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

Joe Davids

j.davids@imperial.ac.uk

Imperial College London https://orcid.org/0000-0002-9257-6722

Mohamed ElSharkawy

Imperial College London https://orcid.org/0009-0009-7091-1807

Hutan Ashrafian

Imperial College London https://orcid.org/0000-0003-1668-0672

Eric Herlenius

Karolinska Institutet https://orcid.org/0000-0002-6859-0620

Niklas Lidströmer

niklas.lidstromer@ki.se

Karolinska Institutet https://orcid.org/0000-0003-2701-5029

Research Article

Keywords: global patient co-owned cloud, GPOC, personal health records, PHRs, technical sandbox, cloud-based health, blockchains, artificial intelligence in medicine, cloud security

Posted Date: February 14th, 2024

DOI: https://doi.org/10.21203/rs.3.rs-3004979/v2

Additional Declarations: No competing interests reported.

Abstract

Cloud-based personal health records increase globally. The GPOC series introduces the concept of a Global Patient co-Owned Cloud (GPOC) of personal health records.

Here, we present the GPOC series' technical sandbox. This to facilitate 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. Both individual patients, clinics, organisations and regulators are invited to test the concept.

The GPOC Sandbox displays a co-ownership of personal health records. Here it is trisected between patients, clinics and clinicians. The patient can actively participate in research and control their health data. GPOC may influence global research and dissemination of artificial intelligence in healthcare. This may impact global health.

INTRODUCTION

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. The structure remains centralised and security breakages have caused great harm. Simultaneously, new technologies maturate, 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.

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.[1,2,3,4] Its systematic review and meta-analysis exposes the core facets of a GPOC.[1] The GPOC Survey shows a global consensus for its necessity.[2] A summit echoes this.[3] An additional review and interview series explores the ethics and policies relevant to a GPOC.[4]

Here, we demonstrate the technical GPOC Sandbox. It is based on the series' conclusions on all aspects of an ideal solutions 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.

The purpose is to let all interested parties explore and contribute to this project. This, since the concept requires a global effort. The Sandbox contains a platform of several protocols. The Sandbox technical design is based on the 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 nave.

The Sandbox investigates biometrical authorisation and hashing protocols.[5,6] It investigates patients' management and movability of PHRs. Further, it presents distributed ledger infrastructure. This permits global healthcare communication.[7,8]

Open-source operating systems visualise the Sandbox. It works with various systems without requiring any particular adaptations. Hence, it is an agnostic platform.

The Sandbox explores several concepts, including integration of Systematized Nomenclature of Medicine (SNOMED) and International Classification of Diseases (ICD-11). This to ease communications and medical research.[9]

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 available on a repository on Zenodo, DOI: 10.5281/zenodo.10547507

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

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 10minute 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-second 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

Name	*Algorithm*	*Programmable*	*Relevance*
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 400ms block time. May have applications for a GPOC.

Blockchains that may be relevant to GPOC. Such healthcare network can share and procure sensitive patient data. It can exchange it between laboratories, clinics, hospitals, and caregivers. Applications of this decentralised blockchains can identify mistakes accurately. Hence, an overview of common blockchains relevant to healthcare and potential use for GPOC. Blockchains may be the cusp of a new healthcare era.[39–51]

The GPOC Sandbox is downloadable with minimal installation requirements. Included are illustrative examples. 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, DOI: 10.6084/m9.figshare.c.7067762

DISCUSSION

A global world with frequent travels requires a patient-centric and movable PHR. The here suggested GPOC concept can be further investigated in the Sandbox. The technical requirements with decentralised blockchains, clouds, adaptable UX/UI and homomorphic encryption have been used.[5] The chosen solutions for the GPOC Sandbox are discussed below.

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, certifying the origin of transactions without the need for a central party. This security is further reinforced by consensus algorithms operating on game theory, ensuring the addition of blocks is a rigorous and secure process.[25]

Blockchain solutions, particularly those emphasizing zero-knowledge proof and decentralization, have been strategically chosen for the GPOC Sandbox. The GPOC concept, with its emphasis on patient co-ownership and secure global healthcare communication, demands robust and trustless transactions facilitated by blockchain technology. The unique requirements of GPOC, such as patient co-ownership and participation in global medical research, have directly influenced the technical design of the sandbox, aligning the chosen blockchain technologies with the GPOC vision of democratizing healthcare.

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

Regulations may require keeping information not longer than necessary. Blockchain solutions for healthcare try to address this with off-chain interaction processing.[15]

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

Blockchain-based Zero-Knowledge Proof (BZKP) is an internet-of-things (IoT) model. It is patient-centric and aims to protect sensitive PHR data.[11] Its scalability, robustness and immutability are suitable to GPOC.[11] Blockchains accumulate loads of data and BZKP reduces storage.

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, MyHealthData permits downloads from multiple institutions via mobiles and a blockchain relay server. It is designed for PHR interoperability.[16] 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. It provides superior performance, accuracy, end-to-end latency and mining time compared to other models.[17]

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.[18] A hybrid-blockchain solution addresses some security issues with sharing. Analysis with the blockchain benchmark tool Hyperledger Caliper, exhibits high performance.[19] For GPOC Hyperledger Besu was used.[14]

Most blockchain-based PHR solutions have focused on single chains. The latest leakage mitigations require multi-chains. Hence, Relay-Chain as a Service (RaaS) and a cross-blockchain PHR solution may be suitable for patients visiting many hospitals.[18] 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 democratizing healthcare and contributing to the dissemination of artificial intelligence within the medical domain.

In the GPOC framework, understanding the nuances of cloud infrastructure becomes pivotal. Clouds, whether decentralized with globally distributed storage or centralized 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. Recognizing 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.[20]

Centralised clouds mean storage and transfer by trusted third parties (like Amazon, Google, Microsoft). Here there are weaknesses that can harm data. Hitherto, 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.[21]

In the context of centralized clouds, considerations align closely with GPOC. The challenges associated with centralized 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.[22] Therefore, we argue that outsourcing solutions for PHRs have critical such issues.[23]

To solve this issue, decentralised blockchains ensure trustless 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.[24,25,26] Hence, this is the chosen solution for the GPOC Sandbox.

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. [27]

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.[28,29,30,31] Layer 2 protocols (e.g., Cellar, Loom, Ark, Cosmos, Tesseract) facilitate scalability and privacy through state transfer channels.[30] In healthcare, GPOC should support state change propagation and reversibility.[32,33] Proposals for scalability, like sharding and block-size modifications, contrast with the limitations of slow and expensive layer 1 networks.[31] Emerging healthcare chains, such as HealthChain, are also under consideration.[32]

Even though, blockchain implementation may be expensive, user costs may be lower and energy consumption higher. Moreover, lost key generation may be impossible, storages may exceed hard disc capacities. The security issue with social engineering remains. Though, there are capable software relying on decentralised or token-based distributed ledgers with effective cryptographics. Figure 1 illustrates some applications of blockchains relevant for the GPOC.

Illustrates 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.

A GPOC should support global medical research on its precious contents. 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 contribution possibility to global research and dissemination of AI needed to be considered. Also, bias mitigation and promotion of equal healthcare access. Potentially the AI development of GPOC may lead to a global increase of evidence based medicine (EBM).

Fully Homomorphic Encryption (FHE) is currently the most relevant to GPOC.[23,34,35,36] It supports analytics on encrypted data.[5]

The most effective and ergonomic UX/UI is a science in itself.[6] 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.[7,8,9] The UX/UI of GPOC should lead to efficient workflow. In contrast, social media design wish to prolong logged in sessions and increase the advertising value. The PHR content is already valuable per se. Hence, less value in digital addiction. Relevant GPOC features are displayed in Fig. 2.

Illustrates the science of optimal UX/UI, which is 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. A suggested collection of ergonomic and minimalist UX/UI wireframes for GPOC is available on the article repository on Figshare, DOI: 10.6084/m9.figshare.c.7067762

Future developments may include large natural language processing, multichains, quantum AI and security for GPOC.[37,38]

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, reinforcing its potential impact on global health and medical research.

Final Remarks

In conclusion, we created a GPOC Sandbox. 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 adaption. Hence, it contributes to the democratisation of healthcare. It facilitates the research and spread of AI within medicine. The GPOC Sandbox may have impact on global health.

METHODS

We used open-source tools to create the GPOC Sandbox.[10] The goal was to incorporate the conclusions from the GPOC-series. We use an open-source cloud service to demonstrate the platform.

Mina Protocol

Mina protocol was used as the underlying smart contract blockchain protocol. Thus, it implements zero knowledge proof through succinct non interactive argument or knowledge (ZK-snark). The aim is to prove information without additional information leak.[11,12]

Mina boasts a 22 KB blockchain size compared to over 250 GB size for other blockchains.[12] These protocols may be optimal for a GPOC. Zero knowledge proof implementation enables security and sustainability.[13] 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 3 illustrates one approach. Ganache, a local blockchain development tool, tests smart contracts. The smart contract Mina implementation is achieved with typescript contrasted to solidity for Ethereum. Now, it is in development and available in a public blockchain format. Though, it has potential to develop into a permissioned use-case for GPOC.[12]

This figure illustrates the use of Mina for on-chain data processing, employing zero-knowledge proofs. A verification proof is stored locally on the private blockchain for network participants, including clinicians, patients, and their families. Data queried undergoes conversion into homomorphic encrypted form, processed through a prover function, and 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.[12]

Ethereum and Hyperledger Protocol

We employed the Ethereum smart contract protocol, implemented using Solidity within an individual permissioned use-case named Hyperledger Besu.[14] 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.

Declarations

Data Availability

All 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. Supplement materials and UX/UI wireframes are available in the article repository on Figshare, DOI: 10.6084/m9.figshare.c.7067762

Ethics Approval and Consent to Carticipate

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. Written consent declaration found in supplement S1.

Consent for Publication

Not applicable.

Competing Interests Statement

All authors declare that they have no conflicts of interest.

Funding

This GPOC study series were supported by the Swedish Research Council (2019-01157) and the Swedish National Heart and Lung (20180505) and Freemasons Children's House foundations grants to Prof Eric Herlenius and scholarship to Dr Niklas Lidströmer.

Dr Joseph Davids and Professor Hutan Ashrafian supported by Institute of Global Health Innovation (IGHI) Infrastructure.

Author Contributions Statement

Niklas Lidströmer (NL) provided conceptualising background research. Joseph Davids (JD) created the coding and the online Sandbox with assistance of Mohamed ElSharkawy (ME). All authors (NL, JD, M), Hutan Ashrafian (HA), 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 authors conducted statistical analyses and contributed to the interpretation of results. NL wrote the manuscript with input from all co-authors. NL made all revisions of the manuscript with input from all authors. NL acted as senior and assembling author. All authors critically reviewed and approved the final version of the manuscript. JD and ME made figure 3. JD created the code repository for the GPOC Sandbox on Zenodo. NL made figures 1-2, table 1, and the featured image. NL created the GPOC UX/UI wireframes and supplements in a repository on Figshare.

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), the staff of the Swedish global network of embassies and consulates; especially Dr Erika Lind in Burkina Faso, Nicole Muñoz Curé in Chile, Daniel Marshall-Heyman in Mozambique, and the Swedish Foreign Ministry's Office to Support Small Missions Abroad (UD KSU).

We acknowledge 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 (Palestine and the Holy See) and the de facto independent non-UN member state (Taiwan). Also, all leaders and advisors representing 18 top-ranked international organisations – especially for technical discussions with International Committee of the Red Cross (ICRC).

References

1. Lidströmer N et al,*Systematic Review and Meta-Analysis for a Global Patient co-Owned Cloud (GPOC),* Nature Communications, DOI: 10.21203/rs.3.rs-3004559/v1
2. Lidströmer N et al,*Necessity of a Global Patient co-Owned Cloud (GPOC),* Nature Communications, DOI: 10.21203/rs.3.rs-3004727/v1
3. Lidströmer N et al, *A Summit on a Global Patient co-Owned Cloud (GPOC)*, DOI: 10.21203/rs.3.rs-3353036/v1
4. Lidströmer N et al,*Review of the Ethics, Policies and Regulations of a Global Patient co-Owned Cloud (GPOC),* DOI: 10.21203/rs.3.rs-3353005/v1
5. Kocabas O, Soyata T. Towards privacy-preserving medical cloud computing using homomorphic encryption. 2015. p. 213-46, DOI: 10.4018/978-1-5225-9863-3.ch005
6. Nikam SS, Kshirsagar JP. Implementation of secure sharing of PHR's with IoMT cloud. International Journal of Recent Technology and Engineering. 2019;8(3):599-602, DOI: 10.35940/ijrte.B2192.098319

7. Fujita K OK, Takemura T, Kuroda T. The Improvement of the Electronic Health Record User Experience by Screen Design Principles. . J Med Syst 2019;Dec 10;44(1):21, DOI: 10.1007/s10916-019-1505-0
8. Leeming G TS, Ainsworth J. . Designing a Solution to Manage Electronic Consent for Children. . Stud Health Technol Inform. 2020;2020 Jun 16;270:1103-1107, DOI: 10.3233/SHTI200333
9. Chang E, Mostafa J. The use of SNOMED CT, 2013-2020: a literature review. J Am Med Inform Assoc. 2021 Aug 13;28(9):2017-2026, DOI: 10.1093/jamia/ocab084
10. Get started with Docker. Docker Inc. Available at: https://docs.docker.com/get-started/ Accessed on 10th February 2024
11. 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 Journal of Basic and Applied Sciences. 2021;28(1):154-71, DOI: 10.1080/25765299.2020.1870812
12. 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 Mar:1-47.
13. 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 February 2024
14. Hyperledger Foundation Hyperledger Besu. Available at https://besu.hyperledger.org/en/stable/private-networks/reference/ Accessed on 10th February 202415.
15. Anton Hasselgren PKW, Margareth Horn, Katina Kralevska, Danilo Gligoroski, Arild Faxvaag. GDPR Compliance for Blockchain Applications in Healthcare. CoRR. 2020;abs/2009.12913, DOI: 10.48550/arXiv.2009.12913
16. Bae YS, Park Y, Kim T, Ko T, Kim MS, Lee E, et al. Development and Pilot-Test of Blockchain-Based MyHealthData Platform. Applied Sciences-Basel.11(17):12, DOI: 10.3390/app11178209
17. Bhattacharya P, Tanwar S, Bodkhe U, Tyagi S, Kumar N. BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications. Ieee Transactions on Network Science and Engineering.8(2):1242-55, DOI: 10.1109/TNSE.2019.2961932
18. 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, DOI: 10.1109/ICC40277.2020.9149326
19. Cao Y, Sun Y, Min JS. Hybrid blockchain-based privacy-preserving electronic medical records sharing scheme across medical information control system. Measurement & Control.53(7):1286-99, DOI: 10.1177/0020294020926636
20. Liu Q, Liu XH, Hu BS, Zhang SB. Fine-grained Access Control with User Revocation in Cloud-based Personal Health Record System. Journal of Electronics & Information Technology.39(5):1206-12, DOI: 10.1109/VTCSpring.2017.8108549

21. Preetha AD, Kumar TSP, editors. MLPPT-MHS: Multi-Layered Privacy Preserving and Traceable Mobile Health System2019 2019, DOI: 10.1016/j.procs.2020.01.054

22. Tembhare A, Chakkaravarthy SS, Sangeetha D, Vaidehi V, Rathnam MV. Role-based policy to maintain privacy of patient health records in cloud. Journal of Supercomputing.75(9):5866-81, DOI: 10.1007/s11227-019-02887-6

23. Jiang S, Wu H, Wang L, editors. Patients-controlled secure and privacy-preserving EHRs sharing scheme based on consortium blockchain2019 2019, DOI: 10.1109/GLOBECOM38437.2019.9013220

24. Buterin V. Ethereum white paper: a next generation smart contract & decentralized application platform. First version. 2014;53.

25. 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, DOI: 10.1145/2976749.2978341

26. 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, , DOI: 10.1007/978-3-662-47854-7_33

27. 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). Association for Computing Machinery, New York, NY, USA, Article 30, 1–15. 2018, DOI: 10.1145/3190508.3190538

28. 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, DOI: 10.1109/COINS49042.2020.9191430

29. Mamache, Hamed Nazim, et al. “Resilience of IOTA Consensus.” ICC 2022 - IEEE International Conference on Communications, May 2022. Crossref, DOI: 10.1109/icc45855.2022.9838683.

30. Gangwal, Ankit, Haripriya Ravali Gangavalli and Apoorva Thirupathi. “A Survey of Layer-Two Blockchain Protocols.” ArXiv abs/2204.08032 (2022): n. pag, , DOI: 10.48550/arXiv.2204.08032

31. Zaman, Shakila, et al. “Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare.” IEEE Access, vol. 10, 2022, pp. 37064–81. Crossref, , DOI: 10.1109/access.2022.3163580.

32. 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, DOI: 10.2196/13556

33. 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, DOI: 10.1109/NC.2017.8263269

34. Barouti S, Aljumah F, Alhadidi D, Debbabi M. Secure and privacy-preserving querying of personal health records in the cloud. 2014. p. 82-97, DOI: 10.1007/978-3-662-43936-4_6

35. Jayaram R, Prabakaran S. Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. Egyptian Informatics Journal.22(4):401-10, DOI: 10.1016/j.eij.2020.12.003

36. 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 transactions on computational biology and bioinformatics. 2019;16(4):1328-41, DOI: 10.1109/TCBB.2018.2854776

37. 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), DOI: 10.48550/arXiv.2110.04236

38. Pointing, J., Padon, O., Jia, Z., Ma, H., Hirth, A., Palsberg, J., & Aiken, A. (2021). Quanto: Optimizing Quantum Circuits with Automatic Generation of Circuit Identities. ArXiv, abs/2111.11387, DOI: 10.48550/arXiv.2111.11387

39. Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. ArXiv, abs/1407.3561, DOI: 10.48550/arXiv.1407.3561

40. Nakamoto, S A Peer-to-Peer Electronic Cash System Available at https://bitcoin.co.uk/white-paper/ Accessed on 10th February 2024

41. Solana Available at https://solana.com/ Accessed on 10th February 2024

42. Cardano Foundation Available at https://cardanofoundation.org/ Accessed on 10th February 2024

43. , Tezos Available at https://tezos.com/ Accessed on 10th February 2024

44. Bitcoin SV Available at https://bitcoinsv.com/ Accessed on 10th February 2024

45. Z-cash Available at https://z.cash/ Accessed on 10th February 2024

46. Bitcoin Gold. Available at https://bitcoingold.org/ Accessed on 10th February 2024

47. Monero. Available at https://www.getmonero.org/ Accessed on 10th February 2024

48. IOTA. Available at https://www.iota.org/ Accessed on 10th February 202449.

49. Peercoin. Available at https://www.peercoin.net/ Accessed on 10th February 2024

50. Primecoin. Available at https://primecoin.io/ Accessed on 10th February 2024

51. Litecoin Available at https://litecoin.com/en/ Accessed on 10th February 2024

Figures

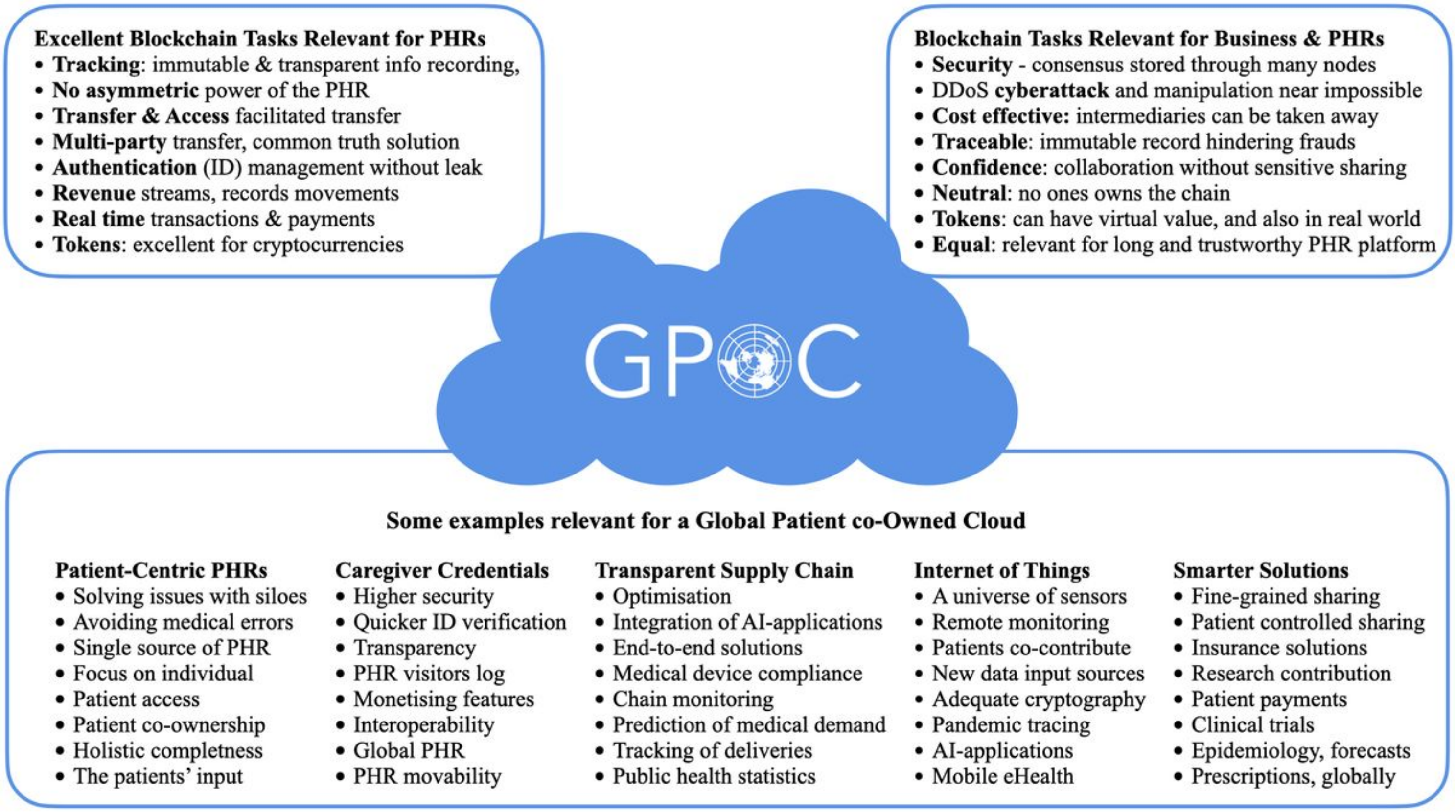
Excellent Blockchain Tasks Relevant for PHRs
• Tracking: immutable & transparent info recording,
• No asymmetric power of the PHR
• Transfer & Access facilitated transfer
• Multi-party transfer, common truth solution
• Authentication (ID) management without leak
• Revenue streams, records movements
• Real time transactions & payments
• Tokens: excellent for cryptocurrencies
Blockchain Tasks Relevant for Business & PHRs
• Security - consensus stored through many nodes
• DDoS cyberattack and manipulation near impossible
• Cost effective: intermediaries can be taken away
• Traceable: immutable record hindering frauds
• Confidence: collaboration without sensitive sharing
• Neutral: no ones owns the chain
• Tokens: can have virtual value, and also in real world
• Equal: relevant for long and trustworthy PHR platform
GPOC
Some examples relevant for a Global Patient co-Owned Cloud
Patient-Centric PHRs
• Solving issues with siloes
• Avoiding medical errors
• Single source of PHR
• Focus on individual
• Patient access
• Patient co-ownership
• Holistic completness
• The patients' input
Caregiver Credentials
• Higher security
• Quicker ID verification
• Transparency
• PHR visitors log
• Monetising features
• Interoperability
• Global PHR
• PHR movability
Transparent Supply Chain
• Optimisation
• Integration of AI-applications
• End-to-end solutions
• Medical device compliance
• Chain monitoring
• Prediction of medical demand
• Tracking of deliveries
• Public health statistics
Internet of Things
• A universe of sensors
• Remote monitoring
• Patients co-contribute
• New data input sources
• Adequate cryptography
• Pandemic tracing
• AI-applications
• Mobile eHealth
Smarter Solutions
• Fine-grained sharing
• Patient controlled sharing
• Insurance solutions
• Research contribution
• Patient payments
• Clinical trials
• Epidemiology, forecasts
• Prescriptions, globally

Figure 1

Applications of Blockchains for GPOC

Illustrates 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.

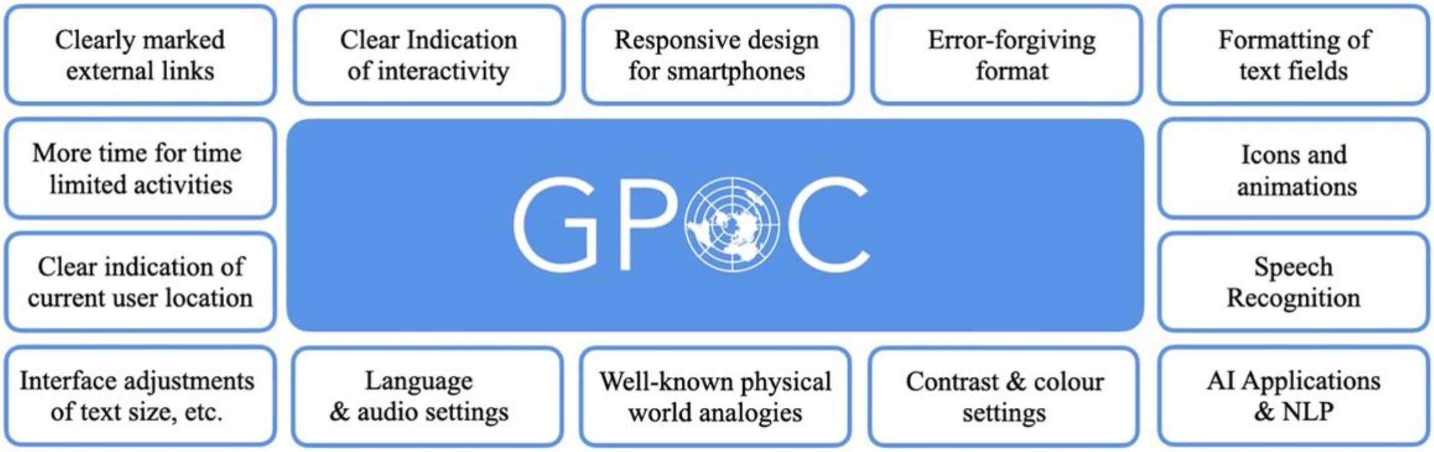
Clearly marked external links
Clear Indication of interactivity
Responsive design for smartphones
Error-forgiving format
Formatting of text fields
More time for time limited activities
GPOC
Icons and animations
Clear indication of current user location
Speech Recognition
Interface adjustments of text size, etc.
Language & audio settings
Well-known physical world analogies
Contrast & colour settings
AI Applications & NLP

Figure 2

Optimal UX/UI for GPOC

Illustrates the science of optimal UX/UI, which is 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. A suggested collection of ergonomic and minimalist UX/UI wireframes for GPOC is available on the article repository on Figshare, DOI: 10.6084/m9.figshare.c.7067762

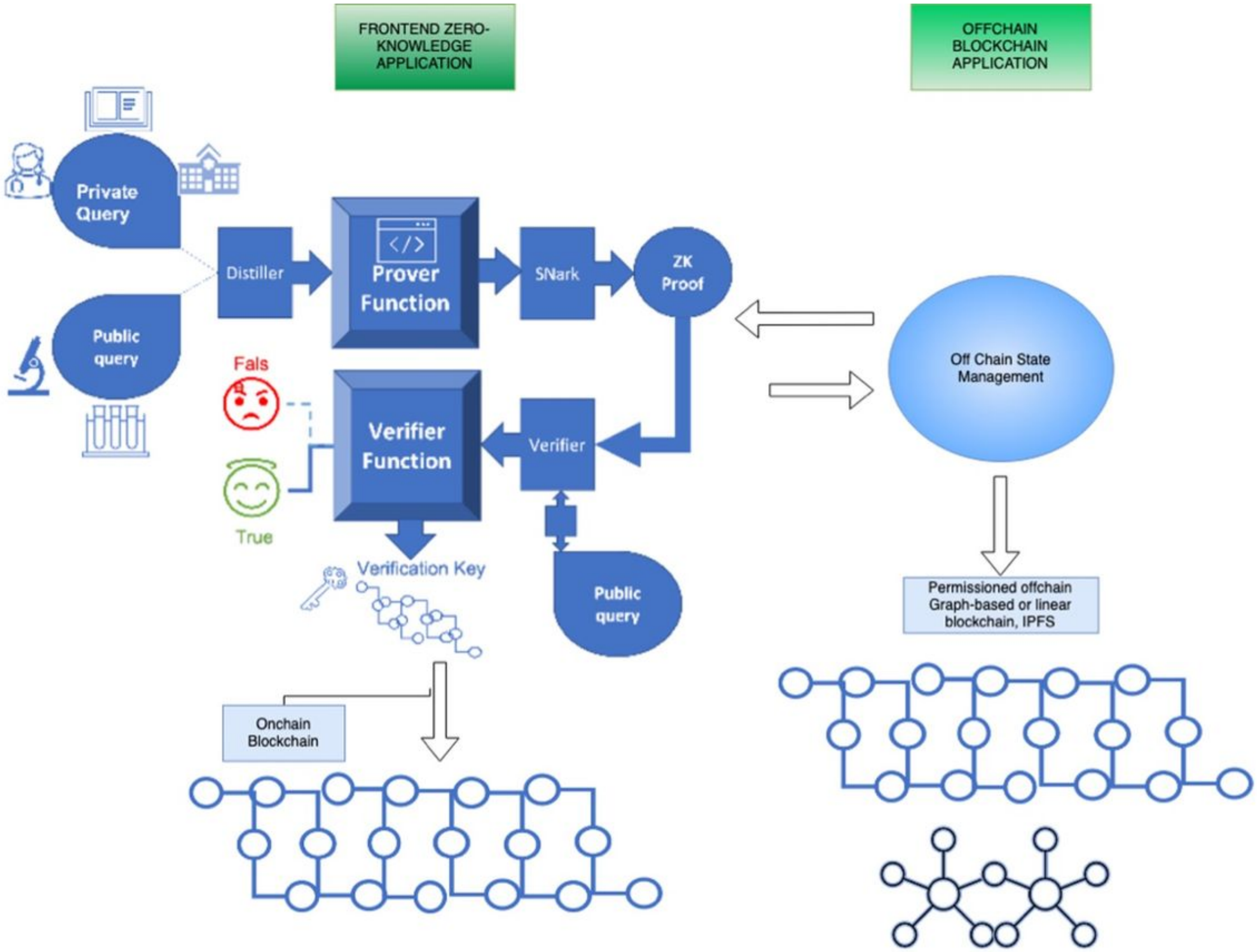
FRONTEND ZERO-KNOWLEDGE APPLICATION
OFFCHAIN BLOCKCHAIN APPLICATION
Private Query
Public query
Distiller
Prover Function
SNark
ZK Proof
Off Chain State Management
Fals
True
Verifier Function
Verifier
Verification Key
Public query
Permissioned offchain Graph-based or linear blockchain, IPFS
Onchain Blockchain

Figure 3

Example Technology Stack for GPOC

This figure illustrates the use of Mina for on-chain data processing, employing zero-knowledge proofs. A verification proof is stored locally on the private blockchain for network participants, including clinicians, patients, and their families. Data queried undergoes conversion into homomorphic encrypted form, processed through a prover function, and verified using ZKSnarks (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.12

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- GPOCUXUIWIREFRAMES.pdf
- InventoryofSupportingInformation.pdf
- GPOCFEATUREDIMAGE.pdf
- SupplementaryInformation.pdf