EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Rampant Smoothing (RTS) Algorithm: an optimized consensus mechanism for private Blockchain enabled technologies

Usman Tariq*

*Correspondence: u.tariq@psau.edu.sa

College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al Khraj 11942, Saudi Arabia

Abstract

Blockchain is a distributed database method of storing electronic information in digital form that makes it challenging to transform, hack, or rogue the system. Each time a new operation transpires on the Blockchain, an irreversible information of that transaction is buffered in all connected ledgers. Each distributed ledger is programmable, immutable and timestamped. This paper follows an immutable policy to ensure chronological trust-administration, security and privacy to resolve anomalies within linearly stored blocks. To prove the validity of submitted data, a consensus mechanism is required, which was attained by implementing a novel 'Rampant Smoothing Algorithm' that was encoded using Solidity (i.e., aimed at developing smart contracts). Experimental policies were aligned with Good Clinical Data Management Practices that portrayed effective 'smart contract modeling' to demonstrate resistance against majority consensus attacks by harnessing the core feature of 'privacy decentralization'. During implementation of Blockchain network, an interconnected system of six hundred nodes (i.e., data points) were gradually configured.

Keywords: Blockchain, Healthcare system, Privacy, Security, Smart contracts, Distributed ledger, Electronic medical records (EMR)

1 Introduction

It requires a distributed system to produce and store data to attain better privacy and accessibility. The notion of decentralization is genuinely engraved into the policy of Blockchain technology. Decentralization means that transaction tracking is spread across multiple devices attached to dissimilar networks. Each block contains specific dataset and is capable of various storage capabilities. Fresh stream of data is mounted on a new block, and attached onto the preceding block in linear order.

Storing essential medical data safe and protected is the widespread Blockchain healthcare requirement. The distributed nature of the technology permits caregivers and patients to share data effectively and securely. To ensure data transparency and security, every new block is stored at the end of Blockchain, which allows any stakeholder to examine transactions in real-time.

To ensure integrity and privacy of health inclined data standards, such as General Data Protection Regulation (GDPR) [1] and Health Insurance Portability and Accountability Act (HIPAA) [2] need to be pre-understood and applied with consensus among all stakeholders. Main sources of patent-related data can be 'physician evaluation, family history, genetic, IoT sensing feed (i.e., wearable connected devices), pathology test outcomes, social history, etc.' A data quality valuation was conducted by determining precise features of the information to see if it satisfy distinct standards such as Good Clinical Data Management Practices (GCDMP) [3]. Data quality can be measured based on (a) completeness, (b) validity (i.e., allowable types), (c) timeliness, and (d) consistency. To ensure data quality, the data administrator must effectively understand and access the required data streams. It will ease the process of data validation, transformation, standardization, enrichment, and monitoring.

Blockchain applied to any distinguished field of interest is prone to several risks, such as (a) Weak link security, (b) Reliability issues related to 'proof of identity', (c) Lack of resilience against 'fifty-one percent attack' in context of 'proof of stake', and (d) Scalability issues encountered because of redundant outcome. Redundancy may occur due to transaction log made available at several linked nodes.

Considering above mentioned technical drawbacks, this paper aims to furnish an effective and efficient technique with the eligibility of trust administration by recognizing security and privacy variables.

Major stakeholder concerns against adoptability of Blockchain technology in health care are:

(a) Necessitates digital defense at all levels
(b) Prerequisites the identity confirmation and validation of all contributors
(c) Requires resilience against 'zero-day attacks' and 'social engineering vulnerability'.

A consensual process allows the Blockchain to authenticate and authorize transactions and processes, without the necessity of a third-party arbitrator. It ensures the subsequent block to be attached to the Blockchain. It also discourages corrupt malicious nodes from intrusive, damaging or thwarting the Blockchain setup. Current used consensus methods are energy exhaustive, necessitates abundant processing resources, prone to 51% attack, denial of service and pre computing attack.

Main contributions of this research are as followed:

(a) In order to ensure distributed security properties, the proposed schema provides an extremely synchronized parameter, presenting scalability, security and assimilation with existing/legacy systems. Moreover, SHA-384 cryptographic hash was examined to ensure (a) address derivation, (b) generation of unique identifiers, and (c) block pay-load and header's integrity;
(b) Generated, processed, and analyzed data formats, which constitute fundamental interoperability proficiencies. Local (Saudis) privacy laws have been respected for data regulation.
(c) Implemented and evaluated 'Blockchain Consensus using novel Rampant Smoothing (RTS) Algorithm', which aid a consensus for distinct data value among dissemi-

nated progressions with three applicable states: (a) follower state, (b) candidate state, and (c) leader state.

(d) In order to identify and blacklist common conflict behaviours, an Epidemic protocol was implemented and reviewed.

Author organized the paper in the following sections: Sect. 2 presents the related work. Section 3 provides a description of the overall architecture of Blockchain. The proposed methodology and associated service configuration can be found in Sect. 4. Section 5 presents the experimental criteria and outcome of our proposed scheme. Section 6 presents the analysis and discussion; the conclusion is set out in Sect. 7.

2 Related work

The rapid progress on the internet of things (IoT) technology has transformed healthcare activities by carrying important improvements in terms of e-health/medical records (EHR/EMR). Blockchain is an applicable paradigm shift that can help to simplify healthcare data administration procedures by providing extraordinary data adeptness and imposing trust. Yaqoob et al. [4] elaborated opportunities and challenges regarding Blockchain adaptation in the healthcare sector. Research stated that the convergence of Blockchain, vital privacy issues can be modelled to healthcare industries relating to data features, availability, and security can be resolved. Thus, it is important to define ruleset to empower the pervasive implementation of technology.

Singh et al. [5] presented a patient-centric strategy of a distributed healthcare administration system with Blockchain-based 'electronic health record (EHR)' using smart contracts, hyper-ledger fabric and composer technology, which assures the defense of the suggested model. The performance of the projected architectural context (latency and throughput) was tested based on pre-defined benchmarks. Configuration parameters (CPU usage, traffic in and out) were tuned rapidly to gain optimum outcome.

Celesti et al. [6] illustrated a Data Anonymization Module (DAM) framework, which was liable for hiding the patient's classified data in EHR. The smart contract admits the participation constraints such as privacy-aware patient/doctor identification, illness, and rug codes, which were stored in a simple data structure. The hash code generated against each transaction was buffered in MongoDB and was later used for authentication. To justify the validity of framework, Ethereum hybrid network was implemented, and experimental outcome portrayed that process cost and response time was diminished as compared to an unconventional public Blockchain approach.

Su et al. [7] proposed an attribute-based signature scheme with feature reversal to guard the confidentiality of the user's identity in Blockchain-Based Healthcare System. Under the proposition of exhausting attributes to classify users and shield their characteristics, the user collects the feature master-key to ensure an easier system management.

3 General architecture of Blockchain

Blockchain is a grouping of computers that are interrelated to each other as an alternative to a central administrative computer, meaning that the entire system is distributed. All Blockchain configurations fall into four types: (a) unrestricted (public), (b) reserved (private), (c) hybrid (private and/or public) and (d) confederation. The feature-driven comparison is as followed:

Deployment of any category should impose (a) enhanced capacity, (b) improved security, (c) immutability (i.e., immutable ledgers), (d) faster clearances, and (e) decentralization. Typically, a Blockchain network encompasses a set of stakeholders, which possesses a matching duplicate of the ledger. A Blockchain ledger is distributed since no particular node has possession of owning it. As an alternative, all simulated replicas are retained in consensus. This phenomenon guarantees transparency, operation resilience, and quicker dispute resolution. According to Table 2, Blockchain has a huge environmental cost (i.e., carbon footprint (Power Consumption per Transaction)). Moreover, nonexistence of common regulation/standard, network enhancement imposes complexity, which makes it harder to harvest appropriate benefits.

4 Proposed methodology

4.1 Security, trust-administration, and performance optimization of Blockchain

4.1.1 Focused case study for healthcare

Medical informatics (MI) emphases on the information technology that empowers the operational aggregation of data by means of technology tools to progress curative information and to expedite the provision of patient health care. The aim of MI is to guarantee access to precarious patient health data at the accurate time and system. Blockchain in healthcare conveys subsequent security, transaction proficiency, and convenience to the diligence. Virtually every task through the healthcare significance chain is clued-up for a Blockchain solution. For example, medical indemnification requires bulky sets of data to plan procedures and custom-built policies, register and progress claims arbitration, and achieve broker-billing disbursement. Even healthcare equipment necessitate efficient flow of source data. The proposed system will contribute to:

(a) Can provide a highly synchronized parameter, presenting scalability, security and uptake with current/legacy systems.
(b) Can provide a safe and well-organized policy for altering and authenticating the patient's identity.
(c) Provides admission to the distributed, real-time, non-volatile databank with clear (i.e., unencrypted) distribution of information for oversight administration.

4.1.2 Adopted rules and standards for private Blockchain

Any disseminated ledger used by a healthcare facility requires process harmonization. Scattered ledgers were programmed to assert authorized data, following the prerequisite process to analyze it. During system design, one observed issue with a broadcast Blockchain was the absence/diminishing impact of privacy of the pooled records. Once an event is occurred, it will generate source data that is stored on edge node and transmitted to affiliate networks. Authorization for ingress and egress data flow depends on subsequent pre-defined guidelines. In case, if there is a trust deficit among interlinked nodes, deployed system enforces a verification protocol to validate the corrections. Conventional elements, which establish the distributed ledger are: (a) data may be stored on a single node or may being exchanged among connected nodes, (b) dissimilar rules may be applicable to individual record depending on source and destination node, (c) ciphering may be practiced on stored or transmitted data stream, and (d) regardless of storage and processing server jurisdiction, all data (sensitive or commercial) should be disseminated as per pre-programmed rules. The following data protection concerns were addressed while implementing the rules:

(a) Generated, processed, and analyzed data formats constitute fundamental interoperability proficiencies. Local (Saudi Arabian) privacy laws were honored for data regulations. Data was segmented as confidential, and sensitive.
(b) In healthcare environment, data protection laws do not apply for unidentified or pseudonymous individuals, so, such data was considered as personal (sensitive).
(c) Outsourced data repositories were considered equally responsible for safeguarding data reliability and protection.
(d) Cross-border data transfer (i.e., electronic transactions, electronic documents and subsequent amendments in distant devices has followed the Gulf Cooperation Council (GCC) consensual data protection rules. To abide by conditional changes (i.e., privacy and data protection laws), stakeholders must understand each piece of applied technology.
(e) Implement flexible procedures concerning Blockchain that are equipped for a rapidly changing technology landscape.
(f) Distributed ledger's performance (i.e., process latency) and capability restrictions (i.e., ratio of energy consumption, scalability, maintenance, and data immutability) were addressed in context of P2P network interaction, transaction data storage and applied consensus algorithm.

4.1.2.1 Blockchain consensus using Rampant Smoothing (RTS) Algorithm Blockchain general architecture rely on independent computing nodes, predefined data structure to buffer transactions (i.e., records), linkage protocol to sequence blocks in a defined order, an analyzation and verification process to validate any change in selected blocks and consensus protocol to conduct the required operations. Each block holds (a) payload, (2) hash of block and (c) hash of preceding block. In proposed scheme, SHA-384 [8] was used for hashing of constant block size of 1088 bits each.

Pseudocode 1. Create an additional block using preceding block's hash

```
functopn createBlock (preceding_Block, Process int, address string ) (Block,
malfunction) {
       var additional_Block
       t_Interval := timestamp()

       additional_Block.Index = preceding_Block.Index + 1
       additional_Block.Timestamp = t.String()
       additional_Block.Process_Administration = Process_Administration
       additional_Block.PrevHash = preceding_Block.Hash
       additional_Block = calculateBlockHash(newBlock)
       additional_Block.Validator = address

       return additional_Block, nil
}
```

Figure 1 demonstrates why a Blockchain system is generally viewed as a secure platform as all engagements performed by system contributors are registered and distributed openly in the ledger; it is difficult to edit a block without identifying it. The Blockchain setup delivers the level of integrity and data protection that is mandatory to operate IoMT modules decentrally without having to depend on third-party amenities. In context of RTS, it was assumed that consensus is a procedure used to accomplish settlement on a distinct data value among disseminated progressions or methods. A consensus process tolerates the Blockchain to authorize and settle transactions and procedures, devoid of the necessity for a third-party arbitrator. When an operation is in progress, miners of the Blockchain instigate algorithms to decipher a cryptographic mystery. The solution to the rebus conveys the subsequent block to be attached to the Blockchain. The conundrum is challenging, but the high-performance computing and processing infrastructure solves the enigma. Private Blockchain infrastructure consumes relatively less energy with higher transaction processing speed in comparison with Public Blockchain (Table 1). Proposed method envisioned consensus protocol to be fault tolerant, furnishes proof of elapsed time, and importance, and must be rigid against DDoS attacks (i.e., a requirement if using consortium Blockchain).

For consensus of any transaction, any given node can have one out of three states: (a) follower state, (b) candidate state, and (c) leader state. Asynchronous system was designed to address the diverse operational requirements of healthcare computing infrastructure. Each device retains a particular native state and can exchange data blocks with other devices. RTS semantics nets driven algorithm was programmed for the potential "steps" that a system can conduct throughout transaction execution. RTS algorithm uses flexible regression modeling to build a conjecturing model without encoding any explicit parameters. RTS analyzes a 'biased average' of all transmission logs to assess the 'response time series dataset'. The outcome weight tends to shrink periodically, rather than hold the persistent ratios. The weights are reliant on perpetual factors, which is recognized as the invariable constraint. The procedure tolerates diverse features in the coding and the deciphering series, so the system can use related block in the encoder and neglect it from the interpreter.

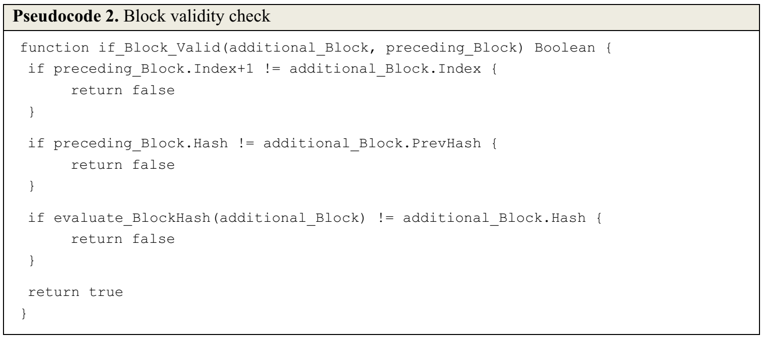
As a security prospective, scheme abide by the regional compliance regulations (e.g., ISO/IEC 27001 [13]) with respect to device necessities regarding data location, amenity

Table 1 Assessment of existing methodologies for healthcare using Blockchain

References	Contribution	Advantages	Disadvantages
De Aguiar et al. [9]	This investigation targeted to address scientific perspective into the applications of the Blockchain healthcare domain knowledge. It sets out by illustrating the administration of healthcare data, as well as the internal distribution of records (text, images, videos, etc.)	Evaluated and presented detailed analysis of benefits and restrictions of the Blockchain related to the medical information	Administration (interchanging medical data at a marketplace) and assessment of medical information access log handling was not elaborated
Fekih et al. [10]	The presented research has acknowledged numerous use cases in the applied Blockchain technology, for example for allocation of EMR, for inaccessible patient nursing, and for medication supply chain	Highlighted research challenges and opportunities that is associated with implementation of domain specific (healthcare) Blockchain network	Limitations related to scalability, security, and privacy of Blockchain technology were not comprehensively addressed
Tariq et al. [11]	Presented a novel security framework for industrial IoT and used Blockchain technology as a participating factor to ensure 'zero-trust security'	Applied a historical threat assessment model to evaluate the data breach ratio from integrated and optimized network devices	Authors did not compare and evaluate the alternative available technologies, such as consortium or hybrid Blockchain paradigm
Jennath et al. [12]	Researchers uncovered the likelihood of implementing reliable Artificial Intelligence methodologies over Blockchain, where a privacy-aware policy for data distribution was programmed	Traceability of source data that is required for constructing and exercising the AI ruleset was taken in an unchallengeable dispersed database	Presented method was not tested and applied to anonymized datasets. Furthermore, the scenario of patient's agility and easiness of handling permissions were highlighted but not effectively expressed in implementation scenarios

provisioning, data discovery requirements, and place of discretion. Applicability of stated regulations deeply impacted on inherited and shared controls (processes), for example: The likelihood at stage $S+1$ is identical to a weighted normal among the current reflection xT and the prior estimate $\hat{}yS|S-1$: $\hat{}xT+1|t=\alpha xS+(1-\alpha)\hat{}xS|S-1$. at this point $0\leq\alpha\leq1$ is the consensus factor. The efficiency of consensus protocol depends on real-time liveness, fault tolerance and security rules, which a node should abide by.

The prime aim of the RTS consensus protocol is to permit the device to interconnect among other devices and bargain a shared set of corroborated transactions, which can be embedded in the ledger. At this level, computation method enquires the discrete protocol about the judgement on the communication. Once an inference is realized, the node broadcasts the conclusion with other nodes in the network. Conclusively, a consensus judgement is compiled based on the total number of judgements acquiesced by all the nodes. This methodology enables a low overhead on the performance of the emulated provision. RTS algorithm demonstrated resilience for the characteristics such as 'crash fault tolerance, verification speed, transactions per second (TPS) throughput, and Byzantine fault tolerance.



Pseudocode 2. Block validity check

```
function if_Block_Valid(additional_Block, preceding_Block) Boolean {
 if preceding_Block.Index+1 != additional_Block.Index {
      return false
 }

 if preceding_Block.Hash != additional_Block.PrevHash {
      return false
 }

 if evaluate_BlockHash(additional_Block) != additional_Block.Hash {
      return false
 }

 return true
}
```

With implementation of novel RTS, the transaction verification process was improved, even in scenario where certain network linked nodes encounter computational mistakes, regardless, it will add only a single copy of the Blockchain. It is worth highlighting that the alternate consensus mechanisms such as 'proof of work' or 'proof of stake' requires hefty amount of computational power, are resource biased, exhibit higher latency and may depends on dedicated hardware.

4.1.3 Consistency

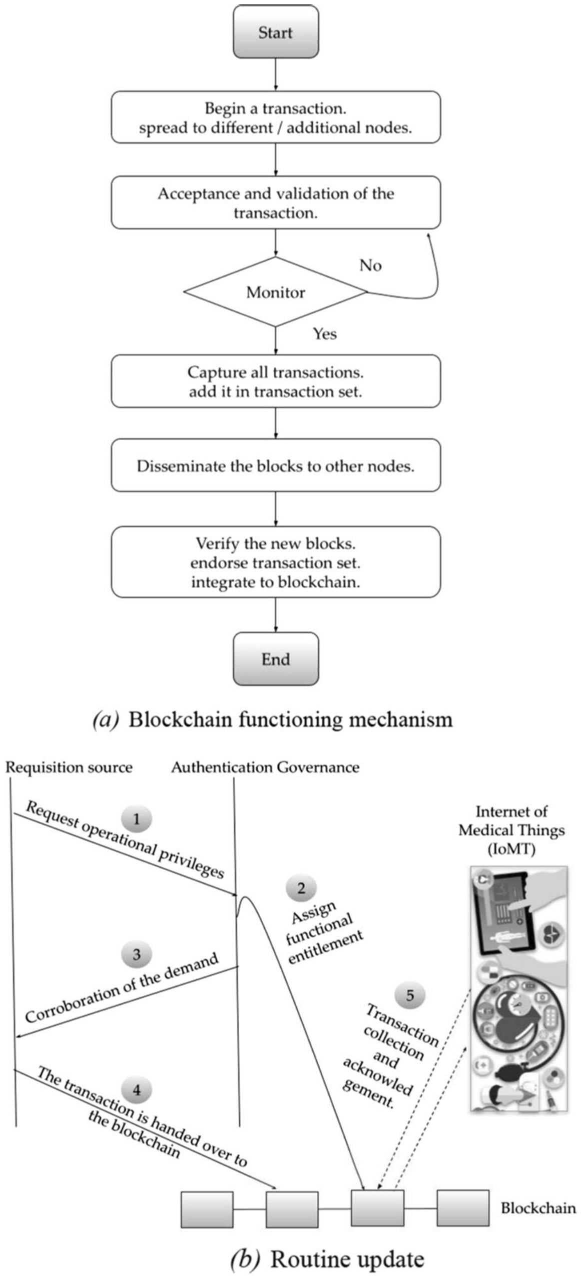
Procedure consistency was implemented as a system, which is programmed to support operational strategy. It makes the system more viable for the reason that administrators or automated auditing processes are able to assess strengths and faults and discover the vulnerable modules. In order to guarantee model conjunction, a classification must identify variances between numerous copies of disseminated data. This involves two parts: (a) swapping versions of data among servers; and (b) selecting a suitable final state when synchronized updates (i.e., read, write and asynchronous) have transpired. Consistency protocol was valuable in the following contexts: (a) data related to performed operation (i.e., initiated, continuous, completed process), (b) comparative imperative of non-overlapping operations, and (c) session of an operation. Implemented procedure follows the same universal principle: aggregated log data is accurate if and only if system can validate it, by supplementing it with some supportive data that clarifies the pragmatic return values (i.e., data type semantics, ordering guarantees, and convergence guarantees). Additionally, epidemic protocol [14] was applied, in which, nodes broadcast native updates to scattered nodes by sporadically propagating a "summary" demonstrating the collective conclusion. This feature is curricular to identify and blacklist any frequent adversarial behavioral (i.e., phishing, bitpoint hack, bugs (associated with 'replication and consensus, validity, agreement, termination')) device.

4.1.3.1 Temper resistance In the occurrence that an attack is sprung in the presence of an active prevention method, attack recognition procedures challenge to discover the attack as early as possible. The intervened time interval amid to the initiation of an anomaly and its exposure (the detection expectancy) signifies a period of defenselessness, and prerequisites to stay at minimum level. Likewise, any functional and secure system should be temper resistance to prevent illegitimate alteration of data. Within selected

Table 2 Detailed comparison of Blockchain categories

Property	Blockchain categories		
	Private	**Public**	**Confederation**
Trust	Needs trust-building	Trustable	Trustable
Competence	High	Low	High
Centralized	Partial	No	Partial
Unanimity process	Yes	No	Partial
Permission (Read)	Hybrid (restricted or public)	Public	Hybrid (restricted or public)
Permission (Write)	Interdentally controlled	Public	Specified devices
Transaction speed (TPS)	Fast (approximately 2400 TPS)	Slow (approximately 7 to 15 TPS)	Fast
Immutability	Tempering is possible	Tempering hard or impossible	Tempering is possible
Proof-of-stake (Minting)	Eligible	Eligible	Eligible
Power consumption per transaction (with network of 104 devices)	101 J	103 J to 108 J	–
Scalability	Dependent on network size (traffic and throughput)		
Example	Corda, etc	Ethereum, etc	R3, etc

Underline: It is a 'Naming Convention' that refers to a convention (agreed scheme) for naming things

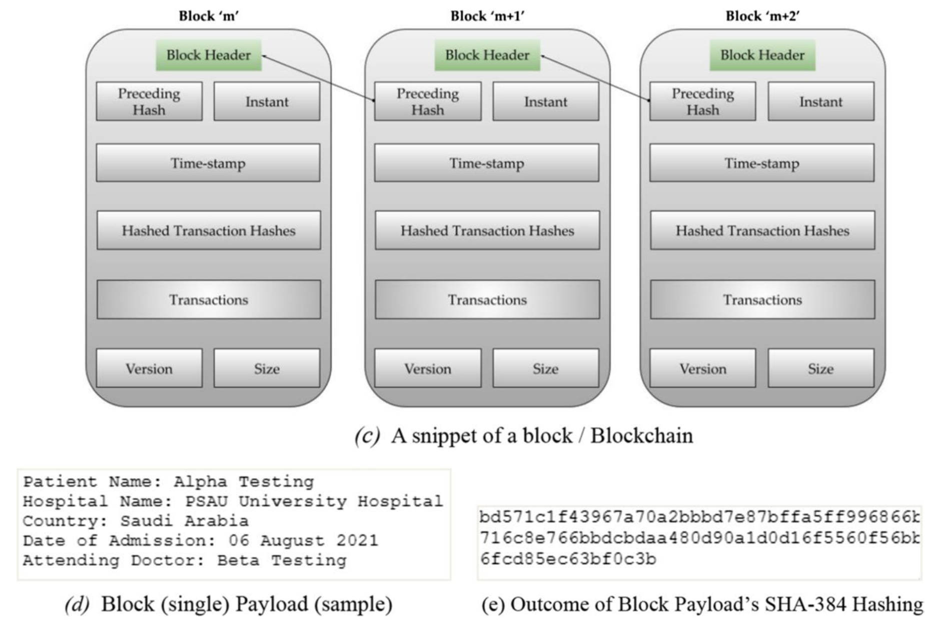

Start
Begin a transaction.
spread to different / additional nodes.
Acceptance and validation of the transaction.
Monitor
No
Yes
Capture all transactions.
add it in transaction set.
Disseminate the blocks to other nodes.
Verify the new blocks.
endorse transaction set.
integrate to blockchain.
End
Requisition source
Authentication Governance
1
Request operational privileges
2
Assign functional entitlement
3
Corroboration of the demand
4
The transaction is handed over to the blockchain
5
Transaction collection and acknowled gement.
Internet of Medical Things (IoMT)
Blockchain

(a) Blockchain functioning mechanism

(b) Routine update

Fig. 1 Individual block's Payload and Hashing outcome. Each block holds **a** payload, (2) hash of block and **c** hash of preceding block. In proposed scheme, SHA-384 was used for hashing of constant block size of 1088 bits each. Within selected Blockchain setup, cryptographic hash (SHA-384 (as mentioned in this figure)) methodology enables: **a** address derivation, **b** generation of unique identifiers, and **c** block payload and header's integrity. Blocks were connected together through each block, comprising the SHA-384 (hash) digest of the preceding block's header, thus creating the Blockchain. If a formerly distributed block was altered, it would yield dissimilar hash. By linking the original state and the capability to authenticate each block, handlers can autonomously approve the present state of the Blockchain

Blockchain setup, cryptographic hash (SHA-384 (as mentioned in Fig. 1)) methodology enables: (a) address derivation, (b) generation of unique identifiers, and (c) block payload and header's integrity. Blocks were connected together through each block, comprising



(c) A snippet of a block / Blockchain

```
Patient Name: Alpha Testing
Hospital Name: PSAU University Hospital
Country: Saudi Arabia
Date of Admission: 06 August 2021
Attending Doctor: Beta Testing
```

(d) Block (single) Payload (sample)

```
bd571c1f43967a70a2bbbd7e87bffa5ff996866b
716c8e766bbdcbdaa480d90a1d0d16f5560f56bb
6fcd85ec63bf0c3b
```

(e) Outcome of Block Payload's SHA-384 Hashing

Fig. 1 continued

the SHA-384 (hash) digest of the preceding block's header, thus creating the Blockchain. If a formerly distributed block was altered, it would yield dissimilar hash. By linking the original state and the capability to authenticate each block, handlers can autonomously approve the present state of the Blockchain. During experimentation, it was observed that some systems within the setup would lack real-time data or have different information. This factor was influenced by system latency (i.e., due to 'low memory space, legacy transmission medium, and number of active network devices') of linked devices. Latency was measured with consideration criteria of (a) Round Trip Time (RTT), and (b) Time to First Byte (TTFB). Hard fork [15, 16] technique prevented backward node compatibility and was applied during optimization process of 'node temper resistance'. Hard forking method enforces those non-updated nodes to discard any block that does not obey its rule (i.e., RTS) of the block requirement.

It is worth mentioning that a defunct Blockchain may not be appropriate for an archived dataset, as devoid of numerous publishing nodes, an adversary could certainly subjugate the limited publishing nodes and interchange required number of blocks.

4.2 Blockchain service

As per Blockchain layer stack, proposed scheme utilized following layers to function appropriately: (a) Application layer (to host decentralized application), (b) Transport layer to manage TCP communication state, (c) Modeling/Contact layer to manage HTTP connection state, (d) Data layer to manage stored information both in database and Blockchain itself, (e) Network layer to manage P2P communication and ensure privacy of shared information, and (f) Semantic layer to follow the ruleset regarding to identify relationship of chained blocks (i.e., previous and forward linked blocks).

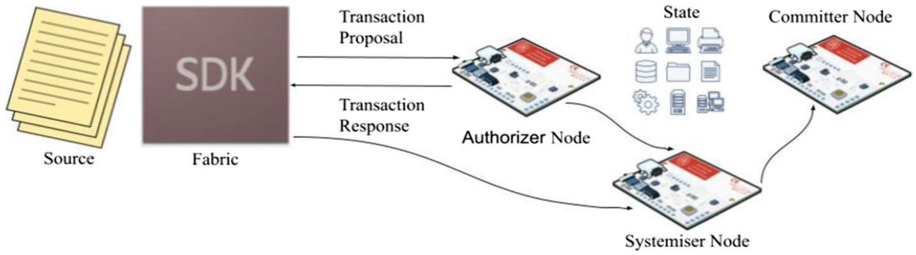


Fig. 2 Basic transaction flow (Hyperledger Fabric). For proposed scheme Hyperledger Fabric modular architecture (Figure) was applied for Blockchain execution. It contributed as exclusive methodology to consensus that permitted a highly modular and efficient (i.e., low latency) permissioned architecture while maintaining privacy. Fabric consists of source, peer, systemiser, and service provider. Service provider manages stakeholder ID and authenticate service users to permit access to the network in which transactions were programmed as per shared ledger in pre-specified regular order.

By splitting out the Blockchain into several layers, scheme was able to manage and mature several properties (such as Security, Liveness, Stability, and Correctness).

4.2.1 Smart contract modeling

A smart contract is a conjoint settlement between stakeholders. It buffers the data, procedure inputs, and write yields based on preset functions. Presenting an original smart contract in the Blockchain is empowered by triggering the constructor utility through a functional operation, whose source turn into the smart contract possessor with an inherent capability to trigger self-destruct function. For proposed scheme Hyperledger Fabric modular architecture [17] (Fig. 2) was applied for Blockchain execution. It contributed as exclusive methodology to consensus that permitted a highly modular and efficient (i.e., low latency) permissioned architecture while maintaining privacy.

Fabric consists of source, peer, systemiser, and service provider. Service provider manages stakeholder ID and authenticate service users to permit access to the network. Proposed method utilized both local and channel-oriented service provider to administer provisions at any level. Source is used to process and communicate any given transaction (read and write data in-state database) on the network using SDK. Node is referred to as logical function that is executed on physical server machine. Nodes are eligible to be grouped in a 'trust domain,' which are distributed logical entities that can be controlled. Nodes may have three states: authorizer, systemizer and committer. Transactions were programmed as per shared ledger in pre-specified regular order.

4.3 Resilience against majority consensus attack (MCA)

Private Blockchain present authorizations to avert certain users in the general entities from accessing all the data on a Blockchain. Medical-IoT systems generate gigantic volumes of data to analyze and buffer, and occasionally private-Blockchain cannot bear the load (hash (SHA-384) rate). Transaction handling in Blockchain exhibit that considerably longer block sizes and block streams will suggestively be time-consuming to process that require to be fully corroborated to be attached to the chain. Proposed scheme was evaluated against MCA by governing the majority of the computing authority on the setup, an attack scenario was intended to affect with the progression of recording new blocks. Through data outcome of proposed scheme, it was observed that altering historical blocks would be particularly challenging in the occurrence of a MCA.

As a countermeasure, multi-tier resistance techniques were applied against a MCA. For example, the number of authorization requests were increased, the confronting entity was rejected and to enforce more aggressive defense, the offensive entities were itself be confronted via a DDoS [18]. It is worth highlighting that as the aggressor has to wait for the operation/process to be complete before initiating MCA, an informal resolution to the identified problem was programmed by up-surging the amount of verifications before making an allowance for the transaction to be fully finalized. Implementation of this scenario provided a greater defense against MCA but also enhanced the process latency of designed Blockchain.

4.4 Privacy decentralization

End-to-end technology run on Blockchain qualifies the classified data to be exchanged securely, whereas handlers continue to be able to regulate their records. Certainly, privileged information is an extremely treasured resource and can be acquired to misuse by adversary. By enabling end-to-end systems to run on Blockchain, proposed decentralized solution empowers confidential data to be transmitted securely, whereas handlers are eligible to be in full control of their information. Decentralized level of privacy-aware defense was accessible by the handler and the internal/external system.

In case of bulky data payload, scheme used 'off-chain transaction protocol', which trigger its functionality when any non-transactional data that is excessively outsized was kept resourcefully in the Blockchain, or, it necessitates the capability to be transformed or removed.

5 Experimental results

Blockchain technology executes on three key philosophies that are decentralization, data privacy, and scalability. The derived technology itself had fundamentally diverse practices as it is applied to dissimilar operational settings by healthcare firms in quest of discovering it's prospective. We envisioned outcome necessity of applied Blockchain as:

(a) For enhancing the performance improvements of the system through refining the established routine and scalability of the programed methods.
(b) Improved resource exploitation so that numerous transactions can be administered
(c) Gain rich perceptibility into the exclusive activities and capability features of Blockchain applications.
(d) To gain capability to testing with Blockchain-specific setup formations, comprising specific CPUs, and energy metering.
(e) For prevention of adversarial effects of tentative (and hypothetically malicious) Blockchain set-up behavior on other functional applications (such as, pervasive, protected network protocols, provable identity and validation application of all contributors, application to securely store electronic health records (privately), etc.).

5.1 Experimental setup

For experimentation of proposed scheme, following flexible and scalable (client/server) hardware/software criteria was used:

The basic implementation exploits the network and consensus layers to assemble fresh blocks chronologically in a chain. In this context, the throughput, runtime performance, extensibility and generality were analyzed by examining the log data. Table 4 illustrates the core input parameters for the emulator.

Input parameters were optimised inconsideration with the number of participant devices, intensity of block transmission and block interval time. Emulation considered each device as an object with a unique ID. Devices were able to handle buffered transaction pools. Each block was assigned with attributes, such as current block-ID, previous block-ID, block-size, number of handled transactions to select suitable ledger. To achieve mentioned goals, RTS consensus protocol was applied.

5.2 Computation time

In comparison with traditional Blockchain, implemented transactional scheme portrayed following characteristics: high (efficiency), reduced latency (scalability), harder to perpetrate, high transmission rate, immune to shadow chain attacks, low (central dependency), high (security), user privacy (physician can only assess record with patient's consensus) and simpler to implement smart-contracts.

Figure 3 illustrates the computational time (latency (in milliseconds)) intake of node for adapted transaction authentication and records access on the existence of a diverse sum of partaking nodes. Amdahl's law [19] was practiced to compute both parallel (N_p) and serial (N_s) transactions. It was observed that by intensifying the number of applied processes (M), the input of N_s in favor of consumed time will remain same. Whereas, N_p will diminish by a factor of M.

$$N(M) = N_\mathrm{s} + \frac{N_\mathrm{M}}{M} \tag{1}$$

Latency of serial processes is:

$$\text{Ratio of serial iteration} = \frac{N_\mathrm{s}}{N_\mathrm{s} + N_\mathrm{M}} \tag{2}$$

Latency of parallel processes is:

$$\text{Ratio of parallel iteration} = \frac{N_\mathrm{p}}{N_\mathrm{s} + N_\mathrm{M}} \tag{3}$$

The investigational outcome demonstrates that the transaction authentication time is larger than the data access time. This is for the reason that numerous authentications such as accounts, exist. Moreover, the admittance to meta-data and endorsement of the transaction is not process intensive, which result in efficiency (in terms of time-consumption).

Hence, the performance of the proposed mechanism is described by the resulting (as shown in Fig. 4):

- *Consistency* The projected technique can handle data with a greater consistency for the reason that of the proficiencies of Blockchain technology.
- *Decentralization* The offered methodology can be applied to project processes that can evade dominations, by means of certain protocols in Blockchain technology, such as consensus systems.
- *Scalability* The recommended project can provision scalability by applying hybrid practices in the synthesis of Blockchains and medical-IoT systems.
- *User privacy* The endorsed methodology can deliver unrecognizability for handlers via P2P and Blockchain technologies.
- *Security and privacy* Blockchain technology guarantees that handlers' data are secure, and integrity is preserved

Figure 5 discover the regular latency performance of RTS and Hyperledger Fabric under situations in which the consensus technique is set up, with the homogeneous evaluation environment (i.e., transactions and device types). Initially, the utilization of each consensus method has presented the specifics of the growing latency equated to the closed condition (consensus on and off). Dissimilar consensus procedures make the regular latency of RTS method considerable lesser than commonly used hyperledger.

One vital experimental outcome is that the chain authentication method was achieved quicker and consumes a lesser amount of energy when connections are clustered in a block. Figure 6 represents when there are four or eight connections clustered in one block, the total processing time per block can be diminished roughly 35–50%.

6 Analysis and discussion

To evaluate the system stress testing, the implemented method was assessed in context of block regeneration in order to offer reliability and efficiency. The novel data 'Y' was characterized by the eigenvalue (i.e., an communication comprising of uncategorized) '$Y_m(d)$' over GF(2^m) of the system $Y_m(d) = \sum_{s=0}^{f-1} f_s d^s$, for $f_s \varepsilon \{0, 1\}$, where the maximum proponent of the variable 'd' is termed as the amount of the eigenvalue. Here, GF(2^m) indicates the effective computations in finite cryptosystems [20]. Error identification was optimized by distributing the entire exemplification array into the valid series (i.e., aggregated log associated to block generation, association and consensus validation) and illegitimate series. An error arises when the Blockchain transaction outcome falls into an illegitimate series.

To avoid system process interruption in the case of methodological failures and adversary-attacks, keeping a stability of transaction associated block data is very significant. In this context, the *response eigenvalue* is '$Y_m(d)$' where degree $Y_m(d) < Q$. Therefore, the entire input size roughly equals to 'Q'. The sum of blocks required for residues is equal to $Q^\wedge$ in the worst case scenario. The block redundancy dilapidation in dissimilar blockchains are the proportion of the implicit data size to the actual dataset minus 1:

$$E = \frac{Q^\wedge}{Q} - 1 \tag{4}$$

Table 3 Applied hardware and software configurations for hyperledger fabric blockchain infrastructure

Class	Clint device	Server device
Operating system	Microsoft 64-bit Windows 10 Pro	Ubuntu Server (20.04 LTS)
Processor	Quad Core 2.0 GHz	2nd Generation Intel Xeon Scalable processors
Chipset	Intel® W480E Chipset	Intel C246 chipset
Number of participants	598	2
Average storage required	Up to 200 GB at each device	3 Terabyte 2933 MHz TruDDR4 memory
Maximum internal storage	8 TB	61.44 TB using 16 × 3.84 TB SAS/SATA SSDs
RAM	Newegg DDR (16 GB per Module)	Newegg DDR (128GN per Module)
Memory protection	Error-correcting code (ECC)	Error-correcting code (ECC)
PCIe slots	PCI-E × 16 ports	7 PCIe slots
Network	Gigabit Ethernet, N-Band wireless	Intel X710-DA2 PCIe 10GbE 2-Port SFP + Ethernet Adapter
NodeJS	Version: 14.17.4	Version: 14.17.4
Internet connection	100 Mbps/T1/Fiber Optics	100 Mbps/T1/Fiber Optics
Connected routers	Gigabit Ethernet, N-Band wireless	Gigabit Ethernet, N-Band wireless
High-efficiency power supply	80 PLUS Platinum certified device	80 PLUS Titanium certified device
Cooling	One non-hot-swap system fan	Four non-hot-swap system fans
Smart contract queries	Using SQL	Using SQL
Crypto implementations	Pluggable	Pluggable
Total record size		27.3 GB
Average patient record size (text, numbers, and images)		2000 KB
Blockchain size		Approximately 593 GB
Total number of blocks		7 million
Computation, authentication and contact time		In milliseconds
Average time for record access from the native DB		45 ms
Average record and block distribution cost		22 Gigabit per second, with overhead of 2 megabits per second
Programming language		Solidity (i.e., aimed at developing smart contracts)

Table 4 Input considerations for the emulator

Type	Parameter	Description
Devices	Dn	Total number of interlinked devices
Blocks	B size	Block size in Kbs
	B intermission	Normal time to produce a block in seconds
	B interruption	Dissemination adjournment of in seconds
Transactions	T size	Transaction size in Kbs
	T adjournment	Dissemination adjournment of in seconds
	Tn	Transaction creation ratio
	T method	Method for forming transactions
	T on/off	Allow or Restrict transactions

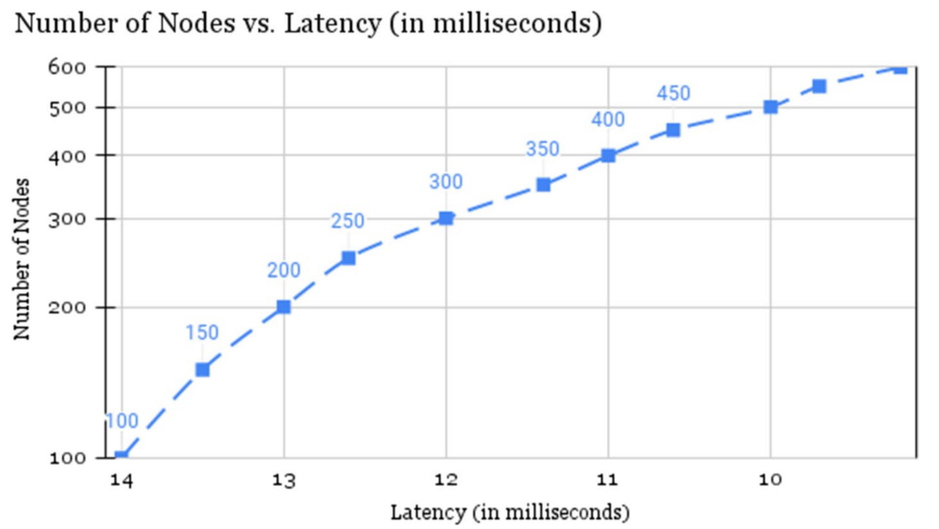


Fig. 3 Computational latency for the transaction authentication and data contact. This figure illustrates the computational time (latency (in milliseconds)) intake of node for adapted transaction authentication and records access on the existence of a diverse sum of partaking nodes. Amdahl's law [19] was practiced to compute both parallel and serial transactions. The investigational outcome demonstrates that the transaction authentication time is larger than the data access time. This is for the reason that numerous authentications such as accounts, exist. Moreover, the admittance to meta-data and endorsement of the transaction is not process intensive, which result in efficiency (in terms of time-consumption)

RTS method selected $f_s(d)$ because $a_s(d)$ applies at most $q_1 = q_2 = \ldots = q_o$ blocks or blockchains. Therefore, the transaction driven block duplication in dissimilar link copies is $o/v - 1$

$$E = \frac{Q^{\wedge}}{Q} - 1 = \frac{(o.e)}{(v.e)} - 1 = \frac{o - v}{v} \tag{5}$$

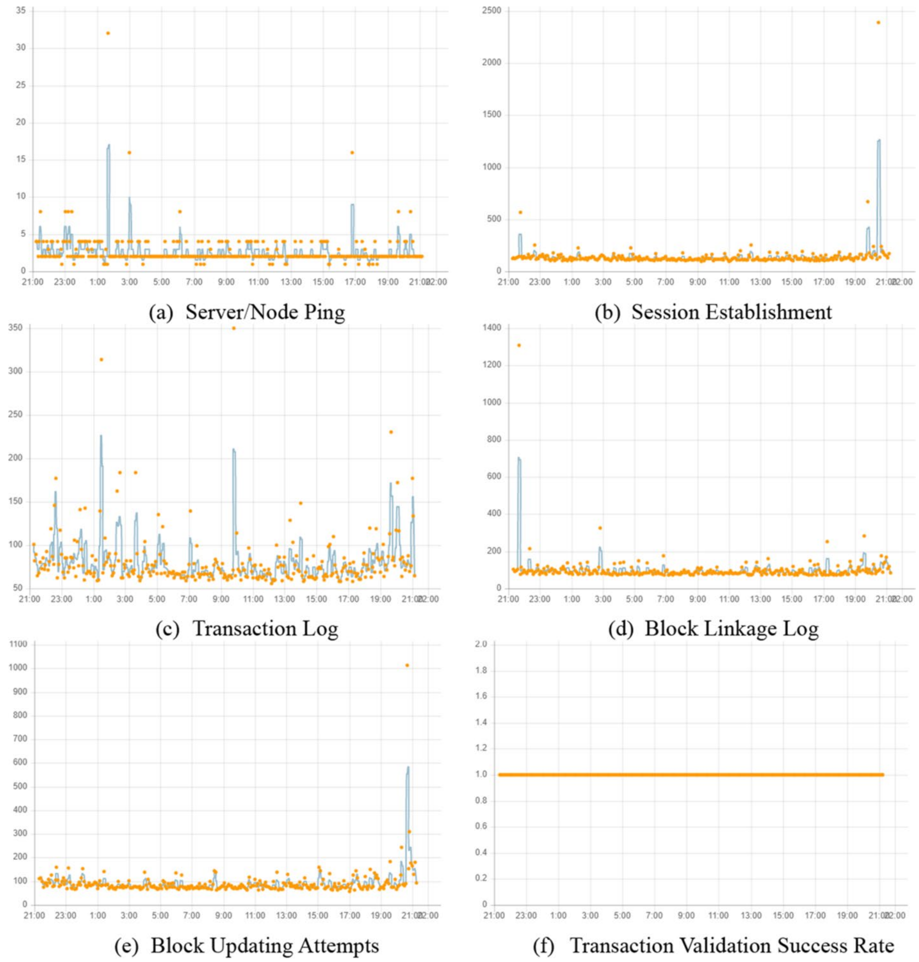
RTS decreases generated block's redundancy through periodic performance tuning of applied system. System efficiency was statistically evaluated as:

$$\text{Efficiency} = \frac{2^{60} \cdot v}{2^{66} \cdot \left(\log_{2\left(\left[\frac{g}{2}\right] \cdot e\right) \cdot g + [g/2]^2 \cdot e}\right)} = \frac{2^{14} \cdot v}{\log_{2\left(\left[\frac{g}{2}\right] \cdot e\right) \cdot g + [g/2]^2 \cdot e}} \tag{6}$$

As per experimental setup specification illustrated in Table 3, number of transactions which can be facilitated per instance are 2^{60}. To identify and fix at least one inaccuracy, 'v' has to fulfill the difference $v \leq o - 2$.

7 Discussion

Blockchain embraces the possibility to transform healthcare. As per technical prospective, connected computing nodes on the blockchain system will produce matching blocks when a linked device conduct any transaction. Due to integrity enforcement, modification to the data can be recognized. Projected paper proposed an optimized and automated consensus method, which intends to make the dispersed record keeping analogous to an integrated database. RTS necessitates a contributor device to verify



(a) Server/Node Ping

(b) Session Establishment

(c) Transaction Log

(d) Block Linkage Log

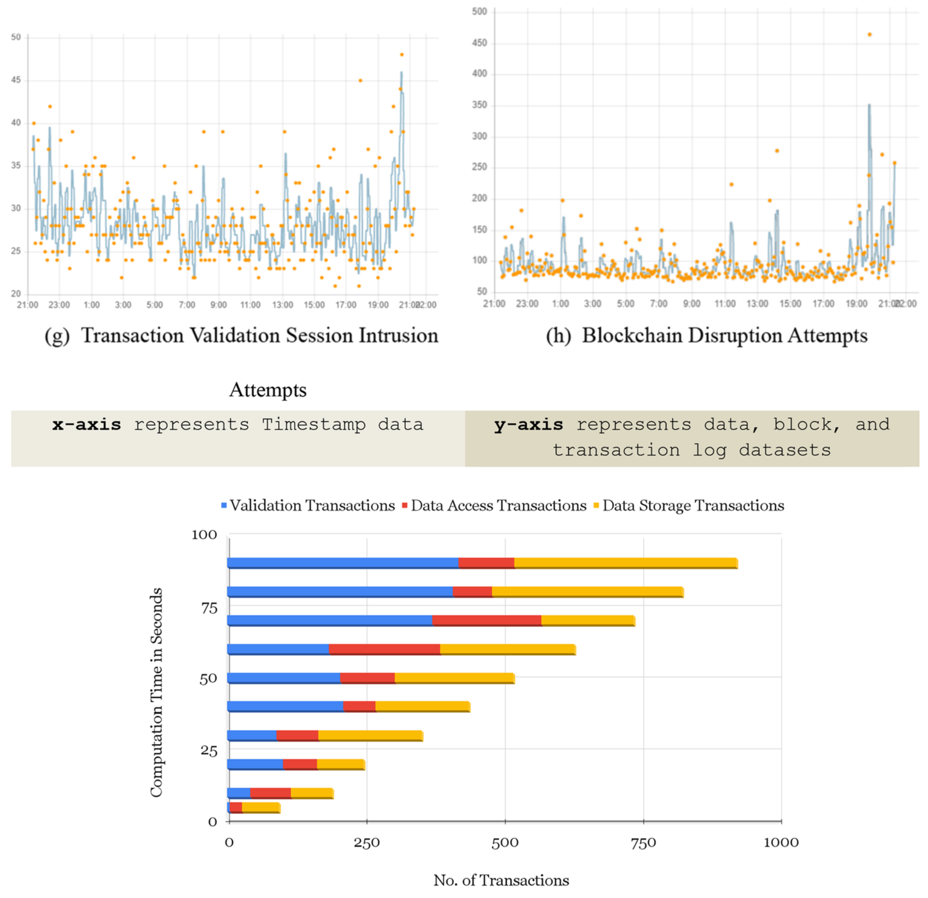
(e) Block Updating Attempts

(f) Transaction Validation Success Rate

Fig. 4 Mandatory computation period for completion of transactions. The performance of the proposed mechanism is described by the resulting (as shown in **a**–**i**): *Consistency*: The projected technique can handle data with a greater consistency for the reason that of the proficiencies of Blockchain technology. *Decentralization* The offered methodology can be applied to project processes that can evade dominations, by means of certain protocols in Blockchain technology, such as consensus systems. *Scalability* The recommended project can provision scalability by applying hybrid practices in the synthesis of Blockchains and medical-IoT systems. *User privacy* The endorsed methodology can deliver unrecognizability for handlers via P2P and Blockchain technologies. *Security and privacy* Blockchain technology guarantees that handlers' data are secure, and integrity is preserved

that the conducted and submitted transaction must meet the pre-defined requirements to qualify it to be a new integrated block to the Blockchain. During implementation of system, we realized that it consumes extraordinary time to establish and interlinking a block. Immense time consumption of required consensus necessities the efficient adoration of optimization scenarios which can obey pre-defined ruleset. As represented in Figs. 4, 5, 6, properties such as fault tolerance, scalability and latency was observed and analyzed. Analysis proved that architecting a worthy consensus protocol should reflect an applicable error and should be adoptive toward dissimilar application states.

Manuscript presented a wide-ranging conversation and assessment of the available options related to the applications of Blockchain, with an explicit concentration on the



(g) Transaction Validation Session Intrusion Attempts

(h) Blockchain Disruption Attempts

x-axis represents Timestamp data	**y-axis** represents data, block, and transaction log datasets

(i) Computational time in seconds Vs. Number of Transactions (*periodic successions (sample dataset)*)

Fig. 4 continued

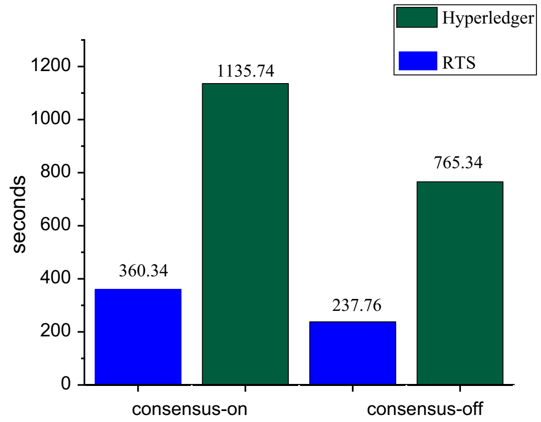


Fig. 5 Regular latency of RTS and Hyperledger with dissimilar consensus rulesets. This figure discover the regular latency performance of RTS and Hyperledger Fabric under situations in which the consensus technique is set up, with the homogeneous evaluation environment (i.e., transactions and device types). Initially, the utilization of each consensus method has presented the specifics of the growing latency equated to the closed condition (consensus on & off). Dissimilar consensus procedures make the regular latency of RTS method considerable lesser than commonly used hyperledger

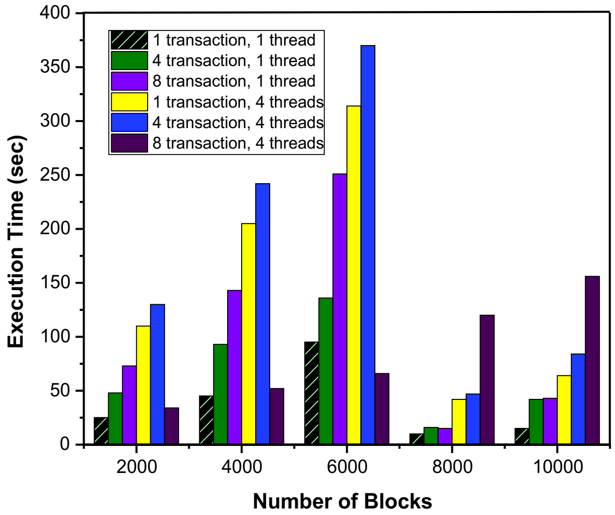


Fig. 6 Performance time of the chain authentication process. One vital experimental outcome is that the chain authentication method was achieved quicker and consumes a lesser amount of energy when connections are clustered in a block. This figure represents when there are four or eight connections clustered in one block, the total processing time per block can be diminished roughly 35–50%

Table 5 Adversary tolerance comparison between exiting schemes (PoW, PoS, and Deligated PoS) and proposed RTS

Attack Vectors	Consensus Methods Vs. Impact of Vulnerability			
	Proof of Work (PoW)	Proof of Stake (PoS)	Delegated Proof-of-Stake	Rampant Smoothing (RTS) algorithm
Sybil Protection Attack	☑	☑	☑	☑
Denial of Service	⊗	⊗	⊗	⊗
Pre-Computing Attack	⊗	☑	☑	☑
Censorship Resistance	☑	⊗	⊗	☑

☑ Effective safeguarding against malicious activity ⊗ Vulnerable to Malicious Event

incorporation of the Blockchain technology with the healthcare infrastructure. Applied application will resolve issues which include but not limited to:

(a) Issues which enforce transaction security to time consuming and energy intensive environments;
(b) Deciphering the confidentiality shield and scalability issues of the Blockchain;
(c) Ensuring legitimacy of data compressed in Blockchain;

Nevertheless, proposed scheme did not focus on:

(a) The event when the underlying ciphering procedure (SHA-384) compromise;
(b) How system will react when it encounters the storage of storage buffer to accommodate much lengthier and payload intensive Blockchain.

Table 5 indicates the performance properties of applied consensus methods. Comparative investigation was conducted to verify throughput, scalability (i.e., bottlenecks, memory access properties, and GPU consumption), latency and energy consumption. Experimental results outline that RTS showed better results when authentication, adversary tolerance, non-reputation, fault tolerance, scalability and latency were computed.

8 Conclusion

The implementation of new technologies in healthcare sector comes with consequences associated to the framework of the concerned technology. Adaptation of Blockchain can eliminate the necessity for arbitrators, thereby decreasing the counter-party hazards. Distributed ledger technology encourages transparency for all contributors in the transaction. Proposed method adopted a novel consensus methodology using Rampant Smoothing (RTS) algorithm, which guarantees integrity, security, and reliance in real-time for dispersed data structures. Contracts and additional vital data were buffered on the Blockchain, instituting a network of reliance between the involved parties. Smart contracts portrayed usability in terms of efficient tracing of health data. In forthcoming work, author aims to advance this research to discover other applicable evaluation metrics and corroborate outcomes using valid Blockchain-centered healthcare use cases. In case of conflict between two or more instances, any of the transaction which acquires the determined sum of validations from the network will be assembled in the blockchain, and the competitive transactions will be rejected. For optimization purpose, while implementing 'smart contacts', RTS was designed in such a way that bytecode, block number and block hashing is effectively indexed and efficiently retrieved by the applied system.

Abbreviations

RTS: Rampant Smoothing; GCDMP: Good Clinical Data Management Practices; EMR: Electronic medical records; GDPR: General Data Protection Regulation; HIPAA: Health Insurance Portability and Accountability Act; EHR/EMR: E-health/medical records; DAM: Data Anonymization Module; TPS: Transactions per second; MI: Medical informatics; GCC: Gulf Cooperation Council; DDoS: Distributed Denial-of-Service; ISO/IEC: International Organization for Standardization/International Electrotechnical Commission; RTT: Round Trip Time; TTFB: Time to First Byte; TCP: Transmission control protocol; HTTP: Hypertext transfer protocol; P2P: Peer-to-Peer; MCA: Majority consensus attack; LTS: Long term support; GB: Gigabit; MHz: Megahertz; RAM: Random access memory; DDR: Double data rate; ECC: Error-correcting code; Mbps: Megabit per second; SQL: Structured query language; ID: Identification; IoT: Internet of things; SHA: Secure Hashing algorithm.

Author contributions

The author read and approved the final manuscript.

Funding

The author would like to acknowledge the support of the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University under the research project 2021/01/17623.

Availability of data and materials

Raw and derived data supporting the findings of this study are available from the corresponding author [Usman Tariq] on request. Partial dataset can be downloaded from https://psauedusa-my.sharepoint.com/:f:/g/personal/u_tariq_psau_edu_sa/EtC_dpg5ctRLqJGie2w7d08BPZWSgRWNSArR_DfdKhrO4A?e=FHz2cf

Code availability

The programming code that supports the findings of this study will be available on request from the corresponding author [Usman Tariq].

Declarations

Ethics approval and consent to participate

All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Consent for publication

The Publisher has the Author's permission to publish the relevant contribution.

Competing interests

The author declares that he has no conflicts of interest to report regarding the present study.

Received: 10 February 2022 Accepted: 21 April 2022
Published online: 21 May 2022

References

1. C. Tikkinen-Piri, A. Rohunen, J. Markkula, EU General Data Protection Regulation: changes and implications for personal data collecting companies. Comput. Law Secur. Rev. **34**, 134–153 (2018). https://doi.org/10.1016/j.clsr.2017.05.015
2. G. Cohen, M.M. Mello, HIPAA and protecting health information in the 21st century. JAMA **320**, 231–232 (2018). https://doi.org/10.1001/jama.2018.5630
3. D.Y.T. Fong, Data management and quality assurance. Drug Inf. J. **35**, 839–844 (2001). https://doi.org/10.1177/009286150103500321
4. I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput. Appl. **S.I.: Healthcare Analytics**, 1–16 (2021). https://doi.org/10.1007/s00521-020-05519-w
5. P. Singh, N.R. Pradhan, A.K. Luhach, S. Agnihotri, N.Z. Jhanjhi et al., A novel patient-centric architectural framework for blockchain-enabled healthcare applications. IEEE Trans. Ind. Inform. **17**, 5779–5789 (2020). https://doi.org/10.1109/TII.2020.3037889
6. A. Celesti, A. Ruggeri, M. Fazio, A. Galletta, M. Villari et al., Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds. Sensors **20**(9), 1–12 (2020). https://doi.org/10.3390/s20092590
7. S. Qianqian, R. Zhang, R. Xue, P. Li, Revocable attribute-based signature for blockchain-based healthcare system. IEEE Access **8**, 127884–127896 (2020). https://doi.org/10.1109/ACCESS.2020.3007691
8. V. Thambusamy, S. Karthiga, Security based approach of SHA 384 and SHA 512 algorithms in cloud environment. J. Comput. Sci. **16**, 1439–1450 (2020). https://doi.org/10.3844/jcssp.2020.1439.1450
9. D. Aguiar, E. Julio, B.S. Faical, B. Krishnamachari, J. Uevama, A survey of blockchain-based strategies for healthcare. ACM Comput. Surv. (CSUR) **53**(2), 1–27 (2020). https://doi.org/10.1145/3376915
10. F. Rim, M. Lahami, Application of blockchain technology in healthcare: a comprehensive study, in *International Conference on Smart Homes and Health Telematics*, Hammamet, Tunisia (2020), pp. 268–276.
11. U. Tariq, A.O. Aseeri, M.S. Alkatheiri, Y. Zhuang, Context-aware autonomous security assertion for industrial IoT. IEEE Access **8**, 191785–191794 (2020). https://doi.org/10.1109/ACCESS.2020.3032436
12. H.S. Jennath, V.S. Anoop, S. Asharaf, Blockchain for healthcare: securing patient data and enabling trusted articial intelligence. Int. J. Interact. Multimed. Artif. Intell. **6**, 15–23 (2020). https://doi.org/10.9781/ijimai.2020.07.002
13. G. Culot, G. Nassimbeni, M. Podrecca, M. Sartor, The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. TQM J. **33**, 76–105 (2021). https://doi.org/10.1108/TQM-09-2020-0202
14. R. Poonam, P.P. Singh, A. Balyan, J. Shokeen, V. Jain et al., A secure epidemic routing using blockchain in opportunistic Internet of Things. Data Anal. Manag. **54**, 101–110 (2021). https://doi.org/10.1007/978-981-15-8335-3_10
15. S. Fabian, Blockchain forks: a formal classification framework and persistency analysis. Singap. Econ. Rev. **101712**, 1–22 (2020). https://doi.org/10.1142/S0217590820470025
16. S.R. Krishna, M.K. Manooj, T.R. Gadekallu, N. Kumar, P.K. Reddy, et al., A blockchain-based credibility scoring framework for electronic medical records, in *IEEE Globecom Workshop*, Taipei, Taiwan (2020), pp. 1–6
17. X. Xiaoqiong, G. Sun, L. Luo, H. Cao, H. Yu et al., Latency performance modeling and analysis for hyperledger fabric blockchain network. Inf. Process. Manag. **58**, 1–13 (2021). https://doi.org/10.1016/j.ipm.2020.102436
18. W. Sharyar, M. Imthiyas, H. Almohamedh, K.M. Alhamed, S. Almotairi et al., Distributed denial of service (DDoS) mitigation using blockchain—a comprehensive insight. Symmetry **13**, 1–21 (2021). https://doi.org/10.3390/sym13020227
19. M.Z.H. Zim, TinyML: analysis of Xtensa LX6 microprocessor for Neural Network Applications by ESP32 SoC (2021). arXiv:2106.10652
20. A. Halbutogullari, C.K. Koc, Parallel multiplication in GF(2k) using polynomial residue arithmetic. Des. Codes Cryptogr. **20**, 155–173 (2000)
21. A. Jabbar, S. Dani, Investigating the link between transaction and computational costs in a blockchain environment. Int. J. Prod. Res. **58**, 3423–3436 (2020). https://doi.org/10.1080/00207543.2020.1754487

Publisher's Note