Privacy-Aware Blockchain Innovation for 6G: Challenges and Opportunities

Tri Nguyen[‡], Ngoc Tran[*], Lauri Loven[‡], Juha Partala[§], M-Tahar Kechadi[*†], Susanna Pirttikangas[‡]
[‡§]{firstname.lastname}@oulu.fi, [*†]{firstname.lastname}@ucd.ie
[‡]Center for Ubiquitous Computing, University of Oulu, Finland
[†]School of Computer Science, University College Dublin, Ireland
[*]Insight Centre for Data Analytics, University College Dublin, Ireland
[§]Center for Machine Vision and Signal Analysis, University of Oulu, Finland

***Abstract*—6G wireless networks improve on 5G by further increasing reliability, speeding up the networks and increasing the available bandwidth. These evolutionary enhancements, together with a number of revolutionary improvements such as high-precision 3D localization, ultra-high reliability and extreme mobility, introduce a new generation of 6G-native applications. Such application can be based on, for example, distributed, ubiquitous Artificial Intelligence (AI) and ultra-reliable, low-latency Internet of Things (IoT).**

Along with the enhanced connectivity and novel applications, privacy and security of the networks and the applications must be ensured. Distributed ledger technologies such as blockchain provide one solution for application security and privacy, but introduce their own set of security and privacy risks. In this work, we discuss the opportunities and challenges related to blockchain usage in 6G, and map out possible directions for overtaking the challenges.

***Index Terms*—5G, 6G, blockchain, privacy, security.**

I. Introduction

One of the goals of the fifth generation wireless networks (5G) is to introduce the Internet of Everything (IoE), which relies on enhanced broadband access for machine-type communications [1], [2]. However, with 5G networks now being introduced into wider usage, this goal is far from being realized. For example, high-frequency millimeter wave connections and support for heterogeneous IoT services are not currently available at the scale required for novel applications such as ubiquitous virtual/augmented/extended reality (XR) or connected autonomous systems [2].

Sixth generation wireless networks (6G) aim to satisfy the requirements of IoE applications and support the growth of technological trends such as ubiquitous, distributed artificial intelligence (AI) [2], [3]. 6G is expected to introduce for example ultra-high reliability, ultra-low latency, and high-accuracy inter-device synchronicity [4]. Indeed, 6G's Key Performance Indicators (KPI) are expected to significantly improve on those of 5G (Table I).

Distributed ledger technologies, in particular blockchain, can assist in realizing advanced IoE applications for 6G. Blockchain builds trust between networked applications, voiding the need for trusted intermediaries. Blockchain does this by building a distributed database, or ledger, which collects the state changes of all participants as data blocks. These blocks, managed by the participants themselves, form a chronological chain, with each block b_{x+1} linked to the previous one b_x in a chronological order by their hash values. To remain in order, the chain of blocks – or blockchain – must be immutable, transparent and traceable [5]. Transparency, in particular, requires that the state changes of all participants are visible to everyone in network. As such, blockchain sacrifices privacy to build trust. Further, due to the complex protocols maintaining the integrity of the distributed blocks, blockchain introduces new attack surfaces for an adversary. 6G further exacerbates these security and privacy risks as high throughput and fast connectivity improve the potential for rapid and complex attacks.

In this paper, we present the following contributions, all related to the combination of 6G and blockchain: 1) We present opportunities, collecting a number of potential blockchain-based 6G use cases suggested in literature; 2) we present challenges, in particular as related to the security and privacy of such applications; and 3) we outline possible solutions to the challenges.

The rest of the paper is organized as follows: Section II outlines privacy in 5G and 6G. Opportunities, challenges and their possible solutions are detailed in Sections III, IV and V. Finally, Section VI sums up the paper.

II. 5G to 6G: Evolution of Security and Privacy

5G intends to connect as many users as possible, moving from rate-centric enhanced mobile broadband (eMBB) services to URLLC [2] and introducing heterogeneous networks for device-to-device (D2D) communications [6]. 5G will provide services such as millimeter-wave (mm-wave) communication, massive multiple-input, multiple-output (MIMO) links and ultra-dense deployment of radio access points for applications based on wide mobile broadband communication [7]. Further, 5G can boost the growth of mobile cloud computing, edge computing, software defined networking (SDN) and network functions virtualization (NFV) [1].

Since 5G connects users, services and applications, security and privacy is of paramount importance. However, data management in 5G is more complicated than in earlier wireless networks, as connected devices may be more diverse in type, their number is expected to grow very high, and the data they generate is both more voluminous and more distributed

TABLE I
KPI COMPARISON BETWEEN 5G AND 6G [2], [7], [11]

KPI	5G	6G
Data rate	0.1Gb/s-20Gb/s	1Gb/s-1Tb/s
Reliability (error rate)	$<10^{-5}$	$<10^{-9}$
Density	10^6/km^2	10^7/km^2
Localization Precision	10cm in 2D	1cm in 3D
Mobility	500km/h	1000km/h
Traffic Capacity	10Mb/s/m^2	$<$10Gb/s/m^3
Latency	1-5ms	10-100ns

logically and geographically. As a result, data access control becomes much more complicated, and a number of novel attack surfaces and data leakage points are revealed [8], [9].

5G security and privacy have been studied from a number of viewpoints [10]. Indeed, the better the coverage and performance of wireless networks, the worse in severity and volume the security threats. For 5G, connecting potentially billions of devices and users and providing critical infrastructure for a number of application verticals (e.g. IoT, cloud RAN, business services, smart phones), security threats (e.g. on network infrastructure) are more dangerous, and the probability of attacks is higher than in earlier wireless generations. Further, along with 5G smart services, ever more sensitive user data such as identity or location is processed and transmitted in the network, increasing the probability of privacy leaks.

6G, with much-improved KPIs and new services will further exacerbate these privacy and security problems [2]. Indeed, early 6G visions emphasize security, privacy and reliability as crucial requirements for industry and high-end users, and discuss embedding an ubiquitous trust model into the networks [4]. Such a trust model would need to coordinate between network entities and users to collect evidence of misbehaviour and support actions including indirect reciprocity and non-repudiation.

III. OPPORTUNITIES

Blockchain is as a transparent, append-only and chronological chain of data blocks, managed by a number of participants to prevent falsification. Prior to adding to the blockchain, a new data block has to be verified and agreed upon by a majority of the participants. For the verification process, those participants require the witness of the previous data. As a result, blockchain is widely regarded as a state-of-the-art trust technology for enabling the next generation wireless networks [1], [2], [4], [6], but it sacrifices privacy to gain transparency for the verification process.

Blockchain technology supports decentralized applications and proliferation of trust, as witnessed by cryptocurriencies, supply chains and reputation systems. Further, blockchains are by design decentralized networks which avoid single points failure. As such, 6G services can use blockchain to guarantee trust and security for example for access control, authentication, distributed key management and audit evidence [12]. As a result, the expected services and high performance of 6G networks further enhance the growth of blockchain-based applications, while the use of blockchain technology in those services is expected to boost their growth, leading to a positive feedback loop.

Further, the following 6G use cases (technologies and services) in particular stand to benefit from blockchain-based proliferation of trust and security:

Edge computing: Cloud computing provides computational capacity for resource-constrained user devices, allowing the offloading of heavy computations to remote servers. Edge computing mitigates the long latencies, heavy burden on backhaul networks, and lack of privacy related to cloud offloading [6], [13]. However, since offloaded computations may involve sensitive information, security and trustworthiness of the computational resources need to be ensured [14], [15]. Blockchain technology can build trust between the user devices and the edge servers, ensuring the integrity of both the offloaded computation and the remote resources [6].

Spectrum sharing: Spectrum management allows multiple categories of users to safely share the same frequency bands, making more efficient use of the radio spectrum available for communication. In spectrum sharing, a primary user deals out leases for other users to use her spectrum. Blockchain technology can enhance spectrum sharing security by preventing tampering of the lease records [5], [6], [11], [16]. However, maintaining user privacy in such a solution is an open problem.

D2D content caching: In 6G networks with ubiquitous, reliable and fast connectivity, high-volume content may be cached on user devices. Such device-based content caching decreases the traffic on both access and backhaul links and enhances quality of service [6]. Since content may contain sensitive information, cache requesters need to trust the cache providers [17]. Blockchain can ensure trust between requesters and providers, at the cost of some privacy.

Energy trading: Exchanging energy through energy trading markets, smart devices (e.g., smart vehicles with surplus electricity) may leak private information such as their location [18]. Blockchain can mitigate trust between market participants, again at the cost of some privacy.

Federated learning: Blockchain can provide a decentralization framework for federated learning, voiding the need for centralized control on learning and inference in edge-based distributed machine learning [19].

Network architecture: An intelligent, distributed mobile network infrastructure, such as one based on open-source wireless networks [20], requires an open market where users, spectrum owners, infrastructure owners, and Internet Service Provider owners can freely participate to exchange their resources [21]. Blockchain can provide such a marketplace, at the can cost of some privacy of the participants.

Network virtualization: Wireless network virtualization increases the capacity and energy efficiency of networks, providing for the growing needs of IoT data. Blockchain can help in non-repudiation and immutability in the management of virtual network slices [22].

Interference management: Blockchain can be used for optimal interference management, avoiding intermediaries when a node pays to become active [23].

IV. Challenges

A. Security risks

Blockchain implementations introduce a number of risks [24], which are carried over to 6G if blockchain is adopted as a core technology. The three main attack types against blockchain are as follows:

Majority vulnerability: Blockchain builds trust without the need for third parties by requiring a consensus of the majority of participants. Accordingly, attackers may try to gain control of the entire system by controlling at least 51% of the participants. In Bitcoin, for example, this means an attacker requires 51% of the computing power of the entire network's computation to control the Bitcoin network [24].

Double-spending aims to break the integrity of the blockchain's distributed ledger. In particular, it refers to attacks against cryptocurrencies where a user completes two distinct transactions from the same amount of currency [24].

Transaction privacy leakage: Blockchain relies in part on transparent transactions. Hence, user privacy is jeopardised in blockchain-based systems.

Further, other attacks against blockchain include selfish mining [25] and sybil attacks [26]. Selfish mining is a way to obtain more reward and waste honest miner resources in a Proof-of-Work consensus mechanism, whereas in a sybil attack, a user creates multiple blockchain accounts in an effort to manipulate it. Finally, blockchain-based smart contracts have greatly expanded blockchain applicability by allowing software-defined contracts between participants as transactions [27]. However, as flexible as smart contracts are, they introduce a number of new attack surfaces in the system. The three main attack surfaces for blockchain-based smart contracts are vulnerabilities in the blockchain itself, in the smart contract, and in the virtual machine executing code [28].

B. Scalability

Due to its decentralized nature, Bitcoin does require a lot of bandwidth, computing and storage to ensure the integrity of the ledger. Blockchain protocol, for example, requires forced delays and a high number of messages being passed and broadcasted between the participants. The performance of a blockchain-based application, especially in terms of latency and scalability, may thus be restrictive [29]. For example, Bitcoin has a maximum throughput of 7 transactions/sec, a latency of 10 min for a confirmed block, and a bootstrap time[1] of 4 days [30]. In stark contrast, Visa credit system promises up to 56k transactions/sec [30]. The computational and communication overhead introduced by blockhchain may prove a challenge for the billions of smart devices and their massive transaction requirements expected for 5G and beyond.

C. Quantum Computing

Commercial quantum computation is expected to be available already in the near future [31]. In particular, we can expect a certain level of quantum computation to be reality during the lifetime of 6G networks. In 6G blockchain, the advent of large-scale quantum computing means that several contemporary public-key primitives need to be replaced with quantum-resistant ones. Due to Shor's quantum polynomial-time integer factoring algorithm [32], factoring and discrete logarithm based cryptographic primitives, such as the elliptic curve signature algorithm (ECDSA), are rendered vulnerable once large-scale quantum computation becomes a reality. Post-quantum resistant alternatives need to replace these security mechanisms in the post-quantum world. Fortunately, in the light of current knowledge, symmetric primitives, such as cryptographic hash functions used in block generation, are not similarly affected.

[1]The time it takes for a new node to download the full blockchain.

V. Solution outlines

A. Incentive Strategies for Blockchain-based Risks

Since the early days of blockchain technology, adversarial behavior has been curbed with stakes and incentives [33]. In particular, to encourage participants to follow the Bitcoin protocols, participation in the Bitcoin network requires Bitcoin currency which is subsequently rewarded to well-behaved participants. A transaction fee can prevent DDOS attacks, mitigate the majority risk and reduce the expected reward of other attacks as conducting them becomes too expensive [34].

B. Cryptographic Algorithms for Privacy Risks

Blockchains are by default transparent, disclosing potentially private information to all participants. Multiple solutions address this risk, including ring signatures, zero-knowledge arguments and coin mixing [35].

Ring signatures are digital signatures generated for a group of blockchain participants. Using the ring signature, group members remains anonymous [36]. In more detail, a ring signature for a blockchain message guarantees that an anonymous member of the group has endorsed that message. Monero[2], a privacy-centred cryptocurrency, uses ring signatures to ensure the privacy of the transactions of its participants.

Zero-knowledge arguments and proofs are methods that allow honest parties convince other participants of the validity of a statement without disclosing any additional information [37]. The first application of zero knowledge arguments in blockchain technology is by Zcash[3], another privacy-protecting cryptocurrency. As a downside, the complexity of the approval of transactions increases [35].

Coin mixers obfuscate the addresses of coin owners to ensure their anonymity. The traditional mix involves a centralized server which shuffles information and transfers coins. However, this solution introduces a centralized component into an otherwise decentralized system. There is also a decentralized coin mixer called CoinShuffle, where each participant attempts to generate an output address before permuting all received addresses and forwarding the information to other participants. Once all participants have their own output addresses, they are

[2]https://www.getmonero.org/

[3]https://z.cash/

broadcasted to the entire network [38]. As a downside, computational burden and bandwidth usage are further increased.

C. Scalability

Scaling up a blockchain must consider multiple abstraction layers in blockchain architecture, as detailed below [30]:

Network layer transmits messages related to transactions and system control. Scaling requires that each node fetches only unprocessed transactions for newly mined blocks; this will effectively halve the number of required transactions. Further, the network plane topology could be redesigned to be more effective, dedicated high-speed relay networks put in place[4], the broadcast protocols improved, and incentivization schemes designed for transaction dissemination [30].

Consensus layer ensures all participants have an identical view on the transactions, their ordering and agreement. Proof-of-Work, the the consensus method using in Bitcoin and involving heavy use of the computing resources of participants, introduces a three-way trade-off among bandwidth, consensus speed and security. Several potential solutions exist for either changing the consensus mechanism (to, e.g., Proof-of-Stake [39] or Practical Byzantine Fault Tolerance [30]), sharding, or side chains. Sharding splits the consensus task among sets of nodes ("shards"), aiming to improve consensus speed when an operation is performed within one shard. However, the performance of operations between shards degrades, and additional layers of shard consensus add to system complexity and operational overhead. Sidechains, on the other hand, split the whole blockchain into smaller pieces, coordinated by a main chain. Again, coordination and operations between sidechains are costly.

Storage layer is the ledger - a global memory which stores the state changes of the participants, resulting from *write* and *read* (and possibly *delete*) operations mutually agreed upon by all participants on the consensus plane, as well as smart contracts or other state-related entities. Possible methods to improve storage layer performance include storage sharding and Distributed Hash Tables [30].

View layer, the term borrowed from databases, contains the current state of all participants and smart contracts, compacted from the full history of state changes stored on the ledger on the storage layer. A number of methods exists for creating views, either by the blockchain participants (e.g. the consensus nodes) themselves, or off-chain, with cryptographic proofs ensuring view integrity. The off-chain methods remove computational burden from the participants, and thus improve system efficiency [30].

Side layer considers off-the-chain operations, where the operations are prepared and authenticated with blockchain operations, but the final execution (e.g. transfer of Bitcoins) is routed along channels not within the blockchain. The protocols for off-chain transactions are and active area of research, with the Lightning Network and full duplex channels proposals for possible implementations. The off-chain channels involve the same trade-offs as blockchain itself, with centralized solutions simplifying the protocols but inducing loss of privacy [30].

[4]See e.g. https://github.com/TheBlueMatt/RelayNode

6G is expected to drastically increase the performance and services of the wireless network, resulting in a dramatic growth of ubiquitous computing resources. The network layer of blockchain benefits directly from the performance boost as well as from the expected increased configurability of the wireless network; the computing resources, on the other hand could be used as blockchain or off-chain nodes, supporting the high processing costs related to chain and storage sharding, sidechains, as well as other computing-heavy proposed improvements.

D. Quantum Computing

Even though large-scale quantum computation renders factoring and discrete logarithm based cryptographic schemes insecure, not all security primitives are vulnerable. Contemporary symmetric-key primitives, such as block ciphers and hash functions, remain secure also in the quantum computation model. It suffices that the length of the security parameter is doubled due to Grover's algorithm [40]. Public-key primitives have to be replaced with quantum-resistant ones. Discrete logarithm based digital signature schemes need to be replaced with quantum-resistant ones based on, for example, lattice-based cryptography used in BLISS signatures [41] or schemes using supersingular elliptic curves [42].

Quantum computation itself can also address the issue of security. For example, Quantum Key Distribution (QKD) enables two parties to share secret keys with security provided by the laws of quantum physics. Another effective solution to avoid quantum risks is a formation of a quantum blockchain [43], [44]. The quantum blockchain [43] consists of two layers including QKD and transmitting messages based on Toeplitz hashing [45] to replace traditional digital signature and hashing function, in turn. Meanwhile, [44] is more detail to describe Greenberger–Horne–Zeilinger states [46] as subsystems and a quantum network in which there are a QKD protocol and states of the quantum blockchain.

VI. Conclusion

In this paper, we reviewed the use of blockchain technology in combination of future 6G technologies especially from the viewpoint of security and privacy. We listed the oppostunities and challenges involved, and outlined a number of possible solutions to the challanges. In conclusion, blockchain supports the growth of 6G by mitigating a number security threats related to, for example, spectrum and content sharing. However, blockchain usage is not without challenges, especially in relation to user privacy. Care must be taken to address those challenges while maintaining the performance and security of the future wireless networks.

Acknowledgment

This work is supported by TrustedMaaS and B-TEA projects by the Infotech institute of the University of Oulu, Academy of Finland 6Genesis Flagship (grant 318927), the MEC-AI

project of the Future Makers program, the Science Foundation Ireland (grant 12/RC/2289_P2), and by the grant for mr. Lovén on EdgeAI research by the Tauno Tönning foundation.

REFERENCES

[1] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[2] W. Saad, M. Bennis, and M. Chen, "A vision of 6g wireless systems: Applications, trends, technologies, and open research problems," *arXiv preprint arXiv:1902.10265*, 2019.

[3] L. Lovén, T. Leppänen, E. Peltonen, J. Partala, E. Harjula, P. Porambage, M. Ylianttila, and J. Riekki, "Edgeai: A vision for distributed, edge-native artificial intelligence in future 6g networks," in *The 1st 6G Wireless Summit*, (Levi, Finland), pp. 1–2, 2019.

[4] B. Aazhang, P. Ahokangas, L. Lovén, *et al.*, *Key drivers and research challenges for 6G ubiquitous wireless intelligence (white paper)*. Oulu, Finland: 6G Flagship, University of Oulu, 1 ed., 2019.

[5] Y.-C. Liang, "Blockchain for dynamic spectrum management," in *Dynamic Spectrum Management*, pp. 121–146, Springer, 2020.

[6] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," *IEEE Network*, vol. 33, no. 3, pp. 10–17, 2019.

[7] E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, and C. Dehos, "6g: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 42–50, 2019.

[8] G. SinghBhathal and A. Singh, "Big data: Hadoop framework vulnerabilities, security issues and attacks," *Array (Elsevier)*, vol. 1-2, 2019.

[9] P. Centonze, "Security and privacy frameworks for access control big data systems," *Tech Science Press CMC*, vol. 59, no. 2, pp. 361–374, 2019.

[10] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements and future directions," *IEEE Communications Surveys & Tutorials*, 2019.

[11] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6g wireless communications: Vision and potential techniques," *IEEE Network*, vol. 33, no. 4, pp. 70–75, 2019.

[12] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5g and beyond networks: A state of the art survey," *arXiv preprint arXiv:1912.05062*, 2019.

[13] T. Lähderanta, T. Leppänen, L. Ruha, L. Lovén, E. Harjula, M. Ylianttila, J. Riekki, and M. J. Sillanpää, "Edge server placement with capacitated location allocation," *arXiv preprint arXiv:1907.07349*, 2019.

[14] J. Partala, L. Lovén, E. Peltonen, P. Porambage, M. Ylianttila, and T. Seppänen, "EdgeAI: A vision for privacy-preserving machine learning on the edge," in *The 10th Nordic Workshop on System and Network Optimization for Wireless (SNOW)*, (Ruka, Finland), 2019.

[15] P. Porambage, T. Kumar, M. Liyanage, J. Partala, L. Lovén, M. Ylianttila, and T. Seppänen, "Sec-EdgeAI: AI for edge security Vs security for edge AI," in *The 1st 6G Wireless Summit*, (Levi, Finland), 2019.

[16] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *ieee vehicular technology magazine*, vol. 13, no. 1, pp. 32–39, 2018.

[17] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, 2018.

[18] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[19] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained on-device federated learning," *IEEE Communications Letters*, 2019.

[20] J. Haavisto, M. Arif, L. Lovén, T. Leppänen, and J. Riekki, "Open-source rans in practice: an over-the-air deployment for 5g mec," *arXiv preprint arXiv:1905.03883*, 2019.

[21] T. Maksymyuk, J. Gazda, L. Han, and M. Jo, "Blockchain-based intelligent network management for 5g and beyond," in *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, pp. 36–39, IEEE, 2019.

[22] D. B. Rawat and A. Alshaikhi, "Leveraging distributed blockchain-based scheme for wireless network virtualization with security and qos constraints," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 332–336, IEEE, 2018.

[23] A. El Gamal and H. El Gamal, "A single coin monetary mechanism for distributed cooperative interference management," *IEEE Wireless Communications Letters*, vol. 8, no. 3, pp. 757–760, 2019.

[24] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[25] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM*, vol. 61, no. 7, pp. 95–102, 2018.

[26] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*, pp. 251–260, Springer, 2002.

[27] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[28] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *International Conference on Principles of Security and Trust*, pp. 164–186, Springer, 2017.

[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] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, *et al.*, "On scaling decentralized blockchains," in *International Conference on Financial Cryptography and Data Security*, pp. 106–125, Springer, 2016.

[31] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, pp. 51 – 71, 2019.

[32] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[33] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[34] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A survey on blockchain: a game theoretical perspective," *IEEE Access*, vol. 7, pp. 47615–47643, 2019.

[35] K. Ikeda, "Security and privacy of blockchain and quantum computation," in *Advances in Computers*, vol. 111, pp. 199–228, Elsevier, 2018.

[36] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 552–565, Springer, 2001.

[37] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on computing*, vol. 18, no. 1, pp. 186–208, 1989.

[38] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in *European Symposium on Research in Computer Security*, pp. 345–364, Springer, 2014.

[39] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, 2012.

[40] L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proc. of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, 1996.

[41] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal gaussians," in *Advances in Cryptology – CRYPTO 2013* (R. Canetti and J. A. Garay, eds.), (Berlin, Heidelberg), pp. 40–56, Springer Berlin Heidelberg, 2013.

[42] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *Post-Quantum Cryptography* (B.-Y. Yang, ed.), (Berlin, Heidelberg), pp. 19–34, Springer Berlin Heidelberg, 2011.

[43] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. Lvovsky, and A. Fedorov, "Quantum-secured blockchain," *Quantum Science and Technology*, vol. 3, no. 3, p. 035004, 2018.

[44] D. Rajan and M. Visser, "Quantum blockchain using entanglement in time," *Quantum Reports*, vol. 1, no. 1, pp. 3–11, 2019.

[45] H. Krawczyk, "Lfsr-based hashing and authentication," in *Annual International Cryptology Conference*, pp. 129–139, Springer, 1994.

[46] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond bell's theorem," in *Bell's theorem, quantum theory and conceptions of the universe*, pp. 69–72, Springer, 1989.