Y. Wang, R. Chen, and D.-C. Wang, ''A survey of Mobile Cloud Computing applications: Perspectives and challenges,'' *Wireless Pers. Commun.*, vol. 80, no. 4, pp. 1607–1623, 2015.

[6] C. R. Merkle, ''Method of providing digital signatures,'' U.S. Patent 4 309 569 A, Sep. 5, 1979.

[7] A. Hari and T. Lakshman, ''The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet,'' in *Proc. 15th ACM Workshop Hot Topics Netw.*, 2016, pp. 204–210.

[8] F. Hawlitschek, B. Notheisen, and T. Teubner, ''The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy,'' *Electron. Commerce Res. Appl.*, vol. 29, pp. 50–63, May 2018.

[9] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, ''Blockchain—The gateway to trust-free cryptographic transactions,'' in *Proc. 24th Eur. Conf. Inf. Syst. (ECIS)*. Springer, 2016, pp. 1–14.

[10] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, ''Challenges of Multi-Factor Authentication for securing advanced IoT applications,'' *IEEE Netw.*, vol. 33, no. 2, pp. 82–88, Mar. 2019.

[11] C. Osborne. (Oct. 2019). *Spending on Wearable Technology to Surge to $52 Billion by 2020: Gartner*. [Online]. Available: http://www.intel.de/content/www/de/de/do-it-yourself/edison.html

[12] Statista, Inc. (Oct. 2019). *Number of Smartphone Users Worldwide from 2016 to 2021*. [Online]. Available: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

[13] (2019). *Experts Exchange, Processing Power Compared*. [Online]. Available: https://pages.experts-exchange.com/processing-power-compared

[14] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, ''An overview on smart contracts: Challenges, advances and platforms,'' *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020.

[15] R. Pirmagomedov, A. Ometov, D. Moltchanov, X. Lu, R. Kovalchukov, E. Olshannikova, S. Andreev, Y. Koucheryavy, and M. Dohler, ''Applying blockchain technology for user incentivization in mmWave-based mesh networks,'' *IEEE Access*, vol. 8, pp. 50983–50994, Mar. 2020.

[16] J. Huang, L. Kong, H.-N. Dai, W. Ding, L. Cheng, G. Chen, X. Jin, and P. Zeng, ''Blockchain based mobile crowd sensing in industrial systems,'' *IEEE Trans. Ind. Informat.*, early access, Jan. 2020, doi: 10.1109/TII.2019.2963728.

[17] D. Frey, M. X. Makkes, P.-L. Roman, F. Taïani, and S. Voulgaris, ''Bringing Secure Bitcoin Transactions to Your Smartphone,'' in *Proc. 15th Int. Workshop Adapt. Reflective Middleware*, 2016, p. 3.

[18] D. Loghin, G. Chen, T. T. A. Dinh, B. C. Ooi, and Y. M. Teo, ''Blockchain goes green? An analysis of blockchain on low-power nodes,'' 2019, *arXiv:1905.06520*. [Online]. Available: http://arxiv.org/abs/1905.06520

[19] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, ''A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling,'' *ACM Comput. Surveys*, vol. 53, no. 1, pp. 1–32, Feb. 2020.

[20] D. Rhodes. (May 2018). *Is Mobile Mining Profitable?* [Online]. Available: https://coincentral.com/is-mobile-mining-profitable/

[21] S. King and S. Nadal, ''PPcoin: Peer-to-Peer crypto-currency with Proof-of-Stake,'' 2012.

[22] A. Kiayias, A. Russell, B. David, and R. Oliynykov, ''Ouroboros: A provably secure proof-of-stake blockchain protocol,'' in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2017, pp. 357–388.

[23] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, ''Proof of Activity: Extending bitcoin's Proof of Work via Proof of Stake [extended abstract]y,'' *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, Dec. 2014.

[24] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev, J. Hajny, J. Niutanen, and Y. Koucheryavy, ''Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices,'' in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2016, pp. 1–6.

[25] K. Zhidanov, S. Bezzateev, A. Afanasyeva, M. Sayfullin, S. Vanurin, Y. Bardinova, and A. Ometov, ''Blockchain technology for smartphones and constrained IoT devices: A future perspective and implementation,'' in *Proc. IEEE 21st Conf. Bus. Informat. (CBI)*, vol. 2, Jul. 2019, pp. 20–27.

[26] T.-H. Kim, ''A study of digital currency cryptography for business marketing and finance security,'' *Asia–Pacific J. Multimedia Services Convergent Art, Humanities, Sociol.*, vol. 6, no. 1, pp. 365–376, Jan. 2016.

[27] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, ''Blockchain technology: Beyond bitcoin,'' *Appl. Innov.*, vol. 2, nos. 6–10, p. 71, 2016.

[28] J. Fiaidhi, S. Mohammed, and S. Mohammed, ''EDI with blockchain as an enabler for extreme automation,'' *IT Prof.*, vol. 20, no. 4, pp. 66–72, Jul. 2018.

[29] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, ''Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm,'' *IEEE Access*, vol. 7, pp. 9714–9723, 2019.

[30] A. Galanopoulos, F. Foukalas, and T. A. Tsiftsis, "Efficient coexistence of LTE with WiFi in the licensed and unlicensed spectrum aggregation," *IEEE Trans. Cognit. Commun. Netw.*, vol. 2, no. 2, pp. 129–140, Jun. 2016.

[31] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis, "The 5G-enabled tactile Internet: Applications, requirements, and architecture," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6.

[32] E. Markova, I. Gudkova, A. Ometov, I. Dzantiev, S. Andreev, Y. Koucheryavy, and K. Samouylov, "Flexible spectrum management in a smart city within Licensed Shared Access framework," *IEEE Access*, vol. 5, pp. 22252–22261, 2017.

[33] H.-J. Kwon, J. Jeon, A. Bhorkar, Q. Ye, H. Harada, Y. Jiang, L. Liu, S. Nagata, B. L. Ng, T. Novlan, J. Oh, and W. Yi, "Licensed-assisted access to unlicensed spectrum in LTE release 13," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 201–207, Feb. 2017.

[34] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[35] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, "Blockchain-based infrastructure sharing in 5G small cell networks," in *Proc. 14th Int. Conf. Netw. Service Manage. (CNSM)*, 2018, pp. 313–317.

[36] J. Backman, S. Yrjölä, K. Valtanen, and O. Mämmelä, "Blockchain network slice broker in 5G: Slice leasing in factory of the future use case," in *Proc. Internet Things Bus. Models, Users, Netw.*, Nov. 2017, pp. 1–8.

[37] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Commun.*, vol. 12, no. 5, pp. 527–532, Mar. 2018.

[38] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Inf. Syst.*, vol. 2018, pp. 1–10, Aug. 2018.

[39] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for Cloud exchange: A survey," *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106526.

[40] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Joint computation offloading and content caching for wireless blockchain networks," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 517–522.

[41] 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.

[42] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T.-H. Kim, "Proof-of-Work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, Aug. 2019.

[43] L. Jiang, S. Xie, S. Maharjan, and Y. Zhang, "Joint transaction relaying and block verification optimization for blockchain empowered D2D communication," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 828–841, Jan. 2020.

[44] A. Rao Kabbinale, E. Dimogerontakis, M. Selimi, A. Ali, L. Navarro, A. Sathiaseelan, and J. Crowcroft, "Blockchain for economically sustainable wireless mesh networks," 2018, *arXiv:1811.04078*. [Online]. Available: http://arxiv.org/abs/1811.04078

[45] Y. Yao and T. Xie, "A blockchain based authentication mechanism in wireless local area network," in *Proc. Int. Conf. Comput., Netw., Commun. Inf. Syst. (CNCI)*, 2019, pp. 227–231.

[46] T. Sanda and H. Inaba, "Proposal of new authentication method in Wi-Fi access using bitcoin 2.0," in *Proc. IEEE 5th Global Conf. Consum. Electron.*, Oct. 2016, pp. 1–5.

[47] Y. Niu, L. Wei, C. Zhang, J. Liu, and Y. Fang, "An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the bitcoin blockchain," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Oct. 2017, pp. 1–6.

[48] C. Li, Q. Wu, H. Li, and J. Liu, "Trustroam: A novel blockchain-based cross-domain authentication scheme for Wi-Fi access," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.* Cham, Switzerland: Springer, 2019, pp. 149–161.

[49] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, and J. S. Deogun, "Identity management using blockchain for cognitive cellular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[50] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Comput. Sci. Rev.*, vol. 30, pp. 80–86, Nov. 2018.

[51] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber., Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1336–1342.

[52] J. Leimgruber, A. Meier, and J. Backus, "Bloom protocol: Decentralized credit scoring powered by Ethereum and IPFS," Early Community Draft Version 0.3 Subject to Change, Longwood, FL, USA, White Paper, Jan. 2018.

[53] S. Homayoun, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A blockchain-based framework for detecting malicious mobile applications in app stores," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2019, pp. 1–4.

[54] W. Meng, W. Li, and L. Zhu, "Enhancing medical smartphone networks via blockchain-based trust management against insider attacks," *IEEE Trans. Eng. Manag.*, early access, Jul. 2019, doi: 10.1109/TEM.2019.2921736.

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

[56] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[57] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," 2017, *arXiv:1706.01730*. [Online]. Available: http://arxiv.org/abs/1706.01730

[58] Z. Gao, L. Xu, G. Turner, B. Patel, N. Diallo, L. Chen, and W. Shi, "Blockchain-based identity management with mobile device," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst. (CryBlock)*, 2018, pp. 66–70.

[59] P. Garcia, "Biometrics on the blockchain," *Biometric Technol. Today*, vol. 2018, no. 5, pp. 5–7, May 2018.

[60] X. Xu, Q. Liu, X. Zhang, J. Zhang, L. Qi, and W. Dou, "A blockchain-powered crowdsourcing method with privacy preservation in mobile environment," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1407–1419, Dec. 2019.

[61] W. Feng and Z. Yan, "MCS-chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain," *Future Gener. Comput. Syst.*, vol. 95, pp. 649–666, Jun. 2019.

[62] E. S. Miguel, R. Timmerman, S. Mosquera, E. Dimogerontakis, F. Freitag, and L. Navarro, "Blockchain-enabled participatory incentives for crowdsourced mesh networks," in *Proc. Int. Conf. Econ. Grids, Clouds, Syst., Services*. Cham, Switzerland: Springer, 2019, pp. 178–187.

[63] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing consensus propagation in Proof-of-Stake based consortium blockchain networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 157–160, Feb. 2019.

[64] C. Chakrabarti and S. Basu, "A blockchain based incentive scheme for post disaster opportunistic communication over DTN," in *Proc. 20th Int. Conf. Distrib. Comput. Netw.*, Jan. 2019, pp. 385–388.

[65] M. Attaran and A. Gunasekaran, "Blockchain for Gaming," in *Applications of Blockchain Technology in Business*. Cham, Switzerland: Springer, 2019, pp. 85–88.

[66] H. Y. Yuen, F. Wu, W. Cai, H. C. B. Chan, Q. Yan, and V. C. M. Leung, "Proof-of-play: A novel consensus model for blockchain-based Peer-to-Peer gaming system," in *Proc. ACM Int. Symp. Blockchain Secure Crit. Infrastruct.*, 2019, pp. 19–28.

[67] G. Agrawal. (Jul. 2018). *How Blockchain Is Completely Disrupting The Gaming Industry*. [Online]. Available: https://medium.com/coinmonks/how-blockchain-is-completely-disrupting-the-gaming-industry

[68] T. Min, H. Wang, Y. Guo, and W. Cai, "Blockchain games: A survey," 2019, *arXiv:1906.05558*. [Online]. Available: http://arxiv.org/abs/1906.05558

[69] N. Chalaemwongwan and W. Kurutach, "State of the art and challenges facing consensus protocols on blockchain," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, 2018, pp. 957–962.

[70] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of Proof of Work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 3–16.

[71] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 2567–2572.

[72] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-Work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.* Zürich, Switzerland: Springer, 2015, pp. 112–125.
[73] A Medium Corporation. (Nov. 2018). *MIB Mining Across the World*. [Online]. Available: https://medium.com/mib-coin/mib-mining-across-the-world-9ae1259a6db8
[74] MIB Team. (Jul. 2018). *Mobile Integrated Blockchain Coin—MIB White Paper*. [Online]. Available: https://drive.google.com/file/d/1V0J0kHNkpMDcPCZEGVtZhbAA_UAsfijl/view
[75] Constantine Pappas. (Aug. 2019). *Enablement for Personal Permission-less Blockchains on Proof-of-Transaction, Mobile Devices and Inter-Planetary File System*. [Online]. Available: https://www.taucoin.io/whitePaper/tauwp2.0.pdf
[76] Electroneum Ltd. (2019). *A Revolutionary New Digital Payments Ecosystem*. [Online]. Available: https://community.electroneum.com
[77] Phoneum. (Dec. 2019). *Mobile Only Cryptocurrency: White Paper*. [Online]. Available: https://neironix.io/documents/whitepaper/28f5089f13bdfd5a9cb1a1951bfc8040.pdf
[78] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1984, pp. 47–53.
[79] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Proc. IMA Int. Conf. Cryptogr. Coding*. Berlin, Germany: Springer, 2001, pp. 360–363.
[80] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[81] A. Ometov, K. Zhidanov, S. Bezzateev, R. Florea, S. Andreev, and Y. Koucheryavy, "Securing network-assisted direct communication: The case of unreliable cellular connectivity," in *Proc. IEEE 14th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Aug. 2015, pp. 826–833.
[82] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.
[83] A. Shevchenko, *Monero Penalizes GPU and ASIC Mining with RandomX Upgrade*. in *Decentral Media Crypto Briefing*. Dec. 2019.
[84] E. Heilman and T. Dryja, "IOTA vulnerability report: Cryptanalysis of the CURL hash function enabling practical signature forgery attacks on the IOTA Cryptocurrency [OL]," MIT Media Lab, Cambridge, MA, USA, Tech. Rep., Sep. 2017.
[85] A. B. Kahn, "Topological sorting of large networks," *Commun. ACM*, vol. 5, no. 11, pp. 558–562, Nov. 1962.
[86] H. Jang and J. Lee, "An empirical study on modeling and prediction of bitcoin prices with Bayesian neural networks based on blockchain information," *IEEE Access*, vol. 6, pp. 5427–5437, 2018.
[87] ENECUUM HK Limited. (2019). *Dynamic Mobile Blockchain With Enecuum: A Synergy of Proof-of-Work, Proof-of-Activity, and Proof-of-Stake*. [Online]. Available: https://new.enecuum.com/files/tp_en.pdf
[88] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2002, pp. 548–566.
[89] Y. Bardinova. (Apr. 2020). *A Dataset of Existing Mobile Blockchain Measurements Executed on Smartphones*. [Online]. Available: https://github.com/yuliabardinova/BCMes
[90] X. Chen, N. Ding, A. Jindal, Y. C. Hu, M. Gupta, and R. Vannithamby, "Smartphone energy drain in the wild: Analysis and implications," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 43, no. 1, pp. 151–164, Jun. 2015.
[91] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, pp. 1–32, Jun. 2015.
[92] J. Daniel, G. Ducatel, and T. Dimitrakos, "Mitigating blockchain attack," U.S. Patent 9 807 106, Oct. 31, 2017.
[93] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Mar. 2016, pp. 305–320.
[94] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Washington, DC, USA: Springer, 2016, pp. 515–532.
[95] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's Peer-to-Peer network," in *Proc. 24th USENIX Secur. Symp. (USENIX Secur.)*, 2015, pp. 129–144.
[96] S. Zhang and J.-H. Lee, "Double-spending with a Sybil attack in the bitcoin decentralized network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5715–5722, Oct. 2019.
[97] D. Meshkov, A. Chepurnoy, and M. Jansen, "Short paper: Revisiting difficulty control for blockchain systems," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Cham, Switzerland: Springer, 2017, pp. 429–436.
[98] J. Kume, M. Abe, and T. Okamoto, "Lottery protocol for cryptocurrency," in *Proc. SCIS*, 2015, pp. 1–5.
[99] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
[100] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.
[101] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. 2nd Int. Conf. Internet-Things Design Implement.*, Apr. 2017, pp. 173–178.
[102] F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera, "Overcoming limits of blockchain for IoT applications," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, 2017, p. 26.
[103] C. Hoymann, D. Astely, M. Stattin, G. Wikstrom, J.-F. Cheng, A. Hoglund, M. Frenne, R. Blasco, J. Huschke, and F. Gunnarsson, "LTE release 14 outlook," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 44–49, Jun. 2016.
[104] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, "Analysis of the communication traffic for blockchain synchronization of IoT devices," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–7.
[105] M. Scherer, "Performance and scalability of blockchain networks and smart contracts," Dept. Comput. Sci., Umeå Univ., Sweden, Umeå, Tech. Rep. 136470, 2017.
[106] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, Jun. 2020.
[107] S. Kim, Y. Kwon, and S. Cho, "A survey of scalability solutions on blockchain," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2018, pp. 1204–1207.
[108] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, Jan. 2020.
[109] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," in *Proc. IEEE Middle East North Afr. Commun. Conf. (MENACOMM)*, Apr. 2018, pp. 1–6.
[110] K. Sarpatwar, R. Vaculin, H. Min, G. Su, T. Heath, G. Ganapavarapu, and D. Dillenberger, "Towards enabling trusted artificial intelligence via blockchain," in *Policy-Based Autonomic Data Governance*. Cham, Switzerland: Springer, 2019, pp. 137–153.
[111] C. A. Vyas and M. Lunagaria, "Security concerns and issues for bitcoin," in *Proc. Nat. Conf. Workshop Bioinf. Comput. Biol., NCWBCB*, 2014.
[112] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and A. Mohaisen, "Exploring the attack surface of blockchain: A systematic overview," 2019, *arXiv:1904.03487*. [Online]. Available: http://arxiv.org/abs/1904.03487
[113] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2016, pp. 467–468.
[114] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.
[115] C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018.
[116] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
[117] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477.
[118] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommun. Policy*, vol. 41, no. 10, pp. 1027–1038, Nov. 2017.
[119] E. Saiedi, A. Broström, and F. Ruiz, "Global drivers of cryptocurrency infrastructure adoption," in *Proc. Small Bus. Econ.*, 2020, pp. 1–54.
[120] G. Prayogo, "Bitcoin, regulation and the importance of national legal reform," *Asian J. Law Jurisprudence*, vol. 1, no. 1, pp. 1–9, 2018.
[121] F. Shahzad, G. Xiu, J. Wang, and M. Shahbaz, "An empirical investigation on the adoption of cryptocurrencies among the people of mainland China," *Technol. Soc.*, vol. 55, pp. 33–40, Nov. 2018.

ALEKSANDR OMETOV (Member, IEEE) received the D.Sc. (Tech.) and M.Sc. degrees from Tampere University of Technology (TUT), Finland, in 2018 and 2016, respectively. He is currently a Postdoctoral Research Fellow with Tampere University (TAU), Finland. He is also working on H2020 MCSA ITN/EJD A-WEAR Project. His research interests are wireless communications, information security, blockchain technology, and wearable applications.

YULIA BARDINOVA received the B.Sc. degree in information security from the Saint Petersburg State University of Telecommunications, in 2020. She is currently pursuing the M.Sc. degree with Tampere University (TAU), Finland. She is also a QA Engineer with Enecuum. Her research interests are distributed systems and protocol development.

ALEXANDRA AFANASYEVA received the B.S. and M.S. degrees in information systems from the Saint Petersburg State University of aerospace instrumentation (SUAI), in 2001 and 2003, respectively. Since 2003, she has been on the faculty of Information Systems and Information Security, SUAI. She is currently with ITMO University. She participated in and managed joint Research and Development projects of SUAI with Samsung, Intel, and EMC, in the field of information security and optimization of resource allocation algorithms in data storage systems. Her research interests include coding theory, cryptography, and distributed storage systems.

PAVEL MASEK (Member, IEEE) received the M.Sc. and Ph.D. degrees in electrical engineering from the Faculty of Electrical Engineering and Communication, Brno University of Technology (BUT), Czech Republic, in 2013 and 2017, respectively. He is currently a Researcher with the Department of Telecommunications, BUT. He is also co-supervising the WISLAB Research Group, where his current research interests include various aspects in the area of heterogeneous wireless communication networks and systems, the Internet of Things, and Industry 4.0-Driven Research Projects. He has coauthored more than 90 research works on a variety of networking-related topics in internationally recognized venues, including those published in the *IEEE Communications Magazine*, as well as several technology products.

KONSTANTIN ZHIDANOV received the Engineering degree from the State University of Airspace Instrumentation (SUAI), Russia, in 2006. He is currently the Tech Lead of Enecuum Limited. His major research interests are information security, blockchain technology, and information theory.

SERGEY VANURIN received the degree in applied mathematics as a specialist from Saint-Petersburg State University, in 2009, and the master's degree from Saint-Petersburg Institute for Informatics and Automation, Russian Academy of Sciences. He worked as a Software Engineer and an IT Project Manager with Banking, UAV, and DLT fields. He is currently the Project Manager with Enecuum Ltd. As a Haskell programming language enthusiast, he is currently teaching a course of Haskell with ITMO University. His research interest is category theory.

MIKHAIL SAYFULLIN received the Specialist degree from the Bonch-Bruevich Saint-Petersburg State University of Telecommunications, in 2002. He is currently the CEO of Enecuum Limited. His research interests include blockchain technology, distributed applications, and protocols development.

VIKTORIIA SHUBINA (Graduate Student Member, IEEE) received the double M.Sc. degree in engineering from the University of Applied Sciences Technikum Wien, Austria, and the M.Sc. degree in business informatics from National Research University Higher School of Economics, Russia, in 2019. She is currently a Postdoctoral Researcher with TAU, as part of H2020 MCSA ITN/EJD A-WEAR project. Her most research interests are data privacy, location privacy, indoor and outdoor positioning, and wearable technologies.

MIKHAIL KOMAROV (Senior Member, IEEE) is currently a Professor with the Department of Innovations and Business in IT, School of Business Informatics, Faculty of Business and Management, National Research University Higher School of Economics. He is also a specialist in wireless data transmission and IT. He is the Vice-Chair of the Special Interest Group on IoT at the Internet Society.

SERGEY BEZZATEEV (Member, IEEE) received the Ph.D. and Dr.Sc. degrees, in 1987 and 2011, respectively. From1993 to 1995, he was a Researcher with the Nagoya University, Japan. Since 1995, he was an Associate Professor with the Department of Information Technologies and Information Security, SUAI. From 2004 till 2007, he was a Project Leader with the Joint Laboratory Samsung-SUAI on Information Security in Wireless Networks. In 2017, he became a Professor with the Secure Information Technologies School, ITMO University. He is currently a Professor and the Head of the Department of Technologies of Information Security, SUAI. He is also a Professor with ITMO University. His main research interests include coding theory and cryptography.