A proposal for a proof-of-proximity system for improving the security of remote patient monitoring systems.

D D J
Department of computing and informatics
Bournemouth University
Poole, England

***Abstract*—Telemedicine is a growing branch of healthcare. The market is projected to triple in value between 2022 and 2027. Health data is quite sensitive and has been the target of numerous cyberattacks. This work proposes a proof of proximity system utilising Bluetooth low energy devices for proof of proximity as a means of ensuring only valid patient data is sent to healthcare providers and uses a proof of authority consensus protocol to validate patient data sent before adding it to an immutable ledger on a consortium blockchain.**

Keywords—remote patient monitoring, healthcare blockchain, proof of proximity, proof of authority, Bluetooth low energy, consortium blockchain.

I. INTRODUCTION

Telemedicine is a system for providing health care through remote technology-based platforms. (Razali et al., 2020) Telemedicine makes use of tools such as remote patient monitoring (Marquez et al., 2020). This involves the transfer of sensitive patient health information over a network, between a patient and their healthcare provider.

The global market for remote patient monitoring is expected to grow from $ 53.6 billion in 2022 to $ 175.2 billion by 2027. This growth is driven by factors such as the high cost of healthcare, an aging population, and the COVID-19 pandemic. (Condry et al., 2023). This expected growth is a reason to understand the challenges faced by the field and provide solutions.

The data on a remote patient monitoring can be subjected to a wide range of attacks, malicious code injections, RFID interference, distributed denial of service, man in the middle attacks, phishing, and others. (Ianculescu et al., 2020). It has been argued that given the sensitive nature of health data, regulators, hospitals, health workers, and patients all have a role to play in maintaining the security of health data sent over the internet to mitigate against data leakage and cyber-attacks. (Yuninda et al., 2022)

Based on a review of the features of a blockchain "distributivity, decentralization, immutability, security, programmability, and consensus mechanisms" (Maftei et al., 2023 p.1). It was proposed by Satoshi Nakamoto that:

"a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power." (2008, p.8)

This work proposes a blockchain system that can increase the security of a remote patient monitoring system, ensuring that healthcare providers receive only valid patient data from remote monitoring systems. The system will verify the data is coming from a medical device within the patient's vicinity, have this validated by a distributed network and stored in an immutable ledger.

II. PROBLEM STATEMENT

Patient data is sensitive information. There have been many attacks on healthcare data. (Qiu et al., 2022). In the context of remote patient monitoring there are additional risks faced: These include the potential for an attacker to intercept and edit patient data enroute to the healthcare provider or tampering with the data therefore propagating false patient data on the network. Such attacks would be noted as man in the middle attack and have been carried out against healthcare devices. (Das et al., 2022)

Patients have expressed surprise when they found out the documentation their clinicians included in their notes. This sometimes leads a patient to feel their clinicians are not honest with the data they include in their records. Such perceptions could undermine trust in the healthcare system, this was discussed by Fernandez et al. (2021). A system which stores patient data in an immutable ledger would provide greater trust.

III. BACKGROUND AND RELATED WORK

A. Exporation of key concepts

This subsection explains the key concepts used in this work.

1) Hash functions

A fundamental part of blockchain technology such as the bitcoin blockchain is a hash algorithm. This is a function like the SHA 256 or keccak 256 algorithm, these can take a string of variable length and convert them into a random output of fixed length which cannot be converted back into the original string. (Di Pierro, 2017) Transactions are grouped into blocks and a hash of the block is generated based on the content of the block. Figure shows how the addition of a period at the end of a paragraph can change the hash output to a completely different string of equal length.

2) Blockchain

A blockchain is formed by linking multiple blocks over time. The cryptographic link between blocks is formed based on the inclusion of the hash of the preceding block in the

blockchain. Over time if any change is to be made to an older block this would change the hash of that block, and the hash of every subsequent block would need to be recalculated. The energy needed to calculate these hashes makes the endeavor computationally expensive. (Sarmah, 2018). A nonce (number only used once) is a 32-bit unsigned integer which needs to be calculated and added to the block that allows the hash of the block to be a hash with a preceding number of zeros decided by the difficulty needed to allow creation of a new block every 10 minutes. (Óskarsdóttir and Mallett, 2021) An example of a hashed chain of cryptographically linked blocks is shown in Fig. 1.

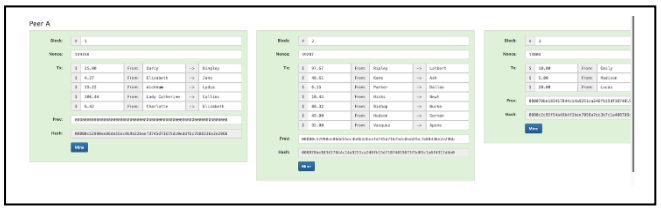

Fig. 1. A chain of cryptographically linked blocks.

3) Consensus Algorithms

a) Proof of work

Is a consensus mechanism in which validators complete to solve a mathematical challenge, the difficulty of which is adjusted based on the compute power of the validator network, and whenever a validator solves the challenge, they are allowed to add a new block to the ledger. Validators can leave and rejoin the network as they choose, and whenever a validator rejoins the network, they consider the longest ledger chain (the one with the most computational work behind it) valid. (Nakamoto, 2008). The challenge with this model is the significant computational resources needed to maintain the security of the network. This system is energy intensive, with a significant carbon footprint, estimated at about 22 metric tons of CO_2 per annum by Stoll et al. (2019). This was a consideration when the discussion for alternate consensus mechanisms was proposed. (King and Nadal, 2012)

b) Proof of stake

This consensus protocol requires validators to place a stake, the participant with the highest stake has the highest likelihood of being chosen to validate the next block and add it to the blockchain. The idea being that a participant with a higher stake has a higher interest in the credibility of the ledger. (Nair and Dorai, 2021). There is also an alternative staking model known as a delegated proof of stake. In a delegated proof of stake model, the network participants with a stake vote on delegates who can add the next block to the ledger, and not add the next block directly by themselves. If the delegates fail to validate a block, they will be reassigned. (Swathi B., et al., 2021).

c) Proof of authority

The validators in the network are chosen by a central party. Since the validators are known before their inclusion in the network, this system is permissioned. The network requires a majority of the network participants to agree to the validity of the transactions in a block before it can be added to the ledger. If the other participants find a validator is accepting fraudulent transactions as valid, they risk being taken off the network. (Maftei et al., 2023)

4) Smart contracts

Smart contracts were first described by Nick Szabo in the 1990s to be a set of instructions written with preset conditions, which executes automatically when the conditions are met, this was described by Zheng et al. (2020) This means that no trusted third party is needed for two entities to transact. Fig. 2 shows a template of solidity code that would take signed patient measurements and form a transaction.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract MedicalMeasurement {
    struct Transaction {
        uint256 medicalMeasurement;
        uint256 peripheralDeviceTimestamp;
        bytes peripheralDeviceSignature;
        uint256 centralDeviceTimestamp;
        bytes centralDeviceSignature;
    }

    mapping(address => Transaction[]) public transactions;

    function addTransaction(
        uint256 medicalMeasurement,
        uint256 peripheralDeviceTimestamp,
        bytes memory peripheralDeviceSignature,
        uint256 centralDeviceTimestamp,
        bytes memory centralDeviceSignature
    ) public {
        Transaction memory transaction = Transaction(
            medicalMeasurement,
            peripheralDeviceTimestamp,
            peripheralDeviceSignature,
            centralDeviceTimestamp,
            centralDeviceSignature
        );
        transactions[msg.sender].push(transaction);
    }
}
```

Fig. 2. A sample format of solidity code for a valid transaction.

5) Bluetooth low energy

Bluetooth low energy (BLE) is a protocol developed by the Bluetooth special interest group. This protocol runs on the 2.4GHz radio frequency band. It was developed for use in healthcare, fitness, industry, and other devices. It is important to note that while BLE was developed by the same group and runs on the same frequency band as classic Bluetooth, it is not the same protocol, and the two protocols are not compatible with each other. (Bluetooth SIG, 2023). BLE is supported natively by Linux, Android, macOS, windows, and most other widely used operating systems.

In BLE we can identify peripheral and central devices. Peripheral devices are typically sensors with power constraints, their role is often to send packages of data and then go into a sleep mode. Central devices are often more capable devices which collect the data from peripherals for analysis or transmission, a smartphone is a popular choice of central device. (Fürst et al., 2018).

An example would be the Dexcom one glucose monitoring device which is a sensor that measures patient's glucose levels, this data is then transmitted to their mobile device via BLE. The device range is within six meters and has a battery life of 3 months as described in the user guide. (Dexcom Inc., 2023)

B. Related work

The paper by Hölbl et al. (2018) the authors discuss the key concepts in blockchain such as blocks, nodes, and consensus mechanisms. The authors explain consensus

mechanisms and base on their review of literature argue why a private blockchain running smart contracts may be a desirable choice of blockchain solution for healthcare projects given the sensitive nature of health data and the ability of smart contracts to automate workflow. The authors gave reasons why proof of work, the most widely used consensus mechanism in healthcare blockchain projects is not optimal, citing its slower speed when compared to proof of stake or proof of authority consensus protocols.

A peer-to-peer network for location-based service. Their system includes participants serving as provers and verifiers connected over short range communication to verify each other's locations avoiding the privacy concerns associated with a centralized location service. The authors propose a proof of stake system in which each transaction is a proof of location claim which must be signed by a verifier within short range communication distance before being broadcast to the network. (Amoretti et al., 2018) These transactions are grouped into cryptographically linked blocks which cannot be changed retroactively.

As new technology becomes available researchers in the medical field often try to understand how this can be used to benefit patient care. Wang et al. proposed a parallel health system, which is a model of the health system and models patient and clinician behavior. (2018). It applies novel technology and models the output for comparison. The system was to run on a consortium blockchain as this system would allow for a broad variety of participants such as various hospitals, health bureaus, and healthcare communities. The authors argued that a consortium blockchain would provide greater integrity and security to the system.

Wu et al. (2020) discussed the benefits of their novel zero knowledge, proof of location architecture for location-based services. A zero-knowledge proof is a way of proving to a verifier a statement is true without revealing any information about the statement. Their proposal would prove presence at a location without revealing the location. This system was proposed in a bid to safeguard sensitive location data.

A delegated proof of proximity consensus model for sensors to prove their proximity to an event, for low power industrial internet of things devices was described (Ledwaba et al., 2020). In the proposal the nodes close to an event would compare their observations and vote on the legitimacy of the observation, without involving the wider network in validation. Their model uses a directed acyclic graph architecture in contrast to a linear block architecture.

Fields such as healthcare have made use of internet of things (IOT) devices. The authors Maftei et al. (2023) note how the features of blockchains decentralization, immutability, consensus mechanisms can benefit IOT devices. They compare three consensus mechanisms: proof of work, proof of stake and proof of authority, based on transaction latency, average block time, and average query time. The authors conclude that proof of stake and proof of authority are better for IOT devices.

IV. PROPOSED BLOCKCHAIN SOLUTION

This work proposes a system for each measurement sent by a remote patient monitoring device to show proof of proximity to a patient before a measurement is accepted as valid. Proof of proximity requests will include medical measurements such as blood pressure or blood glucose and the time when taken.

The medical devices will serve as the peripheral devices in the BLE system, with the patient's smartphone serving as the central device. Each monitoring device on the network will have its own private and public keys. At a predefined interval, the medical measurements, and the time at which the measurements are taken are signed with the device's public key and sent to the central device. If the devices are within BLE range, the signed measurement is received by the central device, this proves proximity. The receipt of the measurement is an event that triggers the smart contract, the central device stamps the time it received the measurement and signs this measurement with its own public key and broadcasts the double-signed measurement to the network. Each double-signed measurement is a transaction. A transaction therefore contains: a medical measurement, a timestamp of when the measurement was taken by the peripheral medical device, a digital signature of the peripheral device, the time the measurement was received by the central device, and the digital signature of the central device. Fig. 3 shows the transaction being completed before broadcasting.

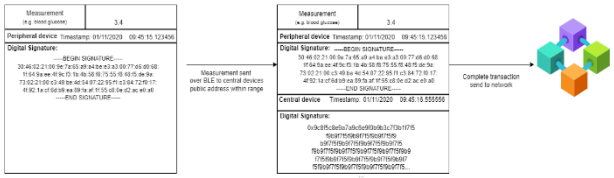

Fig. 3. A schema of details required for a valid transaction.

The transactions are sent over the internet to the validator network. If the validator reviews the transaction and it meets the criteria set in the consensus protocol it is added to a block. The transactions in each block are hashed to form the hash of the block. Each block contains the hash of the preceding block forming a blockchain. If a transaction does not meet the validity criteria it is deemed invalid and is not added to the new block.

The validators would run a proof of authority consensus model, with the patients' healthcare providers serving as validators. Use of a blockchain for storage of this data would allow each validator to maintain an identical copy of the ledger and ensures the data cannot be edited after the validation without a majority of the validators agreeing to such a change ensuring patient data is verified to be sent from their vicinity, at the stated time, and saved to an immutable ledger. (Shen et al., 2022). If a validator is noticed to be including invalid transactions when assigned to create a new block, this would lead to loss of reputation and a potential removal from the validator network.

V. EVALUATION

Key decisions made in this proposal include: 1) Choice of double-signed patient measurements. 2) The choice of Bluetooth low energy devices for proof of proximity. 3) The choice of a consensus.

A. Choice of double-signed patient measurements

Including a valid digital signature from the both the peripheral medical device and the patient's smartphone which can only be done over BLE will be a proof to the validators that the transaction is sent from the devices with the private

keys belonging to the central and peripheral device which are in the same location and not being propagated from a man in the middle attacker.

B. *Choice of Bluetooth low energy for proof of proximity*

The use of BLE technology was considered based on the short range required for data transmission. This would mean an attacker would potentially need to be within BLE range to attempt to send a fake measurement to the central device. The choice of BLE is also in contrast to the use of centralized location services such as GPS, which as Ahmad et al. Argue can be spoofed to give a wrong location (2019), but the use of BLE verifies proximity, without revealing location data.

C. *Choice of proof of authority consensus algorithm*

Based on the related work reviewed, it has been suggested that a system of low powered devices, such as the BLE devices discussed in this work would not have sufficient power for the computationally demanding proof of work calculations needed in a proof of work system and noted that this consensus protocol is also slower than the alternatives as argued by Hölbl et al. (2018).

D. *Choice of consortium blockchain*

The use of healthcare providers as validators provides accountability and transparency on who has validated the transactions. The validators being preselected reduces the chance of a Sybil attack where an attacker would try to create fake identities “Sybils” to try and gain control of the network. Platt and McBurney in their 2021 work titled “Sybil attacks on identity-augmented Proof-of-Stake” discussed how permissionless systems are vulnerable to such attacks and review how they could be carried out on a permissioned system. A healthcare blockchain built as a consortium blockchain provides the security of known participants in the healthcare space and the integrity and security of different participants needed to arrive at consensus. This is supported by the arguments of Wang et al. (2018).

VI. CONCLUSION

In this work we discussed the concept of remote patient monitoring and its projected growth. We discussed the challenges faced in handling patient data. An explanation of the blockchain concepts used for this work provided as well as a description of the Bluetooth low energy protocol and its applications.

A proposal has been made in this work on the combination of BLE devices and blockchain technology to provide proof of proximity and increase the security of remote patient monitoring systems with the data being validated by healthcare providers and stored in an immutable ledger working under a proof of authority consensus protocol. The key decisions made in this proposal were then evaluated.

References

[1] Razali, R., Jamil, N., 2020. A Quick Review of Security Issues in Telemedicine. *In: 2020 8th International Conference on Information Technology and Multimedia (ICIMU).* 24-26 Aug. 2020. Selangor, Malaysia, 2020, pp. 162-165, doi: 10.1109/ICIMU49871.2020.9243549.

[2] Márquez, G., Astudillo, H., Taramasco, C., "Security in Telehealth Systems from a Software Engineering Viewpoint: A Systematic Mapping Study," in IEEE Access, vol. 8, pp. 10933-10950, 2020, doi: 10.1109/ACCESS.2020.2964988.

[3] Condry, M., Quan X., "Remote Patient Monitoring Technologies and Markets," in IEEE Engineering Management Review, vol. 51, no. 3, pp. 59-64, 1 third quarter, Sept. 2023, doi: 10.1109/EMR.2023.3285688.

[4] Ianculescu, M.,Coardoș, D., Bica, O.,Vevera, V., "Security and Privacy Risks for Remote Healthcare Monitoring Systems," 2020 International Conference on e-Health and Bioengineering (EHB), Iasi, Romania, 2020, pp. 1-4, doi:10.1109/EHB50910.2020.9280103.

[5] Yuninda, S., Aga Pasma, S., Mantoro, T., "Patient Data Security in Telemedicine Services from Data Misuse in Health Practice," 2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED), Sukabumi, Indonesia, 2022, pp. 1-4, doi: 10.1109/ICCED56140.2022.10010685.

[6] Maftei, A., Lavric, A., Petrariu, A., Popa, V., "Blockchain for Internet of Things: A Consensus Mechanism Analysis," 2023 13th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, Romania, 2023, pp. 1-5, doi: 10.1109/ATEE58038.2023.10108211.

[7] Nakamoto S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Available from bitcoin.org/bitcoin.pdf [Accessed 12 November 2023].

[8] Qiu, H., Qiu, M., Liu M., Memmi, G., "Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 9, pp. 2499-2505, Sept. 2020, doi: 10.1109/JBHI.2020.2973467.

[9] Das, K., Basu, R., Karmakar, R., "Man-In-The-Middle Attack Detection Using Ensemble Learning," 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2022, pp. 1-6, doi: 10.1109/ICCCNT54827.2022.9984365.

[10] Fernández, L., Fossa, A., Dong, Z., Delbanco, T., Elmore, J., Fitzgerald, P., Harcourt, P., Perez, J., Walker, J., DesRoches, C., 2021. Words Matter: What Do Patients Find Judgmental or Offensive in Outpatient Notes? *J GEN INTERN MED* 36, 2571–2578 (2021). https://doi.org/10.1007/s11606-020-06432-7

[11] Di Pierro, M., "What Is the Blockchain? " In: Computing in Science & Engineering, vol. 19, no. 5, pp. 92-95, 2017, doi: 10.1109/MCSE.2017.3421554.

[12] Sarmah, s., 2018. Understanding Blockchain Technology. Computer Science and Engineering, Volume 8. 23-29. 10.5923/j.computer.20180802.02.

[13] Óskarsdóttir, M., Mallett, J., Strangely mined bitcoins: Empirical analysis of anomalies in the bitcoin blockchain transaction network. PLoS One. 2021 Sep 30;16(9): e0258001. doi: 10.1371/journal.pone.0258001. PMID: 34591921; PMCID: PMC8483420.

[14] Brownworth, A., 2016. Blockchain demo. Avalilable at: https://www.andersbrownworth.com/blockchain/tokens [Accessed 12 November 2023]

[15] Stoll, C., Klaaßen, L., Gallersdörfer, U., 2019. The Carbon Footprint of Bitcoin, in: Joule, Volume 3, Issue 7, 2019, Pages 1647-1661, ISSN 2542-4351,https://doi.org/10.1016/j.joule.2019.05.012.

[16] King, S., Nadal, S., 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Available from: King, S. and Nadal, S. (2012) Ppcoin Peer-to-Peer Crypto-Currency with Proof-of-Stake. Self-Published Paper, 19. - References - Scientific Research Publishing (scirp.org) [Accessed 12 November 2023].

[17] Nair, P., Dorai, R., 2021. Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain. In: Conference: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) 279-283. 10.1109/ICICV50876.2021.9388487.

[18] Swathi, B., Meghana M., Lokamathe, P., 2021. An Analysis on Blockchain Consensus Protocols for Fault Tolerance, In: 2nd International Conference for Emerging Technology (INCET), Belagavi, India, 2021, pp. 1-4, doi: 10.1109/INCET51464.2021.9456310.

[19] Zheng, Z., Xie, S., Dai, H., Chen, W., Chen, X., Weng, J., Imran, M., 2020. An overview on smart contracts: Challenges, advances, and platforms, In: Future Generation Computer Systems, Volume 105, Pages 475-491, ISSN 0167-739X, https://doi.org/10.1016/j.future.2019.12.019.

[20] Bluetooth special interest group, 2023. The Bluetooth® Low Energy Primer Document Version: 1.1.0 Last updated: 17th January 2023.

[21] Fürst, J., Chen, K., Kim, H., Bonnet, P., 2018. "Evaluating Bluetooth Low Energy for IoT," In: IEEE Workshop on Benchmarking Cyber-Physical Networks and Systems (CPSBench), Porto, Portugal, 2018, pp. 1-6, doi: 10.1109/CPSBench.2018.00007.

[22] Dexcom Inc., 2023. Dexcom One user guide. AW00096-07 Rev 004 MT00096-07 Rev Date: 2023/06.

[23] Marko, H., Marko K., Aida, K., Zlatolas, N., 2018. A Systematic Review of the Use of Blockchain in Healthcare. In: Symmetry, doi:10. 470. 10.3390/sym10100470.

[24] Amoretti, M., Brambilla, G., Medioli, F., Zanichelli, F., 2018. Blockchain-Based Proof of Location, In: IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 2018, pp. 146-153, doi: 10.1109/QRS-C.2018.00038.

[25] Wang, S., Wang, J., Xiao, W., Qiu, H., Yuan, Y., Ouyang, L., Guo, Y., Wang, F., 2018. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach, in: IEEE Transactions on Computational Social Systems, vol. 5, no. 4, pp. 942-950, Dec. 2018, doi: 10.1109/TCSS.2018.2865526.

[26] Wu, W., Liu, E., Gong, X., Wang, R., "Blockchain Based Zero-Knowledge Proof of Location in IoT," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-7, doi: 10.1109/ICC40277.2020.9149366.

[27] Ledwaba, L., Hancke, G., Mitrokotsa, A., Isaac, S., 2020. A Delegated Proof of Proximity Scheme for Industrial Internet of Things Consensus, In: IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, Singapore, 2020, pp. 4441-4446, doi: 10.1109/IECON43393.2020.9254661.

[28] Shen, P., Li S., Huang, M., Gao, H., Li, L., Li, J., Lei H., 2022. A Survey on Safety Regulation Technology of Blockchain Application and Blockchain Ecology, In: IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 2022, pp. 494-499, doi: 10.1109/Blockchain55522.2022.00076.

[29] Ahmad, M., Farid, M., Ahmed, S., Saeed, K., Asharf, M., Akhtar, U., 2019. Impact and Detection of GPS Spoofing and Countermeasures against Spoofing, In: 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 2019, pp. 1-8, doi: 10.1109/ICOMET.2019.8673518.

[30] Platt M, McBurney P. Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance. *Algorithms*. 2023; 16(1):34. https://doi.org/10.3390/a16010034