Energy Reports 7 (2021) 8277–8286

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Energy-efficient blockchain implementation for Cognitive Wireless Communication Networks (CWCNs)

Premkumar Chithaluru [a], Fadi Al-Turjman [b], Thompson Stephan [c,*], Manoj Kumar [d,*], Leonardo Mostarda [e]

[a] Associate Professor, Department of CSE, School of Computing, KL University, Vaddeswaram, Andhra Pradesh 522502, India
[b] Artificial Intelligence Engineering Department, Research Centre for AI and IoT, Near East University, Nicosia, Mersin 10, Turkey
[c] Department of Computer Science and Engineering, Faculty of Engineering and Technology, M. S. Ramaiah University of Applied Sciences, Bengaluru, Karnataka, India
[d] School of Computer Science, University of Petroleum & Energy Studies (UPES), Bidoli, Dehradun, 248007, India
[e] Computer Science Division, University of Camerino, Camerino, Italy

ARTICLE INFO

Article history:
Received 29 April 2021
Received in revised form 26 July 2021
Accepted 29 July 2021
Available online 18 August 2021

Keywords:
CWCN
Energy efficiency
Blockchain
Proof of work
Computation time
Resource-constrained

ABSTRACT

Considering the computation resources available with sensor devices and the value and validity of Cognitive Wireless Communication Network (CWCN), traditional blockchain is not feasible for CWCN. Further, considering the security and privacy for CWCN that can directly impact human life (as in the case of ambient assisted living applications), blockchain provides a good solution for such applications, however, with some simplicity in the computation of Proof of Work (PoW). Therefore, the fourth objective solution comes up with a simplified energy-efficient blockchain implementation for CWCN that consumes less energy in computation time. The energy-hungry blockchain has been implemented on resource-constrained CWCN for ambient assisted living applications specialized for elderly care. The process includes a collection of physical environmental parameters on a single board computer-based CWCN. The implementation includes possible simplification in the most energy-consuming process, i.e., the mining process, which makes it energy efficient in computation time as energy consumption is a computation time factor.

1. Introduction

Banks, email service providers, and social networking networks protect the confidentiality and protection of our personal information. However, these neutral observers can be hacked, corrupted, or exploited at any time. It introduces the concepts of distributed consent and confidentiality. However, there is a need for someone who can verify, safeguard, and protect potential records.

The first decentralized virtual currency, Bitcoin, was introduced by Nakamoto (2009). This digital currency was based on cryptographic proof instead of authentication from a trusted third party. The most popular cryptocurrency, Bitcoin (in service since early 2009), drives the multi-million dollar market of anonymous transactions globally without a trusted third party's entanglement. The fluctuating value, expense, use, and legitimacy of cryptocurrency validates its interest in the analysis and business communities.

1.1. Bitcoin

For a bitcoin transaction between two communicating entities, all the transaction data is broadcasted anonymously to each participant in the network, whose responsibility is to validate the transactions. This validation includes a race among network participants for solving a cryptographic puzzle (named PoW) known as mining. The winner of this race is rewarded a few bitcoins or may charge a fee for solving the puzzle. The solution to the mining process is duly verified by all the participants before its addition as a transaction for a block in the blockchain.

Numerically, in January 2009, 50 bitcoins were awarded/generated as computation reward for solving PoW of 1 transaction block. With a limit of total of 21 million bitcoins to be generated by 2140, the rate of generation of coins is controlled by increasing the level of difficulty of PoW such that in addition to halving the reward every 2016 blocks, one new block generation takes approximately 10 min for the increasing amount of computational power (O'Dwyer and Malone, 2014). This implies

* Corresponding authors.
E-mail addresses: bharathkumar30@gmail.com (P. Chithaluru), fadi.alturjman@neu.edu.tr (F. Al-Turjman), thompsoncse@gmail.com (T. Stephan), wss.manojkumar@gmail.com (M. Kumar), leonardo.mostarda@unicam.it (L. Mostarda).

https://doi.org/10.1016/j.egyr.2021.07.136

that the difficulty level is changed approximately every 2 weeks (computation time for 2016 blocks for 10 min per block). Further, this is to be noted that after 2140, no new bitcoins can be generated i.e the reward for computing PoW shall be the transaction fees only.

1.2. Bitcoin energy consumption index

The bitcoin's energy footprint ranges from a small to medium-sized country. Bit-main, the largest fabricator of bitcoin mining machines has already warned us not to produce new coins due to its enormous carbon footprint (Das and Dutta, 2020).

Bit-main floated S15 and T15 ant-miners as the new generation of mining machines in November 2018 with publicized energy consumption of 57 Joules per terahash and 96 Joules per terahash respectively against extant S9, T9, and comparable machines. Although induction of this new generation in the cluster reduces the profit proportion of existing ones due to their higher power consumption. Though it was a tough year for the bitcoin economy even then S15 and T15 appear to be lucrative pact. In the prevailing market conditions by January 2019, a vested passion in ant-miner S15 shall return as much as 34% annually for two years (Das and Dutta, 2020). Because of the monthly network hash rate of 11% over the past year, then a 5% monthly increase in network hash rate shall return a mere 4% annually.

Contrarily, a new advanced generation of machines advocates those earlier archaic ones are doomed to be discarded. The S9 and T9 machines (accessible from mid-2016 till the first half of 2018) stand to become e-waste with the arrival of S15 and T15 machines, creating as high as 19,000 metric tonnes of e-waste, where a single machine weighs around 4.5 kgs. Therefore, a single generation accounts for massive 28,000 metric tonnes of e-waste. This implies that unreal bitcoin has realistic environmental consequences.

The bitcoin sustainability report issued in January 2019 (Das and Dutta, 2020) presents that bitcoin has already employed energy comparable to a country like Singapore in just the first month of the year. It further pointed towards an annual increase of 12% in energy consumption than 2018, while mining revenues amounted lower at the beginning of the year than the previous year. The sustainability report published for February 2019 provided data as compared to the previous month, showed a drop of 8% in mining revenues and a hike of 23% in transaction fees for average fees per transaction as 0.30$. In addition to this, marked 395 KWh per unique transaction which is equivalent to power 1 U.S. household for more than days.

1.3. Blockchain

Bitcoin built on blockchain technology. Blockchain is a distributed, permanent database of all transactions that have ever happened. The term distributed here implies being shared, and every block (constituent unit of blockchain) is duly verified by concord of the majority of participants. In other words, blockchain devises a system of distributed concord in the online digital world, analogous to banks as a credible arbitrator in the physical world as shown in Fig. 1.

The blocks that comprise blockchain are chained in the sense that each block consists of the hash of the previous block, with the base block, known as the genesis block, being hard-coded. As a result, a block usually consists of a series of transactions, the hash of the previous block, and a nonce that is less than the current target τ. The τ is measured on a regular basis to regulate the degree of complexity (O'Dwyer and Malone, 2014). The degree of complexity determines the amount of work required to calculate PoW. This implies that for increasing the level of difficulty, more

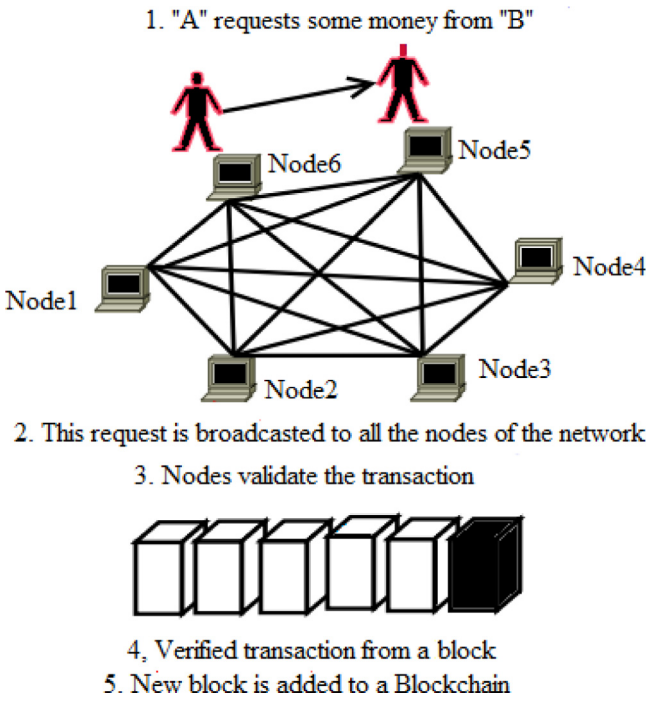


Fig. 1. Process of Bitcoin *w.r.t* Blockchain.

amount of time is required to calculate the PoW as depicted in Fig. 2. The miners want to calculate the coined for one occasion such that $\dot{H}(\beta \times \theta \times E_{\dot{H}}) < \tau$, where β is the set of transactions to be comprehended in the current block, θ is the nonce value, $E_{\dot{H}}$ is the hash of the earlier block, $\dot{H}$ is the cryptocurrency hash function (example: SHA256(SHA256(B)) is the bitcoin hash function).

The high acceptance of blockchain is credited to its sturdy approach to a possible castrate. This accounts for the fact that the blockchain copy is preserved at each participant of the system, unlike a single centralized copy at an unbiased observer say a bank. Therefore, an eavesdropper willing to corrupt the data stored in a blockchain needs to recalculate the PoW for all the blocks in the blockchain for every participant that too within the time frame of addition of new block in the authenticated blockchain, which amounts to a whooping computation task which is usually very high as compared to the value of information being stored on the blockchain.

1.4. Contribution

Considering the high carbon footprint of standard blockchain implementation and the resource-constrained nature of CWCN, the work in this paper outlines the challenges and research opportunities in the domain. In addition to this, the work proposes a simplified blockchain that is more applicable to the CWCN. The simplified blockchain is simple in the sense that it has reduced the amount of computation effort for the calculation of PoW to an extent. The device under consideration is an environmental living or atmospheric assisted living application, which is specialized for elderly treatment in a large hall and collects physical parameters such as temperature, pressure, humidity, vibration, and light on a single board computer (Raspberry Pi). The physical parameters temperature, pressure, and humidity were selected for the application with stable indoor air quality, sound sleep, and bedsores (for bed-ridden elderly people) in mind. Additionally, light and sound parameters were considered to ensure protection against

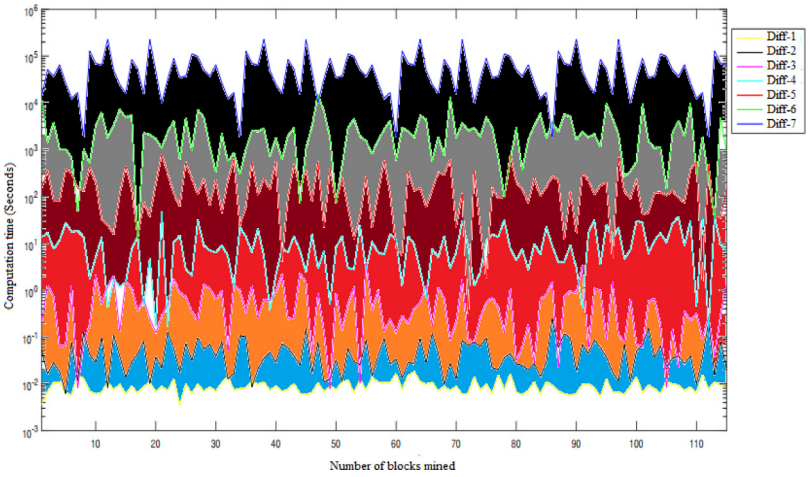


Fig. 2. Increasing level of difficulty over Computation time.

a potential disturbance or to detect irregular elderly activity (such as no movement for a long period, no light or sound even after sunset) so that family or nearest health care center may be informed well in time. In addition to making a self-sufficient blockchain-based CWCN system, where all computations are carried out at CWCN devices instead of setting up a separate machine for PoW computation, the system also assigns the PoW computation task to a few compute efficient machines to reduce the computation time. The standard blockchain implementation for specified applications could compute PoW only till difficulty level 7, after this, the application for computation got killed (even on repeated trials). Therefore, the current work compares the standard blockchain with simplified blockchain only till difficulty level 7.

The research work of this paper has been organized as under: Section 2 describes the work done in the domain of Blockchain-based CWCN. This follows the identification of the literature gap. Section 3 introduces the domain of blockchain implementation in CWCN along with challenges in doing so and possible solutions in the literature. In addition to this, the research opportunities available have been deliberated. The Section 4 proposes an energy-efficient solution to compute PoW. Section 5 described the details of experimental setup used on various machines for energy analysis. Section 6 present the results of a implementation of the proposed energy-efficient solution against standard blockchain implementation. Section 7 concludes the work done.

2. Blockchain: Related work

The work done in the literature domain has been summarized in Table 1.

2.1. Problems identified in literature

A substantial amount of work is being done in the implementation of blockchain for CWCN applications, as well as in the domains of the environmental living and experimental residential care applications, by proposing new models or using other consensus methods for mining processes such as proof of stake, proof of jurisdiction, proof of principle, proof of burn, proof of time, and so on. Instead of replacing standard PoW, efforts should be focused on standard issues while keeping the application domain's requirements and critically in mind. The mining method that calculates the PoW consumes the most resources in bitcoin mining. As a result, the objective should be to optimize the issue of PoW computing while also meeting the application domain's security requirements.

3. Blockchain for CWCN

CWCN refers to anything (any computer, someone, any service, any industry, any location, any context, any time) that is connected to or operated by the Internet. Wearable sensors to consumer goods for surveillance, health care (e.g., environmental living and indoor assisted living), intelligent farming to commercial systems, smart parking to the smart community, and so on are all examples of CWCN applications. Considering the robust attitude of blockchain against any form of compromise, the current work stores the data on the blockchain to protect the system against any security threat. Moreover, instead of storing data on the connected edge device, considering the lifetime of the data set, the historical data may be backed up on the cloud. The data stored on the cloud may be verified for potential security lapse from blockchain data i.e. blockchain also facilitates self-healing of compromised devices.

3.1. Challenges

There exist few challenges for the implementation of blockchain in CWCN applications. The important ones are detailed as under:

3.1.1. Privacy

Blockchains are pseudo-anonymous as different blockchain system participants can be pinpointed based on their public key or its corresponding hash. Third-party agencies can obtain exact user identities by analyzing the transactions in the system (Meiklejohn et al., 2013; Möser et al., 2013). User authentication in CWCN can be crucial: an administrator answerable to user authorization can even block a particular user. Permissioned blockchain (Chithaluru et al., 2019) may be used in such a situation for secure management of multiple CWCN devices in a pool. The recommended solution strengthens the security by using certificate-based authentication along with hash function substitution. On the other hand, a centralized identity management system (Chithaluru et al., 2021c) focused on an automatic authentication system for CWCN. The solution to this problem has been given as a blockchain-based system for CWCN smart homes which authenticate user and appliance by automatically obtaining appliance signatures. Another critical domain is access management, which includes exact specifications regarding capabilities, access lists, and rights of a particular user. Blockchain-based multi-level mechanism (Chithaluru et al., 2020a) solved this problem.

Table 1
Blockchain: Related work.

Reference	Conoscenti et al. (2016)
Advantages	Design identified 18 use cases for blockchain utility, 4 specifically for CWCN.
Lag	Issues on integrity, anonymity, and adaptability.
Remarks	Identified blockchain as pseudo-anonymous.
Reference	Novo (2018)
Advantages	As access control technology, proof of capacity (PoC) was used.
Remarks	For CWCN, designed a highly control architecture used.
Reference	Khan and Salah (2018)
Advantages	Investigated security threats for CWCN, their achievable
Remarks	Discussed, analyzed the efficacy of blockchain in CWCN.
Reference	Lee and Kim (2018)
Advantages	Enhanced the anonymity of blockchain using zero-knowledge proof to avoid personal information disclosure.
Remarks	concentrated on the machine certificate authority.
Reference	Banerjee et al. (2018)
Advantages	Hypothesized the possibility of using blockchain to ensure the integrity.
Remarks	Vulnerability against possible compromise in hardware or software of an CWCN device in case of physical accessibility?
Reference	Gupta et al. (2018)
Advantages	Presented a blockchain consensus model for secure data communication in CWCN.
Remarks	Addressed feasibility of Blockchain in CWCN.
Reference	Fernández-Caramés and Fraga-Lamas (2018)
Advantages	Presented possible changes required to implement blockchain to CWCN.
Remarks	Addressed specific challenges such as privacy, security, energy efficiency, bandwidth, infrastructure, adoption rate, usability, multi-chain management, versioning, mining boycott, smart contract enforcement and autonomy.
Reference	Sankaran et al. (2018)
Advantages	Profiled energy consumption in blockchain implementation.
Remarks	Worked on real-time workload.
Reference	Wan et al. (2017)
Advantages	Focused on the adoption of blockchain in CWCN for effective and reliable healthcare.
Remarks	Worked on ambient living/ambient assisted living application.
Reference	Minoli et al. (2017)
Advantages	Proposed a critical architecture of e-health model for CWCN protocol
Remarks	Not focused on privacy requirement for CWCN.
Reference	Alkhomsan et al. (2017)
Advantages	Identified need for situation awareness in effective domain analysis.
Remarks	Multi modal data analysis.

For a public blockchain, using a different address for every new transaction makes the data analysis difficult, while usage of unique addresses for each different communicating entity shall be a more realistic but less secure approach. Contrarily, in a private blockchain, where accesses are controlled by a neutral access controller, a potential solution could be maintaining an autonomous blockchain for each different entity being communicated with. This solution increases complexity but secludes each user from unwanted monitoring (Chithaluru et al., 2020b).

Another technique to boost privacy is to collect transaction data from different CWCN devices and events along with different addresses with whom communication is being carried out, but this too is vulnerable to statistical disclosure attacks (Prakash et al., 2019), where malicious users may even steal money in case of financial transactions.

Zero-knowledge proving methods can also contribute to enhancing privacy (Chithaluru et al., 2020c; Prakash and Chithaluru, 2021; Ramakuri et al., 2019). The method includes proving that a particular user has certain information regarding a counter-party without letting them know about the information (Schukat and Flood, 2014). The zero-knowledge proofs authenticate without exposing a user's or a device's identity.

Cryptonote (Chithaluru et al., 2021d) based cryptocurrencies such as Byte-coin (Gaurav et al., 2020) and Monero (Kim, 2019) are based on ring signatures where tracking blockchain does not reveal the identity of communicating entities. An entity with

either of the users' private keys or the communicating entities themselves can have the transaction information. The concept of ring signatures specifies the possible set of signers but not the exact signers.

Homomorphic encryption (Moore et al., 2014; Hayouni and Hamdi, 2016) to upholds privacy by encryption followed by data processing through third party agencies without revealing the plain text being communicated. Further, this is to be noted that the cryptographic techniques being implemented to enhance privacy should be feasible for resource-constrained CWCN devices.

3.1.2. Security

The three pillars of security (CIA) i.e. Confidentiality, Integrity, and Availability ensure a secure application. The confidentiality of data associated with the information being communicated is related to privacy. In a secure cloud-based or centralized setup for information storage, the stored information is protected against any possible threats and internal leaks (Jabir et al., 2016; Atya et al., 2017). While the blockchain-based system is decentralized and consensus-based, thus protected even if one of the participating machines is compromised.

An eavesdropper needs the private key of a user to masquerade as an authentic user. Zubaydi et al. (2019) introduced an authentication scheme to relieve users from the burden of encryption identity generation. Blockchain defends IP spoofing and forgery attacks (Kshetri, 2017) for CWCN devices.

Certificate-based security does fail occasionally (Sattar et al., 2019). Google's certificate transparency system (Hussain and Al-Turjman, 2021) monitors and audits Secure Sockets Layer (SSL) certificates in almost real-time by using Merkle hash trees in a distributed environment.

The basic blockchain architecture facilitates that data stored on blockchain cannot be modified. But, for few very exceptional instances (e.g. 2014 vericoin case where a hacker stole almost 30% of the total coins), to ensure data integrity against a serious threat, hard forks have been made for earlier models of blockchain. CWCN depends on third-party agencies for integrity services. Blockchain technology liberate CWCN devices against such agencies by providing a framework for cloud-based CWCN applications (Liu et al., 2017).

Distributed nature of blockchain platform ensures availability even if few participating entities have been compromised. Still, the availability of blockchain can be breached by few attacks. The most popular attack, the majority attack (or the 51% attack) keeps the data available but the transactions being carried out may be controlled by a overall blockchain's consensus.

3.1.3. Adoption rate

Pseudo-anonymity of blockchain hinders its acceptance by government bodies. Government bodies appeal direct link between the real world and online entity, so that culprit may be traced in case of emergency.

The number of participants in the blockchain-based system directly impacts the value and security of information being stored. This implies the higher number of participants makes the application more robust against the most formidable 51% attack.

The participating entities in blockchain-based CWCN application also demand that the participants are competent enough to handle the computation requirement of the system.

3.1.4. Forks and multi-chain management

Forks do occur in blockchain for administrative and versioning purposes, which are difficult enough to be handled by CWCN applications where resources are already constrained.

Generation of new blocks in the system sometimes leads to an instance where multiple block-chains need to be handled. If such an instance occurs in an CWCN application then the system should be robust enough to handle the same.

3.1.5. Smart contract administration

A smart contract duly in place as designed by a governing body needs to be administered to resolve a dispute. Moreover, the issue of binding real-world contracts to smart contracts (Fabiano, 2017) needs to be addressed.

3.1.6. Throughput

A large number of transactions can be processed per unit time by increasing the device computation power, or by processing large blocks, etc., Xu et al. (2020). While bitcoin can process a maximum of 7 transactions per second (Villa-Pérez et al., 2021) but this is very slow as compared to up to 24,000 transactions per second in VISA (Metcalfe, 2020).

On the other hand, a proposed CWCN application may need to handle a large number of transactions per unit time. This high computation power requirement may be a hurdle for blockchain implementation in CWCN.

Blockchain transactions processing is a time-consuming process. For example, Bitcoin takes an average of 10 min to process a block, still, users are suggested to wait for approximately an hour for a transaction to get confirmed while VISA (VisaNet) needs only a few seconds for a similar task (Wang et al., 2020).

For minimizing the time taken in completing the consensus mechanism, a variation in the blockchain which is comparatively faster than standard SHA256 can be a possible solution. For example Litecoin (Loyola-González et al., 2020) use scrypt (Ball et al., 2018).

3.1.7. Energy efficiency

The resource-constrained, battery-powered CWCN devices always expect the application to be energy efficient while the block-chains are usually portrayed as power-hungry attributed to the mining process and P2P communication. Loyola-González (2019) suggests few outcomes where the energy consumed in the computation of PoW can be used parallelly for some other jobs. Alternative mining mechanisms which can anyhow simplify the mining process could be a possible solution (For example Grid-coin (Austin, 2019), prime-coin (Dziembowski et al., 2015)). One such energy-efficient solution working on PoW has been proposed in Section 4. Proof of Capacity is a greener solution to PoW (Indrakumari et al., 2020). Burst-coin (Chithaluru et al., 2021b) uses PoC where a user has to show justifiable interest in a particular service by assigning a certain memory space.

The participating entities in a blockchain communicate with peers to distribute blocks and send updates. Though the more the updates better the blockchain but these updates consume the fixed battery power. Mini-blockchain (Srivastava et al., 2020) could be a solution for CWCN devices to directly reach out with the blockchain as they maintain a record of only the latest transactions.

The popularity of SHA256 is contributed to the fact that it is used for Bitcoin. Although algorithms like scrypt (Ball et al., 2018), X11 (Aumasson et al., 2008), Blake-256 (Fernández-Caramés and Fraga-Lamas, 2018), Myriad (França, 2015) are another option that promises less energy consumption.

3.1.8. Infrastructure

Blockchain implementation in the resource-constrained CWCN domain needs to be proportioned according to the limitations of CWCN applications. For instance, small transaction data may consume a large amount of energy in communication or large transactions involving a huge amount of data that is not capable of resource-constrained CWCN system, etc.

The matter of fact is that most of the CWCN applications are not competent enough to standard blockchain models. Therefore, to suit CWCN applications, lightweight participating entities can

be used, which do not store data but just perform transactions on the blockchain. This architecture needs certain powerful machines which can store data. Another approach uses the concept of mini-blockchain (Mariem et al., 2020; Srivastava et al., 2020) where the account tree store the every participant of the block and the blockchain only in case of new participant joins the system.

3.2. Limitations

Even though blockchain technology as a helping hand to CWCN appears to be quite lucrative and a dazzling future can be foreseen, still there exist compelling challenges which need to be addressed.

- Scalability, security, cryptographic developments, and cohesion prerequisites of blockchain-based CWCN application is still a challenge. In addition to this, the tendency of centralized approaches needs to be worked upon.
- **Interoperability and standardization**, an amalgam of two different technologies i.e resource-constrained CWCN and energy-hungry blockchain need an adjustment on all the collaborating participants of the system. The adjustments scale from different trade-offs along with legal issues to international standards of trust, access control, authorization, etc. For example, at an international level, authentications are provided based on Level of Assurance (LoA) where according to ISO/IEC 29115:2013 standard LOA is defined on a scale ranging from LoA1 till LoA4. The higher the LoA, the better the system. This standard defines the risk, aftereffects of an error in authentication, exploitation of credentials, etc.
- **Government regulatory aspects**: Design of a regulatory framework is a significant aspect to be worked upon in blockchain-based CWCN. This framework shall bring in the interest of different capitalists to invest and popularize the domain.
- **Field testing**: The blockchain-based CWCN applications need to be tested in various real-time domains, so that different loopholes may be identified and worked upon to improve social acceptability. The testing process standardizes the system based on numerous aspects as listed in Section 3.1.1.

4. Energy efficient blockchain for CWCN

On resource-constrained CWCN implementations, the traditional blockchain implementation with PoW as a consensus technique is unlikely. This is attributed to the fact that:

The signature requirement for block 100 (in 2009) was 8 consecutive zeros, which has now increased to 18 consecutive zeros for block 568512 as of March 25, 2019, for an average hash rate of 45.66 $\frac{EH}{s}$ (Bhargava and Zoltowski, 2003; Chithaluru et al., 2021a), demonstrating that PoW computing is the most time consuming and hence energy consuming aspect in the blockchain scheme. Furthermore, this level of protection is not needed for CWCN applications, and this level of hashing power is not possible on standard machines (Sitharthan et al., 2016; Soundarya et al., 2021). As a result, the PoW puzzle must be streamlined to accommodate CWCN applications, available hardware, and the value and age of knowledge.

Assume that the hash output $\dot{H}$ of a cryptographic hash function is $\alpha_0\alpha_1\alpha_2\alpha_3\alpha_4\ldots\alpha_{63}$, where α_i is a four-bit hexadecimal digit. The normal complexity in terms of the number of initial hexadecimal digits, say l, is defined to be 0s, i.e., $\alpha_0\alpha_1\alpha_2\alpha_3\alpha_k\alpha_{l+1}\alpha_{l+2}\ldots\alpha_{63}$, where $\alpha_i = 0$; $i < l$.

The basic blockchain implementation is depicted in Table 2, which uses first l $alpha_i$ to be zero for various levels of complexity l.

Table 2
Standard blockchain hashes for different difficulty levels.

Difficulty level	Eligible hash output
1	0abcdefghijkl..yz
2	00bcdefghijkl..yz
3	000cdefghijkl..yz
4	0000defghijkl..yz
l	00(k-zeros)kl..yz

Table 3
Modified blockchain hashes for different difficulty levels.

Difficulty level	Eligible hash output
2	33bcdefghijkl..yz
3	555cdefghijkl..yz
4	2222defghijkl..yz
5	99999efghijkl..yz
l	l-consecutive kl..yz

The current work proposes a more flexible solution that is more applicable to CWCN systems due to its simplicity. The solution makes the first l hexadecimal digits to be a value from the range ξ = {0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f} i.e. hexadecimal values (0-F). We adjust the complexity as $\alpha_0\alpha_1\alpha_2\alpha_3\alpha_l\alpha_{l+1}\alpha_{l+2}\ldots\alpha_{63}$, where α_i = k; $i < l(0 \leq k \leq F)$.

In other words, the adjusted blockchain for CWCN applications considers first l α_i to be a value from a fixed ξ for a different degree of difficulty l, where ξ = {0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f} so that all ξ have the same value from ξ for a given hash output (as seen in Table 3). It should be remembered that for changed blockchain, the complexity level has been considered from l = 2 since for l = 1, all available hashes would be qualifying hashes, resulting in the insignificance of the τ.

Further, another consideration is that the standard blockchain implementation allowed the following number of hashes from all possible hashes for a given difficulty level:

Difficulty level 1: = $\frac{1}{16} \times 100 = 6.25\%$

Difficulty level 2: = $\frac{1}{16} \times \frac{1}{16} \times 100 = 0.3906\%$

Difficulty level 3: = $(\frac{1}{16})^3 \times 100 = 0.000244\%$

..

..

Difficulty level n: = $(\frac{1}{16})^n \times 100\%$

While the modified blockchain allowed the following number of hashes for a given difficulty level:

Difficulty level 1: = $\frac{16}{16} \times 100 = 100\%$

(This implies allows every possible hash output as an eligible hash which defeats the purpose of τ. Therefore ignoring level 1 for comparison purpose.)

Difficulty level 2: = $(\frac{16}{16\times16}) \times 100 = 6.25\%$

Difficulty level 3: = $(\frac{16}{16\times16\times16}) \times 100 = 0.3906\%$

..

..

Difficulty level n: = $(\frac{1}{16})^{n-1} \times 100$

This implies that the modified solution allows 16 times more hashes as eligible hashes at a particular level of difficulty, which implies less computation time will be required to find eligible hash, thus saving energy as compared to standard blockchain implementation. Table 4 for acronyms as well as variables used in the simulation.

5. Experimental setup

The current work assumes a CWCN application as an intruder detection device in a room where physical parameters such as temperature, pressure, humidity, illumination, and sound can be

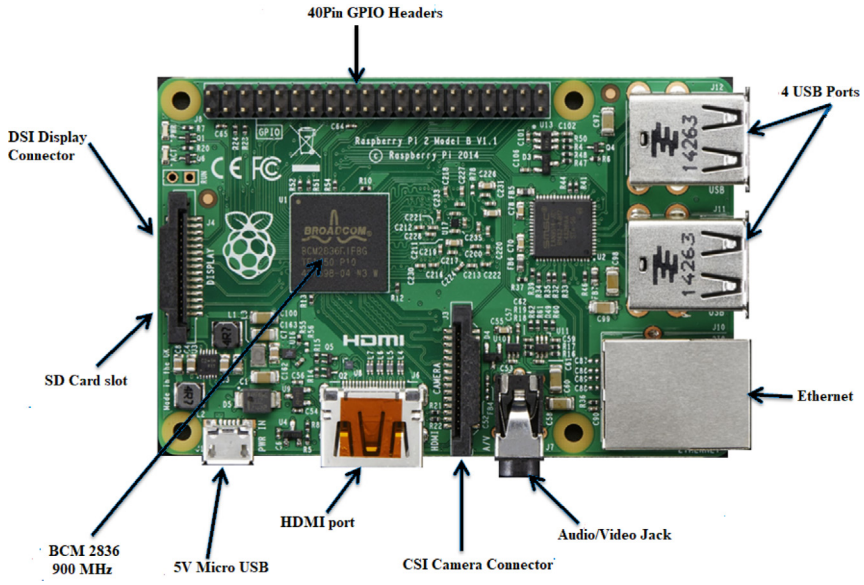


Fig. 3. Hardware design of Raspberry Pi 2.

Table 4
Acronyms.

Symbols	Meaning
τ	Target of current block
$\dot{H}$	Cryptocurrency hash function
θ	Nonce value
$E_{\dot{H}}$	Hash of the earlier block
α	Output of cryptographic hash function
l	Level of complexity
ξ	Hash range set
k	Difficulty level range
I_{EC}	Energy consumed per instruction
T_P	Total time the processor
X	Processor clock frequency

registered for an environmental living application such as elderly care. As seen in Fig. 3, the device collects data using three digital sensors (BME280 (temperature, pressure, humidity), proximity sensor (light), and KY-038 (sound)) attached to a single-board computer (Raspberry Pi 2 Model B). The obtained data is saved on the Raspberry Pi, where it is used for various research activities.

The machine receives data values from the sensors every 60 s, resulting in a transaction. A block is formed by combining the data from 60 transactions. This means that the device generates one transaction per minute and one block every hour, for a total of 24 transactions a day.

To maintain stability in the insecure networking world, the complexity level is regularly increased with ever-increasing computing capacity. The level of complexity for a specific PoW computing task is measured by the amount of time and hashing power needed to locate qualifying hashes (signature). The PoW computing task was carried out on the attached Raspberry Pi for the given experimental configuration, such that data storage along with the corresponding blockchain will guarantee the protection and privacy of the usable framework. As seen in Fig. 2, the Raspberry Pi could compute PoW up to complexity level 7, but after that, it was unable to compute more and the operation was destroyed by the machine (even on repeated trials). As a result, the existing work only considers complexity level 7 for resource-constrained CWCN devices.

Later, as seen in Fig. 4, the PoW computing task was allocated to comparatively more efficient machines to reduce computation time. The different machines taken into consideration are detailed in Table 5.

6. Character of utility

The character of utility has been defined in the terms of energy consumed in the attached machines on which blockchain has been implemented:

- **Raspberry Pi:** For every mining operation, a 0.29-ampere current (averaged over 3000 values) was reported by connecting to 5 volts voltage (recommended voltage for Raspberry Pi) and an ammeter in series with the Raspberry Pi's power supply. When the level of complexity rose, so did the time required for computation. This means that the energy used by the Raspberry Pi is a function of time with a given amount of power consumed to run the device.
- **Intel i7-4770**: Energy consumed by an Intel device is computed as:
  Computation Energy = $I_{EC} \times T_P \times X$
  where I_{EC} is the energy consumed per instruction, T_P is the total time the processor is active and X is the processor clock frequency. Here, this is to be noted that the I_{EC} value and the processor clock frequency are fixed for a particular processor, which means computation energy is directly proportional to processor active time.
- **Intel i7-4510U**: The above technique is applicable in this system too being an Intel device. But there exists one more Linux utility to compute power consumption in battery-powered devices known as "Power-top". Power-top takes power estimates of 197 measurements on battery power, where each measurement is taken at a time duration of 20 s. It gives the average power consumption for running the standard blockchain implementation as 376J (or watt per second). Therefore, to calculate energy which is the product of power and time can be estimated from the time factor which is increasing the difficulty level.
- **Param Shava**k: Similarly, the power consumption for param shavak can be estimated from the same as in wired computer (Intel i7-4770) again being an Intel device.

Therefore, for the sake of simplicity, the energy consumption has been depicted in terms of computation time.

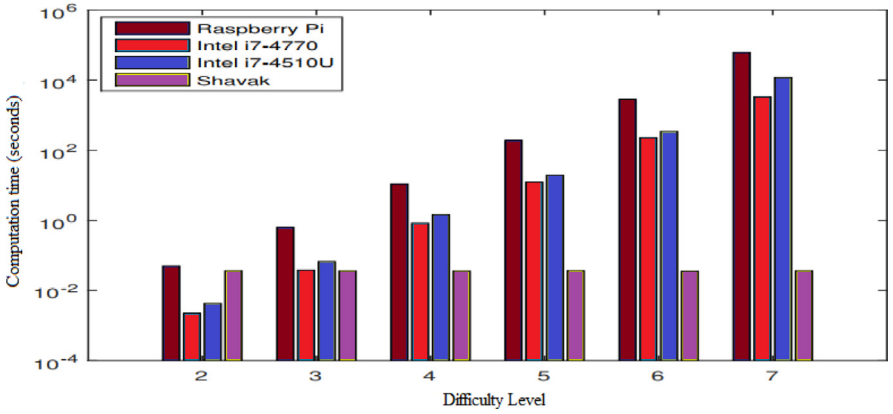
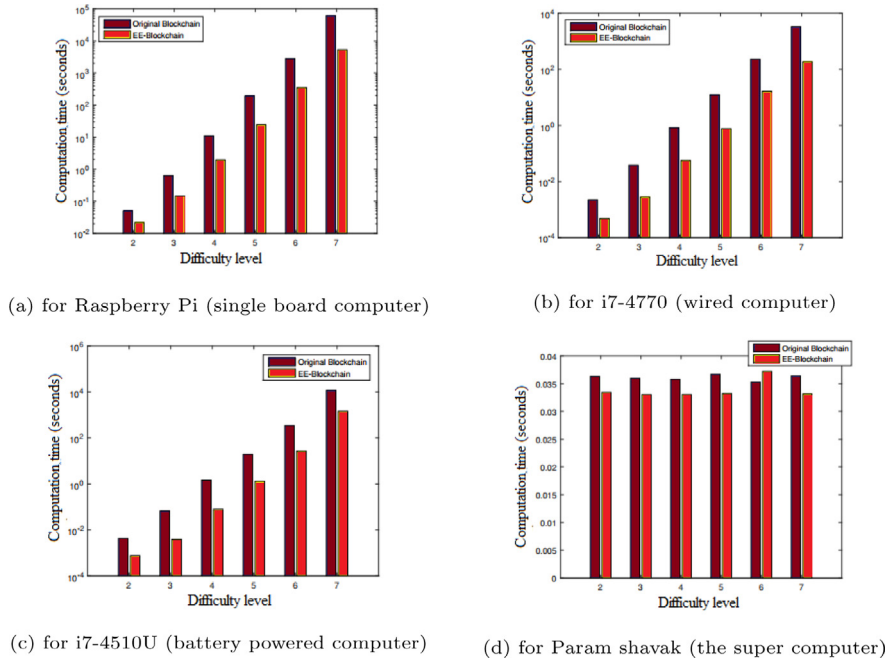


Fig. 4. Computation task of PoW on various machines.



(a) for Raspberry Pi (single board computer)

(b) for i7-4770 (wired computer)

(c) for i7-4510U (battery powered computer)

(d) for Param shavak (the super computer)

Fig. 5. Energy efficient algorithm implementation on different machines.

Table 5
Various machines technical specification.

Parameter	Raspberry Pi 2	Intel i7-4770	Intel i7-4510U	Param Shavak
Computer type	Single board	Wired	Battery Powered	Super
Architecture	armv71	x86_64	x86_64	x86_64
Byte order	Little endian	Little endian	Little endian	Little endian
CPU(s)	4	8	4	24
Threads per core	1	2	2	1
Core(s) per socket	4	4	2	12
Model	5	60	69	63
Model Name	ARM v7 Processor rev 5 (v71)	Intel(R) Core(TM) i7-4770 CPU @ 3.40 GHz	Intel(R) Core(TM) i7-4510U CPU @ 2.00 GHz	Intel(R) Xeon(R) CPU E5-2670 v3 @ 2.30 GHz

6.1. Outcomes

Fig. 5 shows the results for implementation of a modified solution for different machines under consideration as in Table 5 for difficulty levels from 2 to 7 in terms of computation time (in seconds) for the mining process.

Fig. 5(a) depicts the implementation of modified blockchain for CWCN applications where mining is carried out on a single board computer (Raspberry Pi) which collects all the data from all digital sensors.

Where, Diff: Level of Difficulty, EE-Diff: Energy efficient implementation of a difficulty level.

The energy-efficient implementation shows less computation time due to the higher number of possible hashes accepted. Similarly, Figs. 5(b) and 5(c) too show a comparatively less amount of time for computation tasks due to a higher acceptance ratio.

Table 6
Computation time (in seconds) for mining process at different machines and increasing difficulty level.

Difficulty Level	Raspberry Pi 2	Intel i7-4770	Intel i7-4510U	Param Shavak
Diff-2	0.049692	0.002229	0.00426636	0.03631
EE-Diff-2	0.021689	0.00048	0.000754	0.033428
Diff-3	0.633516	0.038282	0.066523	0.035977
EE-Diff-3	0.145693	0.002841	0.003871	0.033043
Diff-4	10.90047	0.0831858	1.458152	0.035789
EE-Diff-4	1.94733	0.056478	0.078535	0.033052
Diff-5	192.3865	12.39542	19.48517	0.036703
EE-Diff-5	24.32805	0.761665	1.309791	0.033228
Diff-6	2819.878	229.4927	346.5656	0.035291
EE-Diff-6	353.9819	16.4279	26.8063	0.037208
Diff-7	61403.99	3326.107	11831.3	0.036403
EE-Diff-7	5268.56	187.5868	1450.932	0.033136

While Fig. 5(d) does not show any significant change in computation time even with an gain in the difficulty level because the computation resources available with the supercomputer are incredibly high as compared to the computation task at hand. Moreover, this too is to be noted that some resources are mandatorily consuming energy to make such large system work. In an energy-efficient implementation, the results also show similar behavior but comparatively less computation time for less computation task at hand. The results for computation time (in seconds) at a given difficulty level for standard and modified energy-efficient blockchain implementation for CWCN applications are given in Table 6. Here this is to be noted that each value in Table 6 is averaged over 113 blocks' computation time. In addition to this, it is to be reported that for over 113 blocks the data of over 4 days have been collected to calculate computation time for PoW.

7. Conclusion

Considering computation resources available with CWCN devices and the value and validity of information in CWCN applications suggest that standard blockchain implementation is neither possible nor required for CWCN applications. Further taking into account the criticality in terms of security and privacy for CWCN applications, which can directly impact human life (as in ambient living or ambient assisted living applications), blockchain is a good solution such applications, but with some simplicity in the computation of PoW. Therefore, the current work proposes modified energy-efficient blockchain implementation for CWCN applications which consume 16% less energy in terms of computation time at each level of difficulty. In addition to this, the current work answers the issues raised in literature work as follows:

First, blockchain can be used as collective security to secure applications in CWCN and related systems. Blockchains and blockchain-based platforms can be optimized by applying simplification in solving the PoW puzzle. Further, blockchain can be used to reduce the possibility of hardware and software vulnerability in a physically approachable CWCN device by matching the hash at a particular block level which cannot be changed easily by an intruder. Last, the proposed solution in the current work may be a cost-effective approach to device a mature blockchain-based security solution.

CRediT authorship contribution statement

Premkumar Chithaluru: Conception and design of study, Analysis and/or interpretation of data. **Fadi Al-Turjman:** Acquisition of data, Revising the manuscript critically for important intellectual content. **Thompson Stephan:** Acquisition of data, Analysis and/or interpretation of data, Drafting the manuscript. **Manoj Kumar:** Conception and design of study, Analysis and/or interpretation of data, Drafting the manuscript. **Leonardo Mostarda:** Analysis and/or interpretation of data, Drafting the manuscript, Revising the manuscript critically for important intellectual content.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Alkhomsan, M.N., Hossain, M.A., Rahman, S.M.M., Masud, M., 2017. Situation awareness in ambient assisted living for smart healthcare. IEEE Access 5, 20716–20725.

Atya, A.O.F., Qian, Z., Krishnamurthy, S.V., La Porta, T., McDaniel, P., Marvel, L., 2017. Malicious co-residency on the cloud: Attacks and defense. In: IEEE INFOCOM 2017-IEEE Conference on Computer Communications. IEEE, pp. 1–9.

Aumasson, J.P., Henzen, L., Meier, W., Phan, R.C.W., 2008. Sha-3 proposal blake. Submission to NIST, 92.

Austin, T.H., 2019. Cryptocurrency project: Assignment description.

Ball, M., Rosen, A., Sabin, M., Vasudevan, P.N., 2018. Proofs of work from worst-case assumptions. In: Annual International Cryptology Conference. Springer, Cham, pp. 789–819.

Banerjee, M., Lee, J., Choo, K.K.R., 2018. A blockchain future for internet of things security: a position paper. Digit. Commun. Netw. 4 (3), 149–160.

Bhargava, A., Zoltowski, M., 2003. Sensors and wireless communication for medical care. In: 14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings. IEEE, pp. 956–960.

Chithaluru, P., Al-Turjman, F., Kumar, M., Stephan, T., 2020a. I-AREOR: An energy-balanced clustering protocol for implementing green IoT in smart cities. Sustainable Cities Soc. 61, 102254.

Chithaluru, P.K., Khan, M.S., Kumar, M., Stephan, T., 2021a. ETH-LEACH: An energy enhanced threshold routing protocol for WSNs. Int. J. Commun. Syst. e4881.

Chithaluru, P., Kumar, S., Singh, A., Benslimane, A., Jangir, S.K., 2021b. An energy-efficient routing scheduling based on fuzzy ranking scheme for internet of things (IoT). IEEE Internet Things J..

Chithaluru, P., Singh, K., Sharma, M.K., 2020b. Cryptocurrency and blockchain. Inform. Security Optim. 143.

Chithaluru, P., Tanwar, R., Kumar, S., 2020c. Cyber-attacks and their impact on real life: What are real-life cyber-attacks, how do they affect real life and what should we do about them? Inform. Security Optim. 61.

Chithaluru, P., Tiwari, R., Kumar, K., 2019. AREOR–adaptive ranking based energy efficient opportunistic routing scheme in wireless sensor network. Comput. Netw. 162, 106863.

Chithaluru, P., Tiwari, R., Kumar, K., 2021c. ARIOR: Adaptive ranking based improved opportunistic routing in wireless sensor networks. Wirel. Pers. Commun. 116 (1), 153–176.

Chithaluru, Premkumar, Tiwari, Rajeev, Kumar, Kamal, 2021d. Performance analysis of energy efficient opportunistic routing protocols in wireless sensor network. Int. J. Sens., Wirel. Commun. Control 11, 24.

Conoscenti, M., Vetro, A., De Martin, J.C., 2016. Blockchain for the internet of things: A systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). IEEE, pp. 1–6.

Das, D., Dutta, A., 2020. Bitcoin's energy consumption: Is it the achilles heel to miner's revenue? Econom. Lett. 186, 108530.

Dziembowski, S., Faust, S., Kolmogorov, V., Pietrzak, K., 2015. Proofs of space. In: Annual Cryptology Conference. Springer, Berlin, Heidelberg, pp. 585–605.
Fabiano, N., 2017. The internet of things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard. In: 2017 International Conference on Internet of Things for the Global Community (IoTGC). IEEE, pp. 1–7.
Fernández-Caramés, T.M., Fraga-Lamas, P., 2018. A review on the use of blockchain for the internet of things. IEEE Access 6, 32979–33001.
França, B.F., 2015. Homomorphic mini-blockchain scheme.
Gaurav, A.B., Kumar, P., Kumar, V., Thakur, R.S., 2020. Conceptual insights in blockchain technology: Security and applications. In: Transforming Businesses with Bitcoin Mining and Blockchain Applications. IGI Global, pp. 221–233.
Gupta, Y., Shorey, R., Kulkarni, D., Tew, J., 2018. The applicability of blockchain in the Internet of Things. In: 2018 10th International Conference on Communication Systems & Networks (COMSNETS). IEEE, pp. 561–564.
Hayouni, H., Hamdi, M., 2016. Secure data aggregation with homomorphic primitives in wireless sensor networks: A critical survey and open research issues. In: 2016 IEEE 13th International Conference on Networking, Sensing, and Control (ICNSC). IEEE, pp. 1–6.
Hussain, A.A., Al-Turjman, F., 2021. Artificial intelligence and blockchain: A review. Trans. Emerg. Telecommun. Technol. e4268.
Indrakumari, R., Poongodi, T., Saini, K., Balamurugan, B., 2020. Consensus algorithms–a survey. Blockchain Technol. Appl. 4.
Jabir, R.M., Khanji, S.I.R., Ahmad, L.A., Alfandi, O., Said, H., 2016. Analysis of cloud computing attacks and countermeasures. In: 2016 18th International Conference on Advanced Communication Technology (ICACT). IEEE, pp. 117–123.
Khan, M.A., Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 82, 395–411.
Kim, J., 2019. A survey of cryptocurrencies based on blockchain. J. Korea Soc. Comput. Inform. 24 (2), 67–74.
Kshetri, N., 2017. Can blockchain strengthen the internet of things? IT Prof. 19 (4), 68–72.
Lee, C.H., Kim, K.H., 2018. Implementation of IoT system using block chain with authentication and data protection. In: 2018 International Conference on Information Networking (ICOIN). IEEE, pp. 936–940.
Liu, B., Yu, X.L., Chen, S., Xu, X., Zhu, L., 2017. Blockchain based data integrity service framework for IoT data. In: 2017 IEEE International Conference on Web Services (ICWS). IEEE, pp. 468–475.
Loyola-González, O., 2019. Understanding the criminal behavior in Mexico city through an explainable artificial intelligence model. In: Mexican International Conference on Artificial Intelligence. Springer, Cham, pp. 136–149.
Loyola-González, O., Medina-Pérez, M.A., Choo, K.K.R., 2020. A review of supervised classification based on contrast patterns: Applications, trends, and challenges. J. Grid Comput. 1–49.
Mariem, S.B., Casas, P., Romiti, M., Donnet, B., Stütz, R., Haslhofer, B., 2020. All that glitters is not bitcoin–unveiling the centralized nature of the BTC (IP) network. In: NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium. IEEE, pp. 1–9.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S., 2013. A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of The 2013 Conference on Internet Measurement Conference. pp. 127–140.
Metcalfe, W., 2020. Ethereum, smart contracts, dapps. In: Blockchain and Crypt Currency. Springer, Singapore, pp. 77–93.
Minoli, Daniel, Sohraby, Kazem, Occhiogrosso, Benedict, 2017. IoT security (IoTsec) mechanisms for e-health and ambient assisted living applications. In: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE, pp. 13–18.
Moore, C., O'Neill, M., O'Sullivan, E., Doröz, Y., Sunar, B., 2014. Practical homomorphic encryption: a survey. In: 2014 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, pp. 2792–2795.
Möser, M., Böhme, R., Breuker, D., 2013. An inquiry into money laundering tools in the bitcoin ecosystem. In: 2013 APWG ECrime Researchers Summit. Ieee, pp. 1–14.
Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system bitcoin: A peer-to-peer electronic cash system. Bitcoin. Org. Disponible en https://bitcoin.org/en/bitcoin-paper.
Novo, O., 2018. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet Things J. 5 (2), 1184–1195.
O'Dwyer, K.J., Malone, D., 2014. Bitcoin mining and its energy footprint.
Prakash, R., Chithaluru, P., 2021. Active security by implementing intrusion detection and facial recognition. In: Nanoelectronics, Circuits and Communication Systems. Springer, Singapore, pp. 1–7.
Prakash, R., Chithaluru, P., Sharma, D., Srikanth, P., 2019. Implementation of trapdoor functionality to two-layer encryption and decryption by using RSA-aes cryptography algorithms. In: Nanoelectronics, Circuits and Communication Systems. Springer, Singapore, pp. 89–95.
Ramakuri, S.K., Chithaluru, P., Kumar, S., 2019. Eyeblink robot control using brain-computer interface for healthcare applications. Int. J. Mob. Devices Wearable Technol. Flex. Electron. 10 (2), 38–50.
Sankaran, S., Sanju, S., Achuthan, K., 2018. Towards realistic energy profiling of blockchains for securing internet of things. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE, pp. 1454–1459.
Sattar, A.M., Ertuğrul, Ö.F., Gharabaghi, B., McBean, E.A., Cao, J., 2019. Extreme learning machine model for water network management. Neural Comput. Appl. 31 (1), 157–169.
Schukat, M., Flood, P., 2014. Zero-knowledge proofs in M2M communication.
Sitharthan, R., Geethanjali, M., Pandy, T.K.S., 2016. Adaptive protection scheme for smart microgrid with electronically coupled distributed generations. Alex. Eng. J. 55 (3), 2539–2550.
Soundarya, G., Sitharthan, R., Sundarabalan, C.K., Balasundar, C., Karthikaikannan, D., Sharma, J., 2021. Design and modeling of hybrid DC/AC microgrid with manifold renewable energy sources. IEEE Can. J. Elect. Comput. Eng. 44 (2), 130–135.d.
Srivastava, S.S., Dwivedi, R., Gunda, A., Meena, D.K., Negi, R., Vasita, N., Singh, A., 2020. Blockchain and its application in cybersecurity. In: Cyber Security in India. Springer, Singapore, pp. 23–32.
Villa-Pérez, M.E., Álvarez-Carmona, M.Á., Loyola-González, O., Medina-Pérez, M.A., Velazco-Rossell, J.C., Choo, K.K.R., 2021. Semi-supervised anomaly detection algorithms: A comparative summary and future research directions. Knowl.-Based Syst. 106878.
Wan, J., Gu, X., Chen, L., Wang, J., 2017. Internet of things for ambient assisted living: challenges and future opportunities. In: 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). IEEE, pp. 354–357.
Wang, Q., Qin, B., Hu, J., Xiao, F., 2020. Preserving transaction privacy in bitcoin. Future Gener. Comput. Syst. 107, 793–804.
Xu, Z., Parizi, R.M., Hammoudeh, M., Loyola-González, O. (Eds.), 2020. Cyber Security Intelligence and Analytics: Proceedings of the 2020 International Conference on Cyber Security Intelligence and Analytics (CSIA 2020), Volume 2 (Vol. 1147). Springer Nature.
Zubaydi, H.D., Chong, Y.W., Ko, K., Hanshi, S.M., Karuppayah, S., 2019. A review on the role of blockchain technology in the healthcare domain. Electronics 8 (6), 679.