David C. Wyld
Dhinaharan Nagamalai (Eds)

Computer Science & Information Technology

International Conference on Big Data, IOT and Blockchain (BIBC 2020)
October 24-25, 2020, Dubai, UAE

AIRCC Publishing Corporation

Volume Editors

David C. Wyld,
Southeastern Louisiana University, USA
E-mail: David.Wyld@selu.edu

Dhinaharan Nagamalai,
Wireilla Net Solutions, Australia
E-mail: dhinthia@yahoo.com

ISSN: 2231 - 5403
ISBN: 978-1-925953-27-5
DOI: 10.5121/csit.2020.101301- 10.5121/csit.2020.101306

Typesetting: Camera-ready by author, data conversion by NnN Net Solutions Private Ltd., Chennai, India

Preface

The International Conference on Big Data, IOT and Blockchain (BIBC 2020) October 24-25, 2020, Dubai, UAE, 6th International Conference on Artificial Intelligence and Soft Computing (AISO 2020), International Conference on Education and Integrating Technology (EDTECH 2020), was collocated with International Conference on Big Data, IOT and Blockchain (BIBC 2020). The conferences attracted many local and international delegates, presenting a balanced mixture of intellect from the East and from the West.

The goal of this conference series is to bring together researchers and practitioners from academia and industry to focus on understanding computer science and information technology and to establish new collaborations in these areas. Authors are invited to contribute to the conference by submitting articles that illustrate research results, projects, survey work and industrial experiences describing significant advances in all areas of computer science and information technology.

The BIBC 2020, AISO 2020 and EDTECH 2020 Committees rigorously invited submissions for many months from researchers, scientists, engineers, students and practitioners related to the relevant themes and tracks of the workshop. This effort guaranteed submissions from an unparalleled number of internationally recognized top-level researchers. All the submissions underwent a strenuous peer review process which comprised expert reviewers. These reviewers were selected from a talented pool of Technical Committee members and external reviewers on the basis of their expertise. The papers were then reviewed based on their contributions, technical content, originality and clarity. The entire process, which includes the submission, review and acceptance processes, was done electronically.

In closing, BIBC 2020, AISO 2020 and EDTECH 2020 brought together researchers, scientists, engineers, students and practitioners to exchange and share their experiences, new ideas and research results in all aspects of the main workshop themes and tracks, and to discuss the practical challenges encountered and the solutions adopted. The book is organized as a collection of papers from the BIBC 2020, AISO 2020 and EDTECH 2020.

We would like to thank the General and Program Chairs, organization staff, the members of the Technical Program Committees and external reviewers for their excellent and tireless work. We sincerely wish that all attendees benefited scientifically from the conference and wish them every success in their research. It is the humble wish of the conference organizers that the professional dialogue among the researchers, scientists, engineers, students and educators continues beyond the event and that the friendships and collaborations forged will linger and prosper for many years to come.

David C. Wyld
Dhinaharan Nagamalai (Eds)

General Chair — Organization

David C. Wyld, Southeastern Louisiana University, USA
Dhinaharan Nagamalai, Wireilla Net Solutions, Australia

Program Committee Members

A.Neela Madheswari, Mahendra Engineering College, India
Abdelbaky Hamadene, AASTMT, Egypt
Abilash, Technopark, India
Addisson Salazar, Universitat Politècnica de València, Spain
Ahmad Aliyu Deba, Abubakar Tafawa Balewa University, Bauchi
Ahmed A. Elngar, Beni-Suef University, Egypt
Ajal.A.J, Federal Institute Of Science And Technology, India
Ajay Jaiswal, Center for Development of Security Excellence, India
Akhil Gupta, Lovely Professional University, India
Ali Qasim Hasan Al- Obaidi, Al- Nahrain University, Iraq
Amala Rajan, Dubai Women's College, United Arab Emirates
Amit Sinhal, JK Lakshmipat University, India
Aml Melad Asan, Al-Gabal Al-Garbi University, Libya
Anandakumar, Sri Eshwar College of Engineering, India
Andrzej Sokolowski, Lone Star college, USA
Asaf Varol, Firat University, Turkey
Auxiliar, University of Beira Interior, Portugal
Bibudhendu Pati, Rama Devi Women's University, India
Biruta SvagZdiene, Lithuanian Sports University, Lithuania
Chandra K Jaggi, University Of Delhi, Delhi
Chandrasekar Vuppalapati, San Jose State University, USA
Ching-Nung Yang, National Dong Hwa University, Taiwan
Chittineni suneetha, R.V.R & j.C. College of Engineering, India
Claudiu Marian bunaiasu, University of Craiova, Romania
Dalila Guessoum, Saad Dahleb University, Algeria
Daniel Asuquo, University of Uyo, Nigeria
Daniel Rosa Canedo, Federal Institute of Goias, Brazil
Daniela Momete, University Politehnica of Bucharest, Romania
Dao Chanh Thuc, An Giang University, Vietnam
Dariusz Jacek Jakobczak, Koszalin University, Poland
Dilip Roy Chowdhury, University of North Bengal, India
Elzbieta Macioszek, Silesian University of Technology, Poland
Esuk Ko, Universidad Mayor de San Andres (UMSA),Bolivia
Ezeji Noella Ijeoma, University of Zululand, South Africa
Faeq A. A. Radwan, Near East University, Turkey
Faouzia Benabbou, University Hassan II of Casablanca, Morocco
Felix J. Garcia Clemente, University of Murcia, Spain
Fernando Zacarias Flores, Universidad Autonoma de Puebla, Mexico
Fitzroy Nembhard, Florida Institute of Technology, USA
Froilan Mobo, Merchant Marine Academy, Philippines
Gabor Kiss, J. Selye University, Slovakia
Gabriela Mircea, West University Of Timisoara, Romania
Gang Wang, University of Connecticut, USA

Technically Sponsored by

Computer Science & Information Technology Community (CSITC)

Artificial Intelligence Community (AIC)

Soft Computing Community (SCC)

Digital Signal & Image Processing Community (DSIPC)

Organized By

Academy & Industry Research Collaboration Center (AIRCC)

TABLE OF CONTENTS

International Conference on Big Data, IOT and Blockchain (BIBC 2020)

The Temtum Consensus Algorithm – A Low Energy Replacement to Proof of Work…….....01 - 15
Richard Dennis and Gareth Owenson

Smart Insurance Contract against Political Risks: Definitions and General Reflections……...…….……..….....17 - 22
Remy Zgraggen

GDPR Compliance for Blockchain Applications in Healthcare …..…..….....23 - 35
Anton Hasselgren, Paul Kengfai Wan, Margareth Horn, Katina Kralevska, Danilo Gligoroski and Arild Faxvaag

6th International Conference on Artificial Intelligence and Soft Computing (AISO 2020)

Data Prediction of Deflection Basin Evolution of Asphalt Pavement Structure Based on Multi-Level Neural Network……....37 – 46
Shaosheng Xu, Jinde Cao and Xiangnan Liu

Stability Analysis of Quaternion-valued Neural Networks with Leakage Delay and Additive Time-varying Delays ……....47 - 58
Qun Huang and Jinde Cao

International Conference on Education and Integrating Technology (EDTECH 2020)

An Investigation of Modern Foreign Language (MFL) Teachers and their Attitudes to Computer Assisted Language Learning (Call) Amid the Covid-19 Health Pandemic……...…...……..…59 – 66
Louise Hanna, David Barr, Helen Hou and Shauna Mc Gill

THE TEMTUM CONSENSUS ALGORITHM – A LOW ENERGY REPLACEMENT TO PROOF OF WORK

Richard Dennis and Gareth Owenson

Department of Computing, University of Portsmouth,
Portsmouth, United Kingdom

ABSTRACT

This paper presents a novel consensus algorithm deployed within the Temtum cryptocurrency network. An overview of the proof of work consensus algorithm is presented, and gaps in the research are outlined. The Temtum consensus algorithm's unique components, including the Node Participation Document (NPD) and the use of the NIST randomness beacon, are outlined and explained. Comparisons on the cost to attack the consensus algorithm and energy consumption between the Temtum consensus algorithm and Bitcoin's proof of work is presented and evaluated. We conclude this paper summarising the findings of the research and presenting future work to be conducted.

KEYWORDS

Blockchain, Peer-to-Peer Networks,Cryptocurrencies, Consensus, Byzantine Fault Tolerance

1. INTRODUCTION

A person under the pseudonym Satoshi Nakamoto emailed a cryptography mailing list; a self-pushed paper titled, Bitcoin: A Peer-to-Peer Electronic Cash System [1]. The paper contained a novel approach to a digital currency without a third party or centralized entity requirement. Through the implementation of the blockchain and the proof-of-work consensus algorithm, the previous double-spend attacks were solved.

The proof of work algorithm is arguably the most innovative component outlined in the Bitcoin whitepaper. This algorithm enabled users on the network to be confident the token received from another user has not been previously spent. This was achieved through a globally agreed state of all transactions called the blockchain.

Bitcoin is the decentralized peer-to-peer network that was created from the Bitcoin whitepaper. Further, Bitcoin can also refer to the token, which is transferred between users on the Bitcoin network.

Due to the peer-to-peer architecture of the Bitcoin, there are no centralized components to the network [2]. Instead, users can participate in the network by downloading the Bitcoin client and donating resources to the network. A machine participating in the network running the Bitcoin client is defined as a Bitcoin node.

David C. Wyld et al. (Eds): BIBC, AISO, EDTECH - 2020
pp. 01-15, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101301

The node architecture contains four components. A node can run none, one, or multiple instances of each component. A full node can be defined as a node that runs at least one instance of each component [3]. These components are; Routing mechanisms for the Bitcoin protocol, A wallet, A complete blockchain since the network launch, and the Bitcoin miner.

The blockchain can be defined as a globally agreed network state of transactions on the network since it was deployed. The blockchain achieves a global state by limiting the ability to amend transactions to the blockchain to a single node that has completed the proof-of-work algorithm before the rest of the network's nodes.

Each node on the network confirms transactions that have occurred on the network. Validtransactions are combined into a data set called blocks. A block contains all valid transactions on the network since the publication of the previous block. In addition to the valid transactions, each block contains a previous block's hash to prevent modification of previously confirmed blocks.

The blockchain, also with the proof of work algorithm, prevents the double-spend attack. This attack is when an adversary attempts to spend previously spent tokens. In addition to the inability of an adversary to rewrite previously confirmed blocks, the globally agreed state of the blockchain ensures as long as a majority of miners are not malicious, the network is considered secure.

The mining algorithm is a full node component that completes a brute force calculation to find the solution to a preset mathematical problem [4]. This problem is defined as the SHA256 hash of the block to be confirmed, which, when combined, a random value results in a value lower than a target value [5]. The target value changes every two weeks to ensure the generation of blocks occurs on average every 10 minutes.

Each miner is conducting this algorithm and competing against all other miners on the network to be the first with a correct solution [6]. This brute force method and competition between miners incentives nodes to add more powerful CPUs or ASICs to the network. The increased performance of the CPUs and ASICs also increases the energy consumption of such devices.

Furthermore, incentives miners to donate their CPU resources to the mining process by rewarding the node that finds the valid value first a reward of newly minted Bitcoin and all the transaction fees collected during the block.

Once the block is valid, and proof-of-work is successfully found, the block is defined as mined. The block then is propagated through the network to enable each node on the network to receive this confirmed block and update the nodes' locally stored blockchain.

2. LITERATURE REVIEW

2.1. The Byzantine Generals Problem

The Byzantine Generals Problem is a description of a known problem in computer science. A situation where all involved participants must agree on a single version of an event to prevent complete failure [7]. There is an assumption that half or less of the involved participants are malicious and attempting to disrupt the event by propagating false information or not propagating data. Furthermore, participants do not know if the messages are authentic or follow the correct procedure.

This problem can be demonstrated in a decentralized peer-to-peer network where a file is propagated through the network. Users participating in the network cannot trust the received file due to their inability to determine which node is malicious and sharing malicious files. Due to the lack of guarantee that nodes on the network are participating following the protocol rules, malicious nodes may participate in the network and attack the network.

Previously described digital currency peer-to-peer networks such as e-cash were not secure against this type of attack; therefore, users could spend the same currency multiple times [8]. This problem was overcome with the inclusion of centralized ledgers.

The Bitcoin network is the first known peer-to-peer decentralized digital currency, which prevents the Byzantine generals problem without a third party's requirement. This was achieved due to the novel components of the blockchain and proof-of-work algorithm. All blocks are cryptographically verified by each node on the network, validating the contained hash and a nonce.

While the hashcash network previously detailed the requirement of hashing data on the network, Nakamoto expanded on implementing such a method to create the proof-of-work algorithm [9][1].

Each full node on the network competes against all other nodes on the network to find a random nonce value that results in a hash below a presettarge value when combined with the block hash. Each block contains the previously confirmed block hash within the body of data. Therefore it is impossible to modify a previously confirmed block without changing its hash [10]. Therefore for any modification of a previous block, the hashes for all blocks since this block would also be required to be recalculated. Failure to do so would alert the node of such an attack.

Since the nodes conducting the mining algorithm compete against each other, the network is considered secure so long as more than 50% of nodes correctly follow the protocol rules [11]. Therefore we can conclude Bitcoin is secure against the Byzantine generals problem.

2.2. Mining

As previously discussed, the mining algorithm is used within the Bitcoin protocol to ensure that computational resources must be donated to the network before a block of transactions can be considered valid.

The mining algorithm ensures the generation of average every 10 minutes by modifying the pre-determined value the block hash, and the nonce, when combined, must be lower than. This process ensures only one block of data is valid and accepted by the network [12]. A globally agreed state of all transactions that have occurred on the network prevents an attacker from spending the same Bitcoin more than once.

The mining algorithm's brute force process requires a random number defined as a nonce to be calculated and combined with the block hash until the hash value contains a pre-determined number of zeros at the start of the hash. This requires each node to calculate billions of nonces, and a node which can calculate nonces quicker than other nodes on the network increases their probability of finding a valid result.

As of 2017, the requirement was for a valid hash to start with 17 zeros; this results in a probability of $1.4X10^{20}$ to find a successful nonce [13].

This requirement of the number of zeros at the start of the hash is defined as the network difficulty. This value is adjusted every 2016 blocks to keep blocks being confirmed on average every 10 minutes. This is required due to increasing resources added to the network by nodes wishing to obtain a greater advantage over other nodes, which results in blocks being computed quicker than this timeframe.

A target 256-bit number is encoded in the block header's nBits field, and it has a maximum value of 0x1d00ffff (≈ 2224). The difficulty can be summarized at the ratio of the maximum target over the current target. D ≈ 2224/target.

Due to the SHA-256 hashing algorithm properties, results are truly random and expensive to compute but are deterministic outputs and cheap to validate [14].

The mining process can be conducted without additional data from other nodes. Therefore this can be considered a genuinely decentralized component of the Bitcoin network, requiring only a valid blockchain to participate.

The computational resources of a node are directly proportional to the time required to find a correct solution. The more computational resources the node processes, the more nonces per second the node can test.

While nodes on the network are adding more and more computational resources to give them a competitive advantage over other network nodes, the consistent publication of blocks every 10 minutes has led to a situation where nodes are required to add computation resources in order to maintain their competitive constantly. This, in turn, increases each node's energy consumption for no greater performance on the network.

The miner responsible for finding a valid nonce to the proof-of-work problem is compensated with a block reward and all fees from the confirmed block's transactions. The block reward was originally 50 BTC per confirmed block; this reward is reduced by half roughly every four years.
Due to the increased probability of finding a valid nonce being directly proportional to a node's computational resources, nodes are combined their resources. This merger of computation resources has created so-called mining pools where thousands of nodes combine their resources to have a greater probability of finding the solution to the nonce and receiving the rewards [15]. Due to this shift to centralized mining pools, it is now statistically impossible for a single node to participate in the mining process and expect to find a valid block.

Therefore, even though the mining algorithm was intended to be a decentralized method to confirm transactions on the network, it has morphed into a centralized confirmation mechanism. Furthermore, due to the financial incentives and limited space within a block, transactions that pay the highest transaction fee are more likely to be included.

This demand for resources has impacted the mining process's energy consumption and excluded the home user from participating without joining a mining pool.

2.3. Mining resource consumption

Due to the direct link between computational resources and the probability of success and the hashing algorithm being deployed at the hardware level, Bitcoin ASICs miners have created. These are hardware devices whose only function is to calculate the required nonce for the proof-of-work algorithm.

The ASICs miners are optimized for the proof-of-work algorithm and can conduct more nonce attempts than the average home computer initially used for the mining process [16]. However, the ability to conduct more proof-of-work algorithm attempts results in more energy being required for the device to function.

A Bitcoin ASIC miner typically continuously runs until the cost of electricity and block reward makes it uneconomically viable or the hardware malfunctions.

As users add more ASICs to the network to increase their probability of finding a valid solution, the network difficulty increases, and the network's energy consumption.

This has resulted in a catch-21 situation, where a user must donate more computing resources to the network to stay competitive, which in turn consumes more energy for no greater performance on the network. ASIC development focuses on increasing nonces per second each device can achieve rather than energy efficiency, resulting in significant growth of the Bitcoin network's energy consumed.

In 2016, the Bitcoin network consumed 0.08% (67.86 TWh) of electricity consumed globally per year. Compared to the Visa network, which in 2016 consumed 674,922 Gigajoules of energy and processed 111.2 Billion transactions, averaging 8,000 transactions per second compared to Bitcoin’s five transactions per second [16][17]. This demonstrates a single Bitcoin transaction is compared in energy to 100,000 transactions conducted on the Visa network.

Due to this significant energy consumption for such a low-performance network, law and policymakers are currently debating regulation on how to reduce Bitcoin’s energy consumption[18].

While it can be argued that users' ability to send transactions without a third party is an approximate use of the energy consumed by the network, in a world focused on reducing carbon emissions and energy consumption, it identifies the mining algorithm requires reinvention to a lower energy consumption algorithm.

2.4. 51% Attack

The foundations of a double-spend attack require a malicious adversary to control 51% or more of the network's hashing power [19]. This is an advancement to the Sybil attack, which decentralized peer-to-peer networks are vulnerable to. This is due to a lack of restrictions on users, which can participate in the network. Furthermore, even is a malicious adversary is detected by other nodes on the network, the lack of centralized authority to remove the nodes means they will always be able to participate in the network.

A malicious adversary controlling 50% of the networks hashing power would produce valid blocks simultaneously as an honest network. This would cause a situation where two valid versions of the blockchain exist simultaneously, a problem known as a network fork. Therefore, one version of the blockchain can contain transactions that are not contained in the other blockchain, enabling the attacker to spend the same Bitcoin on both blockchains.

The greater the computational resources under the control of a malicious adversary, the greater they can modify previously confirmed blocks. With more than 50% of the network hashing power, the attacker would be able to modify a previously confirmed block, for example, by removing a transaction within it and then recalculating the proof of work for the new block and all subsequent blocks [20].

Furthermore, an attacker could also disrupt the network by refusing to forward transactions or blocks to the rest of the network and flooding the network with invalid data.

The 51% attacks have been demonstrated to occur in the real world, with two Ethereum based networks, Krypton, and shift, coming under attack during 2016. Furthermore, several other networks have been attacked since 18 million USD of Bitcoin Gold currency was double-spent during May 2018.

3. Temtum components

This section will outline the core components of the novel consensus algorithm deployed in the Temtum network. We will detail the node participating document, including how it interacts with the nodes on the network and prevents malicious modification. Furthermore, the consensus algorithm itself is described in this section.

3.1. The node participation document (NPD)

Within the Temtum network, there is a subset of nodes classified as authority nodes. These nodes participate in the network as normal nodes while also monitoring nodes participating in the network.

To enable the monitoring of nodes on the network, all nodes must announce themselves to the authority nodes when they first join the network. The authority nodes would request data from the nodes to identify them and add them within the NPD.

The requirement of DNS nodes within the network is no longer required due to the authority nodes replacing these nodes and providing newly joining nodes with a global view of the network through the NPD publication.

The NPD can be defined as a document updated on an hourly rate to provide all nodes on the network a global state of nodes participating. All nodes that have been connected to by the authority nodes are defined as currently actively participating in the network and therefore are listed in this document.

The ability of nodes to have a global view of the network participation will reduce the probability of a network-level attack such as a partition attack. The partition attack excludes nodes from participating in the honest network allowing for attacks such as delaying or not forwarding blocks and transactions. Furthermore, it would be possible for the partition node to receive a different version of the blockchain, allowing a double-spend attack. This attack and resistance to attack are detailed later in this paper.

Multiple authority nodes are deployed on the network to prevent censorship or attack caused by a single malicious adversary in control of the authority node, each operated by a separate entity.
For a single NPD to be published, and agreed NPD state must be agreed amongst a majority of authority nodes. They achieve this by voting on the inclusion of each update of the NPD. While the authority nodes can add nodes to the NPD, they may only remove offline nodes from the NPD and not nodes that they suspect to be malicious to prevent censorship.

Data such as the IP address, the amount of blockchain history locally stored, public identity, and the node's role is stored within the NPD.

Figure 1 is an example of the data fields that are collected and stored in the NPD for each node

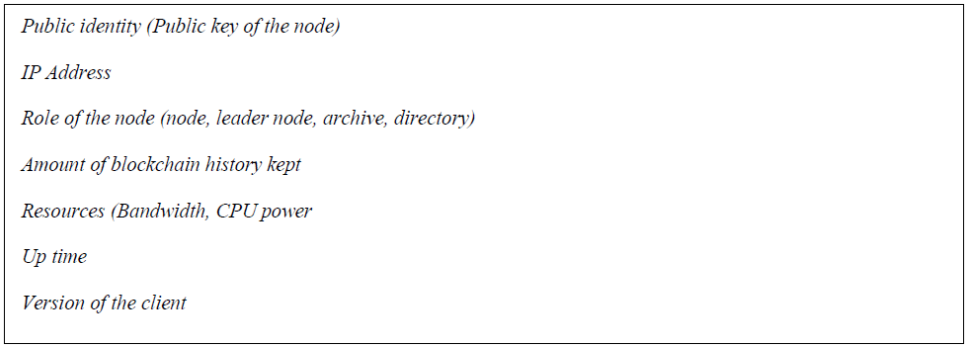

Figure 1. Data stored within the NPD for each node

Due to the components of the temporal blockchain deployed within the Temtum network in which a finite amount of the blockchain history is stored locally, the NPD provides information to nodes on the network to enable the querying of nodes for data which they do not hold locally. Utilizing the NPD nodes that require data can quickly and accurately determine the correct node to query to prevent wasted resources querying all nodes randomly on the network, as is Bitcoin's case.

During the bootstrap process, where a node is attempting to join the network, they must initialize contact with a minimum of one authority node. An “announcement” message is sent from the node bootstrapping to one or more authority node to achieve this. This message contains data to enable the authority nodes to connect back and further query the node.

Table 1. Annoucement message.

Size	Field	Description
32 bytes	Public identity	The public part of the node’s public/private key pair
4 bytes	IPV4 Address	The IP address of the node
2 bytes	Port number	Port number the node can be connected to
4 bytes	Timestamp	Time this block was created (seconds from Unix Epoch)

When an authority node receives this message, they attempt to connect to the node using the provided information and return an “ACK” message. Furthermore, the authority node also returns the last valid NPD; however, the bootstrapping node would not be included in the previous NPD. Within the header of the NPD, a valid time period from and until is defined. This prevents nodes from participating in the network using an out of date NPD. A node attempting to use an older NPD may have a conflicting view of the network, which could be exploited. The NPD is also signed by the authority nodes' private keys to prove the NPD publication source.
Figure 2 displays an example NPD

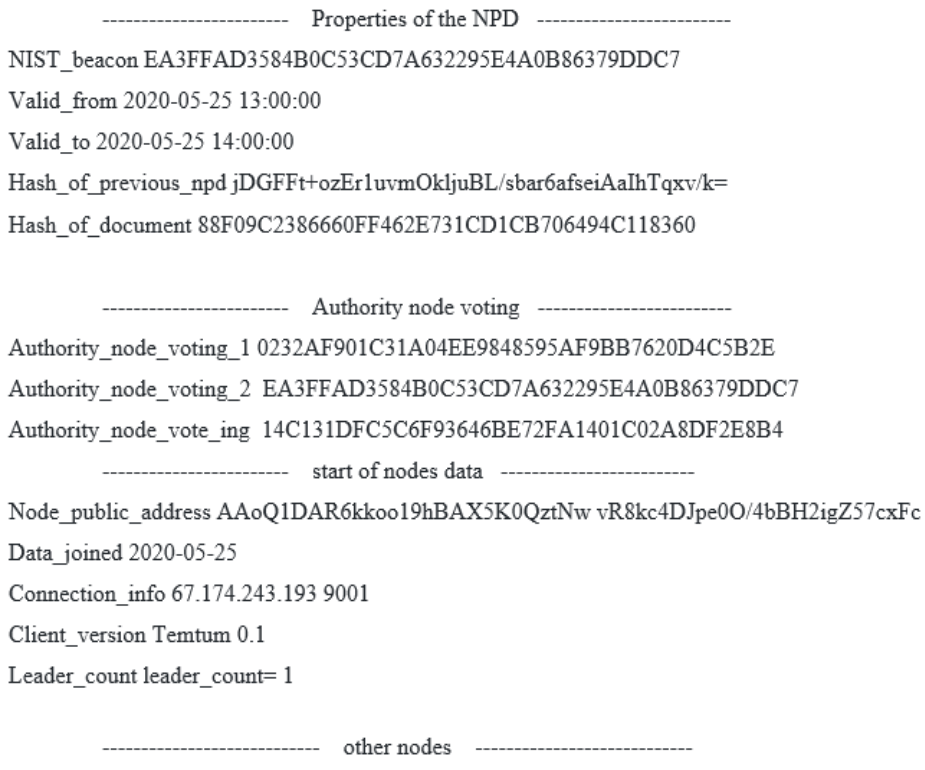

Figure 2. An example NPD document

The NPD is published on an hourly basis. This was calculated as appropriate publication time due to the +4 and -3 network churn, which was observed hourly on the Bitcoin network between 01/05/2015 to 01/05/2018. Furthermore, this approach also is in use on the Tor node document.
A MacBook Pro with 16GB RAM, 150mbit/s available bandwidth, and a 2.8 GHz Quad-Core Intel Core i7 CPU was used during our simulated experiments.

A node entry within the NPD uses 4.49bk of storage, and it was simulated an average authority node would be able to store 481,737 nodes within a single NPD.

Bitcoin currently uses a DNS method to provide bootstrapping nodes with known nodes on the network. It was currently observed 32 nodes per request were received; however, the maximum theoretical IP address to be received per request is 65535.

A vital requirement of the Temtum network is lower-resourced users' ability to participate fully in the network. Therefore a simulated NPD was created and calculated the number of nodes able to be contained within the NPD for a node to download the NPD within a 5-minute window.

A node with an average bandwidth of 1,103 kb/s would require an NPD to be no larger than 0.3309GB, which would, in turn, be able to contain 73,697 node records.

These numbers demonstrate that the NPD structure scale is far in excess of the current Bitcoin network size.

3.2. The consensus algorithm

The proof of work algorithm deployed within the Bitcoin network can be summarised as an expensive operation to determine the node which will be permitted to append a block onto the blockchain.

It was outlined that the resources processed by a node are directly proportionate to the probability of the node finding a correct solution to the proof-of-work algorithm. However, this opens a vector of an attacker where a malicious adversary can pool network resources to enable them to generate blocks at the same speed, or faster than the honest network. This is known as the 51% attack. The ability to generate blocks at the same speed as the honest network would result in two valid blockchains existing on the network at the same time.

A 51% attack does not impact the consensus algorithm deployed in the Temtum network. The Temtum consensus algorithm's unique property is that each node can locally determine which node will be confirming the next block utilizing the NPD data already stored. Since all nodes on the network have the same NPD and conduct the same algorithm, all nodes on the network would select the same node for confirming the next block.

Therefore there can be no fork of the blockchain existing on the Temtum blockchain, making a double-spend attack impossible on Temtum.

The removal of the competition between nodes and the single calculation process reduces the number of computational resources required. Furthermore, since additional resources do not impact the probability of the node being selected, there would be no situation in Bitcoin currency where more computational resources are required to maintain competitiveness.

This property also removes the incentives for nodes to pool their resources together, making the block confirmation process more decentralized than Bitcoin.

The consensus algorithm proposed here will enable the node responsible for confirming the block pre-event rather than Bitcoin's post-event model.

The consensus algorithm:

- Each node can determine the node responsible for confirming the next block using local data but reach a global consensus.
- Two nodes cannot publish blocks at the same time, preventing a fork in the blockchain.
- A single calculation process is conducted,which requires low computation resources.
- Use of a randomness beacon.

The randomness beacon is present to the network from NIST every 60 seconds. Each node would be required to ensure they have downloaded the latest beacon. Each node then performs the same calculations on their NPD to determine the next node to confirm a block.

The NIST beacon 512-bit value is subtracted from the public identity of a node contained within the NPD. This is repeated until every node’s value contained within the NPD has been calculated. The node that results from a closet to zero would be the node responsible for confirming the next block.

```
512 Bit Randomness beacon broadcast to the internet
All nodes retrieve the beacon value
Nodes check the beacon signature to ensure source is valid
Loop through NPD
        Each public id – NIST value = closer to zero than
previous stored value?
                If yes – public node id now potential leader
                If no – Discard public node id
        Loop until all NPD has been queried
```

Figure 3. Pseudo-code for the leader selection algorithm

The probability of two nodes having the same value once the calculation has been conducted is 1.4×10^{77}. While this is a small figure, should this occur, the node with the highest uptime would be selected.

Because each node has an equal probability of confirming the next block irrespectively of their resources, nodes are not disincentivized to pool together. Therefore our consensus algorithm provides more decentralization than Bitcoin.

4. CONSENSUS ENERGY AND RESOURCE CONSUMPTION - BITCOIN AND TEMTUM SIMULATIONS

This section will compare the resource consumption, including energy, of the proof-of-work algorithm deployed within Bitcoin compared to the consensus algorithm used in Temtum.

We first analyzed the energy consumption of the Bitcoin mining method.

We calculated the network hash rate by obtaining the network difficulty contained within the blockchain block headers. To decode the blockchain, we created a blockchain parser which decoded the blockchain into clear text.

We are using data from commercially available products such as Bitcoin miners and energy cost per kilowatt to determine Bitcoin's proof-of-work cost.

Due to the inability to locate miner's physical location, we will use a static value for the electricity cost due to a full node having one, more than one, or zero miners attached to them. Furthermore, since the miners themselves are unable to be queried, it is impossible to determine which model is being operated. Therefore we will use a static value for miners hash rate and energy consumption obtained from the AntMiner S9 ASIC miner.

Using the below formula, we calculated the hash rate using the difficulty we obtained from the block headers. (Where D is the difficulty):

D * 2**256 / (0xffff * 2**208)

Figure 4 shows the estimated terahashes per second on the network since the genesis.

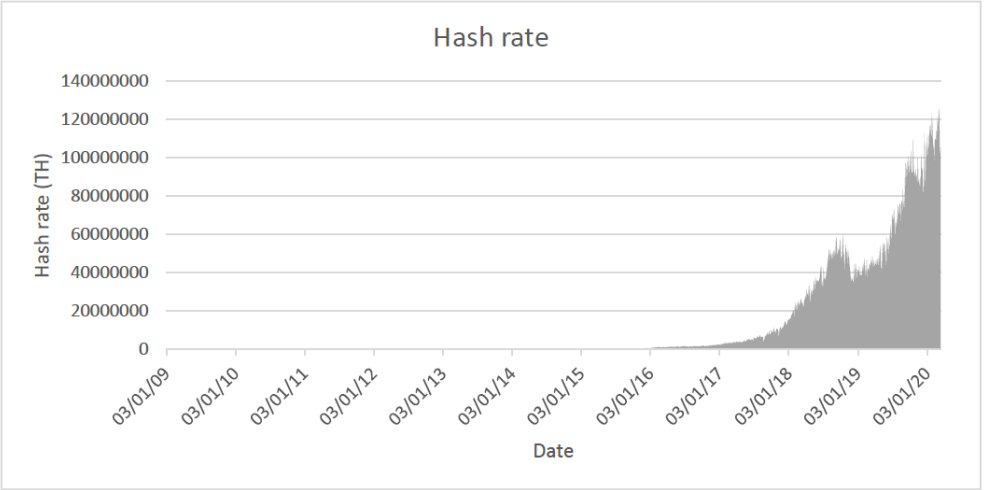

Figure 4. The calculated hash rate of the Bitcoin network since launch

We create models to compare and contrast Bitcoins' proof-of-work energy consumption compared to Temtum's consensus algorithm, which will be evaluated during this section.

The difficulty was observed to increase by 5% every 14 days between February 2016 and August 2017. A fixed cost of electricity of $0.15 per kWh will be utilized for the calculations. This was calculated as the average cost of a US person during the observed period.

Parameters of the experiment (Bitcoin)

Starting Difficulty:	150000000000 Gh/s
Growth (%) 14 days	5
Hash rate per miner (Gh/s)	13500
Power consumption (W)	1300
Cost per kWh ($)	0.15

Our simulations concluded that a single miner conducting the proof-of-work with the current network difficulty would take an average of 148.9 years to find a solution to the proof-of-work.

Expanding the simulation, the average Bitcoin miner consumes 11,388 kWh of electricity yearly, and excluding any profits from block rewards operates a loss of -$3,508.93 during the same period.

The same experiment was conducted on the Temtum network. It has been observed that the average Temtum node consumes 0.05 kWh of electricity. This is due to dedicated ASICs and high-resource computers not participating in Temtum; instead, a basic home laptop can be used.

It was simulated the average Temtum node uses 438 kWh of electricity over the same period, which results in a -$65.76 loss to the node operator.

We can conclude that the Temtum node block confirmation process is 53.4 times cheaper than the Bitcoin network in comparison.

Bitcoin's yearly energy consumption is equivalent to Tajikistan, the world's 84th most energy-consuming country in 2014, with the network consuming 4.56×10^{16} joules of energy. This

country has a population of 8,330,946, which shows how inefficient the consensus algorithm of Bitcoin is.

A Temtum network that operates with the same number of nodes as Bitcoin miners and nodes would consume 8.53×10^{14} joules over the same yearly period, making temtum equivalent to Gibraltar, a country with a population of 29,328.

We calculated Bitcoin to currently has a minimum of 1,100,000 ASICs miners operating at the network.

To enable an accurate comparison, we simulated a Temtum network that contains 1,100,000 nodes. This would result in a node being selected for a to confirm a block on average every 10.57 years

We can conclude that a Temtum node is picked on average 14.09 more often for confirming a block than a single Bitcoin miner. Furthermore

5. ATTACK COMPARISON – BITCOIN COMPARED TO TEMTUM

5.1. DNS Poison Attack

As was previously demonstrated, a node conducting the bootstrap process with Bitcoins DNS nodes would stage would receive an average of 28 nodes,which equates to a 0.38% view of the network

A simulated attack was conducted where an adversary could query the DNS nodes from nodes under the adversary's control. The DNS nodes within Bitcoin relay the most recently queried nodes to nodes, which are bootstrapping on the network. When a node queries the DNS node, they are likely to receive nodes under the adversary's control.

A bootstrapping node attempts to connect to each node received from the DNS. Once eight connections are established to nodes on the Bitcoin network, the download of the blockchain begins.

Due to blockchain properties, if a single honest node is collected to out of a pool of malicious nodes, the honest node will supply the victim node will correct data, even if there are significantly more malicious nodes connected to. This is due to the assumption that the attacker does not process a blockchain with a higher proof-of-work than the honest network.

A graphical representation in figure 5 demonstrates this problem. Where the yellow circle represents the node joining, blue the malicious nodes, and the green nodes represent the honest network.

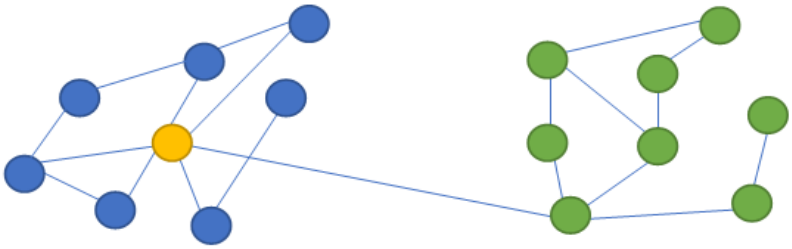

Figure 5. Bootstrap partition attack failure on Bitcoin

For an attacker with 100 US dollars to spend to conduct this attack, they would be able to host 30 malicious nodes on the Bitcoin network. With this small number of nodes, a simulated success rate of 92% in which a bootstrapping node would receive a response containing all nodes under the adversary's control.

When an attacker controls all the nodes the victim node is connected to, they can provide the victim node with a valid but potentially different from the honest network. This would enable double-spend attacks to be conducted against this node.

Due to the global view of the network provided to each bootstrapping node on the Temtum network throughout the NPD, the known list of nodes to the bootstrapping node rises from 28 in Bitcoin to the total network size in Temtum.

To enable a direct comparison, we simulated a 10,000 node Temtum network, of which a malicious adversary controlled 30 of them. Like bitcoin, the bootstrapping node would select eight nodes at random to connect to begin the bootstrapping process. Our simulations showed a 5.210508e-24 probability of this attack succeeding.

We formulated this to be:

Probability of success = ${}^{Y}C_{8} / {}^{x}C_{8.}$

Where y is the number of malicious nodes, and X is the total number of nodes on the network. 8 is the total nodes selected by the bootstrapping node.

This demonstratesthat the consensus algorithm's NPD element also significantly reduces the probability of success from a network partition attack. Furthermore, due to the random selection of nodes from the NPD, the adversary cannot exploit any vulnerability in the nodes' positioning to gain an advantage.

We can conclude that the NPD implementation as a component of the consensus algorithm deployed within the Temtum network provides greater resistance to network-level attacks during the bootstrapping phase. Furthermore, we have demonstrated that the Temtum network is more resistant to Sybil attacks than Bitcoin due to the NPD.

5.2. Sybil Rewrite Attack

We expanded the Sybil attack to demonstrate how an attacker with majority control could potentially rewrite historical data. We assume a malicious adversary has successfully partitioned a node away from the bootstrap's honest network during this section.

There are hardcoded block hashes inserted into the Bitcoin core source code. This is known as checkpoints. The use of checkpoints makes it impossible to alter data before this date due to the invalid hashes that would result from the blocks, even if the blocks are valid.

The last checkpoint to be implemented in the source code occurred at block 295000 and added to Bitcoin Core 0.9.3. This checkpoint was added on April 9, 2014, with a block difficult of 6,119,726,089.

An Antminer S9 uses 0.1 Joule per 10^9 hashes it computes. For a difficultly 6,119,726,089, t was modeled, the miner would need to complete $2.62 * 10^{19}$ hashes costing 73 USD in electricity. The attacker would be able to generate subsequent blocks the same rate until the difficulty adjusted.

This demonstrates the impact of the DNS poison attack on Bitcoin. When we conducted this simulation on the Temtum network, the attack failed.

The failure of this attack on the Temtum network was due to the consensus algorithm and the NPD.

The block validation process is more complicated than Bitcoin due to the block architecture of blocks stored within the temporal blockchain deployed on the Temtum network.

Each block header contains the NIST timestamp of when the block was published and signed by the node that confirmed it. The timestamp's inclusion within the block header demonstrates the block could not be computed ahead of time and had to be generated at that point in time or later. This prevents an attacker from making a longer chain and presenting this to the network as valid can be achieved on Bitcoin.

Furthermore, since the NPD history is made public and the NIST random beacon history, a node can randomly select a block to validate. By reversing the consensus algorithm, the node would compare the node results that should have been responsible for signing to the node, which did sign the block.

This further demonstrates the consensus algorithm deployed within the Temtum network as being more resistant to attack than the Bitcoin proof-of-work model.

The attack could succeed if the NPD publications could be rewritten; however, this assumes a majority of directory nodes being malicious and coordinating to alter previously agreed NPDs. This attack vector is considered unlikely and out of the scope of this section.

6. CONCLUSION

This paper proposed a novel consensus algorithm that was more energy-efficient while maintaining the Bitcoin proof-of-work algorithm's security properties.We outlined the algorithm's consensus algorithm and critical components, such as the NPD within this paper.

We demonstrated a series of attacks on the protocols to simulate a well-resourced adversary through live data collection and simulation.

During each simulation, we demonstrated a measurably way the consensus algorithm of Temtum is either more efficient or more secure when compared under the same constraints as the Bitcoin proof-of-work algorithm.

Therefore, we can conclude the current proof-of-work is inefficient and vulnerable to attacks, which can be easily solved with a solution like a consensus algorithm proposed here.

REFERENCES

[1] S. Nakamoto, "Bitcoin P2P e-cash paper," 2008 October 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] P. Cuccuru, "Beyond bitcoin: an early overview on smart contracts," International Journal of Law and Information Technology, Volume 25, Issue 3, p. 179–195, 2017.

[3] J. Bohr and M. Bashir, "Who Uses Bitcoin? An exploration of the Bitcoin community," in 2014 Twelfth Annual International Conference on Privacy, Security and Trust, 2014.

[4] A. Biryukov, D. Khovratovich and I. Pustogarov, "Deanonymisation of Clients in Bitcoin P2P Network," in CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014.

[5] J. Soria and V. Savolainen, "Too Big to Cheat: Mining Pools' Incentives to Double Spend in Blockchain Based Cryptocurrencies," in SSRN Electronic Journal, 2019.

[6] M. Romiti, A. Judmayer, A. Zamyatin and B. Haslhofer, "A Deep Dive into Bitcoin Mining Pools: An Empirical Analysis of Mining Shares," 2019.

[7] L. Lamport, R. Shostak and M. Pease, "The Byzantine generals problem.," Concurrency: the Works of Leslie Lamport., p. 203–226, 2019.

[8] Y. Chen and J.-S. Chou, "ID-Based Certificateless Electronic Cash on Smart Card against Identity Theft and Financial Card Fraud," in The International Conference on Digital Security and Forensics, 2014.

[9] A. Back, "Hashcash - Amortizable Publicly Auditable Cost-Functions," 2003.

[10] D. M. A. Cortez, A. M. Sison and R. P. Medina, "Cryptographic Randomness Test of the Modified Hashing Function of SHA256 to Address Length Extension Attack," 8th International Conference on Communications and Broadband Networking, pp. 24-28, 2020.

[11] D. Bradbury, "The problem with Bitcoin," Computer Fraud & Security, pp. 5-8, 2013.

[12] A. Lamiri, K. Gueraoui and G. Zeggwagh, "Bitcoin Difficulty, A Security Feature," Information Systems and Technologies to Support Learning, pp. 367-372, 2018.

[13] S. M. Werner, D. I. Ilie, I. Stewart and W. J. Knottenbelt, "Unstable Throughput: When the Difficulty Algorithm," 2020.

[14] E. Budish, "The Economic Limits of Bitcoin and the Blockchain," NBER Working Paper, 2018.

[15] B. Kaiser, M. Jurado and A. Ledger, "The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin," 2018.

[16] A. Vries, "Bitcoin's Growing Energy Problem," Joule, pp. 801-805, 2018.

[17] Visa, "Annual report 2019," Visa, 2019.

[18] A. l. o. o. panelJonTruby, "Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies," Energy Research & Social Science, pp. 399-410, 2018.

[19] C. Ye, G. Li, H. Cai, Y. Gu and A. Fukuda, "Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting," in 2018 5th International Conference on Dependable Systems and Their Applications (DSA), 2018.

[20] N. Shi, "A new proof-of-work mechanism for bitcoin," 2016.

[21] H. Chena, T. N. Conga, W. Yang, C. Tan, Y. Li and Y. Ding, "Progress in electrical energy storage system: A critical review," Progress in Natural Science, pp. 291-312, 2009.

SMART INSURANCE CONTRACT AGAINST POLITICAL RISKS: DEFINITIONS AND GENERAL REFLECTIONS

Remy Zgraggen

University Oldenburg, Switzerland

ABSTRACT

The present research article shall outline how blockchain technology could be combined with insurance solutions against political risks. Through the definitions and the characterization of the key concepts of traditional insurance law and blockchain technology using case examples of specific political risks, it will be shown, how the insurance coverage of political risks could be achieved through smart insurance contracts in the future.

Keywords

Political Risk Insurance, Smart Insurance Contract, Blockchain, Insurance Principle, Insurance Law, Insured Event.

1. INTRODUCTION

1.1. General Remarks

Insurance can be defined as a collective risk-taking based on the insurance principle. Which means that a high number of people pay insurance premiums into a large pot and in the case of the so-called insured event they get compensation for their damages [1]. If the insured event does not occur, the insurance company keeps all the premiums. This model gives a certain incentive to the insurer to not pay claims or to deny that an insured event has occurred, in order to maximize its profits. In this context the question arises, if the collective of persons would not be able to manage the payments of the premiums and the claims themselves, *without* an insurance company or an insurance broker in the middle. Such a model is in general defined as a P2P insurance: individuals with similar interests pool their premiums and share a certain risk between themselves. In this way P2P insurance allows insureds to self-organize and self-administer their own insurance [2]. Within the present article some fundamental reflections shall be made how this idea could be realized through a smart insurance in the example of a political risk insurance.

1.2. Smart Insurance Contracts in the Present Context

For any kind of insurance there is the key question, if the insured event – which must be defined clearly and unambiguously – has occurred or not. Today the insured event is in general defined within the insurance contract between the insures and the insurance company. However, there is the possibility that the insured event is described and defined in a clear and more transparent way in a *blockchain*, and which leads to an automatic payment in case of realization of the insured event. Such kind of smart insurance contracts would help to remove administrative expenses at the insurance companies and speed up processes in general and remove ambiguity for the persons

David C. Wyld et al. (Eds): BIBC, AISO, EDTECH - 2020
pp. 17-22, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101302

insured. However, there are various legal and economic questions and problems that need to be solved, before such a smart insurance could be implemented in practice. Questions and problems, which are in general covered and solved by the insurance company today. There is for example the question about the correct amount of the individual insurance premium in order to be able to guarantee all payments of claims for all insures in the long run in the future. And there can be the question, what will happen in a case of legal dispute between individual policyholders – for example concerning the question of responsibility for the content of the smart insurance contract in the blockchain. In addition, there are several regulatory barriers to smart insurance contracts and other Insurtech-solutions today. In practice it means for example, that it might be difficult for Insurtech providers to get the permission as a licensed insurance company by the competent supervisory authority [See 3].

The present research paper shall explore some legal or regulatory barriers for smart insurance contracts and similar blockchain-based insurance applications, especially through the example whether and under what conditions a political risk insurance could be based on a smart insurance contract. With the aim to understand the legal challenges regarding smart insurance, it is useful to outline some general key principles of insurance law first. In the second part, based on case examples, the definitions and some characteristics of political risk insurance in the context of blockchain-based smart insurance solutions shall be outlined.

2. PRINCIPLES OF INSURANCE LAW

2.1. Insurance Premiums as the Cost of Insurance

The insurance premiums can be defined as the cost for the insurance – the compensation for insurance coverage by the insurance company. In other words, it is the price for the insurance contract [See 4, p. 288]. A quantification of the insurance premium is not necessary – however, a gratuitous contract (insurance coverage free of charge, without any insurance premium) cannot be considered as an insurance contract [5, p. 17]. According to legal literature the insurance premium must be at least determinable [6]. Consequently, an insurance contract can foresee for example that the insurance premium must be paid in crypto currency. This specific amount of crypto currency will be the compensation for insurance coverage. In this way it can be defined in the insurance contract that the policyholder must pay a certain number of coins at regular intervals or single one-time payment in order to receive compensation (for example a certain sum of bitcoins) in the case of occurrence of the insured event in the future. There are in general no fundamental regulatory objections against such an insurance contract. This is at least the case in the European legal framework. Even though there is a clear regulatory trend towards a more conduct-based supervision approach, which includes a review and an approval of the individual insurance product by the responsible supervisory authorities and the insurance undertakings itself through a so-called product oversight process [7]. In general, the lawfulness of an insurance product based on crypto currency under such a product oversight process will depend to a large extent on the concrete design of the underlying insurance contract, especially the contractual definition of the insured event.

2.2. Definition of the Insured Event

Every insurance contract must define the occurrence of the so-called insured event, which is the trigger of loss or damage for the insured. As the most common source of legal disputes between policyholders and insurance companies, the insured event must be defined clearly and in unambiguous terms within the insurance contract. The contract also defines which sum must be paid to the insured in the case of occurrence of the insured event. This can be a fixed sum (e.g. in

the case of a life insurance) or a sum that depends on the extent of the concrete damage (e.g. in the case of a car insurance). In practice the insurance contract is often still paper-based containing the general terms and conditions of insurance (GTCI). Smart contracts- or blockchain based processes could enable cheap and fast policy management and payments, avoiding administrative costs and minimizing legal disputes. Theoretically such blockchain-based insurance contracts could be even paid in crypto currency [8]. Several blockchain-based insurance solutions already exist, such as for example "Fizzy", the smart insurance of AXA against flight delays, which is probably the first blockchain-based insurance product on the market (AXA), even though "Fizzy" is as kind of a hybrid solution between a purely blockchain-based insurance and a traditional insurance product.

3. ABOUT A LINK BETWEEN BLOCKCHAIN, TRADITIONAL INSURANCE AND POLITICAL RISK

3.1. Trust, Insurance and Blockchain

In 1686, when Lloyd's was founded in a London coffee house as the first insurance company, the global insurance industry was a business of good faith, as it is still today. Therefore, a trust engine like blockchain technology is able to radically change the insurance industry while improving transparency and trust across the whole industry. A blockchain database is transparent, which means that anyone online can read it. In addition, it is a distributed database, so the information is spread among many computers around the world, making it difficult or even impossible to destroy the information. And a blockchain database resists to all subsequent manipulations of its past transactions. Finally, blockchain gives the possibility to be *certain*, for example when it must be defined if an insured damage happened on Sunday or on Monday [9].

In the insurance industry, but also in banking, *trust* is essential. The client must trust the insurance company in the way that as an insure he wants to be sure, that the damage will be covered in the case of an insured event – even when this event will happen 20 or 30 years in the future. A blockchain can potentially replace this need for trust, which is guaranteed today mainly by the insurance companies or the insurance brokers. In this way, Fintech or Insurtech solutions can allow insurance solutions where trust is guaranteed through technology instead of traditional companies. For example, a blockchain can specifically define the risk, the premium and the insured event. In the case of a damage, the compensation will then be paid automatically, without any involvement of an insurance company. At this moment this is however still a vision for a future – and products such as "Fizzy" can be considered as a starting point toward this future (See 2.2 above).

3.2. Definitions

3.2.1. Fintech and Insurtech

As the field of Fintech in general is relatively new, scientific literature is limited concerning Fintech and blockchain issues within the scientific communities of insurance and risk. Therefore, there are still broad discussions within the scientific community, how the concepts of Fintech and Insurtech can be described and defined [10, p. 3]. Insurtech can be defined as all technologies of insurance innovation, such as insurances based on artificial intelligences, smart insurance contracts and other blockchain based insurance models [11]. In this way, Insurtech companies can be defined as firms using digitalization, especially blockchain technology, for insurance solutions or insurance services [10]. Fintech can be understood as a generic term, not only covering the insurance sector, but also other sectors of the financial market, such as the banking

or the securities market. In this way, the word Fintech can be defined as computer programs and other technologies used to support the financial industries and it combines in this way two complementary areas: financial services and solutions based on advanced technology, such as for example blockchain applications [12, p. 12]. To summarize, blockchain technology used for insurance is one element of Insurtech – it focuses on the question, how blockchain technology can be used in the insurance industry [See 13].

3.2.2. Blockchain, Technology and Token

Blockchain can be defined as a data protocol for non-trusted partners (with potential conflicts of interest) to collaborate and agree on the validity of transactions without anyone overseeing that process. This is a transparent process providing a distributed, digital, chronological ledger, which is immutable, shared in real time and fully auditable. At the beginning, blockchain was just a protocol that supported recording transactions in which the cryptocurrency bitcoin was being transferred between two individuals. It was needed to make sure that the origin of a bitcoin could be validated and double spending avoided in the absence of a central supervisory authority overseeing the bitcoin market. Today blockchain technology has evolved to become a protocol that allows us to record any type of transactions transferring value [14, p. 8 ff.]. Smart contracts are not necessarily blockchain-based. The term smart contract was already defined in 1996 by [15] as a *"set of promises, specified in digital form, including protocols within which the parties perform on these promises"* [16, p. 124]. Today however, smart contracts are often blockchain- or token-based, which means that the smart contract is stored inside a blockchain, based on a specific token. A token-based blockchain system can be described as a set of information that can be clearly identified and assigned. This set of information can be in designed in different forms and take various kind of functions, such as the function of digital money such as Bitcoin. On certain systems this information is called token. The blockchain technology make sure that this information is unique and unambiguous. Through a so called public and private key, stored and created in crypto wallets, the ownership on a blockchain can be clearly defined [17, p. 124 f.]. In the following section there will be some general reflections based on case examples how a smart insurance solution against political risks could be envisaged.

3.3. Political Risk Insurance: Possible Case Examples

A political risk insurance contract (PRI) can be designed for example with the aim to protect policyholders against the financial consequences of a trade war between different countries, for example between China and the US or between China and Japan. Or, it is conceivable that there will be a smart insurance contract against a natural disaster or a terrorist attack in Europe. In all these examples the insured event must be described and defined in the smart insurance contract. This contract must provide a clear and unambiguous definition of the insured event. In a first step, the risk of the realization of the insured event must be defined from a legal point of view; respectively, the defining criteria for a terrorist attack, a specific natural disaster or a trade war must be found in our cases. After, this legal definition of the risk must be translated into a smart contract through a blockchain. This smart contract is then the basis for the calculation of the individual risk and consequently the amount of the premium. In this way the smart contract will clearly define if the insured event has occurred or not.

There are for example various legal possibilities to define a terrorist attack: for example, an attack can be defined as terroristic, if it has been committed by a terror group, such as for example Al Qaida or ETA. An indication for a terror attack is also the inclusion in an official and independent database, such as the Terrorism Database (https://www.start.umd.edu/gtd/) or the Global Terrorism Index (See for example the Global Terrorism Index 2017). Of course, all these criteria are to a certain extent subjective – however, as the smart contract can be consulted by

everyone involved, it will be at any time transparent, how a terror attack, a trade war or a specific natural disaster is defined. The same principle shall apply for the calculation of the insurance premium: for example, if a country is a high-risk country concerning terrorism, such as for example Iran or Iraq, the premium calculated through the smart contract will be obviously higher, when an insured company is active in one of these countries. The risk-classification of the countries (and other parameters) must be based on criteria, such as for example the FATF-country-list (See FATF-list on http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/). Obviously, the smart contract must be supplied with as much objective data as possible. In this way, the insurance premium will be individualized according to the risk taken, and the occurrence of the insured event will be objectified – in contrast to the situation today, where the definition of the insured event is in general within the discretion of the insurance company, especially in the case when a certain damage should be covered. Concerning the risk of a terrorist attack, the example above can also be applied on other kind of insurances, such as a simple travel insurance. In such a case, the smart contract will define, when and in which country a terrorist attack has occurred, and the contract will be able to pay out the insured sum automatically, when a flight in this country has been booked a certain timespan after the terrorist attack by the policyholder.

4. CONCLUSIVE REMARKS

The way to purely blockchain-based smart insurance contracts against political risk will be a long process and can be undertaken only step by step. From a legal point of view there are barriers in private law, especially in contractual law as smart contracts cannot be considered as contracts in the legal sense, as a legal contract must be based on two corresponding declarations of intent. Therefore, an important step will be the recognition of smart contracts as generally accepted legal contracts. In public law, especially financial supervisory law, the recognition of virtual currencies for the payment of insurance premiums will be a key aspect for the future. When these barriers will be overcome, the fields of application for smart insurance contracts against political risks seem to be unlimited: every political risk, which can be legally and technically translated into a smart insurance contract, can be subject of a smart insurance contract.

REFERENCES

[1] Manes, A., Versicherungswesen, Erster Band, Allgemeine Versicherungslehre, Springer Verlag, Wiesbaden, Germany, 1922.

[2] EIOPA (European Insurance and Occupational Pensions Authority), Report on best practices on licencing requirements, P2P insurance and principle of proportionality in an InsurTech context, Frankfurt, 2018.

[3] EIOPA (European Insurance and Occupational Pensions Authority), Regulatory barriers to InsurTech in European legislation, Frankfurt, 2019.

[4] Roelli, H./Keller M./Tännler K., Kommentar zum Schweizerischen Bundesgesetz über den Versicherungsvertrag vom 2. April 1908, Bd. I: Die allgemeinen Bestimmungen, Art. 1-47, 2. Auflage, Berne, Switzerland, 1968.

[5] Kuhn, M.W., in Müller-Studer L./Eckert M.K. (Ed.), Privatversicherungsrecht – Unter Berücksichtigung des Haftpflicht- und Aufsichtrechts, Schulthess Verlag, 3. Auflage, Zurich, Switzerland, 2010.

[6] Brook, N., Insurance & Reinsurance: Jurisdictional Comparisons, Sweet&Maxwell, London, UK, 2012.

[7] Marano, P./Siri, M., Insurance Regulation in the European Union: Solvency II and Beyond, Springer Verlag, Wiesbaden, Germany, 2017.

[8] Gatteschi, V. et al., Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?, in Future Internet, 10(2):20, 2018.

[9] Gansky, L., Radical Trust: How Blockchain Liberates the Next Economy, PublicAffairs Publications, New York, US, 2018.
[10] Doulger, W., InsurTechs – Status Quo, Entwicklungslinien und Potenziale, Verlag Versicherungswirtschaft, Karlsruhe, Germany, 2016.
[11] Ricciardi, V., InsurTech Definition as its Own Manifesto, in Chishti S./Barberis J. (Ed.), The InsurTech Book, John Wiley & Sons, Hoboken, US, 2018.
[12] Nicoletti, B., The Future of Fintech: Integrating Finance and Technology in Financial Services, Springer Verlag, Berlin, Germany, 2017.
[13] Avdeev, E., Application of the Blockchain Technology in the Insurance Industry, Universität St. Gallen, St. Gallen, Switzerland, 2018.
[14] Fraebel, Y., Die Blockchain-Technologie. Ein Überblick über die Funktionsweise, Grin-Verlag, Munich, Germany, 2018.
[15] Szabo, N., Smart Contracts: Building Blocks for Digital markets, Extropy Magazine #16, 1996.
[16] Mukhopadhyay, M., Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity, Packt Publishing, Birmingham, UK, 2018.
[17] Franco, P., Understanding Bitcoin: Cryptography, Engineering and Economics, Wiley & Sons, Hoboken, 2014.

AUTHORS

Remy Zgraggen

GDPR COMPLIANCE FOR BLOCKCHAIN APPLICATIONS IN HEALTHCARE

Anton Hasselgren[1], Paul Kengfai Wan[2], Margareth Horn[3], Katina Kralevska[4], Danilo Gligoroski[4] and Arild Faxvaag[1]

[1]Department of Neuromedicine and Movement Science, NTNU, Norwegian University of Science and Technology, Trondheim, Norway
[2]Department of Manufacturing and Civil engineering, NTNU, Norwegian University of Science and Technology, Trondheim, Norway
[3]Department of Sociology and Political Science, NTNU, Norwegian University of Science and Technology, Trondheim, Norway
[4]Department of Information Security and Communication Technology, NTNU, Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT

The transparent and decentralized characteristics associated with blockchain can be both appealing and problematic when applied to a healthcare use-case. As health data is highly sensitive, it is therefore, highly regulated to ensure the privacy of patients. At the same time, access to health data and interoperability are in high demand. Regulatory frameworks such as GDPR and HIPAA are, amongst other objectives, meant to contribute to mitigating the risk of privacy violations of health data. Blockchain features can likely improve interoperability and access control to health data, and at the same time, preserve or even increase, the privacy of patients. Blockchain applications should address compliance with the current regulatory framework to increase real-world feasibility. This exploratory work indicates that published proof-of-concepts in the healthcare domain comply with GDPR, to an extent. Blockchain developers need to make design choices to be compliant with GDPR since currently, none available blockchain platform can show compliance out of the box.

KEYWORDS

Blockchain, DTL, health data, GDPR, privacy regulations

1. INTRODUCTION

The current status in data privacy could be categorized as the post-privacy area due to the unintended consequences of the big data revolution. The famous Cambridge Analytica scandal [1] is an example of how re-identification can be achieved by cross-analysing large data sets containing private information. The technology revolution that has driven us to post-privacy has not been stopped through privacy acts such as General Data Protection Regulation (GDPR). At the same time, we are currently in another (r)evolution that can restore data privacy - blockchain.

In 2018, The European Union instituted the GDPR [2], which regulates the collection, processing and securing of personal data, including protected health information (PHI). Art. 4(15) of the EU GDPR, defines data concerning health as: "personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status."

David C. Wyld et al. (Eds): BIBC, AISO, EDTECH - 2020
pp. 23-35, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101303

Health Insurance Portability and Accountability Act (HIPPA) is essential for U.S. healthcare law and deals mainly with privacy rights and access rather than ownership of patient data [3]. Each state has ownership of patient data of its citizens, and in this case, it is controlled by respective state law. Since there are 50 states, there are 50 differing laws, court cases and interpretations of that ownership of patient data. New Hampshire is the only state which enacted the legislation stating that the ownership of health data lies with the patient. How GDPR will interact and comply with U.S. state laws remains to be determined. HIPPA is an important regulatory framework but the scope of this work only covers GDPR compliance.

Blockchain, first introduced with the launch of Bitcoin back in 2008, has become more diluted in its definition. Currently, there is no fixed or a widely accepted definition of the term blockchain. To clarify its use in this research, we have defined blockchain as a distributed, decentralized and tamper-proof ledger without any centralized control. Blockchain technology and other Distributed Ledger Technologies (DLT) could increase our data privacy and empower individuals with control and access over their data, including health data. The objective of this study is twofold: (i) to dissect the various designs of blockchain and explore GDPR compliance for different components in established or proposed blockchain applications in the healthcare sector and, (ii) to provide a future researcher with guidance in how to comply with GDPR when designing blockchain application within the healthcare domain.

The rest of this paper is organized as follows: Section 2 provides a brief introduction to blockchain technology and outlines previous work addressing blockchain compliance with GDPR; Section 3 presents the research approach; Section 4 describes four blockchain applications in healthcare identified through the literature; Section 5presents our results and analysis; Section 6 provides a discussion and conclusion to the work, and givesrecommendations for future work.

2. GDPR AND BLOCKCHAIN

This section gives a brief introduction to blockchain and GDPR. We can broadly categorize blockchain as; public permissionless, private permissioned and federated permissioned. The categorization is important in order to design applications in relevant sectors to achieve social and economic goals. In a public blockchain, everyone in the network holds equal rights and the ability to access the ledger. While nodes need to be certified to join the consensus process in private and federated blockchains, which makes them permissioned. The French National Commission on Informatics and Liberty (CNIL) recommends private permissioned blockchains because of the possible compliance with GDPR [4]. The third blockchain category is a combination between public and private, which are referred to as a federated or hybrid blockchain [5].

Previous research has explored blockchain platforms and their feasibility for healthcare [6] and concluded that none of the most widely used blockchain platforms were ideal for healthcare, out of the box. Other work has identified important properties and characteristics in different types of blockchain, and they need to be considered in the initial design phase; identity management, efficiency according to energy use, immutability, ownership management and transaction approval [5]. Public, private and federated blockchains handle these properties differently and each component may have their limitation [7].

As detailed by the European Union Blockchain Observatory and Forum [4], in principle, there are no contradictions between the goals of GDPR and DLT. However, there seem to be at least three areas in which GDPR still does not offer enough clarity about how real-world DLT applications for the health sector should be developed: (1) accountability and roles (e.g., how to identify a data

controller in a public DLT), (2) anonymization of personal data (e.g., which techniques are sufficient to anonymize personal data to the point where the resulting output can potentially be stored in a DLT), and (3) GDPR rights conflicts (e.g., how to rectify or remove personal data that are recorded in a DLT that is immutable by nature, or who is responsible for requesting and managing the "freely, specific, informed, and unambiguous" consent from a data subject, especially if the data controller is not specified) [8]. With regards to the anonymization of personal data, it is clear that GDPR does not apply to anonymized data and thus, this type of information can be stored on the open ledger. However, what qualifies as anonymized data is still unclear. The only indication today is that it must be irreversibly impossible to identify an individual through any of the means "reasonably" likely to be used [9].

Smart contracts are one of the components that have been proposed on blockchain platforms to reduce the need for a third party. It enables a new type of autonomous regulation that executes transactions when all the requirements are fulfilled [10]. All legal rules and contracts are transposed into digital and software rules, which means that smart contracts can be the regulator in blockchain networks and rules are enforced accordingly [11]. For example, after a user authenticates its digital identity successfully, a smart contract can grant authorization and access to his/her medical records by the requestors [12]. However, Giordanengo at al. analysed some use cases of smart contracts and found out that none of the studies have reached the stage of production and concluded that it is not ready for implementation in the healthcare domain [13].

The design options in a blockchain application are wide, and there is an increase in both research and innovation. In order to design blockchain applications for healthcare use-cases, there are several important design choices the developer has to make, with the three most prominent: (1) choice of platform/network, (2) on/off chain data storage and (3) identity solution for interaction with the system.

2.1. Related Work

This section highlights previous work which has investigated blockchain compliance with GDPR. There is limited published research under this topic in the literature, but previous work has indicated the need for standardization [6] [7].

Two reports published by EU entities: The EU blockchain Observatory and Forum - Blockchain and the GDPR [4] and the European Parliamentary Research Service (EPRS) - Blockchain and the general data protection regulation [14] provide guidance in blockchain compliance with GDPR.

Blockchain and the GDPR is a thematic report published in 2018 where accountability and roles, as well as anonymization of personal data, are addressed. This report highlights the need for each blockchain use-case to be thoroughly analysed and rated in various interpretations - compliance with GDPR is not about the technology but rather, how it is utilized. The report also points out the need to avoid storing personal data on a public blockchain and anonymous data techniques such as obfuscation, encryption and aggregation should be used. The report proposed some principles to consider when designing blockchain architectures such as; considering user perspective, analysing where the personal data appears and who is responsible for the processing.

The Blockchain and the GDPR report have defined roles for three main actors: data subject, data controller and data processor, and outlined in the report that it can be problematic to identify the data controller in blockchain networks. The report also presents some techniques, such as reversible encryption and hashing, to achieve anonymous or pseudo-anonymous data. It is also

important to consider if personal data should be involved when linking private chains with public chains.

In the report by the European Parliamentary Research Service, blockchain is defined as a combination of many different forms of distributed databases that present variation, both in complexity and governance agreement. The report gives an account of difficulties in whether personal data, can be anonymized to the extent that it meets the GDPR threshold of anonymization. Two types of compliance tension are expressed: (1) GDPR assumes that there is a data controller, which is often not the case in blockchains and (2) the right to be forgotten, which is problematic in an immutable ledger. Furthermore, it is expressed that it is difficult to assess the compatibility between blockchain and GDPR without having to pay attention to the nuances in blockchain configurations. There is also a request for further clarifications of concepts such as; ”anonymous data”, ”data controller” and the meaning of”erasure” under Art. 17.

There are some examples where blockchains and GDPR compliance are tested, such as the proof of-concept (PoC) developed for the use case of managing blood glucose data [26]. The concept provides a system for immutable, interoperable and GDPR compliant data exchange. In the PoC, it is highlighted that blockchain has a great potential to improve information transactions in a secure and transparent manner, between patients and providers [26]. Two tested solutions where explored, one based on the public IOTA blockchain and one in combination with public IOTA plus, a private IPFS (Inter Planetary File System) cluster. In the public IOTA it became difficult to eliminate the risk of personal data link ability and combining a public DLT and IPFS has a high degree of complexity. It is also highlighted that there are limitations in identifying a data controller since the public DLT ecosystem is formed by multiple healthcare stakeholders, as well as patient consent management. They argue that each use-case must be carefully considered when blockchain-based system is designed for health data exchange.

A private blockchain is suggested in the CUREX project, which is argued to be in GDPR compliance by design in a decentralized architecture [15]. In this project, it is argued that all data transactions in the health sector and their vulnerability are depend on a private blockchain infrastructure, to integrity of risk management. The CUREX project’s goal is to ensure the integrity of the risk assessment process of all data transactions.

Two other suggested GDPR-compliant design concepts address health data collected by sensors in different types of mobile and smart devices [16][17]. Both designs were described to address the vulnerability in centralised data storage controlled by service providers and ”the right to own and share personal information”. One of the concepts is combining blockchain with cloud storage and machine learning techniques to give users the possibility to share personal data easily and securely. In this model, the data is encrypted before uploaded to the cloud storage and secured by a hash function. The access to the data is distributed among multiple key keepers where no visible personal information is involved because the blockchain allows pseudonyms [16]. While the former considered the limits blockchain has to store large-size data that are continuous-dynamic, [17] propose architecture for efficient access and control mechanisms. In their work, the privacy challenge was addressed, and their design concept is an efficient privacy-preserving access to give the users full control over their own data.

3. METHOD

The research approach in this work has been: (i) review of four different blockchain proof-of concepts in health care; (ii) review of GDPR and how the regulations apply to health informatics; and (iii) an exploratory analysis on how the platforms reviewed in the review (i) comply with the relevant articles identified in GDPR (ii).

The blockchain based proof-of-concepts in (i) were identified through a scoping search in PubMed and Scopus.

The following documents were identified and utilized in (ii):

- GDPR (official document) [2];
- Blockchain and the General Data Protection Regulation [18].

4. BLOCKCHAIN-BASED HEALTHCARE APPLICATIONS

This section describes four different blockchain applications that were identified in a scoping search in PubMed and Scopus. These four applications were included based on their different architecture; the sample is not meant to be comprehensive. MedRec [19] is a blockchain- based solution for personal control of identity and the distribution of health information. The system is designed on the public Ethereum blockchain. This means that transactions, including metadata, which is sensitive in medical context, are visible to everyone who has access to the blockchain. And if someone can identify the patient's real-world identity and Ethereum account, one can determine the relationship between the health providers and the patients. In order to circumvent this privacy issue, MedRec anonymized metadata through disassociating each patient's identity from the provider, where each provider makes a new identity Ethereum account for each patient provider relationship. The purpose is to enable patients to establish public relations without revealing the real-world identities.

EMRshare [20] is a health data sharing application where different entities such as health provider, data scientists and patients interact using the permissioned Hyperledger blockchain. Transactions such as health data requests, approval or rejection action are stored on blockchain. While actual medical data are stored off-chain and encrypted with asymmetric encryption for security purposes. EMRshare also enables patients, the data owner, to anonymize their name or identity in the medical records before reaching the requestors.

VerifyMed [21][23] is a public Ethereum blockchain platform with the aim to validate the authorization and competence of healthcare workers in a virtualized healthcare environment. VerifyMed enables healthcare workers to document their work history and competence in the form of a de-centralized portfolio. VerifyMed combines and stores three forms of data items; evidence of authority, evidence of experience and evidence of competence to build their portfolios. Digital signatures scheme is also incorporated in VerifyMed to ensure ownership is established on each verified evidence. As an example of how a typical user interface looks like in a blockchain- based application, we give Figure 1, which is taken from VerifyMed [22], [23].

Figure 1. Page from the User Interface of VerifyMed for showing detailsabout all data related to a healthcare worker [22], [23]

FHIRChain [24] is a public Ethereum blockchain architecture for secure and scalable clinical data sharing with the goal to meet the requirements of The Office of the National Coordinator for the Health Information Technology (ONC) such as privacy preserving and health information security. FHIRChain stores encrypted metadata on the network rather than storing encrypted sensitive health data. It uses digital health identity, which utilizes public- key cryptography to generate and manage the identities. Often clinical data research data format and structures varies from institution to institution, which makes data sharing challenging, FHIRChain is developed based on HL7 Fast Healthcare Interoperability Resources (FHIR) to enforce consistent data formats for easier information sharing.

These proposed blockchain concepts within the healthcare domain primarily focus on solving interoperability without compromising the privacy and security of sensitive health data. Identity management for both patients and health workers are also considered as part of the proposed applications. However, the research work focusing on the degree of compliance to GDPR and other health data regulatory frameworks remains limited.

5. RESULTS

The results are presented mainly in Table 1 - relevance of GDPR for healthcare and analysis of compliance and Table 2 - Comparative analyses.

GDPR will have a significant impact on the healthcare sector in collecting, processing, and securing protected health information. Healthcare institutions (HI), are obligated to ensure that data is collected for a specific and legitimate use and only used for that purpose. Further, a healthcare organization will be required to obtain exclusive consent or permission from the patients (the data subject) to use their data according to (Art. 7).

GDPR indicates that the ownership of health data should be with the patients, enabling patients to have greater autonomy over their data. Healthcare providers are obligated to furnish patients with complete information when they request it, within specified time limits (Art. 15).

Additionally, GDPR requires organizations to report a data breach within 72 hours (Art. 33) and notify the affected individual (Art. 34). The onus will, therefore, be on healthcare organizations to ensure that data is highly secured and protected from unauthorized access or face rapid reporting requirements of breaches and possible severe financial penalties (see Art. 83). This is important when it comes to embracing new digital technologies like blockchain because issues such as misuse of patients' PHI would result in losing trust in healthcare institutions and delaying the adoption of blockchain in enhancing information sharing.

Table I summarizes what healthcare institutions (HI) must consider when using blockchain and DLT to secure and protect PHI and avoid costly fines for non-compliance.

Table 1. Relevance of GDPR for healthcare

Article in GDPR	Compliance	Impact in healthcare
Art. 30 (Records of processing activities), Art. 35 (Data protection impact assessment)	Able to conduct information audit to demonstrate GDPR compliance	HI is required to keep an up-to-date and detailed list of their processing activities using a data protection impact assessment. The list should include the purposes of the processing, what kind of data you process and who has access to it in the organization
Art. 6 (Lawfulness of processing), Art. 7 (Conditions for consent)	Legal justification for processing health data	HI can justify the purpose according to one of the six conditions. E.g Patients has given consent for the processing. Extra obligation such as the opportunity to revoke consent must be available to patients
Art. 12 (Transparent information, communication and modalities for the exerciseof the rights of the data subject)	Clear information about the data processing and legal justification in privacy policy	HI is obligated to inform patients that health data is collected. HI should explain why this is collected, how it is processed, who has the access and how it is secured using clear and plain language, particularly when addressing specifically to a child.
Art. 33 (Notification of apersonal data breach to the supervisory authority), Art. 34 GDPR (Communication of a personal data breach to the data subject)	Have a process to notify the authorities in the event of a data breach	HI is required to notify the supervisor authority in their jurisdiction within 72 hours learning of the health data breached or exposed. Patients should be notified without undue delay in plain language, if the breach is likely to put them at risk.

Art. 32 (Security of processing)	Encrypt, pseudonymize or anonymize personal data whenever possible	HI is to encrypt, pseudonymize or anonymize PHI whenever feasible.
Art. 25 (Data protection by design and by default), Art. 5 (Principles relating to processing of personal data)	Data protection is considered at all times, including at the beginning of developing aproduct	HI should implement appropriate technical (encryption) and organizational measures (deleting patient's data that is no longer needed) to protect data. HI which adheres to data protection principles when processing of personal data is involved.
Art. 25 (Data protection by design and by default)	Designated person for ensuring GDPR compliance across the organization	HI should designate someone that is accountable for GDPR compliance which includes evaluation of data protection policies and the implementation of policies. HI should be able to verify the patient's identity.
Art. 15 (Right of access by the data subject)	Able to verify the patients' identity	HI is obligated to furnish patients with complete information when they request it and should be able to comply within a month. HI should be able to verify the patient'sidentity.
Art. 17 (Right to erasure/ 'right to be forgotten')	Easy to delete personal data upon request	Patients should have the right to request to delete all health data and HI should honor their request within a month. HI may have grounds to deny the request such as compliance with a legal obligation. HI should be able to verify the patient's identity.
Art. 18 (Right to restriction of processing)	Easy to stop data processing upon request	Patients can request HI to restrict or stop processing their health data if certain grounds apply, such as dispute about the lawfulness of the processing. HI may be allowed to keep storing their data although the processing is restricted.
Art. 24 (Responsibility of the controller)	Establish the responsibility and liability of the controller	Any processing of personal data carried out by HI or on HI's behalf, responsibilities should be established which includes implementing appropriate technical and organizational measures. This is to ensure and to be able to demonstrate that processing is performed lawfully
Art. 20 (Right to data portability)	Easy to receive a copy of your personal data and share with another in a simple format	From a privacy standpoint, GDPR offers higher patients' autonomy over their data, instead of HI. This means patients should be able to receive health data in a readable format or share with other HI.

Blockchain structure can enhance the traceability of data making transactions auditable and transparent. In addition, storing data on the blockchain ledger could increase data integrity due to the inherited immutability property. However, any form of information stored on blockchain remains on blockchain which might violate GDPR since patients should have the right to erase their personal data. Although, it is common that national health data law prohibits the deletion of patient data from medical health records. Storing metadata could be an alternative to storing the full dataset. Storing metadata on the blockchain can pseudonymize a patient's identity and to further protect patient's identity, encryption technology such as zero-knowledge proofs could be implemented to prevent any forms of identification.

Table 2 presents a summary of how four different blockchain-based applications (presented under Section 4) comply with the relevant GDPR articles presented in Table 1.

Table 2. Comperative analysis

Features	GDPR article	Blockchain application			
		MedRec	EMRshare	FHIRchain	VerifyMed
Able to conduct information audit to demonstrate GDPR compliance	Art. 30 GDPR (Records of processing activities)	Yes	Yes	Yes	Yes
	Art. 35 GDPR (Data protection impact assessment)	N/A	N/A	N/A	N/A
Legal justification for processing health data	Art. 6 GDPR (Lawfulness of processing))	N/A	N/A	Yes	N/A
	Art. 7 GDPR (Conditions for consent)	N/A	Yes	Yes	N/A
Clear information about the data processing and legal justification in privacy policy	Art. 12 GDPR (Transparent information, communication and modalities for the exercise of the rights of the data subject)	Yes	Yes	Yes	Yes
Have a process to notify the authorities in the event of a data breach	Art. 33 GDPR (Notification of a personal data breach to the supervisory authority)	No	No	No	No
	Art. 34 GDPR (Communication of a personal data breach to the data subject)	No	No	No	No
Data protection is considered at all times, including at the beginning of developing a product	Art. 25 GDPR (Data protection by design and by default)	Yes	Yes	Yes	Yes
	Art. 5 GDPR (Principles relating to processing of personal data)	N/A	N/A	N/A	N/A
Encrypt, pseudonymize or anonymize personal data whenever possible	Art. 32 GDPR (Security of processing)	Yes	Yes	Yes	Yes
Designated person for ensuring GDPR compliance across the organization	Art. 25 GDPR (Data protection by design and by default)	No	No	No	No
Should be able to verify the patients identity.	Art. 15 GDPR (Right of access by the data subject)	Yes	Yes	Yes	No
Easy to delete personal data upon request	Art. 17 GDPR (Right to erasure/‘right to be forgotten’)	No	No	No	No
Easy to stop data processing upon request	Art. 18 GDPR (Right to restriction of processing)	N/A	No	N/A	No
Establish the responsibility and liability of the controller	Art. 24 GDPR (Responsibility of the controller)	No	No	No	No
Easy to receive a copy of your personal data and share with another in a simple format	Art. 20 GDPR (Right to data portability)	Yes	Yes	Yes	No

All four concepts use slightly different components of blockchain technologies. For example, FHIRchain uses a public blockchain (Ethereum) while EMRshare uses a permissioned blockchain (Hyperledger). These blockchains vary in some properties, such as the degree of visibility, but both types of blockchains can store transaction chronological with high data integrity due to the immutable structure. Blockchain data structure is easily auditable, which can make it inherited compliant with Art 30 and 35.

Identity management also forms a core technology in all these frameworks. This is one of the key compliances to Art 15. ”Right access by the right data”, before executing requests from patients to obtain health information or stop processing their health data. This is to prevent any misuse of private health data by the wrong person. For example, FHIRchain adopts digital identity to verify and authenticate the identity of clinicians. VerifyMed does not incorporate identity management to authenticate as the application utilizes evidence of authority to proof the credential of the clinicians.

Table 2 highlights that the blockchain concepts identified for this work did not fulfill the requirement of the right to forgetting (Art. 17). Patients can have the right to request for deletion of their information but the immutability nature of blockchain contradicts this article. To circumvent this, proposed concepts, such as FHIRchain, only stores metadata and protected with encryptions. Although it is not erasure, it prevents an unauthorized person from obtaining information and linking the pseudonymized metadata to patient’s identity. Currently, these four explored concepts did not state any procedures to notify authorities if any violation of GDPR is detected and might, therefore, lack compliance with (Art 33). A smart contract can be designed by sending a notification to relevant authorities when a breach is detected. In addition to that, a designated person for ensuring GDPR compliance within the network should be considered for future work.

6. DISCUSSION

There is an increased focus on blockchain technology in healthcare sector in both academic spheres and the private sector with the expectation that this technology could have a positive impact on achieving better interoperability and access to health data [25]. This can bring medical advances, such as enabling collaborative treatment and care decision. However, storing patient’s health data or even metadata is considered highly sensitive and could violate patient’s data privacy. In order to protect patient’s health data, GDPR has defined rules and guidelines to ensure that data processing and handling comply. However, research focusing on the degree of compliance of proposed blockchain solutions to GDPR in the healthcare sector remains limited.

The contribution of this paper explores how four different blockchain-based healthcare applications comply with the identified articles in GDPR. This analysis can provide further research guidance on how to achieve GDPR compliance and what architectural design choices that need to be considered.

As outlined under Section 5, compliance with Art 30 and 35 are achieved in the four healthcare applications identified due to the inherited characteristics of blockchain - storage of transaction chronological with high data integrity. Identity management is a core technology for healthcare applications, and it is also a key compliance factor in GDPR with Art 15: Right access by the right data. This is mainly to prevent any misuse of private health data by the wrong person and compliance is achieved with three out of the four concepts.

Currently, none of the proposed concepts fulfil the requirement of the right to be forgotten (Art 17), as shown in Table 2. This indicates that patients should have the right to request the deletion

of their information. However, this is often regulated by national health data laws that prohibit the deletion of data from medical health records. Nevertheless, compliance with this article is problematic due to the immutable nature of blockchain. Compliance can be achieved by making all data stored on the ledger entirely anonymous or fully encrypted. Hence, we encourage researchers to explore full anonymity in blockchain applications for this domain.

None of the investigated blockchain concepts did consider the process of notifying authorities if any violation of GDPR is detected stated in Art. 33 as shown in Table 2. This could potentially be implemented by a smart contract to ensure automated and imitate notifications to relevant authorities upon data breach. A way to ensure that any new blockchain solutions that handle sensitive health data comply with GDPR, is to keep an up-to-date list using Data Protection Impact Assessment (DPIA) (Art. 35) to any authorities or regulators upon requests. This can avoid any solution providers from subjecting to severe penalties, fines of up to 20 million dollars or 4 percent of annual revenue whichever is higher [2] and losing trusts from its users. Therefore, researchers should ensure Art. 33 and 35 are in place before deployment in the real-world scenario.

6.1. Conclusion

Blockchain compliance with GDPR for healthcare applications is highly dependent on how the technology is utilized and the architectural design. It seems infeasible to conclude that specific blockchain frameworks or main blockchain characteristics are more compliant than others, it is rather use-case dependent and based on several design aspects that together could build up towards GDPR compliance. This research shows that blockchain may enhance GDPR in some aspects and be challenging with some others. It is important that this topic is being addressed and highlight potential compliance issues to increase adoption and acceptance of the technology in this field. There is no such thing as GDPR-compliant blockchain technology for healthcare, but it might be GDPR-compliant use cases and applications. We encourage future work to address GDPR compliance to get closer to real-world adoption of blockchain technology in the healthcare sector.

REFERENCES

[1] Hal Berghel. Malice domestic: The Cambridge analytica dystopia. Computer, (5):84–89, 2018.
[2] European Commission. Reform of EU data protection rules, 2018. https://gdpr.eu, accessed 2020-06-10.
[3] George J Annas et al. Hipaa regulations-a new era of medical- record privacy? New England Journal of Medicine, 348(15):1486– 1490, 2003.
[4] European blockchain observatory and forum. Blockchain and the gdpr, 2018. https://www.eublockchainforum.eu/reports, accessed 2020-06-13.
[5] Fran Casino, Thomas K Dasaklis, and Constantinos Patsakis. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36:55–81, 2019.
[6] Tsung-Ting Kuo, Hugo Zavaleta Rojas, and Lucila Ohno-Machado. Comparison of blockchain platforms: a systematic review and healthcare examples. Journal of the American Medical Informatics Association, 26(5):462–478, 2019.
[7] Paolo Tasca and Claudio J Tessone. Taxonomy of blockchain technologies. principles of identification and classification. arXiv preprint arXiv:1708.04872, 2017.
[8] Protection Regulation. Regulation (eu) 2016/679 of the european parliament and of the council. REGULATION (EU), 679:2016, 2016.
[9] Khaled El Emam and Cecilia A´ lvarez. A critical appraisal of the article 29 working party opinion 05/2014 on data anonymization techniques. International Data Privacy Law, 5(1):73–87, 2015.

[10] Henry Kim and Marek Laskowski. A perspective on blockchain smart contracts: Reducing uncertainty and complexity in value exchange. In 2017 26th International Conference on Computer Communication and Networks (ICCCN), pages 1–6. IEEE, 2017.
[11] Primavera De Filippi and Samer Hassan. Blockchain technology as a regulatory technology: From code is law to law is code. arXiv preprint arXiv:1801.02507, 2018.
[12] Paul Kengfai Wan, Lizhen Huang, and Halvor Holtskog. Blockchain-enabled information sharing within a supply chain: A systematic literature review. IEEE Access, 8:49645–49656, 2020.
[13] Alain Giordanengo. Possible usages of smart contracts (blockchain) in healthcare and why no one is using them. 2019.
[14] European Parliamentary Research. Blockchain and the gdpr, 2019. https://www.europarl.europa.eu/RegData/etudes/ STUD/2019/634445/, accessed 2020-06-13. [15]Antonio Jesus Diaz-Honrubia, Alejandro Rodriguez Gonzalez, Juan Mora Zamorano, Jesu´s Rey ime´nez, Gustavo Gonzalez- Granadillo, Rodrigo Diaz, Mariza Konidi, Panos Papachristou, Sokratis Nifakos, Georgia Kougka, et al. An overview of the curex platform. In 2019 IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS), pages 162–167. IEEE, 2019.
[16] Xiaochen Zheng, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaqun Ordieres-Mere. Blockchainbased personal health data sharing system using cloud storage. In 2018 IEEE 20th International Conference on e- Health Networking, Applications and Services (Healthcom), pages 1–6. IEEE, 2018.
[17] Koosha Mohammad Hossein, Mohammad Esmaeil Esmaeili, Tooska Dargahi, et al. Blockchainbased privacy-preserving healthcare architec- ture. In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), pages 1–4. IEEE, 2019.
[18] M Finck. Blockchain and the general data protection regulation: Can distributed ledgers be squared with european data protection law, 2019.
[19] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD), pages 25–30. IEEE, 2016.
[20] Zhe Xiao, Zengxiang Li, Yong Liu, Ling Feng, Weiwen Zhang, Tha- narit Lertwuthikarn, and Rick Siow Mong Goh. Emrshare: A cross- organizational medical data sharing and management framework using permissioned blockchain. In 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), pages 998–1003. IEEE, 2018. [21]Jens-Andreas Hanssen Rensaa, Danilo Gligoroski, Katina Kralevska, Anton Hasselgren, and Arild Faxvaag. Verifymed–a blockchain platform for transparent trust in virtualized healthcare: Proof-ofconcept. In Proceedings of the 2020 2nd International Electronics Communication Conference, IECC, page 73-80, 2020.
[22] Jens-Andreas Hanssen Rensaa. Transparent healthcare. GitHub, 2020.
[23] Jens-Andreas Hanssen Rensaa. VerifyMed - Application of blockchain technology to improve trust in virtualized healthcare services. Master's thesis, Norwegian University of Science and Technology (NTNU), 2020.
[24] Peng Zhang, Jules White, Douglas C Schmidt, Gunther Lenz, and S Trent Rosenbloom. Fhirchain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16:267–278, 2018.
[25] Anton Hasselgren, Katina Kralevska, Danilo Gligoroski, Sindre A Pedersen, and Arild Faxvaag. Blockchain in healthcare and health sciences—a scoping review. International Journal of Medical Informatics, 134:104040, 2020.
[26] Hawig, David and Zhou, Chao and Fuhrhop, Sebastian and Fialho, Andre S and Ramachandran, Navin. Designing a distributed ledger technology system for interoperable and general data protection regulation--compliant health data exchange: a use case in blood glucose data. Journal of medical Internet research, 21:e13665, 2019

AUTHOR

Anton Hasselgren is a research and PhD in the medical faculty at the Norwegian University of Science and Technology, Trondheim Norway. His main research is is blockchain applications in healthcare.

DATA PREDICTION OF DEFLECTION BASIN EVOLUTION OF ASPHALT PAVEMENT STRUCTURE BASED ON MULTI-LEVEL NEURAL NETWORK

Shaosheng Xu[1], Jinde Cao[2] and Xiangnan Liu[2]

[1]School of Automation, Southeast University, Nanjing, China
[2]School of Mathematics, Southeast University, Nanjing, China

ABSTRACT

Aiming at reducing the high cost of test data collection of deflection basins in the structural design of asphalt pavement and shortening the long test time of new structures, this paper innovatively designs a structure coding network based on traditional neural networks to map the pavement structure to an abstract space. Therefore, the generalization ability of the neural network structure is improved, and a new multi-level neural network model is formed to predict the evolution data of the deflection basin of the untested structure. By testing the experimental data of RIOHTRACK, the network structure predicts the deflection basin data of untested pavement structure, of which the average prediction error is less than 5%.

KEYWORDS

multi-level neural network, Encoding converter, structural of asphalt pavement, deflection basins, RIOHTRACK

1. INTRODUCTION

In the past 20 years, Europe and the United States have established the concept of long-life pavement and permanent pavement. Long-life pavement refers to a pavement where the foundation or pavement base layer will not be significantly aged under the condition of correct pavement maintenance [1]. Most of traditional pavements are semi-rigid base asphalt pavements, which have the advantages of good stability and convenient materials. But there are also disadvantages of poor durability and high maintenance costs. Traditional asphalt pavement has structural damage, mainly manifested as fatigue cracking and permanent deformation, which has a short service life and the dismantling and reconstruction have brought huge economic losses. In order to reduce maintenance and other costs in the future, it will be more cost-effective to extend the design life of roads in places with heavy traffic to at least 40 years without the need to strengthen the structure [2].

Many existing literatures analyse the fatigue of pavement structure through mechanical tests and study the corresponding factors that affect pavement mechanics. Yu et al. carried out four-point bending fatigue tests in constant strain and constant stress modes and established the laboratory fatigue prediction models in these two cases. In addition, the transfer function of loading mode is established to realize the fatigue life conversion. Moreover, the laboratory constant strain prediction model was combined with the loading mode transfer function to establish an asphalt pavement fatigue crack prediction model [3]. Jiang et al. evaluated the strength and fatigue

David C. Wyld et al. (Eds): BIBC, AISO, EDTECH - 2020
pp. 37-46, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101304

performance of asphalt mixtures by semi-circular bending strength test and fatigue test [4]. Wang et al. took several base asphalts and modified asphalts as the research objects and simulated the short-term and long-term aging of asphalt by RTFO and PAV respectively [5]. Gschwendt and Ivan introduced a program of pavement management system based on degradation model, and estimated the repair time of asphalt pavement. Using the theory of pavement mechanics, the stress and strain on the two pavement model layers are calculated [6]. Islam et al. used the existing Per Road and AASHTOW are pavement ME Design software to re-examine the design of the existing four permanent pavement sections to investigate the correctness of the assumptions [7]. Assogba et al. studied the mechanical parameter distributions of three new semi-rigid pavement structures with typical functions and structural requirements which are specially designed to deal with a variety of damages of semi-rigid pavements [8]. Yang et al. proposed a reinforced slow-cracking stress absorbing layer and compared it with the ordinary SBS modified asphalt stress absorbing layer. Besides, the dynamic response laws of the two stress absorbing layers under different conditions are analysed by the strain data of the two stress absorbing layers under different loads, speeds and temperatures [9].

With the development of machine learning, the application of artificial neural networks has grown tremendously in several fields of engineering, such as road conditions and performance prediction, road pressure prediction, and structural road system evaluation [10]. Gu et al. applied artificial neural networks to predict the response of any given material and structural characteristics to geo-reinforced pavement. Furthermore, the results are applied to the method of improving material performance in pavement design, so as to consider the influence of reinforcement on pavement design under any traffic load and weather conditions [11]. Tapkin et al. proposed a neural network model using the physical properties of the standard Marshall sample to predict the Marshall test results of polypropylene (PP) modified asphalt mixture, and obtained the explicit expressions of stability, flow rate and Marshall quotient [12]. Qadir developed an artificial neural network (ANN) model to predict the bending stiffness and rut depth of the reinforced asphalt pavement using design parameters from simple laboratory procedures of Marshall and rut depth tests [13].

RIOHTRACK was utilized in 2017 to a trial loading test to collect and study the evolutionary law of multi-use performance under the conditions of the full-life service cycle of nonlinear road structures and materials, and to verify and improve the design methods of road structures and materials. Under different load levels, 19 kinds of structures' deflection basins with different stiffness levels have been regularly tested and data collected, and their changes have been analysed [14]. As an important indicator reflecting the bearing capacity of asphalt pavement structures, deflection has always been the focus of highway builders and scientific researcher [15-17]. This paper uses the data collected from the RIOHTRACK ring road to predict the deflection basin of the road by establishing a multi-level neural network model. The main contribution of this paper is to establish a multi-level neural network model, which mainly includes three parts: encoding converter, coupler and interpreter. The encoding converter is used to convert the original data of structure to high-dimensional coded data, and the coded data is used as an influencing factor to predict the deflection basin data of the road surface. Through the existing experimental data, the performance of untested pavement structures can be analysed and predicted, which reduces the cost and time of experiments on new structures. While, the coupler checks whether the coded data are appropriate in the high-dimensional space. In other words, it is to make sure that the topology of the coded data is reasonable than which of the data of structure. The interpreter is the component that generate the prediction of the deflection basin data finally.
The organization of this paper is as follows. In the second section, a further analysis is given for the problems. After that, the overall framework of the definition and model involved in the paper is given. Subsequently, the multi-level neural network model established in this paper is

introduced in detail, and the experimental results are given. At the same time, it is compared with other methods. The conclusion is given at the end of the paper.

2. PROBLEM ANALYSIS

As mentioned before, the data in this paper was collected from RIOHTRACK, which is a 2039-meter-long full-scale test track. Trial loading tests are implemented in RIOHTRACK. It is obviously that the cost of time, labour and finance of such a test are very huge. For the deflection basin of untested pavement structure, even if an abstract physical model is established to simulate the deflection basin data, it is quite difficult to calculate. The research in this paper is based on 19 kinds of experimental pavement data of structure and corresponding other data including temperature, load, number of standard axle load and deflection basin. It is expected to directly predict the performance of the new pavement structure composed of the structural materials involved in the existing pavement without paving the new test road so as to save the pavement research cycle and costs.

In order to achieve the above goals, this paper establishes a new multi-level neural network model consisting of encoding converter, coupler and interpreter. Using the known structure to train the model, the prediction of the test data of the new structure is completed.

3. DEFINITION AND FRAMEWORK

This paper mainly predicts the pavement deflection basin by extracting and encoding the structural features of pavements and combining with other features. The different structures are related to each other to form a triple represented by $\mathcal{G} = (V, E, X)$, where *G = (V,E)* constitutes a graph; $V = \{v_i\}_{i=1,2,\dots,n}$ represents the set of nodes in the graph ,that is the set of different pavement structures; $E = \{e_{ij}\}$ is the set of edges between the nodes; $X = \{x_1, x_2, \dots, x_n\}$ is the characteristic of nodes, where $x_i \in \mathbb{R}^m$ is a real valued vector. The characteristic of the node in this paper is the deflection basin performance of the pavement structure. In essence, E represents the relationship between different structures, which can be determined by the pavement structure and the deflection basin, that is $E(V, X)$. A method f^* is expected to be found to encode the structure through training the model which satisfies

$$E\big(V, f^*(V)\big) \leq E(V, f(V))$$

Where f represents any encoding method.

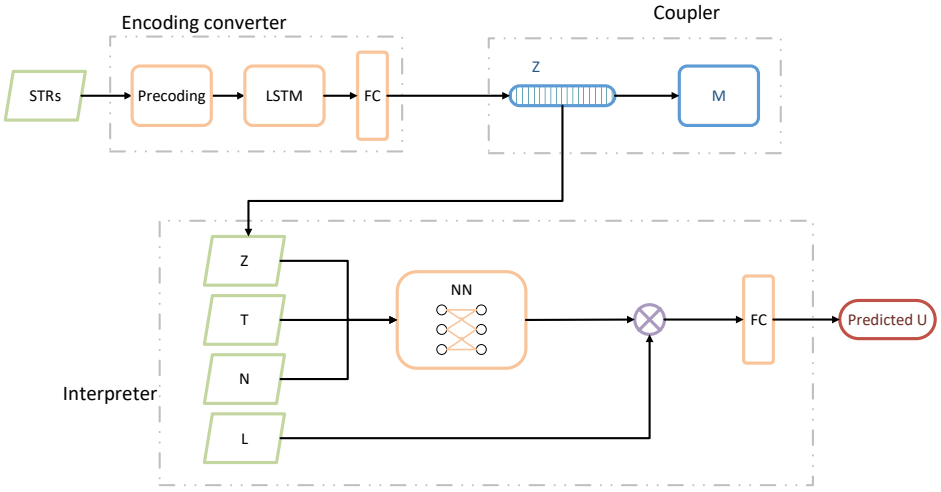

Figure 1. The framework of the model

The overall framework of the model is shown in the Figure 1, which consists of three components: encoding converter, coupler and interpreter. The encoding converter converts the original pavement data into an array through pre-encoding and then encodes further through a Long Short-Term Memory (LSTM) network [18] and a linear layer. The coupler is mainly used to reconstruct the graph and train the network. The interpreter takes the learned coding vector and other factors that affect the deflection basin as input to realize the prediction of deflection basin.

4. MODEL AND METHODOLOGY

In this section, a multi-level neural network model is designed in details. First, the data of structure pass the encoding converter and the coupler to learn the potential encoding vector. Then, the learned encoding vector is used as an explanatory factor to predict the deflection basin with the interpreter.

4.1. Encoding converter

The encoding converter mainly includes two processes. To begin with, original data of structure was pre-encoded. The original data of structure contains two parts of information including the structural thickness of each layer and the structural material. As shown in TABLE I, where MAWA refers to the modified asphalt waterproof adhesive layer.

Table 1. The original data of structure.

	STR1	STR2	STR3	STR4	STR5
Layer1	4cm SBS-SAC13	4cm SBS-SAC13	4cm SBS-SAC13	4cm SBS-SAC13	4cm SBS-SAC13
Layer2	MAWA Tpye1	MAWA Tpye1	MAWA Tpye1	MAWA Tpye1	MAWA Tpye1
Layer3	8cm A30-AC20	8cm A30-AC20	8cm A30-AC20	6cm A30-AC20	6cm A30-AC20
Layer4	MAWA Tpye2	MAWA Tpye2	MAWA Tpye2	clay particles	clay particles
Layer5	20cm CBG-A	20cm CBG-A	20cm CBG-A	2cm SBS-AC10	2cm SBS-AC10
Layer6	20cm CBG-A	20cm CBG-A	20cm CBG-A	Layer of clay particles	Layer of clay particles
Layer7	20cm CS	20cm CS	20cm GB	24cm LCC	24cm CC
Layer8	20cm CS	None		20cm CBG-A	20cm CBG-A
Layer9	None			20cm CS	20cm CS
AC layers	12cm	12cm	12cm	12cm	12cm

Let S denote the set of all materials involved in the pavement structures in V, and number s_j as 1 to k respectively. Therefore, the material thickness and the serial number of the material of each layer together constitute the precoding matrix $\{P_i\}_{i=1,2,\dots,n}$, where $P_i \in \mathbb{R}^{l\times 2}$ and l is determined by the number of structural material layers.

Next, the further encoding is completed through a LSTM network (see Figure 2.) and a linear layer. The space of the precoding matrix is defined as the coding space $\mathbb{F}$. After the precoding matrix is converted by LSTM, the coding expression on the abstract space $\mathbb{H}$ is obtained and the mapping from the coding space to the abstract space is realized and the result is denoted by $\widetilde{z_t}$, which is followed by the normalization process $z = W_z \cdot \widetilde{z_t} + b_z$. Let $Z = \{z_1, z_2, \dots, z_n\}$ represents the coding vector for all the structures.

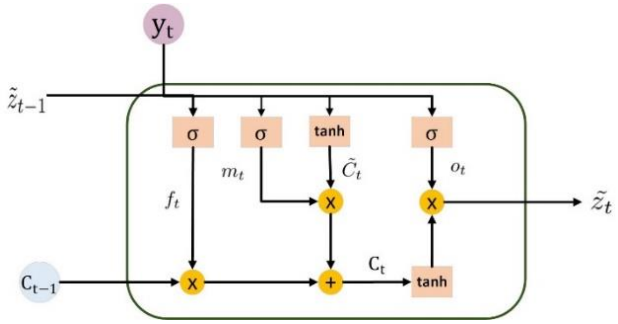

Figure 2. The structure of LSTM

It should be noted that the serial number of structural materials in the precoding process can be in any order, without considering the similarity and correlation between the materials. Because the similarity and association of the structure can be reflected by the output of LSTM as long as the serial number of the same material is the same.

4.2. Coupler

Coupler is mainly used to train the aforementioned LSTM network through reconstruction. A variety of existing decoder scan achieve structural reconstruction [18]. In this paper, characteristics are used for reconstruction. Firstly, transform the characteristic (i.e. deflection basin) as follows to obtain the matrix M,

$$M = DFT(IX - (IX)^T)$$

where DFT is discrete Fourier transform, I is an array whose elements are all one and matrix M is defined as attribute adjacency matrix. The coding sequence Z is used to obtain the reconstructed matrix M' as follows,

$$M' = IZ - (IZ)^T$$

where W and b are the weight matrix and bias respectively. The reconstruction loss function is defined as $L_s = loss_1(M', M)$.

The parameters of LSTM network are adjusted by minimizing the loss function.

4.3. Interpreter

The ultimate goal of this paper is to predict deflection basins of untested pavements. The existing results show that the deflection basin has a great relationship with temperature, load, the number of standard axle load, and obviously has a close relationship with the pavement structure. The features of the pavement structure have been extracted above, and the coding structure sequence can reflect the structural features and connections of different pavements. Through a simple linear regression analysis of the data, it can be seen that there is a clear linear relationship between the deflection basin and the load. Therefore, a semi-display neural network interpreter as shown in Figure 1 is designed. The input of the interpreter is the coding sequence Z, the number of standard axle load N, the temperature T and the load L. In this paper, the accumulative number of standard axle load is adopted as N.

First, input Z, N, T into a neural network to get the compressed feature $g = g(Z, N, T)$. The compression feature g and the load L are subjected to the Hadamard product, and the dimension compression is performed through the fully connected layer to obtain the predicted deflection basin $\widehat{U} = W_h(g * L) + b_h$, where * is Hadamard product. It can be seen that the black box part of the network is only for the extraction of the compression feature g, and the relationship between the load and the deflection basin is fully displayed by the parameters of the fully connected layer. The final forecast error is defined as $L_P = loss_2(\widehat{U}, U)$.

The parameters in the interpreter are updated by back propagation of errors to achieve the minimum error loss.

5. EXPERIMENTS

In this section, the data used in the experiment is introduced and the evaluation criteria of the model is explained, so as the parameter settings. And the results of the experiment are analysed after the results' display. The whole experiment is implemented by Python/Pytorch.

5.1. Data and Setting of Parameters

The data used in this paper comes from China's first full-scale pavement test ring road named RIOHTRACK. As shown in the Figure 3, the ring road is an oval closed curve divided into two sections of straight and cylinder. A total of 19 kinds of pavement structures have been designed (In view of the large amount of data loss in STR19, the data of this experimental structure is abandoned), including the flexible, semi-rigid and rigid base structure, as well as different asphalt structure layers and material combination modes [14].

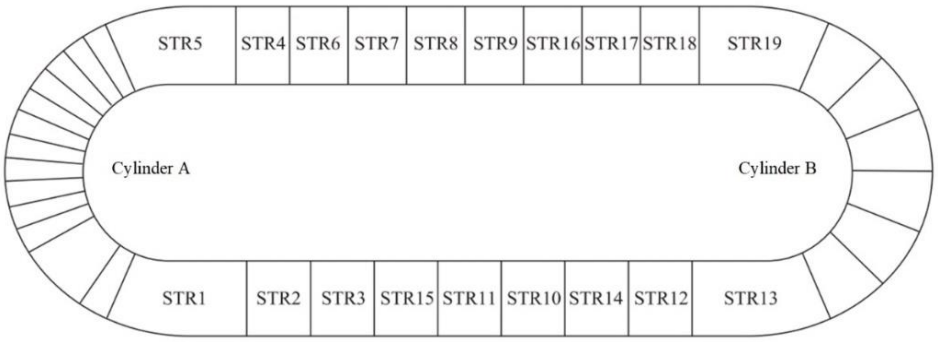

Figure 3. Schematic diagram of RIOHTRACK test section

The 19 kinds of pavement structures are divided into a training set and a test set. The training set contains 16 structures, D = {STR1, STR2, STR3, STR4, STR5, STR6, STR7, STR8, STR9, STR10, STR11, STR12, STR13, STR14, STR15, STR17} and the remaining two structures constitute the test set V = {STR16, STR18}. By deleting the missing data, there are 256 data for each pavement structure. Therefore, there are $256 \times 16 = 4096$ data in training set and $256 \times 2 = 512$ data in test set when predicting and the mean square errors (MSE) are used as the evaluation criteria to estimate the effectiveness of the model. The loss functions of both components are MSE loss and the learning rates are set to 0.02. The number of training iterations is 3000 and 1000 respectively. Due to the lack of the training data, the complexity of coding layer is reduced, such as using single-layer LSTM and single-layer FC, to prevent overfitting.

5.2. Experiment Results

The Figure 4 shows the prediction results of the two structures of STR16 and STR18 in the test set. It can be seen that the overall performance of the model proposed in this paper is well, but at some peaks, it looks like a little bad. The average MSE of all the data in the test set is 0.0455, which also shows that the overall prediction is effective. It can be seen from Figure 4 that the predicted value of the upper peak position is often significantly higher, because the horizontal axis in Figure 4 represents time, and the position of the upper peak is in the summer period, so it can be concluded that the prediction of this model has obvious upper deviations under high temperature. The specific analysis is given in the discussion section.

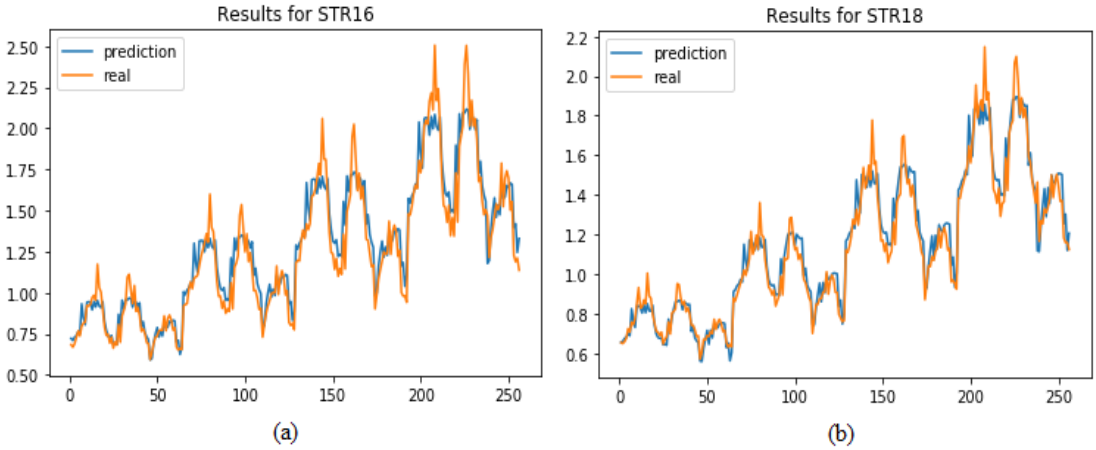

Figure 4(a) Result of the multi-level neural network for STR16 and Figure 4(b) Result of the multi-level neural network for STR18

In order to verify the important role of the encoding converter in prediction, as a comparison, the precoding structure vector is used directly as a prediction factor and other factors to predict the deflection basin through the interpreter. The distribution of training data and test data is the same as before. As shown in Figure 5, it can be seen that the prediction results are worse than our model intuitively and the MSE of the normal network is over 79.3 in the test set.

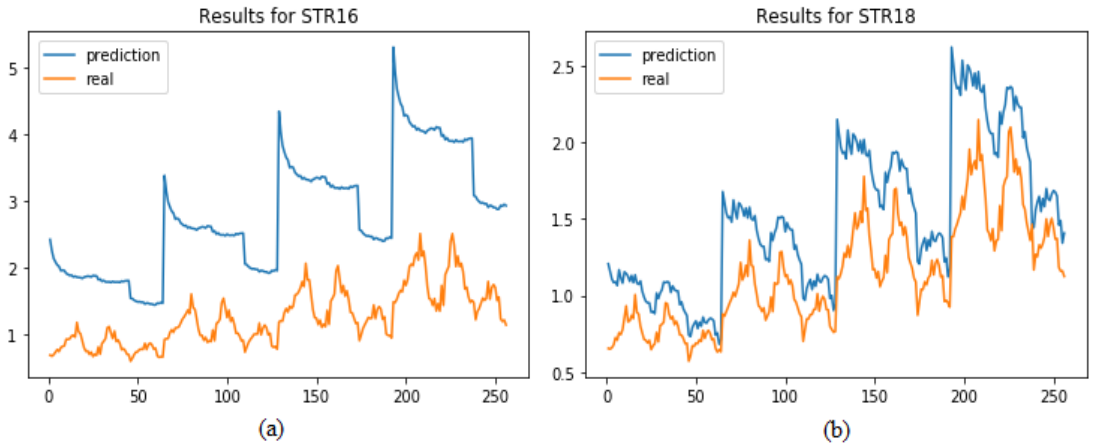

Figure 5(a) Result of the normal neural network for STR16 and Figure 5(b) Result of the normal neural network for STR18

6. DISCUSSION

In preliminary analysis, the reason for the larger prediction error of the normal neural network is that the characteristics of the space in which the data of structure is located are significantly different from the characteristics of the space in which the physical quantity is being tested. The former is a logical expression space on the intuitive level with a spatial order structure, while the latter is a physical space on the dynamic level with a temporal order structure. However, it is difficult to analyse the time sequence of the multi-level structural space, so the nonlinear fitting function of the normal neural network is difficult to play its due role.

It is may be noticed that the data of structure and the one of experimental test variables have different dimensions, and considered that the different dimensions cause the larger deviation of the normal neural network prediction results. Here a different opinion is. Because even in the interpreter module, the dimensions of the input variables are not the same, but the multilayer neural network proposed in this paper has a less error (the average error is less than 5%). At present, a large number of neural network models can input variables of different dimensions at the same time and achieve good results, which means that neural network models can overcome the problems caused by different dimensions to a certain extent.

In the problem dealt with in this paper, the data of structure is a vector in an abstract space (human intuitive cognitive space) compared to variables such as temperature, load, etc., which is like the direct transcoding of textual expressions. The encoding module and coupler module proposed in this paper are similar with the function of Word2Vec in the natural language processing. After the coding is completed, the topological structure between codes can better express the topological relationship between them at the time of testing, so it can directly reflect the physical meaning represented by a structure, that is, the original intuitive cognitive space is mapped to the physical space, and the consistency of the two spaces is guaranteed, so that a better calculation result can be obtained.

The reason for the upper deviation of the upper peak position forecast is not yet conclusive. In view of the poor interpretation ability of the neural network itself, it is difficult to analyse it theoretically. What is certain at present is that the period when the predictions show a significant upward shift occurs in the summer, when is during the high temperature period of a year. Therefore, it can be concluded that high temperature may be an important cause of prediction errors. It is precisely because of this inference that this issue can be considered from the

following two aspects. First, the objective pavement structure has a sudden change in response to temperature switch. That is, near some high temperature, the material mechanical properties of the overall structure change suddenly. Some local mechanical laws suddenly change from approximate linear laws to obvious nonlinear laws. An important reason which supports this guess is that asphalt is a non-Newtonian fluid, so whether its multilayer composite materials will also have similar properties is a question, and which may lead the peak value to be significantly lower than the predicted value. Of course, if one wants to verify this conjecture, a large amount of experimental data is needed. The related experiments are currently underway. Second, in terms of the model receiving temperature data, the proportion of high temperature data is very small. That is, for temperature data, the data sample lacks balance, which causes large errors in high temperature training to be flattened as a whole during the back-propagation process. For this reason, a novel interpreter module is under research at the same time.

7. CONCLUSIONS

In this paper, a multi-level neural network model has been proposed that can encode data of structure and predict the deflection basin of asphalt pavements. It can be seen from the experimental results that structure coding is effective and important. The method proposed in this paper can use the existing data to directly predict the deflection basin of untested pavement, saving the time and capital cost of repeated experiments and the mean prediction loss is under 5%. However, this method relies on a large amount of historical experimental data. Therefore, besides the present research mentioned in the discussion section above, the model development based on small sample training is still in progress.

ACKNOWLEDGEMENTS

Thanks to the Highway Science Research Institute of the Ministry of Transport, they have provided enough experimental data on asphalt pavements of various structures.

REFERENCES

[1] E. A. P. Association et al., (2007) “Long-life asphalt pavements–technical version”.
[2] M. Nunn, A. Brown, D. Weston, and J. Nicholls, (1997) “Design of long-life flexible pavements for heavy traffic”, TRL Limited.
[3] J. Yu, B.-W. Tsai, X. Zhang, and C. Monismith, (2012) “Development of asphalt pavement fatigue cracking prediction model based on loading mode transfer function”, Road Materials and Pavement Design, Vol. 13, No. 3, pp. 501–517.
[4] J. Jiang, F. Ni, Q. Dong, F. Wu, and Y. Dai, (2018) “Research on the fatigue equation of asphalt mixtures based on actual stress ratio using semi-circular bending test”, Construction and Building Materials, Vol. 158, pp. 996–1002.
[5] Z. Wang and F. Ye, (2020) “Experimental investigation on aging characteristics of asphalt based on rheological properties”, Construction and Building Materials, Vol. 231, p. 117158.
[6] I. Gschwendt, (2018) “Extending the service life of pavements”, Slovak Journal of Civil Engineering, Vol. 26, No. 1, pp. 25–32.
[7] S. Islam, A. Sufian, M. Hossain, R. Miller, and C. Leibrock, (2020) “Mechanistic-empirical design of perpetual pavement,” Road Materials and Pavement Design, Vol. 21, No. 5, pp. 1224–1237.
[8] O. C. Assogba, Y. Tan, X. Zhou, C. Zhang, and J. N. Anato, (2020) “Numerical investigation of the mechanical response of semi-rigid base asphalt pavement under traffic load and nonlinear temperature gradient effect”, Construction and Building Materials, Vol. 235, p. 117406.
[9] S. Yang, P. Li, M. Guo, S. Liao, and H. Wu, (2020) “Study on dynamic load monitoring of an enhanced stress absorption layer”, Frontiers in Materials, Vol. 7, p. 148.
[10] H. Ceylan, M. B. Bayrak, and K. Gopalakrishnan, (2014) “Neural networks applications in pavement engineering: A recent survey”, International Journal of Pavement Research & Technology, Vol. 7, No. 6, pp. 434–444.

[11] F. Gu, X. Luo, Y. Zhang, Y. Chen, R. Luo, and R. L. Lytton, (2018) "Prediction of geogrid-reinforced flexible pavement performance using artificial neural network approach", Road Materials & Pavement Design, Vol. 19, No. 5–6, pp. 1147–1163.
[12] S. Tapkin, A. Cevik, and U. Usar, (2010) "Prediction of marshal test results for polypropylene modified dense bituminous mixtures using neural networks", Expert Systems with Applications, Vol. 37, No. 6, pp. 4660–4670.
[13] A. Qadir, U. Gazder, and K. U. N. Choudhary, (2020) "Artificial neural network models for performance design of asphalt pavements reinforced with geosynthetics", Transportation Research Record, Vol. 4, p. 0361198120924387.
[14] X. D. Wang, (2017) "Design of pavement structure and material for full-scale test track", Journal of Highway and Transportation Research and Development, Vol. 34, No. 6, pp. 30–37.
[15] X. Wang, (2015) "Discussion of asphalt pavement deflection indicator," Journal of Highway and Transportation Research and Development, Vol. 32, No. 1, pp. 1–12.
[16] J. Liao, et al. (2019) "A Correction Model for the Continuous Deflection Measurement of Pavements Under Dynamic Loads", IEEE Access, Vol. 7, pp. 154770-154785.
[17] C. Wu, H. Wang, et al., (2020) "Asphalt pavement modulus back calculation using surface deflections under moving loads", Computer-Aided Civil and Infrastructure Engineering, doi:10.1111/mice.12624
[18] C. Wang, S. Pan, R. Hu, et al., (2019) "Attributed graph clustering: A deep attentional embedding approach," arXiv preprint arXiv:1906.06532.

AUTHORS

Shaosheng Xu received the B.S. degree from University of Jinan, Jinan, China, in 2011 and M.S. degrees from Anhui Normal University, Wuhu, China, in 2016. He is currently pursuing the Ph.D. degree with the School of Automation, Southeast University, Nanjing, China. His current research interests include stochastic optimal control, multi-agent system, multi-robot system and artificial intelligence.

Jinde Cao (F'16) received the B.S. degree from Anhui Normal University, Wuhu, China, the M.S. degree from Yunnan University, Kunming, China, and the Ph.D. degree from Sichuan University, Chengdu, China, all in mathematics /applied mathematics, in 1986, 1989, and 1998, respectively. He is an Endowed Chair Professor, the Dean of the School of Mathematics, the Director of the Jiangsu Provincial Key Laboratory of Networked Collective Intelligence of China and the Director of the Research Center for Complex Systems and Network Sciences at Southeast University. Prof. Cao was a recipient of the National Innovation Award of China, Obada Prize and the Highly Cited Researcher Award in Engineering, Computer Science, and Mathematics by Thomson Reuters/Clarivate Analytics. He is a fellow of IEEE, a member of the Academy of Europe, a member of the European Academy of Sciences and Arts, a fellow of Pakistan Academy of Sciences, and an IASCYS academician.

Xiangnan Liu received the B.Sc. degree in statistics from Southeast University, Nanjing, in 2019.She is currently a postgraduate in Southeast University. Her research interest is machine learning.

STABILITY ANALYSIS OF QUATERNION-VALUED NEURAL NETWORKS WITH LEAKAGE DELAY AND ADDITIVE TIME-VARYING DELAYS

Qun Huang and Jinde Cao

School of Mathematics, Southeast University, Nanjing, China

ABSTRACT

In this paper, the stability analysis of quaternion-valued neural networks (QVNNs) with both leakage delay and additive time-varying delays is proposed. By employing the Lyapunov-Krasovskii functional method and fully considering the relationship between time-varying delays and upper bounds of delays, some sufficient criteria are derived based on reciprocally convex method and several inequality techniques. The stability criteria are established in two forms: quaternion-valued linear matrix inequalities (QVLMIs) and complex-valued linear matrix inequalities (CVLMIs),in which CVLMIs can be directly resolved by the Yalmip toolbox in MATLAB. Finally, an illustrative example is presented to demonstrate the validity of the theoretical results.

KEYWORDS

Quaternion-valued Neural Networks, Stability Analysis, Lyapunov-KrasovskiiFunctional, Leakage Delay, Additive Time-varying Delays

1. INTRODUCTION

In the past decades, real-valued neural networks (RVNNs) have been successfully appliedin secure communication, information processing, engineer optimization, automatic control engineering and other areas. Correspondingly, numerous meaningful results have been reported [1-6]. However, RVNNs have its own limitations, such as the detection of symmetry problem cannot be resolved by a real-valued neuron, while it can be well solved by a complex-valued neuron [7]. In addition, the problem involving with ultrasonic wave, electromagnetic processing, quantum wave can be also well resolved by the complex number. Therefore, the performance of complex-valued neural networks (CVNNs) is more preferable than that of RVNN sin practical application with complex signals, and CVNNs have captured plenty of attentions from different areas [8-9]. In the past few years, it has drawn considerable attention to the dynamics of complex-valued neural networks and there have been lots of significant results associated with such kind of topics, see [10-11] and the references cited therein.

The quaternions are members of a noncommutative division algebra invented independently by William Rowan Hamilton in 1843. Some operation laws such as the commutativtiy of multiplication are not yet applicable for quaternions, which is quite different from the real or complex numbers. Owing to this difficulty, the research of quaternion had almost remained stagnant for a long period of time in the past. Recently, the resurgence of the study for quaternion systems is underway and an increasing spectrum of applications based on quaternions are found

David C. Wyld et al. (Eds): BIBC, AISO, EDTECH - 2020
pp. 47-58, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101305

in various fields, such as quantum mechanics, attitude control, computergraphics and signal processing [12-13]. It has been proven that neural networks along with quaternion possess better performances and wider applications than both RVNNs and CVNNs. Actually, the three-dimensional and four-dimensional data can be expressed as an entirety, which is more authentic and reliable in modeling of practical application, and quaternion-valued neural networks (QVNNs) emerge at the right moment. Nowadays, increasing scholars are dedicated to investigating the dynamical behaviors of QVNNs. For instance, some sufficient criteria were proposed in the form of LMIs to guarantee the μ-stability of QVNNs with unbounded and non-differentiable time-varying delays in [14] and [15], respectively. In [16], by employing matrix measure and Halanay inequality technique, the problem of global exponential stability for delayed QVNNs was addressed successfully. Chen and Song [17] concentrated on the robust stability issue for delayed QVNNs based on homeomorphism mapping theorem and inequality techniques. Furthermore, the stability issue for both continuous-time and discrete-time QVNNs was investigated in [18]. Besides, some algebraic conditions were established to guarantee the global dissipativity for delayed QVNNs [19].

Time delays are inevitable in neural system owing to the limited propagation velocity between different neurons. Dynamical behaviors of neural networks could become more complicated owing to the existence of time delays, and it may result in performance degradation, such as instability, oscillation, bifurcation and so forth. Usually, the time delay in the state is supposed to appear in a singular form. Nevertheless, Zhao et al. [20] demonstrated that signals transmissions may experience a few segments of networks in several practical situations and different conditions of network transmission probably result in successive delays with different properties. By applying the convex polyhedron method, a less conservative delay-dependent stability criterion was proposed in [21]. Tian and Zhong [22] conducted further investigation on this issue by constructing augmented Lyapunov-Krasovskii functional and employing the reciprocally convex method, which is initially proposed by Park et al. [23]. Liang et al. generalized the reciprocally convex method to the complex domain and investigated the state estimation problem for complex-valued neural networks with two additive time-varying delays [24]. To the best ofthe authors' knowledge, up to now, few scholars have taken the stability problem of quaternion-valued neural networks with additive time-varying delays into consideration.

Enlightened by the aforementioned discussions, the aim of this paper is to conduct the stability analysis for quaternion-valued neural networks with both leakage delay and two additive time-varying delays. The remainder of this paper is organized as follows. In Section 2, the model description, several necessary hypotheses and lemmas are given. In Section 3, some sufficient criteria for the global asymptotical stability of QVNNs are derived based on reciprocally convex method and several inequality techniques. In Section 4, an illustrative example is presented to validate the effectiveness of the obtained results. Finally, conclusions are drawn in Section 5.

Notations: Let $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}$ stand for the real field, the complex field and the skew field of quaternions, respectively. Let $\mathbb{R}^{m\times n}$, $\mathbb{C}^{m\times n}$ and $\mathbb{Q}^{m\times n}$ separately denote $m\times n$ matrices with entries from $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}$. The notations A^T,$\bar{A}$ and A^* represent the transpose, the conjugate and the conjugate transpose matrix of A, respectively. A is referred to as Hermitian if $A = A^*$. The notation $X \geq Y (X > Y)$ means that $X - Y$ is positive semidefinite (positive definite, respectively). Moreover, the notation $*$ denotes the conjugate transpose of an appropriate block in a Hermitian matrix, while the notation ■ denotes the negative transpose of an appropriate block in a skew-symmetric matrix.

2. PRELIMINARIES

2.1. Quaternion Algebra

The quaternion is an extension of the complex number, and a quaternion $m \in \mathbb{Q}$ can be described in the following form:

$$m = m_0 + m_1 i + m_2 j + m_3 k,$$

where $m_0, m_1, m_2, m_3 \in \mathbb{R}$. The quaternion imaginary units i, j, k obey the following rules:

$$i^2 = j^2 = k^2 = ijk = -1,$$

$$ij = -ji = k, ik = -ki = j, jk = -kj = i.$$

From which one can note that the quaternion multiplication is not commutative.
We proceed to introduce some basic operations of quaternion algebra. For two quaternions $m = m_0 + m_1 i + m_2 j + m_3 k$ and $n = n_0 + n_1 i + n_2 j + n_3 k$, the sum and product of $m$and$n$are defined as:

$$m + n = (m_0 + n_0) + (m_1 + n_1)i + (m_2 + n_2)j + (m_3 + n_3)k,$$

And

$$\begin{aligned} mn = {} & (m_0 n_0 - m_1 n_1 - m_2 n_2 - m_3 n_3) + (m_0 n_1 + m_1 n_0 + m_2 n_3 - m_3 n_2) \\ & + (m_0 n_2 + m_2 n_0 - m_1 n_3 + m_3 n_1)j + (m_0 n_3 + m_3 n_0 + m_1 n_2 - m_2 n_1)k. \end{aligned}$$

In addition, the conjugate transpose of m is defined as $m^* = m_0 - m_1 i - m_2 j - m_3 k$. The modulus of $m$is denoted by $|m|$ and denoted as

$$|m| = \sqrt{mm^*} = \sqrt{(m_0)^2 + (m_1)^2 + (m_2)^2 + (m_3)^2}.$$

2.2. Model Formulation and Basic Lemmas

Consider the following quaternion-valued neural networks with both leakage delay and additive time-varying delays:

$$\dot{y}(t) = -Cy(t - \delta) + Ag\big(y(t)\big) + Bg\Big(y\big(t - d_1(t) - d_2(t)\big)\Big) + h(t), \quad (1)$$

where $y(t) = (y_1(t), y_2(t), \dots, y_n(t))^T \in \mathbb{Q}^n$ denotes the state vector, $C = diag\{c_1, c_2, \dots, c_n\} \in \mathbb{R}^{n\times n}$ with $c_i > 0$ is the self-feedback connection weight matrix for $i \in \{1,2, \dots, n\}$.$A, B \in \mathbb{Q}^{n\times n}$ are the interconnection matrices which stand for the weight coefficients of the neurons. $g\big(x(t)\big) = \big(g_1\big(y_1(t)\big), g_2\big(y_2(t)\big), \dots, g_n\big(y_n(t)\big)\big)^T \in \mathbb{Q}^n$ represents the neuron activation function at time t; $h(t) \in \mathbb{Q}^n$ denotes the external input vector; δ is referred to as the leakage delay which satisfies $\delta \geq 0$; $d_1(t)$and $d_2(t)$ represent the two delay components in the state.

In order to simplify the model, we assume thaty^* is an equilibrium point for (1). By applying the transformation $x(t) = y(t) - y^*$, system (1) is further converted to:

$$\dot{x}(t) = -Cx(t-\delta) + Af\big(x(t)\big) + Bf\Big(x\big(t-d_1(t)-d_2(t)\big)\Big), \quad (2)$$

where

$$x(t) = (x_1(t), x_2(t), \dots, x_n(t))^T, f\big(x(\cdot)\big) = (f_1\big(x_1(\cdot)\big), f_2\big(x_2(\cdot)\big), \dots, f_n\big(x_n(\cdot)\big))^T, f_i\big(x_i(\cdot)\big) = g_i(x_i(\cdot) + y_i^*) - g_i(y_i^*)\ (i = 1,2, \dots, n).$$

Throughout this paper, several assumptions play a crucial role and thus are presents as:

Assumption 1: $d_1(t)$ and $d_2(t)$are continuous functions and satisfy

$$0 \le d_1(t) \le d_1, \quad 0 \le d_2(t) \le d_2,$$
$$\dot{d}_1(t) \le \mu_1, \quad \dot{d}_2(t) \le \mu_2,$$

where $d_i$and μ_i $(i = 1,2)$are positive constants.

Assumption 2: For any $j \in \{1,2, \dots, n\}$, there exists a positive constant γ_j such that

$$\big|f_j(u_1) - f_j(u_2)\big| \le \gamma_j |u_1 - u_2|$$

for all $u_1, u_2 \in \mathbb{Q}$.

Subsequently, we denote $d(t) = d_1(t) + d_2(t), d = d_1 + d_2, \mu = \mu_1 + \mu_2$ and $\Gamma = diag\{\gamma_1, \gamma_2, \dots, \gamma_n\}$ for simplicity. Before deriving the main results, the following lemmas are instrumental.

Lemma 2.1. Let $u, v \in \mathbb{Q}, A, B \in \mathbb{Q}^{n\times n}, C \in \mathbb{C}^{n\times n}$. Then

(i) $|u+v| \le |u| + |v|$, and $|uv| \le |u||v|$;
(ii) $(AB)^* = B^*A^*$;
(iii) $(AB)^{-1} = B^{-1}A^{-1}, if\ A, B\ are\ invertible$;
(iv) $(A^*)^{-1} = (A^{-1})^*, if\ A\ is\ invertible$;
(v) $u\ can\ be\ uniquely\ expressed\ as\ u = u_1 + u_2 j, where\ u_1, u_2 \in \mathbb{C}$;
(vi) $jC = \bar{C}j\ and\ jCj = -\bar{C}$.

Remark 2.1. According to property (5) in Lemma 2.1, any quaternion matrix $A \in \mathbb{Q}^{n\times n}$ can be uniquely expressed as $A = A_1 + A_2 j$, where $A_1, A_2 \in \mathbb{C}^{n\times n}$.

Lemma 2.2. Let $A = A_1 + A_2 j, B = B_1 + B_2 j$,where $A, B \in \mathbb{Q}^{n\times n}$ and $A_1, A_2, B_1, B_2 \in \mathbb{C}^{n\times n}$. Then

(i) $A^* = A_1^* - A_2^T j$;
(ii) $AB = (A_1B_1 - A_2\bar{B}_2) + (A_1B_2 + A_2\bar{B}_1)j$.

Lemma 2.3. Let $A \in \mathbb{Q}^{n\times n}$be a Hermitian matrix and $A = A_1 + A_2 j$, where $A_1, A_2 \in \mathbb{C}^{n\times n}$. Then $A < 0$is equivalent to

$$\begin{pmatrix} A_1 & -A_2 \\ \bar{A}_2 & \bar{A}_1 \end{pmatrix} < 0.$$

Remark 2.2. Lemma 2.3 reveals the equivalence between the negative definiteness of a $n \times n$quaternion matrix and the negative definiteness of a $2n \times 2n$complex matrix.

Lemma 2.4. Suppose $M \in \mathbb{Q}^{n\times n}$ is a positive definite Hermitian matrix and $\omega(s):[a,b]\to\mathbb{Q}^n$is a vector valued function. If the integrations concerned are well-defined, then

$$\left(\int_a^b \omega(s)ds\right)^* M\left(\int_a^b \omega(s)ds\right) \le (b-a)\int_a^b \omega^*(s)M\omega(s)ds.$$

Lemma 2.5. For any vector $\xi \in \mathbb{Q}^m$,$\alpha \in (0,1)$, a positive Hermitian matrix $P \in \mathbb{Q}^{n\times n}$, and matrices $W_1, W_2 \in \mathbb{Q}^{n\times m}$, define the function $\Xi(\alpha,P)$as

$$\Xi(\alpha,P) = \frac{1}{\alpha}\xi^* W_1^* P W_1\xi + \frac{1}{1-\alpha}\xi^* W_2^* P W_2\xi.$$

If there exists a matrix $X \in \mathbb{Q}^{n\times n}$satisfying

$$\begin{pmatrix} P & X \\ * & P \end{pmatrix} \ge 0,$$

then

$$\min_{\alpha\in(0,1)} \Xi(\alpha,P) \ge \begin{pmatrix} W_1\xi \\ W_2\xi \end{pmatrix}^* \begin{pmatrix} P & X \\ * & P \end{pmatrix}\begin{pmatrix} W_1\xi \\ W_2\xi \end{pmatrix}.$$

Remark 2.3. Lemma 2.5 is the alleged reciprocally convex inequality in the quaternion domain.

3. MAIN RESULTS

Theorem 3.1. Suppose Assumptions 1 and 2 hold. If there exist positive diagonal matrices$M_1, M_2, M_3 \in \mathbb{R}^{n\times n}$, positive definite matrices $P_\iota(\iota = 1,2,3), Q_\varsigma\,(\varsigma = 1,2,\dots,6), R_1, R_2 \in \mathbb{Q}^{n\times n}$ and appropriate matrices $U, V, S_1, S_2 \in \mathbb{Q}^{n\times n}$such that the following quaternion-valued LMIs hold:

$$\begin{pmatrix} R_1 & U \\ * & R_1 \end{pmatrix} > 0, \qquad (3)$$

$$\begin{pmatrix} R_2 & V \\ * & R_2 \end{pmatrix} > 0, \qquad (4)$$

$$\Omega = (\Omega_{ij})_{11\times 11} < 0, \qquad (5)$$

where

$$\begin{aligned}
\Omega_{ji} = \Omega_{ij}^*(i\neq j), &\Omega_{11} = -P_1C - CP_1 + P_2 + \delta^2 P_3 + Q_1 + Q_3 + Q_5 + Q_6 - R_1 + \Gamma M_1\Gamma, \Omega_{14} \\
&= R_1 - U^*, \Omega_{16} = U^*, \Omega_{18} = P_1A, \Omega_{1,10} = P_1B, \Omega_{1,11} = CP_1C, \Omega_{22} \\
&= d_1^2R_1 + d_2^2R_2 - S_1 - S_1^*, \Omega_{23} = -S_1^*C - S_2, \Omega_{28} = S_1^*A, \Omega_{2,10} = S_1^*B, \Omega_{33} \\
&= -P_2 - CS_2 - S_2^*C, \Omega_{38} = S_2^*A, \Omega_{3,10} = S_2^*B, \Omega_{44} \\
&= -(1-\mu_1)Q_1 - R_1 - R_1^* + U + U^* + \Gamma M_2\Gamma, \Omega_{46} = R_1 - U^*, \Omega_{55} \\
&= -(1-\mu)Q_3 - R_2 - R_2^* + V + V^* + \Gamma M_3\Gamma, \Omega_{56} = R_2^* - V, \Omega_{57} \\
&= R_2 - V^*, \Omega_{66} = -Q_5 - R_1 - R_2, \Omega_{67} = V^*, \Omega_{77} = -Q_6 - R_2, \Omega_{88} \\
&= Q_2 + Q_4 - M_1, \Omega_{8,11} = -A^*P_1C, \Omega_{99} = -(1-\mu_1)Q_2 - M_2, \Omega_{10,10} \\
&= -(1-\mu)Q_4 - M_3, \Omega_{10,11} = -B^*P_1C, \Omega_{11,11} = -P_3.
\end{aligned}$$

Then the quaternion-valued neural networks is globally asymptotically stable.

Proof. Construct the following Lyapunov-Krasovskii functional

$$V(t) = \sum_{i=1}^{4} V_i(t) \quad (6)$$

Where

$$V_1(t) = \left(x(t) - C\int_{t-\delta}^{t} x(s)ds\right)^* P_1 \left(x(t) - C\int_{t-\delta}^{t} x(s)ds\right), (7)$$

$$V_2(t) = \int_{t-\delta}^{t} x^*(s)P_2\, x(s)ds + \delta\int_{-\delta}^{0}\int_{t+\theta}^{t} x^*(s)P_3 x(s)ds d\theta\,, (8)$$

$$\begin{aligned} V_3(t) &= \int_{t-d_1(t)}^{t} (x^*(s)Q_1x(s) + f^*(x(s))Q_2 f(x(s)))ds \\ &+ \int_{t-d(t)}^{t} (x^*(s)Q_3x(s) + f^*(x(s))Q_4 f(x(s)))ds + \int_{t-d_1}^{t} x^*(s)Q_5x(s)ds \\ &+ \int_{t-d}^{t} x^*(s)Q_6x(s)ds\,, (9) \end{aligned}$$

$$V_4(t) = d_1\int_{-d_1}^{0}\int_{t+\theta}^{t} \dot{x}^*(s)R_1\dot{x}(s)ds d\theta + d_2\int_{-d}^{-d_1}\int_{t+\theta}^{t} \dot{x}^*(s)R_2\dot{x}(s)ds d\theta. \quad (10)$$

Then the derivatives ofV_i $(i = 1,2,3,4)$ can be calculated and estimated straightforwardly:

$$\begin{aligned} \dot{V}_1(t) &= -x^*(t)(P_1C + CP_1)x(t) + x^*(t)P_1Af\big(x(t)\big) + f^*\big(x(t)\big)A^*P_1x(t) \\ &+ x^*(t)P_1Bf\left(x\big(t-d(t)\big)\right) + f^*\left(x\big(t-d(t)\big)\right)B^*P_1x(t) \\ &+ \left(\int_{t-\delta}^{t} x(s)ds\right)^* CP_1Cx(t) + x^*(t)CP_1C\left(\int_{t-\delta}^{t} x(s)ds\right) \\ &- \left(\int_{t-\delta}^{t} x(s)ds\right)^* CP_1Af\big(x(t)\big) - f^*\big(x(t)\big)A^*P_1C\left(\int_{t-\delta}^{t} x(s)ds\right) \\ &- \left(\int_{t-\delta}^{t} x(s)ds\right)^* CP_1Bf\left(x\big(t-d(t)\big)\right) \\ &- f^*\left(x\big(t-d(t)\big)\right)B^*P_1C\left(\int_{t-\delta}^{t} x(s)ds\right), (11) \end{aligned}$$

$$\begin{aligned} \dot{V}_2(t) &\le x^*(t)(P_2 + \delta^2P_3)x(t) - x^*(t-\delta)P_2x(t-\delta) \\ &+ \left(\int_{t-\delta}^{t} x(s)ds\right)^* P_3\left(\int_{t-\delta}^{t} x(s)ds\right), (12) \end{aligned}$$

$$\dot{V}_3(t) \le x^*(t)(Q_1+Q_3+Q_5+Q_6)x(t) - x^*(t-d_1)Q_5x(t-d_1) - x^*(t-d)Q_6x(t-d) - (1-\mu_1)x^*\big(t-d_1(t)\big)Q_1x\big(t-d_1(t)\big) - (1-\mu)x^*\big(t-d(t)\big)Q_3x\big(t-d(t)\big) + f^*\big(x(t)\big)(Q_2+Q_4)f\big(x(t)\big) - (1-\mu_1)f^*\Big(x\big(t-d_1(t)\big)\Big)Q_2f\Big(x\big(t-d_1(t)\big)\Big) - (1-\mu)f^*\Big(x\big(t-d(t)\big)\Big)Q_2f\Big(x\big(t-d(t)\big)\Big), (13)$$

$$\dot{V}_4(t) = \dot{x}^*(t)(d_1^2R_1+d_2^2R_2)\dot{x}(t) - d_1\int_{t-d_1}^{t}\dot{x}^*(s)\,R_1\dot{x}(s)ds - d_2\int_{t-d}^{t-d_1}\dot{x}^*(s)\,R_2\dot{x}(s)ds, (14)$$

where Lemma 2.4 has been applied in the estimate of $\dot{V}_2(t)$in (12). Based on Lemma 2.5, we further estimate two integration terms in$\dot{V}_4(t)$ as

$$-d_1\int_{t-d_1}^{t}\dot{x}^*(s)\,R_1\dot{x}(s)ds = -d_1\int_{t-d_1(t)}^{t}\dot{x}^*(s)\,R_1\dot{x}(s)ds - d_1\int_{t-d_1}^{t-d_1(t)}\dot{x}^*(s)\,R_1\dot{x}(s)ds$$

$$\le -\frac{d_1}{d_1(t)}\left(\int_{t-d_1(t)}^{t}\dot{x}(s)ds\right)^*R_1\left(\int_{t-d_1(t)}^{t}\dot{x}(s)ds\right) - \frac{d_1}{d_1-d_1(t)}\left(\int_{t-d_1}^{t-d_1(t)}\dot{x}(s)ds\right)^*R_1\left(\int_{t-d_1}^{t-d_1(t)}\dot{x}(s)ds\right)$$

$$\le -\begin{pmatrix} x(t)-x\big(t-d_1(t)\big) \\ x\big(t-d_1(t)\big)-x(t-d_1)\end{pmatrix}^*\begin{pmatrix} R_1 & U \\ * & R_1\end{pmatrix}\begin{pmatrix} x(t)-x\big(t-d_1(t)\big) \\ x\big(t-d_1(t)\big)-x(t-d_1)\end{pmatrix}$$

$$= -\begin{pmatrix} x(t) \\ x(t-d_1) \\ x\big(t-d_1(t)\big)\end{pmatrix}^*\begin{pmatrix} R_1 & -U^* & -R_1+U^* \\ -U & R_1 & -R_1+U \\ -R_1+U & -R_1+U^* & 2R_1-U-U^*\end{pmatrix}\begin{pmatrix} x(t) \\ x(t-d_1) \\ x\big(t-d_1(t)\big)\end{pmatrix}. (15)$$

Analogously, one can obtain that

$$-d_2\int_{t-d}^{t-d_1}\dot{x}^*(s)\,R_2\dot{x}(s)ds = -d_2\int_{t-d(t)}^{t-d_1}\dot{x}^*(s)\,R_2\dot{x}(s)ds - d_2\int_{t-d}^{t-d(t)}\dot{x}^*(s)\,R_2\dot{x}(s)ds$$

$$\le -\begin{pmatrix} x(t-d_1) \\ x(t-d) \\ x\big(t-d(t)\big)\end{pmatrix}^*\begin{pmatrix} R_2 & -V^* & -R_2+V^* \\ -V & R_2 & -R_2+V \\ -R_2+V & -R_2+V^* & 2R_2-V-V^*\end{pmatrix}\begin{pmatrix} x(t-d_1) \\ x(t-d) \\ x\big(t-d(t)\big)\end{pmatrix}. (16)$$

In addition, it follows from Assumption 1 that

$$0 \le x^*(t)\Gamma M_1\Gamma x(t) - f^*\big(x(t)\big)M_1f\big(x(t)\big), (17)$$

$$0 \le x^*(t-d_1(t))\Gamma M_2\Gamma x(t-d_1(t)) - f^*\big(x(t-d_1(t))\big)M_1f\big(x(t-d_1(t))\big), (18)$$

$$0 \le x^*\big(t-d(t)\big)\Gamma M_3\Gamma x\big(t-d(t)\big) - f^*\Big(x\big(t-d(t)\big)\Big)M_3f\Big(x\big(t-d(t)\big)\Big). (19)$$

By applying the free weighting matrix method, we gather from (3) that

$$0 = [S_1\dot{x}(t) + S_2x(t-\delta)]^*H + H^*[S_1\dot{x}(t) + S_2x(t-\delta)], (20)$$

Where

$$H = -\dot{x}(t) - Cx(t-\delta) + Af\big(x(t)\big) + Bf\Big(x\big(t-d(t)\big)\Big). (21)$$

By substituting (21) into (20), we proceed to obtain that

$$\begin{aligned} 0 = {} & -\dot{x}^*(t)(S_1 + S_1^*)\dot{x}(t) - \dot{x}^*(t)(S_1^*C + S_2)x(t-\delta) - x^*(t-\delta)(CS_1 + S_2^*)\dot{x}(t) \\ & + \dot{x}^*(t)S_1^*Af\big(x(t)\big) + f^*\big(x(t)\big)A^*S_1\dot{x}(t) + \dot{x}^*(t)S_1^*Bf\Big(x\big(t-d(t)\big)\Big) \\ & + f^*\Big(x\big(t-d(t)\big)\Big)B^*S_1\dot{x}(t) - x^*(t-\delta)(CS_2 + S_2^*C)x(t-\delta) \\ & + x^*(t-\delta)S_2^*Af\big(x(t)\big) + f^*\big(x(t)\big)A^*S_2x(t-\delta) \\ & + x^*(t-\delta)S_2^*Bf\Big(x\big(t-d(t)\big)\Big) + f^*\Big(x\big(t-d(t)\big)\Big)B^*S_2x(t-\delta). (22) \end{aligned}$$

Therefore, it follows from (11)-(19) and (22) that

$$\dot{V}(t) \le \eta^*(t)\Omega\eta(t), (23)$$

Where

$$\begin{aligned} \eta(t) = \Big(& x^*(t),\ \dot{x}^*(t),\ x^*(t-\delta),\ x^*\big(t-d_1(t)\big),\ x^*\big(t-d(t)\big),\ x^*(t-d_1),\ x^*(t-d), \\ & f^*\big(x(t)\big),\ f^*\Big(x\big(t-d_1(t)\big)\Big),\ f^*\Big(x\big(t-d(t)\big)\Big),\ \Big(\int_{t-\delta}^{t} x(s)ds\Big)^*\Big)^*. \end{aligned}$$

Then it follows from (5) and (23) that$\dot{V}(t) < 0$, which together with the radial unboundedness of$V(t)$ guarantee the global asymptotical stability of the QVNNs (2). The proof is completed.

Remark 3.1. Since the QVLMIs (3)-(5) cannot be straightforwardly resolved via the Matlab LMI toolbox, it is necessary to convert QVLMIs into CVLMIs to acquire a set of feasible solutions with the assistance of Lemmas 2.2 and 2.3. Based on Lemma 2.2, we first conduct plural decomposition on the quaternion matrix appeared in Theorem 3.1: $P_\iota = P_{\iota 1} + P_{\iota 2}j$ $(\iota = 1,2,3), Q_\varsigma = Q_{\varsigma 1} + Q_{\varsigma 2}j$ $(\varsigma = 1,2,\dots,6), R_1 = R_{11} + R_{12}j, R_2 = R_{21} + R_{22}j, U = U_1 + U_2j, V = V_1 + V_2j, S_1 = S_{11} + S_{12}j, S_2 = S_{21} + S_{22}j$. Then the following corollary can be immediately obtained by resorting to Lemma 2.3.

Corollary 3.1. Suppose Assumptions 1 and 2 hold. The equilibrium of system (2) is globally asymptotically stable if there exist positive diagonal matrices, Hermitian matrices, skew symmetric matrices and matrices such that the following complex-valued LMIs hold:

$$\begin{pmatrix} P_{i1} & -P_{i2} \\ \bar{P}_{i2} & \bar{P}_{i1} \end{pmatrix} > 0, \quad \begin{pmatrix} Q_{j1} & -Q_{j2} \\ \bar{Q}_{j2} & \bar{Q}_{j1} \end{pmatrix} > 0, \qquad (24)$$

$$\begin{pmatrix} X_1 & -X_2 \\ \bar{X}_2 & \bar{X}_1 \end{pmatrix} > 0, \quad \begin{pmatrix} Y_1 & -Y_2 \\ \bar{Y}_2 & \bar{Y}_1 \end{pmatrix} > 0, \quad \begin{pmatrix} \Omega_1 & -\Omega_2 \\ \bar{\Omega}_2 & \bar{\Omega}_1 \end{pmatrix} < 0, \qquad (25)$$

Where

$$X_1 = \begin{pmatrix} R_{11} & U_1 \\ * & R_{11} \end{pmatrix}, \quad X_2 = \begin{pmatrix} R_{12} & U_2 \\ \blacksquare & R_{12} \end{pmatrix}, \quad Y_1 = \begin{pmatrix} R_{21} & V_1 \\ * & R_{21} \end{pmatrix}, \quad Y_2 = \begin{pmatrix} R_{22} & V_2 \\ \blacksquare & R_{22} \end{pmatrix}$$

and $\Omega_1 = (\Omega_{ij}^{(1)})_{11\times 11}, \Omega_2 = (\Omega_{ij}^{(2)})_{11\times 11}$with $\Omega_{ij}^{(1)}, \Omega_{ij}^{(2)}$omitted here due to the limited space.

4. A NUMERICAL EXAMPLE

In this section, an illustrative example is provided to validate the effectiveness of the theoretical results.
Consider the two-dimensional QVNNs (2) with parameters given as follows:

$$C = diag\{8,12\}, A = (a_{ij})_{2\times 2}, B = (b_{ij})_{2\times 2}, \delta = 0.5,$$

$$d_1(t) = 0.45\sin(t) + 0.25, d_2(t) = 0.15\cos(t) - 0.05, f_1(s) = f_2(s) = 0.2\tanh(s), s \in \mathbb{Q}$$

Where

$$\begin{aligned} a_{11} &= 1.2 + 3.0i - 3.6j + 2.0k, & a_{12} &= 1.8 + 1.6i - 2.0j - 1.9k, \\ a_{21} &= 3.8 - 3.8i + 2.0j - 2.1k, & a_{22} &= 1.5 + 3.2i - 3.6j + 3.0k, \\ b_{11} &= 1.5 - 3.3i + 2.6j + 1.1k, & b_{12} &= 1.5 + 2.6i + 0.9j - 2.9k, \\ b_{21} &= 2.5 + 3.2i - 0.7j - 1.5k, & b_{22} &= 2.9 + 3.5i + 1.3j + 1.5k. \end{aligned}$$

In accordance with Remark 2.1, the quaternion-valued matrices $A$and$B$can be uniquely expressed as $A = A_1 + A_2 j$and $B = B_1 + B_2 j$respectively, where

$$A_1 = \begin{pmatrix} 1.2 + 3.0i & 1.8 + 1.6i \\ 3.9 - 3.8i & 1.5 + 3.2i \end{pmatrix}, \ A_2 = \begin{pmatrix} -3.6 + 2.0i & -2.0 - 1.9i \\ 2.0 - 2.1i & -3.6 + 3.0i \end{pmatrix},$$

$$B_1 = \begin{pmatrix} 1.5 - 3.3i & 1.5 + 2.6i \\ 2.5 + 3.2i & 2.9 + 3.5i \end{pmatrix}, B_2 = \begin{pmatrix} 2.6 + 1.1i & 0.9 - 2.9i \\ -0.7 - 1.5i & 1.3 + 1.5i \end{pmatrix}.$$

In addition, it can be readily verified that Assumptions 1 and 2 are satisfied, and $d_1 = 0.7, d_2 = 0.1, d = 0.8, \mu_1 = 0.45, \mu_2 = 0.15, \mu = 0.6$. Therefore, a set of feasible solutions to CVLMIs (24)-(25) can be established via the Yalmip toolbox in Matlab (only partial matrices in the solutions are listed here due to the limited space):

$$M_1 = diag\{0.3635,0.3544\}, M_2 = diag\{0.1306, 0.1306\}, M_3 = diag\{0.3254,0.3341\},$$

$$P_{11} = \begin{pmatrix} 0.4610 + 0.0000i & 0.0012 - 0.0025i \\ 0.0012 + 0.0025i & 0.1332 + 0.0000i \end{pmatrix},$$

$$Q_{11} = \begin{pmatrix} -0.2628 + 0.0000i & 0.0001 - 0.0001i \\ 0.0001 + 0.0001i & -0.2561 + 0.0000i \end{pmatrix},$$

$$U_1 = \begin{pmatrix} -0.1404 + 0.0000i & -0.0001 + 0.0002i \\ -0.0001 - 0.0002i & -0.1423 - 0.0000i \end{pmatrix},$$

$$V_1 = \begin{pmatrix} -0.1698 + 0.0000i & -0.0000 + 0.0001i \\ -0.0000 - 0.0001i & -0.1686 - 0.0000i \end{pmatrix},$$

$$S_{11} = \begin{pmatrix} 0.3059 - 0.0000i & 0.0634 - 0.1002i \\ 0.0634 + 0.1001i & 0.2655 + 0.0000i \end{pmatrix},$$

$$S_{21} = \begin{pmatrix} 0.2465 + 0.0000i & 0.0766 - 0.1211i \\ 0.0511 + 0.0807i & 0.3208 + 0.0000i \end{pmatrix}.$$

Therefore, the equilibrium of the QVNNs (2) is globally asymptotically stable according to Corollary 1. Fig. 1 depicts the transient behavior of the neuron state in (2).

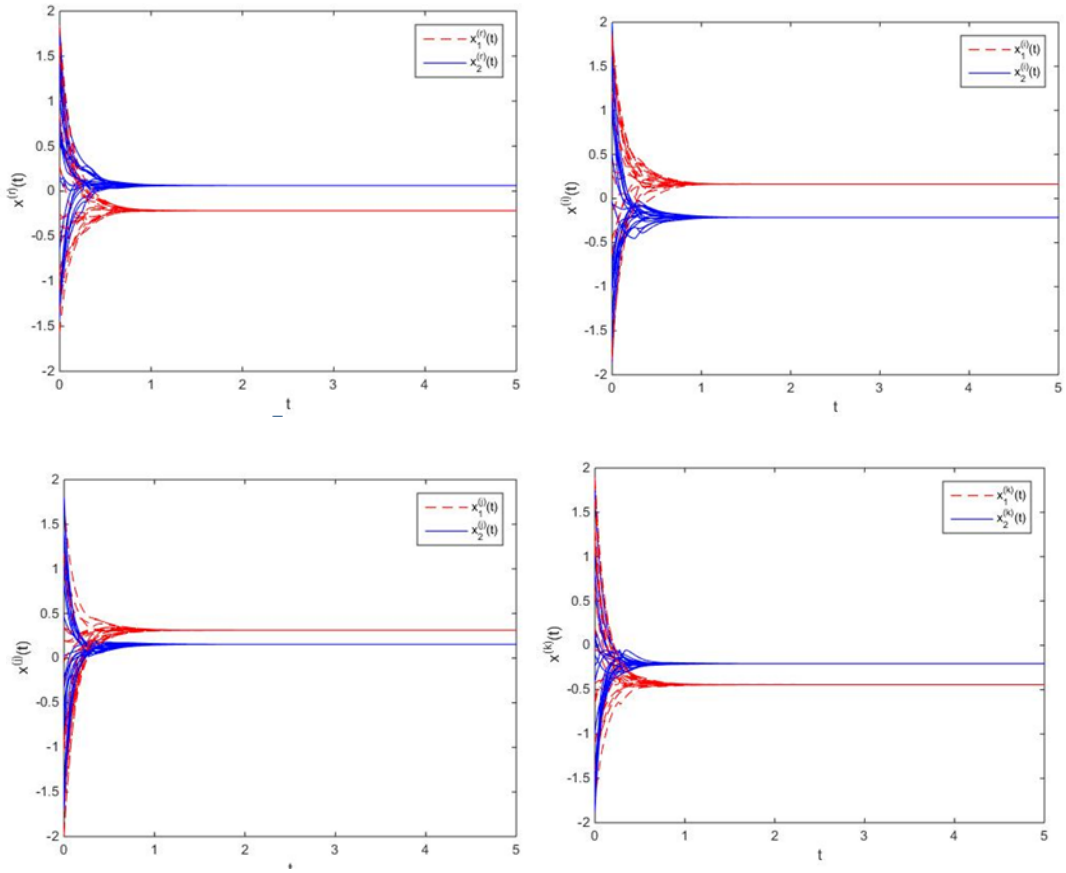

Figure 1. The transient behaviors of neuron states of QVNNs (2).

5. CONCLUSIONS

This paper is concerned with the stability analysis of quaternion-valued neural networks with both leakage delay and additive time-varying delays. Based on the Lyapunov functional method and inequality technique, some delay-dependent criteria are provided by fully considering the relationship between time-varying delays and upper bounds of delays. It is worth mentioning that the stability criteria are established in two forms. Finally, a numerical example is proposed to demonstrate the validity of theoretical results.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that help improve the quality of this manuscript.

REFERENCES

[1] H. Bao, Ju H. Park, and J. Cao, (2016) "Exponential synchronization of coupled stochastic memristor-based neural networks with time-varying probabilistic delay coupling and impulsive delay",IEEE Transactions on Neural Networks,Vol. 27, No. 1, pp. 190–201.

[2] J. Cao and R. Li, (2017) "Fixed-time synchronization of delayed memristor-based recurrent neural networks",Science China: Information Sciences, Vol. 60, No. 3, pp. 108–122.

[3] X. Li and J. Cao, (2017) "An impulsive delay inequality involving unbounded time-varying delay and applications",IEEE Transactions on Automatic Control, Vol. 62, No. 7, pp. 3618–3625.
[4] J. Wang, H. Wu, and T. Huang, (2015) "Passivity-based synchronization of a class of complex dynamical networks with time-varying delay",Automatica, Vol. 56, pp. 105–112.
[5] R. Yang, B. Wu, and Y. Liu, (2015) "A halanay-type inequality approach to the stability analysis of discrete time neural networks with delays", Applied Mathematics and Computation, Vol. 265, pp. 696–707.
[6] X. Yang and J. Lu, (2016) "Finite-time synchronization of coupled networks with markovian topology and impulsive effects", IEEE Transactions on Automatic Control, Vol. 61, No. 8, pp. 2256–2261.
[7] S. Jankowski, A. Lozowski, and J.M. Zurada, (1996) "Complex-valued multistate neural associative memory", IEEE Transactions on Neural Networks, Vol. 7, No. 6, pp. 1491–1496.
[8] H. Bao, Ju H. Park, and J. Cao, (2016) "Synchronization of fractional-order complex-valued neural networks with time delay", Neural Networks, Vol. 81, pp. 16–28.
[9] W. Gong, J. Liang, and J. Cao, (2015) "Matrix measure method for global exponential stability of complex-valued recurrent neural networks with time-varying delays",Neural Networks, Vol. 70, pp. 81–89.
[10] A. Hirose and S. Yoshida, (2012) "Generalization characteristics of complex-valued feedforward neural networks in relationto signal coherence", IEEE Transactions on Neural Networks and Learning Systems, Vol. 23, No. 4, pp. 541–551.
[11] R. Rakkiyappan, G. Velmurugan, X. Li, and D. O'Regan, (2016) "Global dissipativity of memristor-based complex-valued neural networks with time-varying delays", Neural Computing and Applications, Vol. 27, No. 3, pp. 629–649.
[12] N. Matsui, T. Isokawa, H. Kusamichi, F. Peper, and H. Nishimura, (2004) "Quaternion neural network with geometrical operators", Journal of Intelligent and Fuzzy Systems, Vol. 15, No. 3, pp. 149–164.
[13] B.C. Ujang, C.C. Took, and D.P. Mandic, (2011) "Quaternion-valued nonlinear adaptive filtering",IEEE Transactions onNeural Networks, Vol. 22, No. 8, pp. 1193–1206.
[14] Y. Liu, D. Zhang, J. Lu, and J. Cao, (2016) "Global μ-stability criteria for quaternion-valued neural networks with unbounded time-varying delays",Information Sciences, Vol. 360, pp. 273–288.
[15] H. Shu, Q. Song, Y. Liu, Z. Zhao, and F.E. Alsaadi, (2017) "Global μ-stability of quaternion-valued neural networks withnon-differentiable time-varying delays" ,Neurocomputing, Vol. 247, pp. 202–212.
[16] Y. Liu, D. Zhang, and J. Lu, (2016) "Global exponential stability for quaternion-valued recurrent neural networks with time-varying delays", Nonlinear Dynamics, Vol. 87, No. 1, pp. 1–13.
[17] X. Chen, Z. Li, Q. Song, J. Hu, and Y. Tan, (2017) "Robust stability analysis of quaternion-valued neural networks with time delays and parameter uncertainties", Neural Networks, Vol. 91, pp. 55–65.
[18] X. Chen, Q. Song, Z. Li, Z. Zhao, and Y. Liu, (2018) "Stability analysis of continuous-time and discrete-time quaternion-valued neural networks with linear threshold neurons", IEEE Transactions on Neural Networks, Vol. 29, No. 7, pp. 2769–2781.
[19] Z. Tu, J. Cao, A. Alsaedi, and T. Hayat, (2017) "Global dissipativity analysis for delayed quaternion-valued neural networks", Neural Networks, Vol. 89, pp. 97–104.
[20] Z. Yu, H. Gao, and S. Mou, (2008) "Asymptotic stability analysis of neural networks with successive time delay components", Neurocomputing, Vol. 71, No. 13-15, pp. 2848–2856.
[21] H. Shao and Q. Han, (2011) "New delay-dependent stability criteria for neural networks with two additive time-varying delay components", IEEE Transactions on Neural Networks, Vol. 22, No. 5, pp. 812–818.
[22] J. Tian and S. Zhong, (2012) "Improved delay-dependent stability criteria for neural networks with two additive time-varying delay components", Neurocomputing, Vol. 77, pp. 114–119.
[23] P.G. Park, J.W. Ko, and C. Jeong, (2011) "Reciprocally convex approach to stability of systems with time-varying delays", Automatica, Vol. 47, No. 1, pp. 235–238.
[24] J. Liang, K. Li, Q. Song, Z. Zhao, Y. Liu, and F.E. Alsaadi, (2018) "State estimation of complex-valued neural networks with two additive time-varying delays" ,Neurocomputing, Vol. 309, pp. 54–61.

AUTHORS

Qun Huang received the B.S. degree from Southeast University, Nanjing, China in 2014. He is currently pursuing the Ph.D. degree with the School of Mathematics, Southeast University,Nanjing, China. His current research interests include quaternion-valued neural networks and dynamic equations on time scales.

Jinde Cao (F'16) received the B.S. degree from Anhui Normal University, Wuhu, China, the M.S. degree from Yunnan University, Kunming, China, and the Ph.D. degree from Sichuan University, Chengdu, China, all in mathematics/applied mathematics, in 1986, 1989, and 1998, respectively. He is an Endowed Chair Professor, the Dean of the School of Mathematics, the Director of the Jiangsu Provincial Key Laboratory of Networked Collective Intelligence of China and the Director of the Research Center for Complex Systems and Network Sciences at Southeast University. Prof. Cao was a recipient of the National Innovation Award of China, Obada Prize and the Highly Cited Researcher Award in Engineering, Computer Science, and Mathematics by Thomson Reuters/Clarivate Analytics. He is a fellow of IEEE, a member of the Academy of Europe, a member of the European Academy of Sciences and Arts, a fellow of Pakistan Academy of Sciences, and an IASCYS academician.

AN INVESTIGATION OF MODERN FOREIGN LANGUAGE (MFL) TEACHERS AND THEIR ATTITUDES TO COMPUTER ASSISTED LANGUAGE LEARNING (CALL) AMID THE COVID-19 HEALTH PANDEMIC

Louise Hanna, David Barr, Helen Hou and Shauna Mc Gill

School of Education, Ulster University, United Kingdom

ABSTRACT

A study was performed with 33 Modern Foreign Language (MFL) teachers to afford insight into how classroom practitioners interact with Computer Assisted Language Learning (CALL) in Second Language (L2) pedagogy. A questionnaire with CALL specific statements was completed by MFL teachers who were recruited via UK based Facebook groups. Significantly, participants acknowledged a gap in practice from the expectation of CALL in the MFL classroom. Overall, respondents were shown to be interested and regular consumers of CALL who perceived its ease and importance in L2 teaching and learning.

KEYWORDS

Computer Assisted Language Learning (CALL), Modern Foreign Languages (MFL), teacher attitudes, digital technologies, Second Language (L2) pedagogy.

1. INTRODUCTION

The role of Computer Assisted Language Learning (CALL) has been area of interest for researchers for more than forty years (Zou & Thomas, 2019[1]). Significantly, the global Coronavirus pandemic has reinforced the importance of digital technologies in Second Language Acquisition (SLA). This study was undertaken in the summer of 2020 with 33 Modern Foreign Language (MFL) teachers in the UK as a means to comprehend their relationship with CALL at this time of a health crisis and considerable challenges in education. Overall, the investigation sought to gain an insight into MFL teachers perceive the importance, value and ease of CALL in their own teaching and learning.

Simply speaking, 'CALL refers to the application of a variety of technologies for language learning including computer, internet, online reference materials, online exercises and quizzes' (Rahimi, 2015[2]). The interdisciplinary subject of CALL has developed at breakneck speed in line with the continued evolution of digital tools and computerised technologies in education and beyond. Nonetheless, the onset of the Coronavirus outbreak heralded the most significant and radical change to the teaching and learning landscape as teachers had to adapt to the challenges of online education (Dhawan, 2020[3]). 'However, the extent to which teachers have successfully mastered these challenges and which factors are most relevant remain unknown' (König, Jäger-Biela & Glutsch, 2020[4]). Therefore, this provides the rationale to undertake this small-scale study with MFL in the UK context.

David C. Wyld et al. (Eds): BIBC, AISO, EDTECH - 2020
pp. 59-66, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101306

2. RELATED WORK

The massive global shift to online and distance learning in 2020 has been an area of significant research interest. An investigation of the attitudes of Mathematics teachers during the COVID-19 pandemic found that practitioners expressed positive opinions towards the engagement of digital devices and technological tools for the purpose of teaching and learning (Marpa, 2021[5]). In fact, a Finnish study revealed that teachers reacted quickly to learn the new technologies and perceived digital education as problematic, except for the quality of interactions with students (Niemi & Kousa, 2020[6]). With specific relation to CALL in English as a Foreign Language (EFL) instruction, teachers had 'diverse perceptions of online EFL teaching over COVID-19 as they compared it with traditional classroom language teaching to explore the features of online EFL teaching' (Gao & Zhang, 2020[7]). Furthermore, English teachers in Iran displayed positive perceptions towards the engagement of CALL for students at home whilst in lockdown (Khatoony & Nezhadmehr, 2020[8]). Overall, this study was motivated to uncover the attitudinal positions of MFL teachers towards the application of digital technologies within the UK context. In fact, 'researching teachers' beliefs are important for their professional development, particularly in the midst of a pandemic" (Zhang, 2020[9]).

3. METHODOLOGY

A plea for participation was issued on various MFL teaching Facebook groups. Participation entailed completing a questionnaire with specific statements relating to CALL adoption in L2 pedagogy. This type of research tool sought to obtain reactions from participants relating to their attitudes of CALL in their own teaching and learning that could be empirically measured and statistically analysed. This snapshot of teacher perceptions to the implementation of digital technologies in MFL was established, therefore, on a positivist methodology. This means that the findings are unable to account of the depth and diversity of personal and professional teacher opinion to CALL realisation. Instead, the findings provide an overview of the MFL teacher alliance with CALL that could be more thoroughly investigated via a large-scale study.

4. FINDINGS

Firstly, 21.1% of research participants reported having had more than twenty-years of MFL instruction. Interestingly, however, the highest level of participation involved relatively new MFL teaching practitioners who had between one to five years of MFL classroom experience (24.2%) (Table 1).

Table 1: A table exhibiting the number of years' of MFL teaching by participants.

Years' of teaching experience	**Percentage (%)**
Less than 1 year	6.1
1-5 years	24.2
6-10 years	18.2
11- 15 years	15.2
16- 20 years	15.2
+20 years	21.1

In fact, these recent entrants to the teaching profession may still be transitioning from their teacher education programme to the daily demands and reality shock of the initial years of teaching. This may be particularly pronounced in the disconnect of CALL instruction in Initial

Teacher Education (ITE) with the possibilities and practicalities of using digital technologies in the Newly Qualified Teacher (NQT) induction period and beyond (Woolfolk & Margetts, 2012[10]). 78.8% of study respondents agreed to the existence of such a gap between institutional expectations and implementation of CALL in the MFL classroom setting (Figure 1).

Figure 1: A bar chart highlighting the perception that there is a gap between expectation and practice of CALL usage by MFL teachers.

This technological lag has been widely documented in CALL literature as the intentions and realities of classroom innovation are mismatched (Clark-Wilson, Robutt & Sinclair, 2014[11]; Kobayashi, 2008: 105[12]). In fact, this divergence in project versus actual technological usage in pedagogy can be attributed to a number of key factors. These include concerns around the technological competencies of both teachers and learners, difficulty in accessing digital resources, issues in achieving pedagogical outcomes with CALL and a lack of comprehensive training for teaching practitioners (Visvizi, 2019[13]). Moreover, the role of educational policy can create a wedge between the expectation and the reality of CALL implementation. The small-scale study has offered a strong confirmation that a bridge between projected and actual CALL usage is desired by more than three quarters of participants (Vrasidas et al., 2006[14]).

However, this discrepancy in expectancy versus practice in CALL is not necessarily indicative of a lack of interest in digital technologies in MFL teaching and learning from the perspective of L2 teachers. This study demonstrated that 24.2% of respondents were extremely interested in CALL and 33.3% were very interested in the subject. This is presented visually in the pie chart of Figure 2. Such a claim has been authenticated - though on a higher level - in a research study by Lytras and Lytras; 70% of teachers reported an enthusiasm and readiness to adopt computer technologies and mobile innovations in their pedagogical practice (Lytras & Lytras, 2010[15]). In reality, it has often been the case that teachers have been subject to critical discourse and presented as 'outmoded, obstructive or ignorant' in relation to CALL and digital technologies (Selwyn, 2016[16]). Therefore, this could be a fruitful area of further investigation to effectively comprehend the relationship teachers have with CALL in terms of their interest to digital technologies.

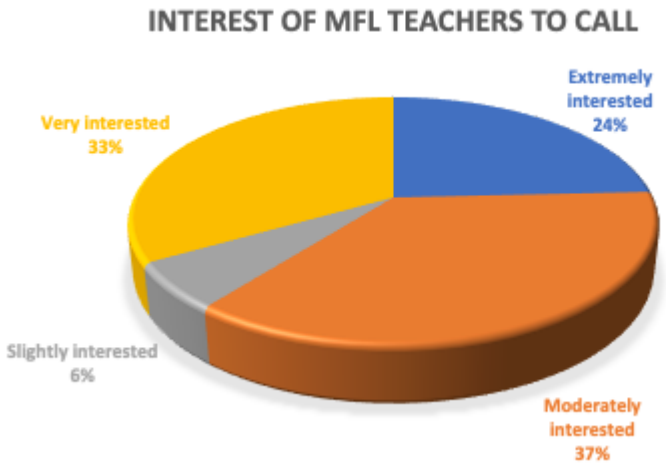

Figure 2: A pie chart showing the level of interest of MFL teacher participants to CALL.

Significantly, the finding that teachers are interested consumers of digital technologies demonstrates how the detachment between theory and practice in CALL contexts is not intrinsically bound to a lack of interest or, what is more, a perception that CALL realisation is strenuous or intellectually demanding (Lin, Zhang & Zheng, 2017[17]). In fact, 67% of respondents remarked that CALL in MFL instruction was extremely or somewhat easy (Figure 3).

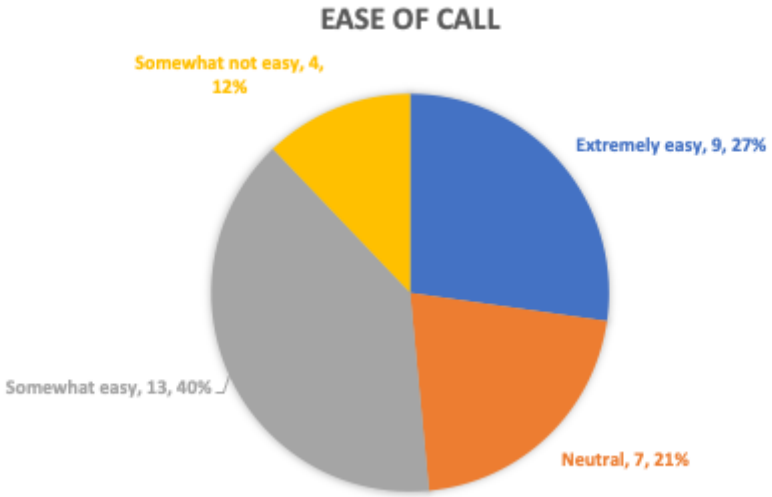

Figure 3: The perceived ease of CALL from the perception of MFL teachers.

This is an alternative perspective to the belief propagated in research literature that CALL is a complex phenomenon that constantly challenges and frequently frustrates MFL instructors (Gibson & Baek, 2009[18]; Kidd, 2008[19]). In fact, the engagement of teaching practitioners with CALL and digital technologies has been depicted as an arduous challenge (Carreira et al., 2018[20]). However, 'the products for digital teaching or learning are easier to use than the past ten years (Haghi & Luppicini, 2010[21]). In the words of one participant, adopting CALL is '*like fish in water'*. This gives the impression that innovative practice is effortless, natural and comfortable in L2 pedagogy. The results of this study point to a potentially smaller divergence in CALL practice from the perspective of the participating 33 MFL teachers. In fact, 33.3% of

respondents reported always using CALL in every lesson. These findings are represented below in Table 2.

Table 2: A table depicting the frequency of CALL use in the MFL classroom.

Frequency of CALL usage	**Percentage (%)**
Always (every lesson)	33.3
Never (not use)	6.1
Often (every other lesson)	30.3
Rarely (once a term)	6.1
Sometimes (once a month)	24.2

This sample of contributing teachers are integrating digital innovations everyday into their daily MFL instruction (Bain & Weston, 2012[22]). This supports the prediction made years before that CALL would assume a normalised position in L2 pedagogy, like a pen and paper. Significantly, it was projected that CALL would be 'used every day by language students and teachers as an integral part of every lesson' (Torsani, 2016[23]). This regular engagement with digital technologies strongly denotes a positive belief to CALL from the research participants. This is for the reasoning that attitude to technology is inextricably linked to classroom innovation in MFL (Eshetu, 2015[24]). Overall, 'the relationship between teacher beliefs and technology integration has also surfaced as a critical factor in technology integration' (Brown & van der Merwe, 2015[25]). With relation to this study, participants championed the importance of CALL in MFL pedagogy. Figure 4 highlights how 37% of respondents rated CALL as extremely important and 33% appraised it as very important. This supports the claim that it is 'important for teachers to recognize the transformative value of technology for their own practice, not just for their students' (Pahomov, 2014[26]). This is particularly strong in the results of this study, although it is important to acknowledge the evident limitations of the investigation.

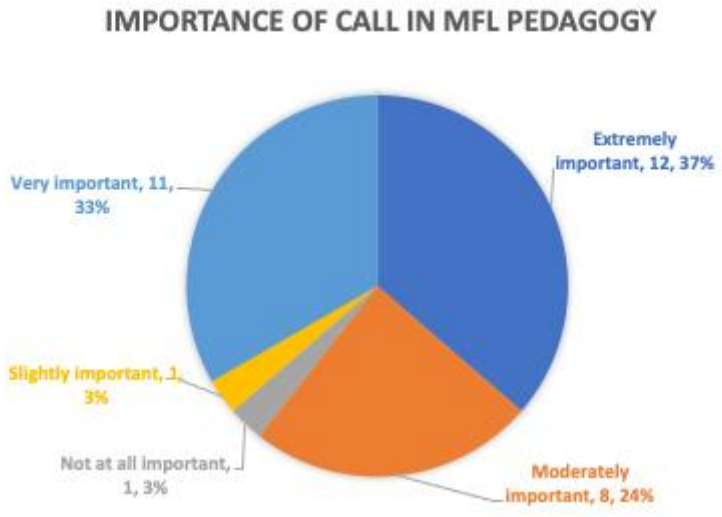

Figure 4: A pie chart presenting how important CALL is in L2 pedagogy for pilot study respondents.

Overall, MFL teachers of this study exhibited a largely positive affect to CALL which is consistent with their frequent technological practice (Ball et al., 2018[27]). A number of participants commented that CALL was 'essential', 'enriching, 'effective', 'exciting', 'helpful', 'invaluable', 'beneficial', 'necessary', 'positive' and 'fabulous'. However, this positive narrative

to CALL was not shared by all respondents. Several teachers noted that CALL was 'in need of direction', 'labour intensive', 'frustrating', 'extremely challenging', 'time-consuming', 'not the be all and end all, especially if the Internet is down' and 'overrated'. Nevertheless, the guidance to use CALL was offered by a third of study participants in their one piece of advice to aspiring MFL teachers (Figure 5).

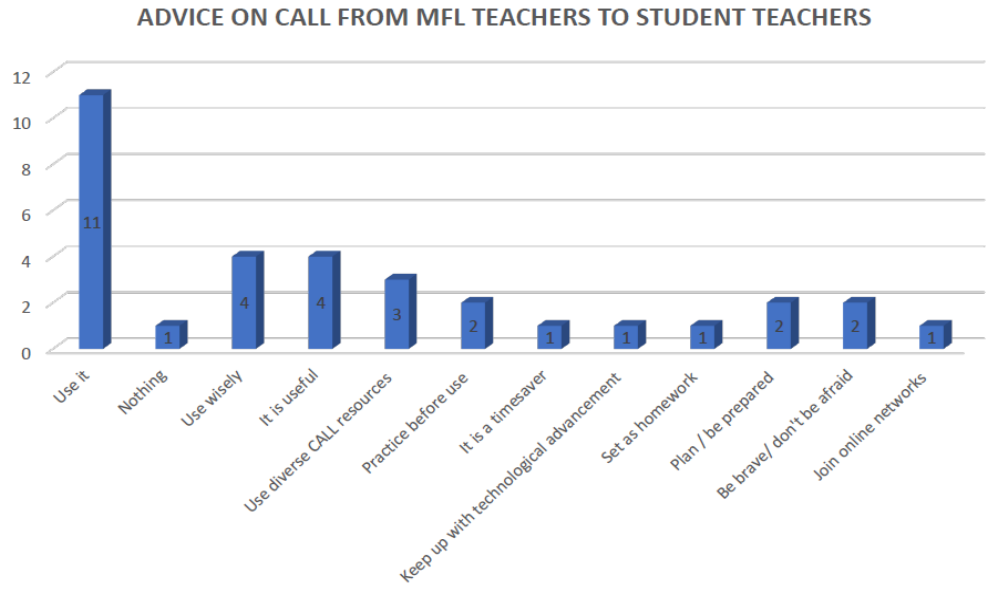

Figure 5: A bar chart representing the advice of MFL teachers to student teachers.

Such a recommendation indicates that this sample of MFL teachers were open-minded and enthusiastic in encouraging the next generation of teaching practitioners to embrace the opportunities of CALL. This has been supported in research studies investigating factors and barriers to implementation. The willingness of MFL teachers to capitalise on CALL has been thwarted externally, financially and situationally by resourcing problems, funding issues and inequitable access to infrastructure (Schul, 2019[28]; Underwood & Farrington-Flint 2015[29]). For one MFL teacher participant, CALL is only possible 'if laptops/iPads/computers room are available. I would like to be able to use more CALL as it's the way forward with technology obsessed children'. This connects to the political landscape of education and the role of Local Education Authorities (LEA) in CALL. One participant remarked that 'as decision-making stakeholders, they are the ones deciding budgets and priorities for communities'. With the onset of the COVID-19 pandemic, a number of participants remarked on the importance of General Data Protection Regulation (GDPR) and privacy in Zoom video calls. Therefore, there are wide array of factors to consider in CALL implementation for MFL teachers. Simply speaking, this study has been only able to offer a snapshot into how MFL teaching practitioners interact and relate to digital technologies in their L2 pedagogy. Therefore, the study could be viewed as a springboard from which additional investigations could be conducted to better appreciate the MFL teacher alliance to CALL.

5. LIMITATIONS AND FUTURE RESEARCH

A primary limitation of this study is that it was established on a positivist approach to data collection. As a consequence, conclusions are restricted by the empirical data obtained. However, richer, more detailed and in-depth information could have been acquired by a qualitative or mixed-methods approach. Such an adjustment to research methodology could have

compensated for this limitation. Therefore, this opens up the possibility of conducting further investigations to better comprehend how MFL teachers perceive digital technologies. Another issue to note with this research is that it involved quite a small sample of MFL teachers (33 in total). A larger sample of participants would have enhanced the researcher's understanding of how MFL teachers interact with CALL. Future research could encompass a longitudinal understanding of MFL teachers and their relationship with computer technologies over the course of the pandemic. Additional research could be undertaken with pre-service MFL teachers to obtain a sense of their rapport with CALL while in Initial Teacher Education (ITE) during the global pandemic

6. CONCLUSIONS

In summary, this study presented the researcher with the occasion to gauge teacher perceptions to CALL in the L2 classroom. It has showcased that MFL teachers are daily users of CALL in L2 pedagogy. The attitudinal perspectives of participants demonstrated that a gap between expectation and practice in CALL exist -a finding that could form the basis of a follow-on study. In addition, respondents were shown to recognise the importance of digital technologies in L2 teaching and learning and readily encouraged new student teachers to adopt CALL in the classroom. In addition, participants were interested adopters of technology in the MFL classroom who perceived its usage as being easier than difficult. This, too, could be an additional study for researcher investigation. It is important to acknowledge that there are evident limitations with the study as a positivist methodology and sample size of 33 participants. Nonetheless, it has provided a snapshot of MFL teachers and their cognitions of CALL amid a global health pandemic and widespread disruption to education.

REFERENCES

[1] Zou, B. & Thomas, M. (2019). *Recent Developments In Technology-Enhanced & Computer-Assisted Language Learning*, Hershey: IGI Global, pp. xv.

[2] Rahimi, M., (2015). *Handbook of research on individual differences in computer-assisted language learning*, Hershey, PA: Information Science Reference, an imprint of IGI Global, pp. 45.

[3] Dhawan, S. (2020). Online Learning: A Panacea in the Time of COVID-19 Crisis. *Journal of Educational Technology Systems*, 49(1), 5–22. Available online: https://doi.org/10.1177/0047239520934018

[4] König, J. Jäger-Biela, D.J. & Glutsch, N. (2020) Adapting to online teaching during COVID-19 school closure: teacher education and teacher competence effects among early career teachers in Germany, *European Journal of Teacher Education*, 43:4, 608-622. Available online: https://doi.org/10.1080/02619768.2020.1809650

[5] Marpa, E. P. (2021). Technology in the teaching of mathematics: An analysis of teachers' attitudes during the COVID-19 pandemic. *International Journal on Studies in Education (IJonSE)*, 3(2), 92-102. Available online: https://doi.org/10.46328/ijonse.36

[6] Niemi, H. M., & Kousa, P. (2020). A case study of students' and teachers' perceptions in a Finnish high school during the COVID pandemic. *International Journal of Technology in Education and Science (IJTES)*, 4(4), 352-369. Available online: https://doi.org/10.46328/ijtes.v4i4.167

[7] Gao, L..X & Zhang, L.J. (2020). Teacher Learning in Difficult Times: Examining Foreign Language Teachers' Cognitions About Online Teaching to Tide Over COVID-19. *Front. Psychol.* 11:549653. Available online: https://doi.org/10.3389/fpsyg.2020.549653

[8] Khatoony, S., & Nezhadmehr, M. (2020). EFL teachers' challenges in integration of technology for online classrooms during Coronavirus (COVID-19) pandemic in Iran. *AJELP: Asian Journal of English Language and Pedagogy*, 8, 1-16. Available online: https://doi.org/10.37134/ajelp.vol8.sp.1.2020

[9] Zhang, C. (2020). From Face-to-Face to Screen-to-Screen: CFL Teachers' Beliefs about Digital Teaching Competence during the Pandemic. *International Journal of Chinese Language Teaching*, 1(1), 35-52. Available online: https://doi.org/10.46451/ijclt.2020.06.03

[10] Woolfolk, A & Margetts, K. (2012). *Educational Psychology*, third edition. Frenchs Forest, NSW, Australia: Pearson Australia, pp. 7.
[11] Clark-Wilson, A. Robutti, O. & Sinclair, N. (2014). *The Mathematics Teacher in the Digital Era. An International Perspective on Technology Focused Professional Development*. Dordrecht: Springer, pp.11.
[12] Kobayashi, R. (2008). *New educational technology*. New York: Nova Science Publishers, pp.105.
[13] Visvizi, A., (2019). *The future of innovation and technology in education policies and practices for teaching and learning excellence*, United Kingdom: Emerald Publishing, pp.116.
[14] Vrasidas, C. et al. (2006). *Preparing teachers to teach with technology*. Greenwich Conn: Information Age Publishing, pp.366.
[15] Lytras, M. D. & Lytras, M. D. (2010). *Technology Enhanced Learning: Quality of Teaching and Educational Reform: 1st International Conference, TECH-EDUCATION 2010, Athens, Greece, May 19-21, 2010. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp.462.
[16] Selwyn, N., (2016*). Education and technology: key issues and debates*, New York: Bloomsbury Academic, pp.127.
[17] Lin, C.-H. Zhang, D. & Zheng, B. (2017*). Preparing foreign language teachers for next-generation education*. Hershey, PA: Information Science Reference (an imprint of IGI Global), pp.32.
[18] Gibson, D. & Baek, Y. (2009). *Digital simulations for improving education: learning through artificial teaching environments*, Hershey, PA: Information Science Pub, pp. 428.
[19] Kidd, T. (2008). *Handbook of research on instructional systems and technology*, Hershey, PA: Information Science Reference, pp.227.
[20] Carreira, S. et al., (2018). *Youngsters Solving Mathematical Problems with Technology #x98;The Results and Implications of the Problem#x9C;Web Project*, Cham: Springer International Publishing, pp.viii.
[21] Haghi, A.K. & Luppicini, R., (2010). *Cases on digital technologies in higher education: issues and challenges*, Hershey, PA: IGI Global, pp.214.
[22] Bain, A. & Weston, M. E. (2012). *The learning edge: what technology can do to educate all children.* New York: Teachers College Press, pp.xi.
[23] Torsani, S., (2016). *CALL teacher education: language teachers and technology integration*, Rotterdam: Sense Publishers, pp.55.
[24] Eshetu, G. (2015). *Factors Affecting Instructional Leaders Perception towards Educational Media Utilization in Classroom Teaching*. Hamburg, Germany: Ancho, pp.25.
[25] Brown, T.H. & van der Merwe, H.J. (2015). *The mobile learning voyage - from small ripples to massive open waters: 14th World Conference on Mobile and Contextual Learning, mLearn 2015, Venice, Italy, October 17-24, 2015, proceedings*, Cham: Springer, pp.33/
[26] Pahomov, L., (2014). *Authentic learning in the digital age: engaging students through inquiry*, Alexandria, VA: ASCD, pp.9.
[27] Ball, L. Drijvers, P. Ladel, S. Siller, H.-S. Tabach, M. & Vale, C. (2018). *Uses of Technology in Primary and Secondary Mathematics Education: Tools, Topics and Trends*. Cham: Springer International Publishing, pp.416.
[28] Schul, J. E. (2019). *Paradoxes of the public school: historical and contemporary foundations of American public education*. Charlotte, NC: Information Age Publishing, Inc, pp.183.
[29] Underwood, J. D. M. & Farrington-Flint, L. (2015). *Learning and the E-Generation*. Chichester, West Sussex: John Wiley & Sons Inc, pp.156.

AUTHORS

Louise Hanna is a second year PhD researcher at Ulster University in Northern Ireland. Her interests are extensively centred on the usage of digital technologies in L2 pedagogy. Prior to undertaking her PhD, Louise was a MFL teachers in both England and Northern Ireland.

AUTHOR INDEX

Anton Hasselgren	*23*
Arild Faxvaag	*23*
Danilo Gligoroski	*23*
David Barr	*59*
Gareth Owenson	*01*
Helen Hou	*59*
Jinde Cao	*37*
Jinde Cao	*47*
Katina Kralevska	*23*
Louise Hanna	*59*
Margareth Horn	*23*
Paul Kengfai Wan	*23*
Qun Huang	*47*
Remy Zgraggen	*17*
Richard Dennis	*01*
Shaosheng Xu	*37*
Shauna Mc Gill	*59*
Xiangnan Liu	*37*