BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE
TECHNICAL BRIEFS & SHORT REPORTS

My Holistic Data Share: A WEB3 Data Share Application: Extending Beyond Finance to Privacy-Protected Decentralised Share of Multi-Dimensional Data to Enhance Global Healthcare

Sathya Krishnasamy, MS

ChainAim, Newington, Connecticut, USA

DOI: https://doi.org/10.30953/bhty.v7.341

Corresponding Author: Sathya Krishnasamy, Email: sathya.krishnasamy@chainaim.com

Keywords: access control, blockchain, distributed ledger, healthcare, privacy, threshold cryptography

Abstract

WEB3 technologies on network architectures, distributed ledgers and decentralised artificial intelligence represent a transformative shift in how data are handled, stored and shared. These innovations promise to significantly enhance consumer data privacy rights by addressing fundamental vulnerabilities associated with traditional centralised systems and self-custody wallets. Data breaches in traditional systems operated mainly by third parties are more common, resulting in significant data leaks because of centralised storage and excessive data movement, sometimes unnecessarily. Healthcare data breaches have been a growing concern globally. Several hospitals faced operational halts on account of the impact of ransomware on patient care and privacy. WEB3 Wallets are a vital component emerging as a significant force for global financial inclusion, especially in developing economies. They promote inclusion, reduce costs and empower individuals through self-custody. Though major improvements are needed in these wallets, their use is rising steadily. The global cryptocurrency user base is expected to reach over 500 million by 2025, with substantial growth in emerging markets, according to a report by Statista in 2023. This paper introduces a concept beyond cryptocurrencies and finance into everyday real-world use cases that need combinatorial access to a person's holistic data, including financial and health records, genomic data, advanced directives, among others, that need to be privacy protected and shared with specific actors identified for their roles in the WEB3 ecosystem through decentralised identifiers and non-fungible token badges identifying particular recipients. The author introduced the concept at ETHBoston in April 2024, won accolades for a primitive implementation using underlying threshold cryptography technologies, and enhanced it into a conceptual holistic data share application for global healthcare as presented in this paper.

Received: August 1, 2024; Accepted: August 25, 2024; Published: August 31, 2024

WEB3 is a collection of emerging technologies. It includes distributed ledgers, self-sovereign identifications (IDs), and artificial intelligence (AI), and promotes data and asset ownership concepts. WEB3 offers a decentralised alternative to traditional banking systems.[1] WEB3 technologies provide access to financial services for the unbanked and underbanked populations,[2] reduce transaction costs and empower individuals for consumer-mediated data sharing through self-custody WEB3 wallets. In addition, Web 3.0 data share principles align with modern data privacy laws, enhancing user control over personal information. These innovations promise to significantly improve consumer data privacy rights by addressing some fundamental vulnerabilities associated with traditional centralised systems.

Data breaches in conventional systems are more common, resulting in significant data leaks because of centralised storage vulnerabilities and excessive data movement, sometimes unnecessarily. The potential of WEB3 technologies to enhance consumer data privacy rights is a step towards a more secure future. Healthcare data breaches are a growing concern globally. Several hospitals faced operational halts because of ransomware, impacting patient care and privacy.[3]

Data Sovereignty and Control with Self-Custody

Concerning WEB3 wallets, self-custody refers to managing one's digital assets by holding one's private keys with oneself without relying on third-party intermediaries, who might misuse the keys. Self-custody fundamentally aligns with data privacy principles because it emphasises individual control over personal data. Many articles in the Union's general data protection regulation define personal data, data minimisation, lawfulness and security-first designs appropriate to the risk and notifications. Similarly, sections of California Consumer Privacy Act cover provisions that define personal information, right to know, opt-out, delete and non-discrimination for dissent. Specifically for the compliance of the Health Insurance Portability and Accountability Act, the key rules are privacy – ensuring that any covered entities and business associates protect consumer data, security (mandating administrative, physical and technical safeguards) and notification – on any breaches. These regulations stipulate that individuals have ownership of their data, must provide explicit consent to the users of their data and minimally needed information is collected to be retained for a specific period for specific uses, with full audibility of access privilege, use and revoke actions on the data. Self-custody reduces reliance on third-party service providers, potentially reducing data mishandling or breaches whose systems are not secure enough.

Limitations of Current Wallets

Current wallets hold crypto-native assets like cryptocurrencies and non-fungible tokens (NFTs) predominantly for financial applications and services and, to some extent, for storing digital collectibles. These use cases hold collectibles stored in decentralised storage like the InterPlanetary File System (IPFS) and have a pointer to it in the wallet and the metadata. However, many use cases are possible as the same concepts can equally apply to managing access to other forms of personal information on top of financial records. These include health records, genomic records, advanced directives, among others, where different forms of data might need to be seen by people playing specific roles in the social context, which are more logical uses.

Self-custody requires individuals to be knowledgeable and savvy about handling their private keys. Also, the wallet user experience is still not very user-friendly and requires some technical sophistication and a set of non-trivial steps to follow. Some users might need technical support to manage their keys and might need to rely on third parties. Depending on the custodians' security capabilities and integrity, this can lead to risks, including identity theft, loss of funds, privacy breaches, among others.

This opens the need for decentralised protocols that are more resilient than centralised custodians and a data-blind protocol-level decentralisation that increases the resilience of data management by encrypting users' information and using critical management systems that are decentralised and managed by cryptographic mechanisms that can reassemble the credentials for accessing the data, based on granular roles for specific periods. A key technology that attempts to achieve this decentralisation is threshold cryptography.

Threshold Cryptography

Threshold cryptography is a cryptographic scheme where a cryptographic key is divided into multiple shares, distributed among different parties. A predefined number of these shares (the threshold) must be combined to perform cryptographic operations such as decryption or signing. For instance, if a key is divided into 10 shares and the threshold is set to 6, any 6 shares can be used to reconstruct the key, but fewer than 6 shares will provide no information about the key. Each share will be with a specific custodian, and they only know a piece of the key, not the entire one.

Benefits of Threshold Cryptography

The benefits of threshold cryptography include enhanced security, redundancy and reliability, and multi-party authorisation.

Enhanced Security

By distributing key shares among multiple parties, threshold cryptography ensures that no single entity has complete access to sensitive information. This approach mitigates the risk of unauthorised access and provides an additional layer of security for managing critical records. In practice, this means that even if a malicious actor compromises one share, they cannot access the sensitive data or perform operations without obtaining the minimum required number of shares. No single individual has the power to compromise the data independently, drastically reducing the likelihood of data breaches and insider threats.

Redundancy and Reliability

Threshold cryptography allows for operations even if some key shares are lost or compromised as long as the threshold number of shares remains intact. This ensures that critical records remain accessible and secure in the face of technical issues or security breaches.

Multi-party Authorisation

Threshold cryptography helps ensure that data cannot be tampered with without the consensus of multiple parties. This facilitates secure collaboration by allowing researchers to share and analyse data without exposing it in its entirety to any single participant. This is particularly

Citation: Blockchain in Healthcare Today 2024, **7**: 341 - https://doi.org/10.30953/bhty.v7.341

important in clinical trials and research studies, where data integrity is essential for deriving valid conclusions and ensuring patient safety. In scenarios involving multiple stakeholders, such as estate planning or advanced directives, threshold cryptography enables secure multi-party authorisation. This ensures that decisions or actions related to sensitive records require the consensus of multiple authorised parties, enhancing security and integrity.

Limitations and Challenges of Threshold Cryptography

Complexity, availability, and scalability are limitations and challenges.

Complexity

Splitting the cryptographic key and managing shares requires sophisticated protocols. Implementing them correctly and ensuring resilience under various security attacks is a challenge.

Availability

Reconstructing the key requires the active participation of multiple parties, which can be inefficient if parties are geographically dispersed or have inconsistent availability.

Scalability

As the number of participants and shares increases, the complexity, communication and availability overhead increases, which can cause scalability issues.

The specific implementation of threshold cryptography can vary based on how the distribution of cryptographic keys is disseminated and how the access control is configured for data retrieval. The mechanism of reassembling the key shares and threshold is also configurable. In a decentralised mode of operation, protocol implementation can decentralise the key shards across validator nodes.

MyHolisticDataShare and Possibilities in Global Healthcare

MyHolisticDataShare is a WEB3 data share application that addresses the limitations and introduces newer concepts of organising and storing types of user data beyond financial data and digital collectibles into real-world assets such as medical records. These advanced directives can be managed by extending the cryptographic primitives for secure data sharing. Access to these records can be individually provisioned and metered to specific parties and their roles in the social context, or it could be a combination of assets for a particular recipient or a role.

MyHolisticDataShare is a revised and enhanced adaptation of the SocialSecureShare application, initially conceived by the author at ETHBoston in April 2024, which won the best project for privacy and community vote. MyHolisticDataShare is a technical prototype for consumers and recipients of such data, combining many aspects of consumer-directed data share and its implications for healthcare and combinational data with health in regular and emergency settings, and health and finance for efforts such as social determinants of care.

These emerging privacy protection technologies, like threshold cryptography and access control, show possibilities for promoting consumer-mediated data share while allowing for enhanced privacy by reducing single points of failure, granular and composable access control, and possibilities of checks and balances entities also participating as nodes to have improved visibility.

MyHolisiticDataShare Technical Design

MyHolisticDataShare uses cryptographic privacy primitives and decentralised mechanisms – like threshold cryptography for privacy-protecting the decryption access of the encrypted data stored in decentralised storage – based on NFTs that are tokens to identify unique items. The NFTs are unique tokens that represent one thing and one thing only, and can be used to represent a specific badge. The governance of the protocol and the application can assign these badges.

MyHolisiticDataShare is built on the decentralised implementation of threshold cryptography using the Threshold Protocol and Threshold Access Control (TACo) protocol.[4] These NFTs are mapped to specific identity badges associated with individuals or roles that provide access to the consumer's data based on the decentralised identity verification of the wallets holding those access badges.

The threshold network offers a full suite of decentralised threshold cryptography services to increase user privacy and sovereignty in permission blockchains (Figure 1). Threshold cryptography protects data by distributing operations across a network of independent nodes, increases security and availability, and reduces reliance on trusted parties. Threshold network uses the service TACo protocol for access control. The data owner can encrypt their payload, which can have multiple sections, and can store them in offline locations. As needed, these storage elements can also be used in decentralised storage. In this example, the data owner stores the encrypted data in the IPFS, a popular decentralised storage solution.

The TACo splits a joint secret – a decryption key – into multiple *shares* and distributes those among authorised and collateralised node operators (i.e., stakeholders in the threshold network). A minimum number – a *threshold* – of those operators holding the key shares must be online and actively participate in partial decryptions. These are subsequently combined on the requester's client to reconstruct the original plaintext data. Every data payload is attached to conditions that can restrict access granularly. The data owner can define a range of access conditions that can have access control checks such as, "Does the

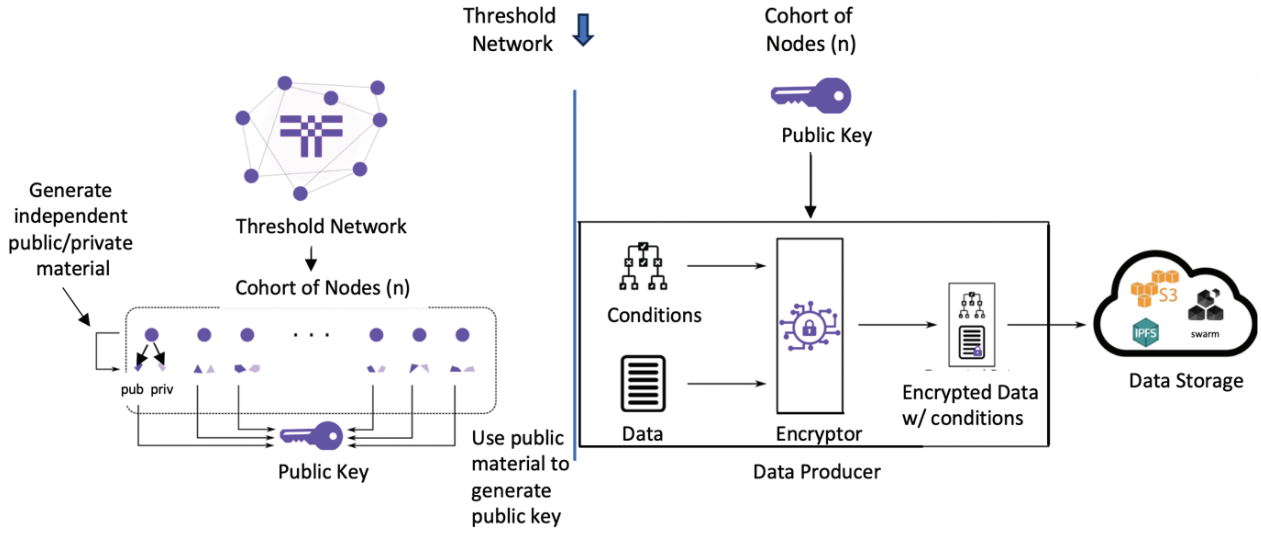

Fig. 1. Screenshots of threshold network implementation of threshold cryptography. Source: https://docs.threshold.network/applications/threshold-access-control/key-concepts.
Source: Copyright by the author, 2024.

requestor own a specific NFT that represents a badge of an emergency medical worker?" or "…a social worker helping patients?" It can also combine them with other elements like, "Is the requestor asking for access during a time for which the data owner gives access, etc.?"

The requesters prove their association with condition fulfilment – their right to receive a threshold number of decrypting shares – by signing a transaction that verifies their ownership of a given WEB3 wallet (in this case, MetaMask wallet on Polygon Test Network Amoy). That wallet is checked for fulfilment of the specific condition (e.g., owning an NFT in order to access the data assets).

MyHolisticDataShare is designed to be composed of different types of records, as illustrated in Figure 2, that a consumer could store in a decentralised storage infrastructure like the IPFS, with metadata defining the URI.

The implementation is in Polygon blockchain Amoy Test Network, with the MetaMask wallet access storing the access control through NFT badges.

Users can flexibly store different kinds of records, including financial, health, genomic and advanced directives.

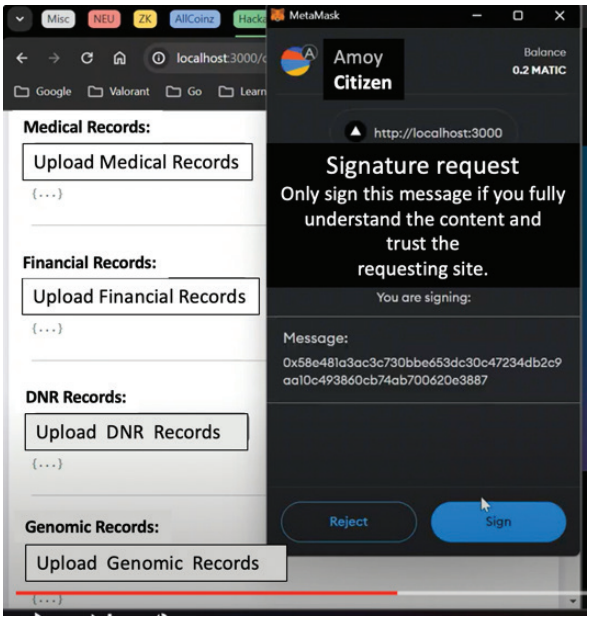

Fig. 2. Screenshot of a user record encrypt.
Source: Copyright by the author, 2024.

Financial Records

These might include traditional financial accounts, crypto accounts, bank statements, letters of credit, among others, that the user could securely store and decide to share with specific recipients that the user deems necessary to share with for specific finance-related purposes.

Health Records

These might include basic health records, including lab reports, diagnostics, diagnostic imagery and appointments that the user deems necessary to share for specific health-related purposes.

Genomic Records

These might include specific granular, highly specialised and personal information like genomic records that the user can share with specific researchers and clinicians of interest.

Advanced Directives

These might include specific health proxy information about things like "Do Not Resuscitate" (DNR) preferences, among others, that are important for healthcare workers and emergency technicians.

Citation: Blockchain in Healthcare Today 2024, **7**: 341 - https://doi.org/10.30953/bhty.v7.341

Figure 2 shows a screenshot of the process where the data owner and a citizen in a social setting sign the transaction when storing the different data payloads they want to encrypt to be stored in decentralised storage. Figure 3 shows a screenshot of the data payload load and decentralised storage location details, and also shows the acknowledgment feedback messages.

MyHolisticDataShare Recipient Badges

Blockchain network participants are given specific NFT badges administered by a governing data autonomous organisation that registers the decentralised IDs. For example, decentralised identifiers (DID) in the network can be assigned a primary doctor badge, and another DID can be assigned an emergency medical technician (EMT) worker badge, representing the specific social context for the data needs.

The social data context badges and their configurations are made available in a registry that indicates to the user which badges can access what kind of data. For example, in the default configuration, an EMT worker might have access to medical records and DNR records but not financial records. A genomic researcher might possess a badge that showcases an interest in a specific type of genomic data he might have. Combinatorial access could be controlled granularly as well. For example, a social worker might have access to health and financial records to help plan coordination help for social determinants of health. Figure 4 shows the different types of badges, stored as NFTs to be stored in the data recipient wallets. When the

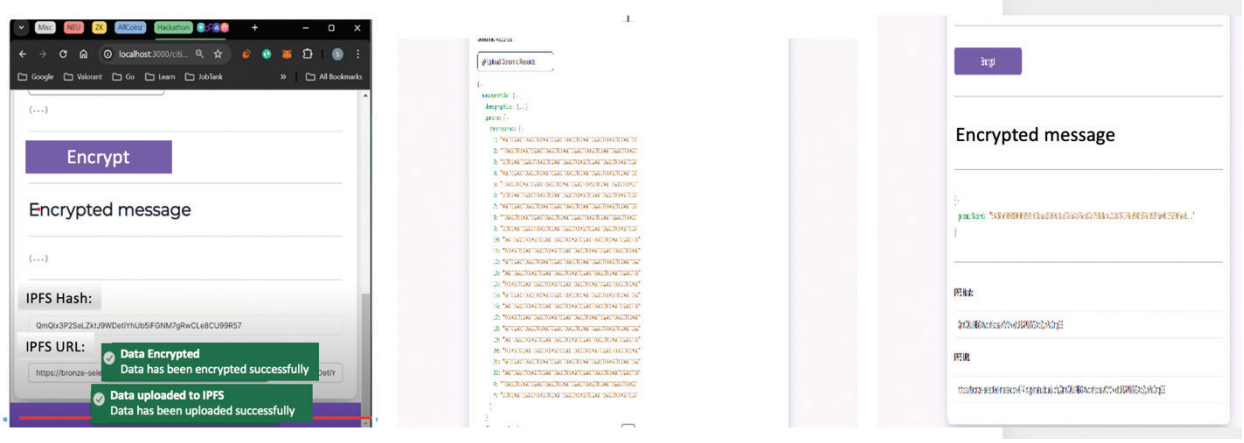

Fig. 3. Successfully encrypted content based on synthetic sample data.
Source: Copyright by the author, 2024.

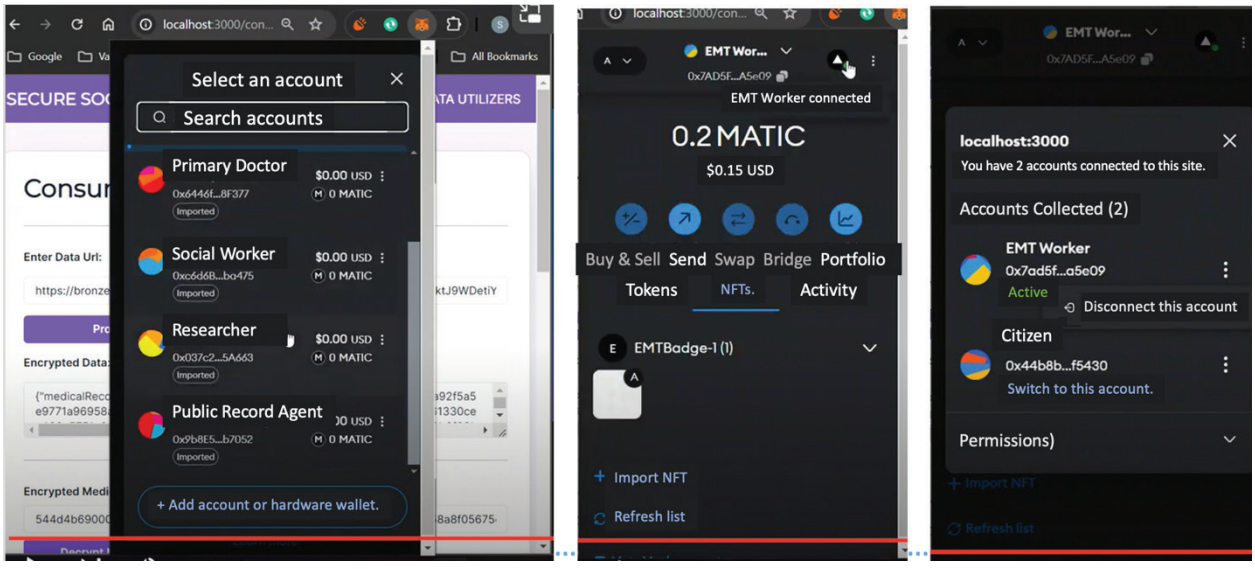

Fig. 4. Different distinct badges modelled as NFTs assigned to Decentralised IDs. EMT: emergency medical technician; ID: identification; NFTs: non-fungible tokens.
Source: Copyright by the author, 2024.

data recipient tries to access the data owner's encrypted data, based on the access controls defined, the presence of these NFT badges are checked to allow or deny access.

Decryption Results and Data Availability

Based on the network's decentralisation quorum configurations and the NFT definitions, the user might sign their transactions to encrypt them so that they are available for decryption for specific DIDs holding specific data needs modelled as unique NFT definitions. These can also be modelled, and the decentralised protocol will check for a specific time for decryption.

The badge and the protocol definitions would give access to decryption. Access to any other data will not be available. Figure 5 shows the situation where a specific NFT badge is checked for during decryption, the right to decrypt is verified and executed, and the decryption is successful. Examples include legitimate access to genomic records for a designated researcher or an EMT healthcare worker with access to DNR data. Figure 6 depicts a situation where someone who does not have the required NFT badge cannot decrypt the data. For example, someone who does not have a Social Worker NFT Badge does not have access to the owners' health and financial summary records data.

In real-world settings, the governance behind this protocol and application will involve offline verification for issuing the badges, possibly involving a combination of health systems and social organisations that define the roles and access criteria for authorisation of access. For example, a designated social worker with specific access controls, who might be working on care coordination or community care roles, can access both the medical and financial records to find holistic care for that patient based on their socio-economic standing where the care could include more than medical care, but also finding housing, transportation and other functions proving their need.

As permissionless blockchains mature, we see an increasing trend from the consumer end to adopt permissionless blockchains, measured by self-custodial wallets and participation in WEB3-based social applications from diverse entities and individuals. Those activities can be leveraged for consumer-mediated health data privacy adoption as well if they are carefully planned with adequate checks and balances, including some regulatory nodes to be run on public/hybrid blockchains, which is slowly starting to happen.

Threshold cryptography is not a contender to other privacy protection techniques but complements other techniques such as fully homomorphic encryption and multi-party computing. In those cases, threshold systems can still add another layer of security, in which the encrypted content can be access-controlled when the

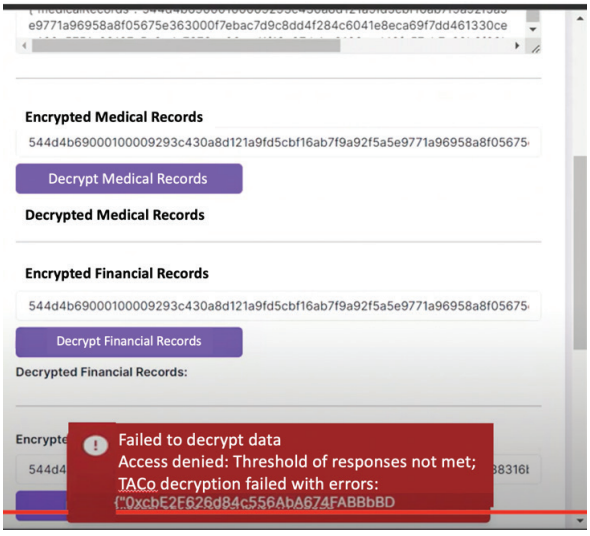

Fig. 6. Screenshot of denied access based on the granular access control. TACo: Threshold Access Control.
Source: Copyright by the author, 2024.

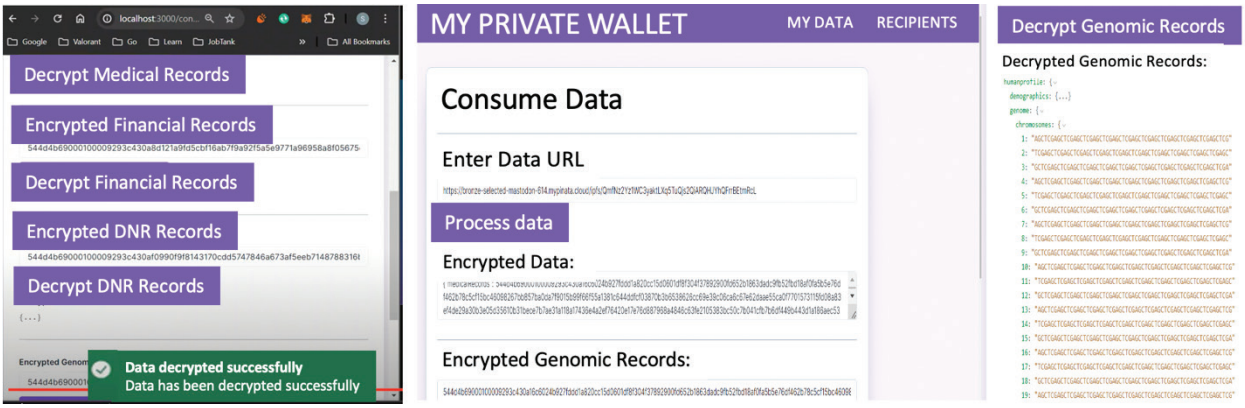

Fig. 5. Example encryption and decryption of sample synthetic data with legitimate access. URL: uniform resource locator.
Source: Copyright by the author, 2024.

Citation: Blockchain in Healthcare Today 2024, **7**: 341 - https://doi.org/10.30953/bhty.v7.341

requesting system accesses data from distributed endpoints or performs computations on the encrypted data. It could become even more critical in those contexts for access control systems to be "bulletproof." In another contemporary paper, the author discusses the emergence of zero-knowledge proofs and machine learning, which is also very complementary, where the data share can be minimalised by presenting proofs for verifiers. This privacy-preserving holistic data sharing could also address another issue, which is cross-organisational and cross-domain data breaches. For example, when data breaches happen in retail or the banking sector, it could compromise access to health records as some personal information gets leaked and provide more ammunition to malicious users. However, with such holistic data shares and granular and composable access, consumers could have more control over their data and be in a position to respond much better to adversities.

One major improvement needed in WEB3 is the ease of use for consumers, as it is challenging for users to keep track of the steps and the uncanny addresses. This effort has already attempted to keep the UI/UX (user interface design/user experience design) very close to a Web 2 webpage, at least concerning managing their data. It uses consumer usability-oriented conceptualisation around JSON (JavaScript Object Notation) data structures, standards and simple screens. In the subsequent iterations, efforts will be made to examine how the data definitions can also be in a browser extension and use advanced account abstraction and identity simplification mechanisms to increase usability.

Conclusions and Future Work

MyHolisticDataShare has demonstrated a new extension of WEB3 technologies based on decentralised data share and threshold cryptography for decentralising the decryption access to non-centralised quorum and configurable threshold definitions. This is still an introductory concept, and the final version of the implementation will depend on regulatory context definitions, the governance design of the Decentralized Autonomous Organization, and maturity and successful DID governance processes in a social context.

Any attempts to trial blockchains in mainstream settings will have to be planned carefully and depend on specific blockchains, including particular public/private/hybrid architectures. This conceptual prototype shows alternative ways the WEB3 technologies open up potential solutions for chronic problems faced in centralised systems with data privacy and sharing, primarily reducing single point of trust failures and granular and composable access control.

The author intends to extend this app into a browser extension wallet app as the landscape matures, specifically around how wallets and WEB3 data share applications and their responsibilities get defined more precisely. Complementary technologies like Zero-Knowledge Systems and fully homomorphic encryptions can enhance this conceptualisation to create enhanced privacy-protected designs for consumer-initiated and provenanced data sharing. The author's efforts at ChainAim continue to build relationships with standards organisations and technology foundations to identify the scalability needs and governance needs for advancing such data sharing.

Funding

None.

Conflicts of Interest

None.

Contributors

Sathya Krishnasamy is the President and Principal of ChainAim Technologies. His 25 years of background spans extensive experience in managed care payor settings in leading US healthcare firms, including Aetna and Anthem. He focusses on emerging technologies, including artificial intelligence/machine learning systems and distributed ledger technologies. He also serves as an advisor in many industry efforts in payor-provider collaboration, standards organisations, and efforts such as Account Aggregators in India advancing Fintech, Healthcare, and Skills sectors. He currently serves as president and principal at ChainAim, offering technical strategy consulting and application and development services.

Sathya Krishnasamy contributed to the research, conceptualisation, and overall implementation.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

No data repositories.

Application of AI-Generated Text or Related Technology

None.

Acknowledgments

Pankhuri Gupta, a Master's student in Software Engineering at Northeastern University, Boston, Massachusetts USA, helped the principal with the UI design and implementation. She can be reached at gupta@pankh@northeastern.edu.

References

1. Buterin V. Ethereum whitepaper [Internet]. ethereum.org; 2014 [cited 2024 Aug 01]. Available from: https://ethereum.org/en/whitepaper/
2. WEB3 and financial inclusion: bridging the gap [Internet]. www.linkedin.com. [cited 2024 Aug 01]. Available from: https://

www.linkedin.com/pulse/WEB3-financial-inclusion-bridging-gap-liveplexplatform-ojazc/
3. U.S. Department of Health & Human Services [Internet]. HHS.gov.; 2019 [cited 2024 Aug 01]. Available from: https://www.hhs.gov
4. Threshold Access Control (TACo). Threshold.network; 2024 [cited 2024 Aug 15]. Available from: https://docs.threshold.network/applications/threshold-access-control

Citation: Blockchain in Healthcare Today 2024, **7**: 341 - https://doi.org/10.30953/bhty.v7.341