A Taxonomy of the Risks and Challenges of Embracing Blockchain Smart Contracts in Facilitating Renewable Electricity Transactions

Olakunle Alao
School of Electrical and Electronic Engineering
University College Dublin
Dublin, Ireland
olakunle.alao@ucdconnect.ie

Paul Cuffe
School of Electrical and Electronic Engineering
University College Dublin
Dublin, Ireland
paul.cuffe@ucd.ie

***Abstract*—Environmental imperatives and global energy supply crisis are driving interests in the renewable electricity industry. Yet, the revenue risks of renewable generators make it challenging for them to attract finance from traditional investors. Several mechanisms have been proposed to minimize these risks but have their limitations. Blockchain smart contract arrangements have emerged as a new marketplace, addressing the shortcomings of these traditional electricity hedging mechanisms. However, they have their peculiar challenges, potentially impeding their mainstream adoption in the renewable electricity industry. Hence, this paper develops a novel taxonomy of the risks and challenges of embracing blockchain smart contracts in facilitating renewable electricity transactions. Examining these issues indicates that the adoption of blockchain smart contracts in the renewable energy industry can be facilitated by cooperation and partnerships between technology developers and researchers, renewable energy companies, as well as governments.**

***Keywords*—Blockchain, smart contract, renewable electricity, decentralized finance, electricity market**

I. Introduction

ENVIRONMENTAL imperatives and global energy supply crisis are necessitating increased renewable electricity investment. However, the revenue risks of renewable generators make it difficult for them to attract investments at favorable rates and advantageous terms from conventionally risk-averse financial institutions [1]. Several traditional techniques have been proposed to hedge these revenue risks. Still, they have their limitations such as low flexibility, high hedging cost, and liquidity, credit, margining, basis, third-party, legal, and process risks, better discussed in [1]–[4]. Blockchain smart contract arrangements have emerged as a game-changing method for addressing the risks introduced by traditional hedging mechanisms [2]–[7].

A blockchain is a growing series of interconnected blocks, as in Fig. 1, recording transactions between participants decentrally, consistently, transparently, and immutably [8], [9]. The chain of blocks and transactions within each block are linked through a cryptographic hash, a function that maps arbitrary-sized data to fixed-size values. In popular blockchains like Bitcoin, transactions per block result in a single *Merkle Root*, a hash trail of all transactions in the block. The block hash is derived when the block information: the *Previous Block Hash*, *Nonce*, an arbitrary number used to vary the difficulty level of the *Proof-of-Work* (PoW) problem, and Merkle Root are passed through a hash function [6]. Blocks are then appended to each other by miners via the previous block's hash. Miners attempt to add blocks to the blockchain after competing to solve a difficult and computationally- and energy-intensive mathematical puzzle called PoW problem. The successful miner thereafter disseminates the transactions in the block to other miners on the network. The block is accepted and added to the canonical blockchain after over 50% of miners accept the veracity of the transactions [2].

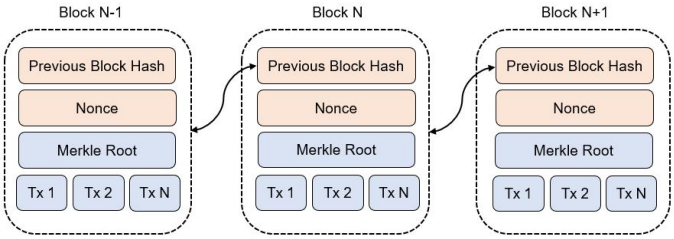

Fig. 1. Structure of a typical blockchain network, such as Bitcoin

Smart contracts run on blockchains, allowing pre-programmed autonomous actions amongst network parties while maintaining all the features of such decentralized network, including immutability, security, etc [10]. The most popular blockchain-based smart contract is Ethereum. Its smart contracts reside in the Ethereum Virtual Machine (EVM), isolating them from the underlying blockchain to prevent the executed code from interfering with other activities [8].

The workings of Ethereum smart contracts are conceptualized in Fig. 2, where the mining operation of the underlying blockchain is excluded [11]. Here, the smart contract is designed and deployed by an independent entity, *Smart contract deployer*. Two parties, a *Renewable generator* and its *Contracting counterparty* vet the terms and conditions (i.e., the source code) of the smart contract and agree to enter the arrangement. This smart contract is compiled into machine-level byte code, where each byte signifies an operation, and

This publication has been funded by the Sustainable Energy Authority of Ireland under the SEAI Research, Development & Demonstration Funding Programme 2018, grant number 18/RDD/373 and additional funding provided by the UCD Energy Institute.

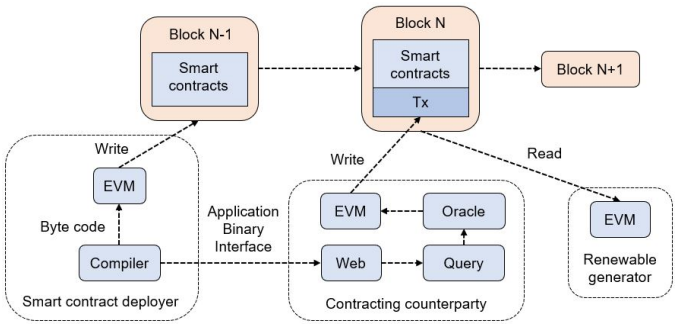

Fig. 2. Demonstration of a typical smart contract mechanism between a renewable generator and its contracting counterparty

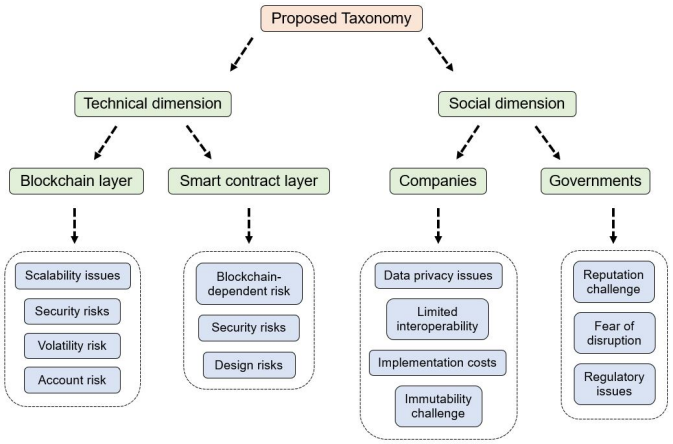

Fig. 3. Proposed taxonomy of the risks and challenges of embracing blockchain smart contracts in facilitating renewable electricity transactions

then committed to the blockchain (i.e., *Block N-1*) in the form of a transaction by *EVM 1*. Consider a scenario where the arrangement requires negotiating a particular term, such as the electricity strike price. We can say a counterparty like an electricity supplier first submits an arbitrary price to the generator through the web interface. Then, the *EVM 2* queries the data from the web, embeds it into transaction *Tx*, and deploys it on the blockchain (i.e., *Block N*). If the generator later intends to check the price proposed by the supplier, it must *Read* the data via *EVM 3*. This action is recorded in *Block N+1*.

II. Research Motivation and Proposed Taxonomy

While blockchain-based smart contracts hedge the risks of traditional renewable electricity arrangements, they introduce new risks and challenges to participants, potentially impeding their mainstream adoption in the industry. Therefore, this paper classifies, describes, and analyzes these impediments to embracing blockchain smart contracts in facilitating renewable electricity transactions under two dimensions, *Technical* and *Social*, as shown in Fig. 3.

III. Technical Dimension

This section focuses on the technological risks and challenges posed by blockchains and smart contracts, inhibiting their adoption in the renewable electricity industry.

A. Blockchain layer

The risks at the blockchain layer refer to those issues specific to the blockchain technology itself. Central to a successful blockchain is the simultaneous balancing of the so-called trilemma: decentralization, security, and scalability [12]. Decentralization, allowing parties to act independently and transparently without the need for a central coordinating entity, can be considered as the core motivation of blockchain networks [13]. Blockchains typically achieve decentralization by consensus, where transactions are immutably ratified by a group of nodes rather than a single individual. Still, the majority of nodes could conspire to attack the network, exposing the system to security risks. Consensus requirements also moderate transaction speed, as such transactions require multiple confirmations before being accepted by the network [12], [13]. The rest of this section details the risks associated with balancing the blockchain trilemma.

1) Scalability issues: Scalability is essential for the mainstream adoption of blockchain smart contracts in diverse industries. Blockchain transactions are executed in chronological order; a rule of computation executes after another rule completes. Hence, transaction completions are generally slow and could be expensive, as parallel processing is not supported [2]. Particularly, the most common consensus mechanism, the PoW, underpinning leading blockchains such as Bitcoin and Ethereum, requires a long time to conclude due to the lengthy computationally- and energy-intensive process involved in adding blocks to the canonical chain [7]. Newer consensus mechanisms such as Proof of Stake (PoS) and Proof of Authority (PoA), etc., guarantee faster transaction completion and lower energy use and transaction fees [6]. However, researchers continue to argue that some of the new consensus mechanisms (e.g., the PoA) go against decentralization and are not as secure (e.g., PoA and PoS) as the legacy PoW [10].

2) Security risks: These risks comprise the blockchain-specific security vulnerabilities of renewable generators transacting on such networks. Notably, these threats are dependent on the blockchain type and underlying consensus mechanism. While several mechanisms have been explored to hedge these security risks, such as in [6], [14], [15], the threat they introduce remains significant. The rest of this section will describe some of these risks, particularly the prevalent threats, under three categories: blockchain network, transaction verification, and selfish mining attacks.

a) Blockchain network attacks: Some of the primary blockchain network attacks include Distributed Denial of Service (DDoS) and Sybil attacks [6], [14]. In DDoS attacks, malicious actors attempt to overload the network by consuming all its processing resources with redundant requests, allowing the disconnection of the network from its digital wallets, etc. [6]. In Sybil attacks, hackers intend to take over the network by allotting numerous identifiers to the same node, resulting in an unbalanced network control that can cause hijacking of the system [14].

b) Transaction verification attacks: Again, electricity transactions on the blockchain will only be ratified after a majority of the mining nodes agree; until then, transactions remain unverified. The window before transactions are verified

creates an attack vector for malicious actors. Double-spending is a widespread attack exploiting such windows, where hackers use the same coins or tokens in multiple transactions [15]. One of the principal security vulnerabilities in the transaction verification category is the 51% attack, which is possible when a malicious party assumes control of the majority of the network to create an alternative chain that eventually takes precedence over the original existing chain [10], [15]. A classic example is the attacks on the Ethereum Classic (ETC), a modified version of the Ethereum blockchain, in 2020. Here, around US$9 million worth of cryptocurrency was stolen by hackers [16].

c) Mining nodes attacks: Mining nodes attacks are perpetrated by selfish miners intending to control mining pools by exploiting vulnerabilities in the blockchain consensus mechanism [16]. Here, miners withhold mined blocks from the public blockchain to create an alternate chain, continuously mined to advance past the public blockchain. If the malicious miners' blockchain progresses ahead of the honest blockchain, they can introduce their newest block to the original network. Since the network assumes the longest chain as the *true* blockchain, the malicious miners' blockchain would overwrite the original blockchain [15]. Selfish mining attacks are effectively committed to obtain unearned rewards or waste the computing power of honest miners. Such attacks can cripple the blockchain, as fair and balanced mining is central to the integrity and endurance of the network.

3) Volatility risks: The *volatility* of cryptocurrencies could inhibit the mainstream adoption of blockchain technologies in the renewable electricity industry. For instance, in traditional renewable energy finance, relatively stable fiat currencies such as the US$ are utilized as the mode of exchange for participants. Employing the blockchain's native currency as a replacement could expose investors to volatility risk, negating their primary aim of stable and predictable returns on investments [3]. Similarly, electricity markets typically settle and clear using such fiat currencies, disincentivizing the adoption of the volatile blockchain native currencies [2]. The volatility issue has now been resolved, given the introduction of stablecoins that can be integrated into blockchain-based smart contracts, discussed in Section III-B1a.

4) Account risks: Account risks refer to the challenges of handling and managing blockchain-based digital wallets. Renewable generators transacting on blockchain networks possess two cryptographic keys comprising numeric or alphanumeric characters, a secret private key, and a public key, which can be distributed with other participants in the network [10]. Essentially, the identification of participants is enabled by public keys, while private keys authorize access to wallets. Therefore, if renewable generators happen to lose their private keys, the funds associated with them become irrecoverable. Similarly, unintended fund transfer to a wrong public key (address) implies permanent loss of funds [3].

B. Smart contract layer

The risks at the smart contract layer refer to the several challenges associated with creating, deploying, executing, and completing smart contracts on blockchain networks [6]. Before delving into some of these specific challenges, we note that smart contracts are developed on the blockchain layer and, as such, naturally possess the risks inherent in the underlying blockchain network (i.e., *Blockchain-dependent risk*) [8]. For instance, an electricity derivative smart contract deployed on an Ethereum blockchain, presently based on the computationally- and energy-intensive PoW consensus mechanism, could result in potentially high transaction costs for renewable generators. While there is a wide range of smart contract challenges that have been identified in [6], [8], [11], [14], the rest of this section describes the most popular issues in the context of renewable electricity transactions.

1) Security Risks: Security threats, with potentially devastating outcomes, including significant financial losses [14], persist as the leading smart contract-related risk to the adoption of blockchain technologies in the renewable energy industry [3]. Many security challenges have been identified in several studies in [2], [3], [6], [8], [11], [14]. The significance of security issues is furthered because smart contracts, once deployed on the blockchain, cannot be altered or revised. Likewise, there is limited support for debugging faults in smart contracts since their development is a burgeoning area, and most source codes are unique to the specific vendor [8]. The DAO hack in the Ethereum blockchain represents the most significant example of the devastating outcome that security loopholes in smart contract codes can introduce to blockchain network participants. Furthermore, the integration of other applications to the smart contract, can expose renewable electricity generators to security risks [2], [3], described as follows.

a) Hedging volatility risks: Stablecoin services incorporated into smart contracts can hedge the cryptocurrency volatility risks of renewable generators transacting on blockchain networks [2]–[4]. Today, three types of stablecoins have been proposed: centralized "I Owe You" IOU, crypto-collateralized, and non-collateralized stablecoins. Centralized IOU stablecoins are backed by fiat currencies, while crypto-collateralized stablecoins are underwritten by cryptocurrencies. Non-collateralized stablecoins are not backed by any financial asset. Instead, they are algorithmically programmed on-chain to autonomously manage demand and supply, similar to a central bank [17]. Of these proposals, the crypto-collateralized and non-collateralized stablecoins are considered as *true* blockchain stablecoins, with the former now becoming the most popular and mature stablecoin in the blockchain ecosystem [18]. However, integrating stablecoin services to blockchain-based smart contracts introduces an attack vector and thus potentially exposes renewable generators transacting on such platforms to security risks.

b) Oracle Problem: Smart contracts have no knowledge of *real world* events. As such, entities known as oracles are typically employed to relay real-world happenings to the smart contract, to enforce specific pre-defined actions [7]. In blockchain derivative transactions, smart contracts might require a *human* or *software* oracle to provide the varying electricity spot price published by the Market Operator, to invoke payments to or from renewable electricity generators [2]. Human oracles are trusted participants delegated to provide off-chain data to the smart contract while software oracles feed smart contracts with data obtained from the web [19]. Similarly, renewable energy project finance arrangement could require a *hardware* oracle, recording end-users electricity

consumption data and feeding it to the smart contract for settlement purposes [3]. Hardware oracles supply smart contracts with data obtained directly from the physical world, e.g., through meters or sensors [3], [19]. Overall, a malicious oracle could manipulate the real-world data stream to game the operation of the smart contract. Therefore, the oracle introduces a possible attack vector to the smart contract, regarded in the blockchain ecosystem as the *Oracle Problem*. Several solutions have been proposed to minimize the security risks posed by addressing the Oracle Problem [6]. Still, the security risk they pose persists.

2) Design risks: Design risk concern issues related to structuring and implementing the smart contract's *business logic*. These risks might also relate to business logic structural limitations that could cause unintended actions of the smart contract, such as *freezing*. Blockchain smart contracts for renewable electricity transactions are typically complex arrangements requiring sequential or simultaneous inputs from several moving parts [3]. For example, a smart contract design that does not sufficiently incentivize an action required to invoke a payout to a participant might suffer from freezing, whereby such actions might never be actualized. Design risks might also cover how computationally efficient the source code, implementing the business logic, is designed to run. Smart contracts facilitating renewable energy transactions have an added cost beyond ratifying the arrangement's transaction on the underlying blockchain network. This cost is primarily due to the computation power of implementing the smart contract's logic. In Ethereum, for example, smart contract transactions incur a fee called *gas* [2]. This fee is proportional to the length and complexity of the smart contract. Hence, inefficient source codes will result in elevated transaction costs for renewable generators.

IV. Social Dimension

The social dimension of the risks and challenges of employing blockchain smart contracts in facilitating renewable electricity transactions includes issues that do not explicitly result from the technical layer but society's perception and use of the technology. The remainder of this section will describe this social dimension via the lens of two entities: companies and governments.

A. Companies

The main concern for renewable energy companies to transact via blockchain smart contracts outside the risks of the technical dimensions are data privacy issues, immutability challenge, implementation costs, and limited interoperability. These challenges are discussed as follows.

1) Data privacy issues: Although data on blockchains are encrypted and anonymous, they are stored decentrally and persistently, introducing data privacy concerns. A party interested in deciphering the identity of transacting entities can create patterns and establish connections between addresses to make informed conclusions about the actual identities behind them [20]. Data privacy issues could discourage renewable generators from embracing blockchain platforms. Here, they might intend to protect their trade secrets and other sensitive information to maintain a competitive advantage against other generators operating in the same electricity marketplace. Policies on electricity consumption data protection might also mean that renewable generators under a form of contract with these users are restricted from transacting on any platform that could jeopardize their confidentiality [10].

2) Limited interoperability: Interoperability includes the ability of different blockchains and smart contracts within those networks to seamlessly synchronize and interact with each other without the need for a central intermediary [11], [15]. As more renewable generators transition to blockchains, they are likely to adopt separate network versions, with varying governance rules, consensus models, programming languages, etc. These distinct blockchains do not function alike, and there is currently no universal standard to enable them to connect with each other [15]. Interoperability issues also persist for smart contracts within the same blockchain network, given that there are presently no standards for these contracts to collaborate with each other. One of the main potential benefits of blockchain smart contracts identified for renewable generators is lower risk management cost due to *liquidity*, the availability of numerous parties willing to take the opposite position to the generators in an arrangement [3]. With limited interoperability, renewable generators might be unable to harness the *ecosystem effect*, where for instance, revenues collected on behalf of investors by one smart contract can autonomously connect to another smart contract and be employed to achieve a different purpose.

3) Implementation costs: Incorporating blockchain systems into the existing operation of renewable generators might prove to be cost-prohibitive. Generators embarking on such transitions must entirely restructure their previous system, involving new technology infrastructure and highly skilled professionals, requiring a significant amount of time and resources. There is also the fear that transitioning to blockchain might result in data loss or corruption [10]. Further, in some niche use cases, blockchains may presently be less cost-effective than existing solutions [11]. For instance, simply relaying electricity consumption data from smart meters to conventional databases are likely to be faster and cheaper than using blockchains. However, traditional databases cannot guarantee the enhanced security and data integrity provided by blockchains. As blockchains become widespread, these generators are likely to become better aware of the benefits afforded by the technology.

4) Immutability challenge: While irrevocability is one of the benefits of blockchains, renewable generators could be reluctant to transition to such solutions because transaction immutability might have commercial implications [11]. For instance, an underlying agreement between a renewable generator and its contracting party could become void or need revision due to applicable statutory provisions, including disputes with consumer protection laws and regulations or formal requirements.

B. Governments

The main concern for governments to support the traction of renewable energy transactions on blockchain smart contracts, outside the risks of the technical dimension, are reputation challenge and regulatory issues.

1) Reputation challenge: Many governments are reluctant to facilitate blockchain adoption because of its supposed connection to the *crypto* world, known to comprise malicious actors, such as criminals, hackers, and fraudsters. Governments must accept and support blockchains for mainstream adoption of the technology in the renewable electricity industry. While government bans on blockchains can not entirely eradicate their use, they can stifle the proliferation of the technology [11]. Moreover, unlike in the financial sector, renewable generators usually have physical assets that are already directly regulated or controlled in some ways by policies, laws, regulations by the government. Hence, they are likely not to attempt to circumvent government policies and rules, inhibiting their adoption of the technology.

2) Fear of disruption: Governments' acceptance of blockchains, which are essential for their proliferation, might also be connected to their *fear of disruption*. Cryptocurrencies are often regarded as a rival to the conventional monetary systems, potentially eroding the central banks' authority over money supply [7]. In the electricity sector, regulators could be concerned that blockchain-based grids, especially at the wholesale physical electricity market level, would entirely destabilize the existing legacy infrastructure system, mainly controlled by the government [10]. Further, blockchain project finance mechanisms for the massive roll-out of microgrid-tied independent renewable generators [3] can lead to grid-defection that can hurt the sustainability and utilization of government-owned electricity generation and transmission assets. These social issues can effectively delay blockchain adoption in the renewable electricity sector.

3) Regulatory issues: Even where blockchains are legal, most governments' limited regulatory capabilities stifle the proliferation of the technology. While blockchains are not controlled by any entity, they require regulatory support for mainstream adoption and increased ecosystem investment [10], [11]. The absence of regulatory clarity is also one of the significant impediments to blockchain adoption in diverse industries. Furthermore, it is currently unclear how governments might encourage the proliferation of blockchains while fulfilling their mandate to protect consumers and markets. These regulatory issues must be resolved by governments worldwide for blockchains to kick off fully.

V. Conclusion

This paper has categorized the risks and challenges of embracing blockchain smart contracts in the renewable energy industry. A description and analysis of these impediments indicate that despite the ominous task of addressing such issues, cooperation and partnerships between developers and researchers, renewable energy companies, and governments can produce significant and sustainable impacts. Technology developers and researchers must continue to investigate these threats, analyze them, and objectively quantify their implications to the community. Renewable energy companies must fully understand the strengths and weaknesses of the technology to create viable, sustainable, and interoperable business models that benefit society. Lastly, governments must create an enabling policy and regulatory environment to support the diffusion of the technology.

References

[1] J. Hull, *Options, Futures and Other Derivatives*. 2012, ISBN: 0135009944. DOI: 10.1007/978-1-4419-9230-7_2.

[2] O. Alao and P. Cuffe, "Towards a blockchain contract-for-difference financial instrument for hedging renewable electricity transactions," in *2020 6th IEEE International Energy Conference (ENERGYCon)*, 2020, pp. 858–863. DOI: 10.1109/ENERGYCon48941.2020.9236436.

[3] O. Alao and P. Cuffe, "Structuring special purpose vehicles for financing renewable generators on a blockchain marketplace," *IEEE Transactions on Industry Applications*, pp. 1–1, 2021. DOI: 10.1109/TIA.2021.3135252.

[4] M. Shamsi and P. Cuffe, "A prediction market trading strategy to hedge financial risks of wind power producers in electricity markets," *IEEE Transactions on Power Systems*, 2021.

[5] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2901–2925, 2021, ISSN: 19366450. DOI: 10.1007/s12083-021-01127-0.

[6] Z. Zheng, S. Xie, H. N. Dai, *et al.*, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020, ISSN: 0167739X. DOI: 10.1016/j.future.2019.12.019. arXiv: 1912.10370.

[7] A. de Villiers and P. Cuffe, "A three-tier framework for understanding disruption trajectories for blockchain in the electricity industry," *IEEE Access*, vol. 8, pp. 65 670–65 682, 2020.

[8] W. Zou, D. Lo, P. S. Kochhar, *et al.*, "Smart Contract Development: Challenges and Opportunities," *IEEE Transactions on Software Engineering*, vol. 47, no. 10, pp. 2084–2106, 2021, ISSN: 19393520. DOI: 10.1109/TSE.2019.2942301.

[9] V. Y. Kemmoe, W. Stone, J. Kim, D. Kim, and J. Son, "Recent Advances in Smart Contracts: A Technical Overview and State of the Art," *IEEE Access*, vol. 8, pp. 117 782–117 801, 2020, ISSN: 21693536. DOI: 10.1109/ACCESS.2020.3005020.

[10] M. Andoni et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019, ISSN: 18790690. DOI: 10.1016/j.rser.2018.10.014.

[11] Y. Hu, M. Liyanage, A. Mansoor, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "Blockchain-based Smart Contracts - Applications and Challenges," pp. 1–26, 2018, ISSN: 2331-8422. arXiv: 1810.04699.

[12] F. Mogavero, I. Visconti, A. Vitaletti, and M. Zecchini, "The Blockchain Quadrilemma: When Also Computational Effectiveness Matters," *Proceedings - IEEE Symposium on Computers and Communications*, vol. 2021-Septe, 2021, ISSN: 15301346. DOI: 10.1109/ISCC53001.2021.9631511.

[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[14] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare, and M. Ylianttila, "Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research," *IEEE Access*, vol. 9, pp. 87 643–87 662, 2021, ISSN: 21693536. DOI: 10.1109/ACCESS.2021.3068178.

[15] S. Singh, A. S. Sanwar Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13 938–13 959, 2021, ISSN: 21693536. DOI: 10.1109/ACCESS.2021.3051602.

[16] Apriorit, *Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology*, 2020.

[17] Y. Dong, "Elasticoin : Low-Volatility Cryptocurrency with Proofs of Sequential Work," *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 205–209, 2019. DOI: 10.1109/BLOC.2019.8751402.

[18] Maker Team, "The Dai Stablecoin System," Tech. Rep., 2017.

[19] H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, "Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges," *IEEE Access*, vol. 8, no. January, pp. 85 675–85 685, 2020, ISSN: 21693536. DOI: 10.1109/ACCESS.2020.2992698.

[20] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, ISSN: 21693536. DOI: 10.1109/ACCESS.2016.2566339.