BMC Digital Health

RESEARCH

Open Access

Technical sandbox for a Global Patient co-Owned Cloud (GPOC)

Joe Davids[1], Mohamed ElSharkawy[1], Hutan Ashrafian[1], Eric Herlenius[2,3] and Niklas Lidströmer[2,3*]

Abstract

Background The use of Cloud-based storage personal health records has increased globally. The GPOC series introduces the concept of a Global Patient co-Owned Cloud (GPOC) of personal health records. Technical sandboxes allow the capability to simulate different scientific concepts before making them production ready. None exist for the medical fields and cloud-based research.

Methods We constructed and tested the sandbox using open-source infrastructures (Ubuntu, Alpine Linux, and Colaboratory) and demonstrated it on a cloud platform. Data preprocessing utilised standard and in-house libraries. The Mina protocol, implementing zero-knowledge proofs, ensured secure blockchain operations, while the Ethereum smart contract protocol within Hyperledger Besu supported enterprise-grade sandbox development.

Results Here, we present the GPOC series' technical sandbox. This is to facilitate future online research and testing of the concept and its security, encryption, movability, research potential, risks and structure. It has several protocols for homomorphic encryption, decentralisation, transfers, and file management.

The sandbox is openly available online and tests authorisation, transmission, access control, and integrity live. It invites all committed parties to test and improve the platform. Individual patients, clinics, organisations and regulators are invited to test and develop the concept.

The sandbox displays co-ownership of personal health records. Here it is trisected between patients, clinics and clinicians. Patients can actively participate in research and control their health data. The challenges include ensuring that a unified underlying protocol is maintained for cross-border delivery of care based on data management regulations.

Conclusions The GPOC concept, as demonstrated by the GPOC Sandbox, represents an advancement in healthcare technology. By promoting patient co-ownership and utilising advanced technologies like blockchain and homomorphic encryption, the GPOC initiative enhances individual control over health data and facilitates collaborative medical research globally. The justification for this research lies in its potential to improve evidence-based medicine and AI dissemination. The significance of the GPOC initiative extends to various aspects of healthcare, patient co-ownership of health data, promoting access to resources and healthcare democratisation. The implications include better global

*Correspondence:
Niklas Lidströmer
niklas.lidstromer@ki.se
Full list of author information is available at the end of the article

health outcomes through continued development and collaboration, ensuring the successful adoption of the GPOC Sandbox and advancing innovation in digital health.

Keywords Global patient co-owned cloud, GPOC, Personal health records, PHRs, Technical sandbox, Cloud-based health, Blockchains, Artificial intelligence in medicine, Cloud security

Background

Documentation in healthcare around the world is fragmented. The will and voice of patients are absent. They lack ownership and control of their health data. Previous work has shown the need for interoperability, but the focus had been on centralised architectures [1, 2]. The structure remains centralised and security breakages have caused great harm. Simultaneously, new technologies have matured, enabling more secure solutions for globally distributed health care platforms. Blockchain-based Personal Health Records (PHR, ISO/TR 14292:2012) have emerged as a predominant solution in the healthcare landscape, offering enhanced security and patient control [3].

Here, the idea of a Global Patient co-Owned Cloud (GPOC) encompasses a globally distributed and securely blockchain protected and patient co-owned platform of PHRs.

This is presented in the GPOC-series [4–7]. Its systematic review and meta-analysis expose the core facets of a GPOC [4]. The GPOC Survey shows a global consensus for its necessity [5]. A summit echoes this [6].An additional review and interview series explored the ethics and policies relevant to a GPOC [7]. However, the entire scientific focus of the series is to eventually deliver a functional online platform.

Here, we demonstrate the technical GPOC Sandbox. It is based on the series' respective scientific methods and conclusions on all aspects of an ideal solution given the current technical possibilities. The gathered insights range from the optimal security, privacy, blockchain, platform architecture and encryption types to regulatory adaptations, e.g., GPDR-compliance, ethical considerations and feedback from key option leaders from all UN member states and 18 of the largest international health organisations. Our meta-analysis gave insights on cross-border data transfers and the GPOC ethics article on international data protection regulations.

The purpose is to allow all interested parties to explore and contribute to this project. This is because the concept requires a global effort. The Sandbox contains a platform of several protocols. The Sandbox's technical design is based on insights from the GPOC Series. The structure is modular and explores several new technologies. It is consensus-based and patient-centric. Co-ownership is its core.

The Sandbox investigates biometrical authorisation and hashing protocols [8, 9]. It investigates patients' management and movability of PHRs. Furthermore, it presents distributed ledger infrastructure. This permits global healthcare communication [10, 11]. The challenges for a GPOC include ensuring a unified underlying protocol is maintained for cross-border delivery of care based on data management regulations. This currently does not exist, and it is what the GPOC seeks to address. Open-source operating systems visualise the sandbox. It works with various systems without requiring any particular adaptations. Hence, it is an agnostic platform.

Technical sandboxes in domains outside healthcare, such as software development and finance, provide isolated environments for testing new code and innovative products, respectively. These sandboxes facilitate innovation while ensuring compliance and security before broader implementation. Similarly, the GPOC Sandbox aims to test and validate the integration, security, and functionality of a co-owned global cloud for personal health records. After launch the sandbox will provide performance metrics and testing benchmarks to validate security, efficiency, and usability.

The GPOC Sandbox explores several concepts, including the integration of Systematised Nomenclature of Medicine (SNOMED) and the International Classification of Diseases (ICD-11). This is done to ease communications and medical research [12]. These standardised terminologies ensure consistent, precise, and interoperable data exchange across different healthcare systems, facilitating accurate diagnosis, treatment, and global health analytics [12, 13].

Here, we will present the GPOC Sandbox's technical components and implications. The results elaborate on the sandbox's twelve modules, its blockchain technologies, and its accessibility. The discussion explores the role of blockchain in the GPOC framework, alongside decentralisation, security considerations, and future developments. The methods outline the construction process of the sandbox, highlighting the integration of blockchain protocols and data availability. Finally, we conclude the possible global impact and that the ongoing and future development of the GPOC concept will require international partnerships.

Methods

We used open-source tools to create the GPOC Sandbox [14]. The goal was to incorporate the conclusions from the GPOC Series. We use an open-source cloud service to demonstrate the platform. Data preprocessing was dependent on the data-type to be processed, which included text data, numerical, tabular data, imaging data etc. For all forms of data standard pre-processing libraries for natural language processing and machine learning were utilised, but we also utilise in-house and various globally accessible libraries to pre-process the data. The challenge for some countries is firewall restricting access to some of these libraries and a good reason why a sandbox is necessary. It is also desirable because it allows a standardised and agreed protocol and libraries to be assembled and assessable to all interested developers.

Mina protocol

The Mina protocol was used as the underlying smart contract blockchain protocol. Thus, it implements zero knowledge proof through succinct non interactive arguments or knowledge (ZK-Snarks). The aim is to prove information without additional information leakage [15, 16].

Mina boasts a 22 KB blockchain size compared to more than 250 GB size for other blockchains [16]. These protocols may be optimal for a GPOC. Zero knowledge proof implementation enables security and sustainability [17]. It has a lightweight carbon footprint. The described technology stack may have two sections. One frontend working on-chain and one backend off-chain allowing verified data management on an additional private blockchain network.

Figure 1 illustrates one approach. Ganache, a local blockchain development tool to tests smart contracts. The implementation of the smart contract Mina implementation is achieved with TypeScript, in contrast to Solidity for Ethereum. Currently, it is in development and available in a public blockchain format. However, it has the potential to be developed into a permissioned use case for GPOC [16].

Illustration of an example use of Mina for on-chain data processing, employing zero-knowledge proofs. The figure shows step 1 (left) with the frontend zero-knowledge application and step 2 (right) with the offchain blockchain application. A verification proof is stored locally on the private blockchain for network participants, including clinicians, patients, and their families. The queried data undergo conversion into a homomorphic encrypted form, are processed through a prover function, and are verified using ZK-Snarks (zero-knowledge-succinct non-interactive argument of knowledge). When queried by a public network participant, such as a company or researcher, and with owner permission, the data query's proof is verified by a verifier function with a cryptographic key stored on-chain. The state of the blockchain during interaction can be stored off-chain to expedite subsequent queries. The off-chain stack can also be accessed offline [16]. The Mina protocol was selected and is sufficient as it offers an environmentally friendly alternative to traditional blockchain architectures falling in line with the UN sustainable development goals and carries a smaller data storage footprint. The image is free

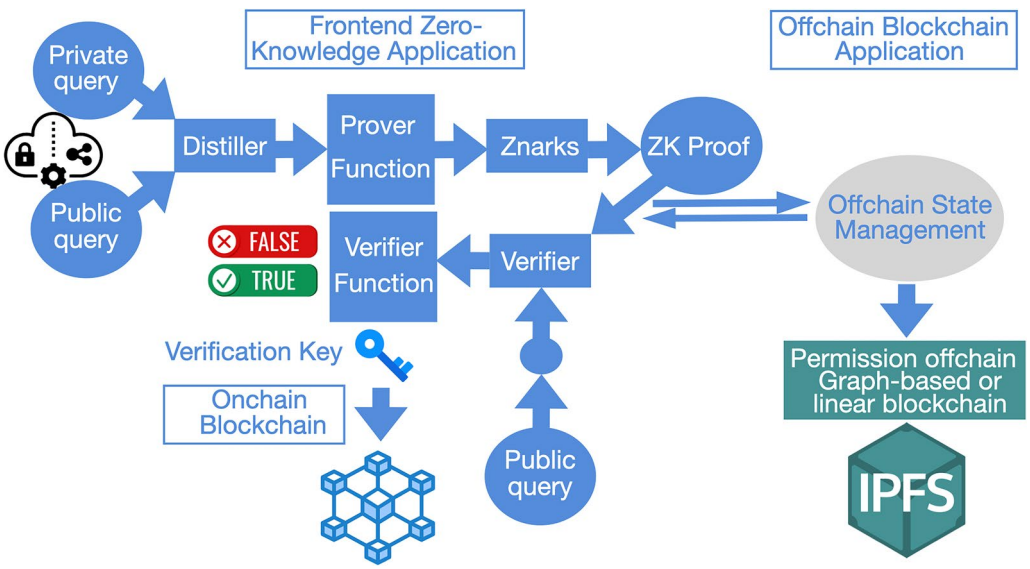

Fig. 1 Example technology stack for gpoc

to use and was created using Keynote 11 and Adobe Photoshop 2021 for the study by the last author.

Ethereum and hyperledger protocol

We employed the Ethereum smart contract protocol, implemented using Solidity within an individual permissioned use-case named Hyperledger Besu [18]. This configuration facilitates enterprise-grade platforms specifically tailored for sandbox development. Notably, Hyperledger Besu provides flexibility in supporting various networking protocols, liberating sandbox users from infrastructure limitations. This ensures a familiar working environment, enabling users to create their relevant GPOC.

Data availability

All the data and code generated in this study are provided in the Supplementary Information. Source data are provided with this paper. There are two repositories associated with this study:

1) The generated code and source data are available in the GPOC Sandbox, DOI: 10.5281/zenodo.10547507
2) Supplemental materials and UX/UI wireframes are available in the article repository on Figshare, DOI: 10.6084/m9.figshare.c.7067762

Results

The GPOC Sandbox comprises twelve modules. Its backend design emphasises portability and module scalability, leveraging blockchain technology. Users have the flexibility to choose and research the type of GPOC they wish to create. The GPOC Sandbox is openly available on a repository on Zenodo, https://doi.org/10.5281/zenodo.10547507.

The roadmap for constructing the sandbox, outlining the flow of steps, research gaps, limitations, and assumptions, is presented in the GPOC Series, summarised in Fig. 2. It also illustrates the sandbox architecture. The GPOC Sandbox will be officially launched upon the publication of this research article. Hence, future research will be able to report how it has been utilized.

The technical requirements of decentralised blockchains, clouds, adaptable UX/UI and homomorphic encryption have been used [8].

Blockchain technologies for the GPOC sandbox

Blockchain solutions, particularly those emphasising zero-knowledge proof and decentralisation, have been strategically chosen for the GPOC Sandbox. With its emphasis on patient co-ownership and secure global healthcare communication, the GPOC concept demands robust and trust-less transactions facilitated by blockchain technology. The unique requirements of GPOC, such as patient co-ownership and participation in global

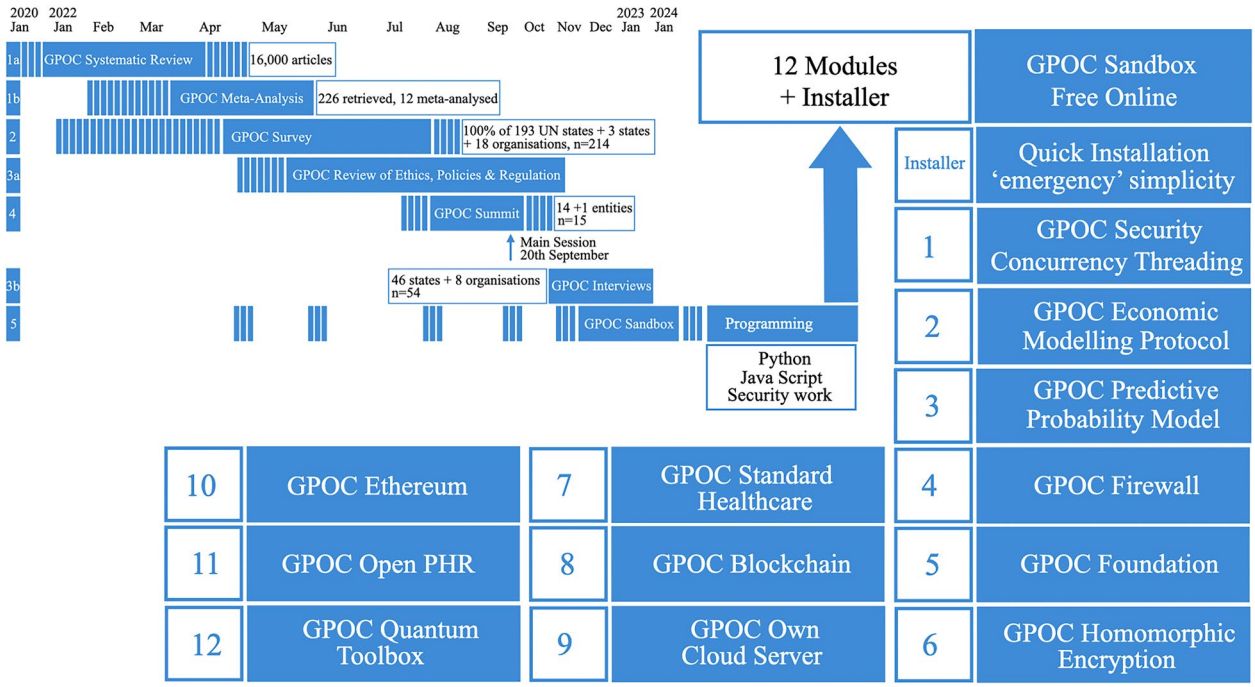

Fig. 2 Overview of the GPOC series and roadmap to the GPOC sandbox and its architecture

medical research, have directly influenced the technical design of the sandbox, aligning the chosen blockchain technologies with the GPOC vision of democratising healthcare.

Scalability and robustness

The GPOC Sandbox incorporates Blockchain-based Zero-Knowledge Proof (BZKP), aimed at achieving scalability and robustness in protecting sensitive PHR data. The implementation strives to align with the patient-centric goals of GPOC, facilitating secure and efficient healthcare data management.

Data storage reduction

Through the use of BZKP, the GPOC framework anticipates a reduction in data storage requirements, addressing challenges commonly associated with blockchain technology in healthcare applications. This approach supports the sandbox's goal of enhancing data security and accessibility.

Table 1 shows several blockchains relevant to GPOC. Moreover, the Internet of Things (IoT) increases the number of PHR sources. These are often owned by patients. Thus, patients become co-contributors to their own PHRs.

Blockchains that may be relevant to GPOC. Such healthcare networks can share and procure sensitive patient data. It can be exchanged between laboratories, clinics, hospitals, and caregivers. Applications of these decentralised blockchains can be used to accurately identify mistakes. Hence, we provide an overview of common blockchains relevant to healthcare and their potential use for GPOC. Blockchains may be the cusp of a new healthcare era [19–30].

Table 1 Blockchain technologies relevant to Global Patient Co-Owned Cloud (GPOC) in healthcare: overview and potential applications

Name	*Algorithm*	*Programmable*	*Relevance*
Bitcoin	Proof of work	Yes (scripts)	The most well-known blockchain, which token has the highest crypto value. Energy inefficient at present for a GPOC
Litecoin	Proof of work	Yes (scripts)	An open-source peer to peer cryptocurrency. May be inefficient for GPOC
Primecoin	Proof of work	Yes	Long Cunningham chains of prime numbers is the centre of the blockchain. May be inefficient for a GPOC
Ethereum	Proof of work/ Migrated to Proof of Stake	Yes	After Bitcoin, the most valuable token. Recently attracted attention to its grand merge where it tried to switch to proof of stake, for energy consumption reasons. Programmable widely supported smart contracts
Peercoin	Proof of stake/Proof of Work	Yes (scripts)	An early pioneering blockchain that is presented as being sustainable. May be slower than other networks with a 10 min block-time. May have applications for the GPOC
Bitcoin Cash	Proof of work	Yes	Derived from Bitcoin. At present may be too energy inefficient for GPOC
Cardano	Proof of stake	Yes	First to be founded on peer-reviewed research and evidence-based methods that is currently integrating smart contract technology. May have applications for GPOC
Tezos	Proof of stake	Yes	User-governed & user-centric movement
Bitcoin SV	Proof of work	Yes (scripts)	A second-generation spin-off from Bitcoin
Hedera Hashgraph	Asynchronous Byzantine Fault-Tolerant (aBFT) consensus	Yes	Does not use a classic blockchain, but a directed acyclic graph. It may apply to a GPOC system as it is privacy-enabled and GDPR compliant
Zcash	Zero Knowledge proof	Yes	Zero-knowledge proofs for privacy protection but a digital currency. It is like the Mina protocol, using ZK-Snarks with a 75-s block time
Monero	Proof of work	No	Anonymous, untraceable, undecipherable. It has a two-minute block time. However, may be energy inefficient for a GPOC
Bitcoin Gold	Proof of work	Yes (scripts)	Mined on common GPUs instead of specialty ASICs. Energy inefficient for GPOC at present
IOTA	Proof of work, TaPoW	No	Designed for Internet of Things (IoT). May be applicable for the GPOC due to its DAG-based form
Solana	Proof of Stake	Yes, with Rust	Scalable operates on Berkeley Packet Filter with a fast 400 ms block time. May have applications for a GPOC

Blockchains that may be relevant to GPOC. Such healthcare networks can share and procure sensitive patient data. It can be exchanged between laboratories, clinics, hospitals, and caregivers. Applications of these decentralised blockchains can be used to accurately identify mistakes. Hence, we provide an overview of common blockchains relevant to healthcare and their potential use for GPOC. Blockchains may be the cusp of a new healthcare era [38–50].

The GPOC Sandbox is downloadable with minimal installation requirements. Illustrative examples are included. However, users have the freedom to adapt and research their GPOC version and user interface (UI/UX). Moreover, a collection of ergonomic and minimalist UX/UI wireframes for GPOC is available on the article repository on Figshare, https://doi.org/10.6084/m9.figshare.c.7067762. A forthcoming article will deliver user feedback on the overall usability.

In 2020 the structure of the GPOC Series' five parts was planned. The initial GPOC systematic review and meta-analysis was recently published [1]. The following GPOC Survey received answers from 100% of the 193 UN member states and three other states and 18 organisations participating [2]. Hereafter, the review and inquiries on ethics, policies and regulations were assembled [3]. Finally, we organised a Delphi-style GPOC Summit [6]. All these four publications in the GPOC Series emanated in the eventual GPOC Sandbox construction. Thus, it is based on all the insights from the entire GPOC Series. This roadmap is illustrated in the upper left quadrant of the figure. At the centre the start of the programming of the sandbox is visible. It results in a tailored structure of 12 modules and quick installation module, that is adapted for 'emergency' study situations in the field. The modules include security features such as firewall, blockchains and homomorphic encryption. It also provides economic and predictive models for public health usage. Finally, it is equipped with modules for standardised evidence based healthcare, open PHR and a Quantum Toolbox for research, international development and dissemination of AI in medicine. In the event of the creation of GPOC Foundation for global collaboration a dedicated module for this purpose has been added. The image is free to use and was created using Keynote 11 and Adobe Photoshop 2021 for the study by the last author. For details and Source Data, see the respective publications.

The study resulted in displaying a range of applications of blockchains relevant for the GPOC, which is illustrated in Fig. 3.

Illustration of some applications of blockchains relevant for the GPOC technical solution. Note that tokens have both virtual and real-world values, i.e., there are also disadvantages with blockchains, which are elaborated below. The image is free to use and was created using Keynote 11 and Adobe Photoshop 2021 for the study.

Homomorphic encryption

Fully Homomorphic Encryption (FHE) is currently the most relevant method to GPOC [40, 52–54]. It supports the use of analytics on encrypted data [8]. This technology ensures that sensitive patient information remains secure while allowing for meaningful analysis and insights to be derived, thus supporting the sandbox's objectives of secure data management and patient co-ownership.

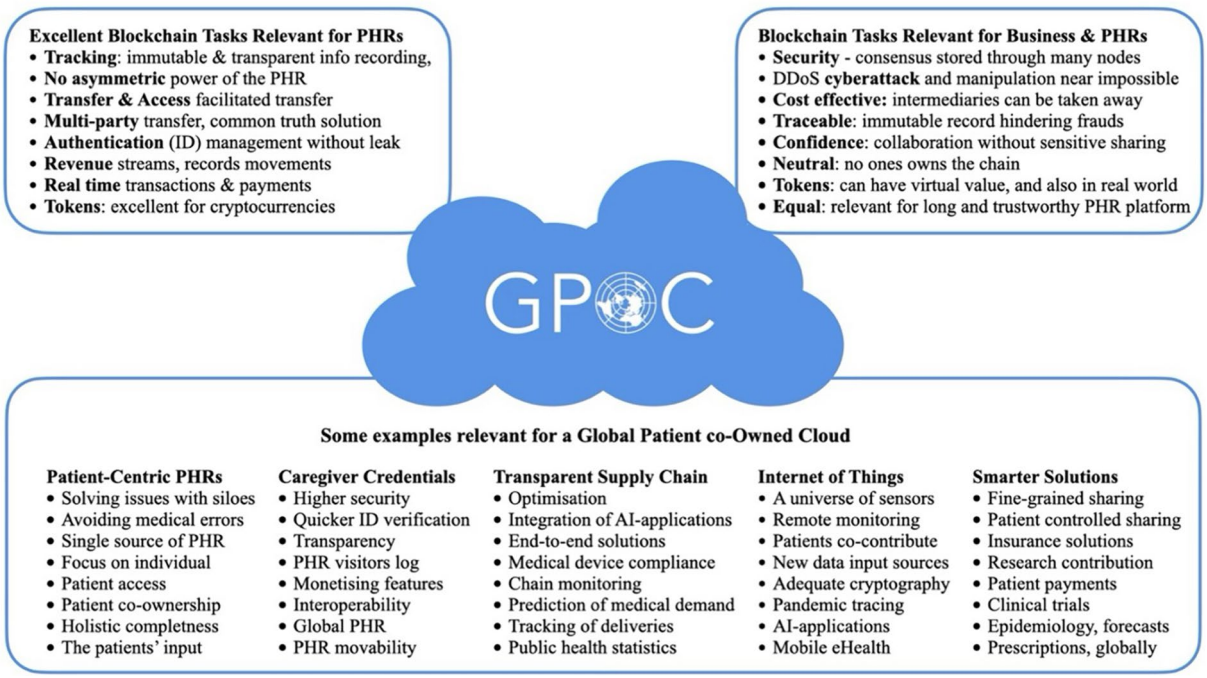

Fig. 3 Applications of blockchains for GPOC

The study resulted in relevant GPOC features that are displayed in Fig. 4.

Illustration of the science of optimal UX/UI, relevant for a global platform such as GPOC. The central mission is to make it as accessible as possible and prevent discrimination against those with a disability, etc. It should present a solution that is simple, inclusive, adaptive, efficient, and truly global. The image is free to use and was created using Keynote 11 and Adobe Photoshop 2021 for the study by the last author. A suggested collection of ergonomic and minimalist UX/UI wireframes for GPOC, also free to use and created for the study by the last author, is available on the article repository on Figshare, https://doi.org/10.6084/m9.figshare.c.7067762.

Discussion

Introduction

A global world with frequent travel requires a patient-centric and movable PHR. The GPOC concept suggested here can be further investigated in the Sandbox. The chosen solutions for the GPOC Sandbox are discussed below.

Blockchains in general

Blockchain technology serves as a decentralised and transparent ledger system that records transactions across a network of computers. Its widespread adoption extends beyond healthcare, finding utility in domains like finance, supply chain management, and voting systems. Blockchain's immutable and tamper-resistant nature ensures data integrity and trust in various applications, revolutionising processes through disintermediation and enhanced security measures.

Role of blockchain in GPOC framework

Blockchains play a crucial role in the GPOC framework by allowing the permanent recording of encrypted data, rendering access nearly impossible without the requisite encryption codes. Within a peer-to-peer network-driven system, users collaboratively solve complex cryptographic nonce-based hashes, creating fingerprints that serve to prove the authenticity of transactions. The trust-less nature of this interaction is key, as it certifies the origin of transactions without the need for a central party. This security is further reinforced by consensus algorithms operating on game theory, ensuring that the addition of blocks is a rigorous and secure process [31].

Decentralisation and security

A blockchain is a linear transaction ledger that is duplicated and distributed across an entire network of peer-to-peer (P2P) computers. Each user stores one ledger copy, and all user computers are nodes. Validation of the encrypted data creates durability and transparency, resulting in traceability from the genesis block.

Regulations may require keeping information no longer than necessary. Blockchain solutions for healthcare try to address this issue with off-chain interaction processing [32].

For healthcare, the decentralised and transparent blockchain technology is strategic for solving issues and providing complications. PHRs require both privacy protection and accessibility in the event of appropriate healthcare actions. This is accentuated in a GPOC.

Zero-knowledge proof and IoT model

Blockchain-based Zero-Knowledge Proof (BZKP) is an Internet-of-Things (IoT) model. It is patient-centric and aims to protect sensitive PHR data [15]. Its scalability, robustness and immutability are suitable to GPOC [15]. Blockchains accumulate large amounts of data and BZKP reduces storage.

PHR interoperability and blockchain-based solutions

As discussed earlier, the prominence of blockchain-based PHRs in healthcare reflects their widespread adoption. Their popularity is attributed to the heightened security and patient empowerment they afford, aligning seamlessly with the goals of GPOC. For instance,

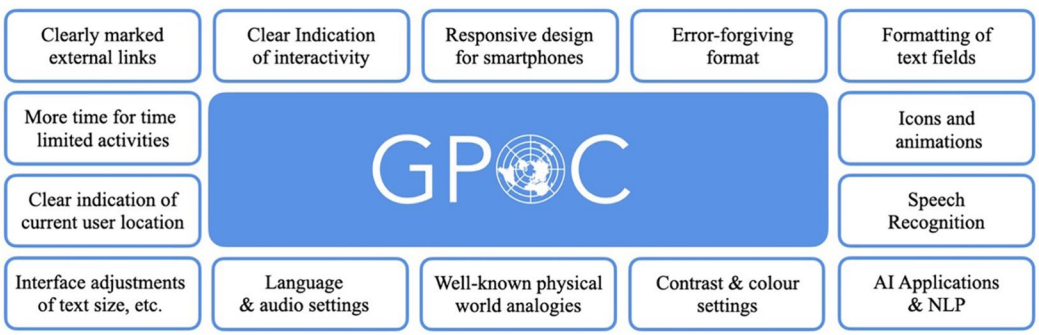

Fig. 4 Optimal UX/UI for GPOC

MyHealthData permits downloads from multiple institutions via mobile devices and a blockchain relay server. It is designed for PHR interoperability [33]. The recently published Blockchain-Based Deep Learning as-a-Service (BinDaaS) is a combination of blockchain and a deep-learning platform with inbuilt clinical predictions. This provides superior performance, accuracy, end-to-end latency and mining time compared to other models [34].

Outsourced PHR clouds and security features

For the usage of outsourced PHR clouds, key features of a secure health cloud have been presented in a case study of blockchain-assisted PHRs [35]. A hybrid-blockchain solution addresses some security issues with sharing. Analysis with the blockchain benchmark tool Hyperledger Calliper revealed high performance [36]. For GPOC Hyperledger Besu was used [18].

Most blockchain-based PHR solutions have focused on single chains. The latest leakage mitigations require multi-chains. Hence, the Relay-Chain as a Service (RaaS) and a cross-blockchain PHR solution may be suitable for patients visiting many hospitals [35]. This was deemed relevant to GPOC and can be further explored in the sandbox.

Moreover, the unique requirements of GPOC, such as patient participation in global medical research, have been considered in the technical design of the sandbox. The chosen blockchain technologies align with the GPOC vision of democratising healthcare and contributing to the dissemination of artificial intelligence within the medical domain.

Centralised vs decentralised clouds

In the GPOC framework, understanding the nuances of cloud infrastructure becomes pivotal. Clouds, whether decentralised with globally distributed storage or centralised under singular control, directly impact the co-ownership and security aspects of GPOC. As we navigate through the intricacies of PHR data encryption, a crucial facet in GPOC's commitment to secure health data management, we encounter challenges such as time consumption and escalating costs, particularly with an increasing number of access policy attributes. Recognising the need for enhanced performance, GPOC introduces Fine-Grained Access Control with User Revocation (FGUR). This not only addresses performance concerns but also aligns with GPOC's overarching goal of empowering patients in managing their health data. A strategic combination of Broadcast Ciphertext-Policy Attribute-Based Encryption (BCP-ABE) and attribute hierarchies of Comparison-Based Encryption (CBE) further reinforces the GPOC commitment to robust security measures [37].

Challenges with centralised clouds

Centralised clouds mean storage and transfer by trusted third parties (such as Amazon, Google, and Microsoft). Here there are weaknesses that can harm the data. Currently, most PHR solutions are centralised. However, the Diagonal Digital Signature Algorithm (DDSA) using Merkle Patricia Hash Trie (MPHT) algorithm is a PHR sharing solution with blockchain [38].

Decentralised blockchain solutions

In the context of centralised clouds, considerations align closely with GPOC. The challenges associated with centralised clouds directly impact GPOC's mission of co-ownership and secure health data management. The GPOC Sandbox addresses these challenges by adopting a decentralized approach, ensuring trustless transactions and empowering users in co-managing their health data securely.

A main issue with centralised clouds is the loss of privacy and security of sensitive PHRs [39]. Therefore, we argue that outsourcing solutions for PHRs have critical such issues [40].

Ethereum and smart contracts

To solve this issue, decentralised blockchains ensure trust-less transactions. Each network member possesses an identical copy of data in a distributed ledger; any alteration is rejected by the other users. For instance, Ethereum, a decentralised and open-source blockchain, incorporates smart contract functionality. Serving as the native cryptocurrency of the platform, Ethereum empowers the development of applications on its blockchain [31, 41, 42]. Hence, this is the chosen solution for the GPOC Sandbox.

Hyperledger for secure health data

Hyperledger, a platform for collaborative, permissioned private blockchains, aligns with GPOC's focus on secure and co-owned health data. Its support for emerging architecture design, including hybrid infrastructures that unify permissioned and public networks, underscores its suitability for GPOC [43].

Diverse blockchain ecosystems

Diverse ecosystems, like Directed Acyclic Graph (DAG)-based (e.g., Hedera Hashgraph, Holochain) and blockchain-like systems (e.g., Nano, IOTA, Obyte), demonstrate unique designs for efficiency and privacy [44–47].

Scalability and layer 2 protocols

Layer 2 protocols (e.g., Cellar, Loom, Ark, Cosmos, and Tesseract) facilitate scalability and privacy through state transfer channels [46]. In healthcare, GPOC should support state change propagation and reversibility [48, 49]. Proposals for scalability, sich as sharding and block-size modifications, contrast with the limitations of slow and expensive layer 1 networks [30]. Emerging healthcare chains, such as HealthChains, are also under consideration [48].

Future developments in blockchain for healthcare

Even though, blockchain implementation may be expensive, user costs may be lower and energy consumption may be higher. Moreover, lost key generation may be impossible, and storages may exceed hard disc capacities. The security issue with social engineering remains. However, there is software capable of relying on decentralised or token-based distributed ledgers with effective cryptographics. Recent solutions have been suggested, such as Healthfetch, an influence-based context-aware prefetch scheme in citizen-centred health storage clouds and a cloud-dew architecture based PHR framework [50, 51]. These were considered, but they were not relevant for GPOC's decentralised protocol.

Integration with global medical research

A GPOC should support global medical research on its valuable content. However, the co-owning patients should be able to opt-in for participation. Hence, a microflow of payments to patients needed to be modelled in the sandbox. Moreover, the possibility of contributing to global research and the dissemination of AI needs to be considered. Additionally, bias mitigation and the promotion of equal healthcare access are important. The development of AI for GPOC may lead to a global increase in Evidence-Based Medicine (EBM).

UX/UI design for patient-centric care

The most effective and ergonomic UX/UI is a science in itself [9]. Its adaptability to local or personal preferences is relevant in patient-centric care. Large swathes of the world may access PHRs via smartphones. It is pivotal to adapt the UX/UI for elderly or impaired individuals [10–12]. The UX/UI of GPOC should lead to an efficient workflow. In contrast, social media designers often wish to prolong logged in sessions and increase the advertising value. The PHR content is already valuable per se. Hence, there is less value in digital addiction.

Future developments may include large natural language processing, multi-chains, quantum AI and security for GPOC [55, 56].

In summary, every technical decision made in the development of the GPOC Sandbox has been intentionally aligned with the core principles of the GPOC concept. Thus, reinforcing its potential impact on global health and medical research.

Future work and partnerships

Partnerships with organisations such as the United Nations, International Committee for Red Cross, World Health Organisation and the World Economic Forum would allow us to build a more robust GPOC architecture for alpha and beta testing. Specifically, for PHR data management this will be in a form of an application incorporating the ratified protocol from the underlying unified consensus in current and future GPOC Summits. Ongoing multi-institutional research organisational partnerships will further enable us to develop the sandbox to cater for individual global patient data management. Additionally, we intend to build on top of the Mina protocol because of its environmentally friendly footprint.

Global collaborations include several universities, institutes and advanced technological frameworks. These include Karolinska Insitutet, MIT, Harvard, Oxford University and Imperial College London with its Global Health Innovation Network (GHIN). With these partners a detailed roadmap for implementing the GPOC sandbox, including timelines, milestones, and resource requirements will be included in the forthcoming article.

Limitations of sandbox implementation

The sandbox implementation is limited by the current lack of international collaboration on PHR design and data protection regulation. This limitation is further affected by various design preferences and constraints based on specific local regulations that may affect the use of a sandbox.

Conclusions

In conclusion, a global multi-institutional collaboration for a sandbox allows standardised PHR data access, streamlining the delivery of care for various patients across various locations. It is freely available online for all interested parties to research and explore. Here, we incorporate the GPOC concept. It encompasses a PHR co-ownership, trisected between the patient, clinicians and clinic. It is a distributed platform based on blockchains. We aimed to include the insights from the articles in the GPOC-series. Thus, the presented cloud-based ledger-like sandbox is the result. Its modules lie open for global research and adaptation. Hence, it contributes

to the democratisation of healthcare. It facilitates the research and spread of AI within medicine. The GPOC Sandbox may have an impact on global health.

Abbreviations

GPOC	Global Patient co-Owned Cloud
PHR	Personal Health Record
AI	Artificial Intelligence
GPDR	General Data Protection Regulation
UN	United Nations
SNOMED	Systematised Nomenclature of Medicine
ICD	International Classification of Diseases
ZK-Snarks	Zero-Knowledge-Succinct non-interactive argument of knowledge
BZKB	Blockchain-based Zero-Knowledge Proof
UI/UX	User Interface/User Experience
FHE	Fully Homomorphic Encryption
P2P	Peer-to-peer
IoT	Internet-of-Things
BinDaaS	Blockchain-Based Deep Learning as-a-Service
FGUR	Fine-Grained Access Control with User Revocation
BCP-ABE	Broadcast Ciphertext-Policy Attribute-Based Encryption
CBE	Comparison-Based Encryption
DDSA	Diagonal Digital Signature Algorithm
MPHT	Merkle Patricia Hash Trie
DAG	Directed Acyclic Graph
EBM	Evidence-Based Medicine

Supplementary Information

The online version contains supplementary material available at https://doi.org/10.1186/s44247-024-00128-2.

Supplementary Material 1.

Acknowledgements

We acknowledge the librarians at Karolinska Institutet Narcisa Hannerz and Anja Vikingson, Professor Sabine Koch at Karolinska Institutet, the librarians at Imperial College London, Michael Gainsford, Sarah Feehan, Jackie Kemp, the Swedish Foreign Ministry, Karin Berlin and the team at the Permanent Mission of Sweden to the United Nations in New York, John Mark Esplana and the team at International Committee of the Red Cross (ICRC), all the health ministries, health ministers, cabinet advisors, affiliated advisors, key opinion leaders and medical experts representing 100% of all 193 member states of the United Nations, and the two UN observer states and the de facto independent non-UN member state Taiwan. Additionally, all leaders and advisors representing 18 top-ranked international organisations, especially for technical discussions with International Committee of the Red Cross (ICRC).

Authors' contributions

Niklas Lidströmer (NL) provided conceptualising background research. Joe Davids (JD) created the coding and the online Sandbox with the assistance of Mohamed ElSharkawy (ME). All authors (NL, JD, ME), Hutan Ashrafian (HA), and Eric Herlenius (EH)) contributed to the GPOC Series, on which the sandbox is based. All authors contributed to the data interpretation and provided critical intellectual input throughout the study. All the authors conducted the statistical analyses and contributed to the interpretation of the results. NL wrote the manuscript with input from all the co-authors. NL made all the revisions to the manuscript with input from all the authors. NL acted as a senior and assembling author. All authors critically reviewed and approved the final version of the manuscript. JD and ME conceptualised Fig. 1, which was then made by NL. JD created the code repository for the GPOC Sandbox on Zenodo. NL made Figs. 1-4, Table 1, and the featured image. NL created the GPOC UX/UI wireframes and supplements in a repository on Figshare.

Funding

Open access funding provided by Karolinska Institute. This GPOC study series was supported by the Swedish Research Council (2019-01157 and 2023-02613) and the Swedish National Heart and Lung (20180505 and 2021 0579), the Stockholm County Council (2019–0400, 2019–0974 and FoUI-966 449) and Freemasons Children's House Foundation grants to Prof Eric Herlenius, including a scholarship to Dr Niklas Lidströmer.
Dr Joe Davids and Professor Hutan Ashrafian were supported by the Institute of Global Health Innovation (IGHI) Infrastructure.
The funding bodies had no role in the study's design, execution, or the decision to submit results.

Availability of data and requirements

The data generated in this study are provided in the supplementary information**.** Source data are provided with this paper. Source data and raw data generated in this study, have been deposited in the article repositories. All data are available on the repository without restrictions. The timeframe for response to requests is immediate. All data are free to use.
There are two repositories associated with this study:
1. The generated code and source data are available in the GPOC Sandbox, https://doi.org/10.5281/zenodo.10547507
2. Supplemental materials and UX/UI wireframes are available in the article repository on Figshare, https://doi.org/10.6084/m9.figshare.c.7067762

Declarations

Ethics approval and consent to participate

Ethical approval for the GPOC Series was obtained from the Imperial College London University Research Ethics Committee. Prior to distribution, all participants provided informed consent in accordance with the guidelines outlined in the Nature Portfolio participant release form. The declaration of written consent is provided in (S1).

Consent for publication

All participants have consented in writing to appear and be quoted in this publication. Individual who are showing their human faces in the featured image consented in writing, as shown in the Consent to Publish declaration & Featured Image Licence Information related article file.

Competing interests

The authors declare no competing interests.

Author details

[1]Institute of Global Health Innovation and the Hamlyn Centre for Robotic Surgery, Imperial College London, London, UK. [2]Department of Women's and Children's Health, Karolinska Institutet, CMM L8, Stockholm 17176, Sweden. [3]Astrid Lindgren Children´s Hospital, Karolinska University Hospital, Stockholm 171 64, Sweden.

Received: 11 February 2024 Accepted: 17 July 2024
Published online: 03 October 2024

References

1. Kiourtis, Athanasios, et al. "Electronic health records at People's hands across Europe: The InteropEHRate protocols." pHealth 2022. IOS Press, 2022. 145–150. https://doi.org/10.3233/SHTI220973.
2. Honka A, et al. Rethinking health: ICT-enabled services to empower people to manage their health. IEEE Rev Biomed Eng. 2011;4:119–39. https://doi.org/10.1109/RBME.2011.2174217.
3. Zhang P, Walker MA, White J, Schmidt DC. A blockchain-based approach to health information exchange networks. In: Proceedings of the 2018 IEEE Intenational conference on blockchain (Blockchain). 2018. p. 204–10.
4. Lidströmer N, et al. Systematic review and meta-analysis for a Global Patient co-Owned Cloud (GPOC). Nat Commun. 2024;15:2186. https://doi.org/10.1038/s41467-024-46503-5.
5. Lidströmer N et al, Necessity of a Global Patient co-Owned Cloud (GPOC). Nat Commun. https://doi.org/10.21203/rs.3.rs-3004727/v1
6. Lidströmer N et al, A Summit on a Global Patient co-Owned Cloud (GPOC). BMC Dig Health. https://doi.org/10.1186/s44247-024-00112-w.
7. Lidströmer N et al, Review of the ethics, policies and regulations of a Global Patient co-Owned Cloud (GPOC). https://doi.org/10.21203/rs.3.rs-3353005/v1

8. Kocabas O, Soyata T. Towards privacy-preserving medical cloud computing using homomorphic encryption. 2015. p. 213–46. https://doi.org/10.4018/978-1-5225-9863-3.ch005.
9. Nikam SS, Kshirsagar JP. Implementation of secure sharing of PHR's with IoMT cloud. Int J Recent Technol Eng. 2019;8(3):599–602. https://doi.org/10.35940/ijrte.B2192.098319.
10. Fujita KOK, Takemura T, Kuroda T. The improvement of the electronic health record user experience by screen design principles. J Med Syst. 2019;44(1):21. https://doi.org/10.1007/s10916-019-1505-0.
11. Leeming GTS, Ainsworth J. Designing a solution to manage electronic consent for children. Stud Health Technol Inform. 2020;2020(270):1103–7. https://doi.org/10.3233/SHTI200333.
12. Chang E, Mostafa J. The use of SNOMED CT, 2013–2020: a literature review. J Am Med Inform Assoc. 2021;28(9):2017–26. https://doi.org/10.1093/jamia/ocab084.
13. Lete SA, Cavero C, Lustrek M, Kyriazis D, Kiourtis A, Mantas J, Montandon L. Interoperability Techniques in CrowdHEALTH project: The Terminology Service. Acta Inform Med. 2019;27(5):355–61. https://doi.org/10.5455/aim.2019.27.355-361.
14. Get started with Docker. Docker Inc. Available at: https://docs.docker.com/get-started/. Accessed on 10th Feb 2024.
15. Al-Aswad H, El-Medany WM, Balakrishna C, Ababneh N, Curran K. BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. Arab J Basic Appl Sci. 2021;28(1):154–71. https://doi.org/10.1080/25765299.2020.1870812.
16. Bonneau J, Meckler I, Rao V, Shapiro E. Mina: decentralized cryptocurrency at scale. New York Univ. O (1) Labs, New York, NY, USA: Whitepaper; 2020. p. 1–47.
17. UN General Assembly, transforming our world : the 2030 Agenda for sustainable development, 21 October 2015, A/RES/70/1. Available at: https://www.refworld.org/docid/57b6e3e44.html. Accessed on 10th Feb 2024.
18. Hyperledger Foundation. Hyperledger Besu. Available at https://besu.hyperledger.org/en/stable/private-networks/reference/. Accessed on 10th Feb 2024.
19. Benet, J. IPFS - Content addressed, versioned, P2P file system. (2014). ArXiv, abs/1407.3561, https://doi.org/10.48550/arXiv.1407.3561
20. Nakamoto, S A Peer-to-Peer electronic cash system Available at https://bitcoin.co.uk/white-paper/. Accessed on 10th Feb 2024.
21. Solana Available at https://solana.com/. Accessed on 10th Feb 2024.
22. Cardano Foundation Available at https://cardanofoundation.org/. Accessed on 10th Feb 2024.
23. Tezos Available athttps://tezos.com/. Accessed on 10th Feb 2024.
24. Bitcoin SV Available at https://bitcoinsv.com/. Accessed on 10th Feb 2024.
25. Z-cash Available athttps://z.cash/. Accessed on 10th Feb 2024.
26. Bitcoin Gold. Available at https://bitcoingold.org/. Accessed on 10th Feb 2024.
27. Monero. Available at https://www.getmonero.org/. Accessed on 10th Feb 2024.
28. IOTA. Available at https://www.iota.org/ Accessed on 10th Feb 202449. Peercoin. Available at https://www.peercoin.net/ Accessed on 10th Feb 2024.
29. Primecoin. Available at https://primecoin.io/. Accessed on 10th Feb 2024.
30. Litecoin Available at https://litecoin.com/en/. Accessed on 10th Feb 2024.
31. Gervais, A, Karame, G, Wüst, K et al. On the security and performance of proof of work blockchains. In proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for computing machinery, New York, NY, USA, 3–16, https://doi.org/10.1145/2976749.2978341
32. Anton Hasselgren PKW, Margareth Horn, Katina Kralevska, Danilo Gligoroski, Arild Faxvaag. GDPR compliance for blockchain applications in healthcare. CoRR. 2020;abs/2009.12913, https://doi.org/10.48550/arXiv.2009.12913
33. Bae YS, Park Y, Kim T, Ko T, Kim MS, Lee E, et al. Development and pilot-test of blockchain-based MyHealthData platform. Appl Sci-Basel. 11(17):12. https://doi.org/10.3390/app11178209
34. Bhattacharya P, Tanwar S, Bodkhe U, Tyagi S, Kumar N. BinDaaS: blockchain-based deep-learning as-a-service in healthcare 4.0 applications. Ieee Trans Network Sci Eng. 8(2):1242–55. https://doi.org/10.1109/TNSE.2019.2961932
35. Cao, Sheng, Jing Wang, Xiaojiang Du, Xiaosong Zhang and Xia Qin. "CEPS: A Cross-Blockchain based Electronic Health Records Privacy-Preserving Scheme." ICC 2020 - 2020 IEEE International Conference on Communications (ICC) (2020): 1–6, https://doi.org/10.1109/ICC40277.2020.9149326
36. Guggenberger T, Sedlmeir J, Fridgen G, Luckow A. An in-depth investigation of the performance characteristics of hyperledger fabric. Comput Ind Eng. 2022;173:108716 ISSN 0360–8352.
37. Liu Q, Liu XH, Hu BS, Zhang SB. Fine-grained Access Control with User Revocation in Cloud-based Personal Health Record System. J Electron Inf Technol. 39(5):1206–12. https://doi.org/10.1109/VTCSpring.2017.8108549
38. Preetha AD, Kumar TSP, editors. MLPPT-MHS: multi-layered privacy preserving and traceable mobile health system. 2019;2019. https://doi.org/10.1016/j.procs.2020.01.054
39. Tembhare A, Chakkaravarthy SS, Sangeetha D, Vaidehi V, Rathnam MV. Role-based policy to maintain privacy of patient health records in cloud. J Supercomputing. 75(9):5866–81, https://doi.org/10.1007/s11227-019-02887-6
40. Jiang S, Wu H, Wang L, editors. Patients-controlled secure and privacy-preserving EHRs sharing scheme based on consortium blockchain. 2019;2019. https://doi.org/10.1109/GLOBECOM38437.2019.9013220
41. Buterin, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. GitHub repository. 2013;1:22–3. Available at: https://ethereum.org/en/whitepaper/. Accessed 22 July 2024.
42. Lewenberg, Y., Sompolinsky, Y., Zohar, A et al. Inclusive block chain protocols. In: Böhme, R., Okamoto, T. (eds) Financial cryptography and data security. FC 2015. Lecture notes in computer science(), vol 8975. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-47854-7_33
43. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: proceedings of the thirteenth EuroSys Conference (EuroSys '18). New York, NY, USA: Association for computing machinery; 2018. https://doi.org/10.1145/3190508.3190538. Article 30, 1–15.
44. Baird, Leemon C. and Atul Luykx. "The hashgraph protocol: efficient asynchronous bft for high-throughput distributed ledgers." 2020 International Conference on Omni-layer Intelligent Systems (COINS) (2020): 1–7, https://doi.org/10.1109/COINS49042.2020.9191430
45. Mamache, Hamed Nazim, et al. "Resilience of IOTA Consensus." ICC 2022 - IEEE International Conference on Communications, May 2022. Crossref. https://doi.org/10.1109/icc45855.2022.9838683.
46. Gangwal, A, HR Gangavalli and A Thirupathi. "A survey of layer-two blockchain protocols." ArXiv abs/2204.08032 (2022): n. pag. https://doi.org/10.48550/arXiv.2204.08032
47. Shakila Z, et al. Thinking out of the blocks: holochain for distributed security in IoT healthcare. IEEE Access. 2022;10:37064–81. https://doi.org/10.1109/access.2022.3163580. Crossref.
48. Xiao Y, Xu B, Jiang W, Wu Y. The healthchain blockchain for electronic health records: development study. J Med Internet Res. 2021;23(1):e13556 Published 2021 Jan 22.
49. Magyar G. Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. 30th Neumann Colloquium (NC); November 24–25, 2017; Budapest, Hungary. 2017. pp. 135–140, https://doi.org/10.1109/NC.2017.8263269
50. Symvoulidis C, et al. Healthfetch: An influence-based, context-aware prefetch scheme in citizen-centered health storage clouds. Future Internet. 2022;14(4):112. https://doi.org/10.3390/fi14040112.
51. Khan FA, et al. Awareness and willingness to use PHR: a roadmap towards cloud-dew architecture based PHR framework. Multimed Tools Appl. 2020;79(13):8399–413. https://doi.org/10.1007/s11042-018-6692-z.
52. Barouti S, Aljumah F, Alhadidi D, Debbabi M. Secure and privacy-preserving querying of personal health records in the cloud. 2014. p. 82–97, https://doi.org/10.1007/978-3-662-43936-4_6
53. Jayaram R, Prabakaran S. Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. Egypt Inform J. 22(4):401–10. https://doi.org/10.1016/j.eij.2020.12.003
54. Raisaro JL, Troncoso-Pastoriza JR, Misbach M, Sousa JS, Praderv S, et al. MedCo: enabling secure and privacy-preserving exploration of

distributed clinical and genomic data. IEEE/ACM Trans Comput Biol Bioinf. 2019;16(4):1328–41. https://doi.org/10.1109/TCBB.2018.2854776.
55. Kartsaklis, Dimitri, Ian Fan, Richie Yeung, A. N. Pearson, Robin Lorenz, Alexis Toumi, Giovanni de Felice, Konstantinos Meichanetzidis, Stephen Clark and Bob Coecke. "lambeq: An Efficient High-Level Python Library for Quantum NLP." ArXiv abs/2110.04236 (2021), https://doi.org/10.48550/arXiv.2110.04236.
56. Pointing, J., Padon, O., Jia, Z., Ma, H., Hirth, A., Palsberg, J., & Aiken, A. Quanto: Optimizing Quantum Circuits with Automatic Generation of Circuit Identities. (2021). ArXiv, abs/2111.11387, https://doi.org/10.48550/arXiv.2111.11387.

Publisher's Note