Decentralized Health Data Bank [DhdBank]

DhdBank: Decentralized Health Data Bank

Ini Abasi Ekanem
iniabasie@yahoo.com
September 21st, 2020

Abstract

The author introduces DhdBank, a blockchain for decentralized health data storage. DhdBank would enable storage contracts which are a form of agreement between a client and a storage provider (validator). A validator would agree to store an encrypted health data for a period of time at a price, while uploading proof of storage to the blockchain periodically until the contract expires. In a world revolving around digital information, the emergence of decentralized health data storage would bring convenience, efficiency and satisfaction in patient care.

What is DhdBank?

DhdBank is a decentralized health data storage bank that would provide decentralized electronic storage for health data and records, using end-to-end data encryption. These encrypted health data would be stored on a node network and can be managed and retrieved by the client or authorized user anytime within the storage contract duration. A blockchain similar to the bitcoin blockchain is used for this purpose. In each storage contract, the node provider would agree to store a client's encrypted health data on the node network for a period of time at a particular price. Each storage contract would have a unique hash that can be traced on the blockchain. DhdBank would launch on Cosmos and use the Tardigrade protocol before migrating to its own blockchain.

The Problem?

The traditional system of using papers and files to manually or centrally store patient's health data has resulted to data loss, data theft, sale of data to third parties and inefficiencies limiting patient care and medical practice. Health data include patient's medical history, diagnosis, medication, treatment plan, immunization dates, allergies, radiology images, test results and medical recommendations. The major problems of storing these health data are: Data Quality, Data Security, Data Interoperability and Policy setting.

I. Data Quality: Data is considered by many as the fuel that powers information systems; therefore, data integrity also entails ensuring a system's functionality and effectiveness. The problem of low-quality of data and dirty data in health care - characterized by the incompleteness, invalidity, inaccuracy, duplication, non-standardization and meaninglessness of data has resulted to errors that directly or indirectly threaten the well being of patients, while also damaging the reputation of health care providers and initiating lawsuits. Low-quality data has also impacted negatively on daily health operations including inefficiencies in communication, erroneous payments, delayed treatments and invalid research.

II. Data Security: According to Verizon's 2018 Data Breach Investigation Report, security breaches in the health care system makes up about 28% of all security breaches in the world, with a majority of these breaches being caused by human errors. In 2018, Australia's doctor appointment system, HealthEngine, intentionally disclosed personal data of about 200 patients per month between March and August, 2017 to law firms searching for clients with personal injury claims. These cases of data insecurity has limited patient care due to data loss and frequent litigation against care givers.

III. Data Interoperability: According to Kelsey (2018) for data to be most useful to any industry or sector, it needs to yield constant data and should be shared and transferred among people, organizations and systems. The inability for health care to share information or data has resulted to less success in some treatments, inconsistency in treatment, poor collaboration between specialists and an over reduced efficiency.

IV. Policy Setting: Different nations and regions have different policies regarding health data. Understanding the security risks associated with health data, most nations have very strict laws controlling health data. These laws have prevented many nations and regions from maximizing the full potential of health care data. Most regulations and policies do not only protect patient data but also limit the availability of patient data, making it inaccessible in research and expert review.

The Solution

As technological advancement continues, the need for efficiency in health care increases. **DhdBank would solve the above mentioned health care problems by combining blockchain technology with the traditional database technology, creating a decentralized health data storage system for web 3.0**. DhdBank would link its user application to its decentralized non- hierarchical node network where data would be stored. These nodes would be owned by validators/ storage providers using a Delegated Proof-of-Stake Consensus. **Instead of owning a storage cloud, DhdBank would provide cheap, efficient and operational data storage by creating a blockchain where node owners/ validators use computing space to store data securely, making DhdBank 'the Airbnb of Health Data Storage'.**

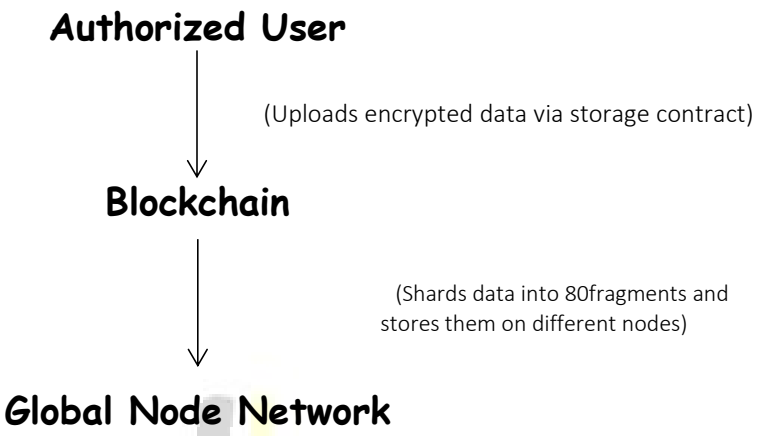
DhdBank Architecture

DhdBank structure would consist of 7 components:

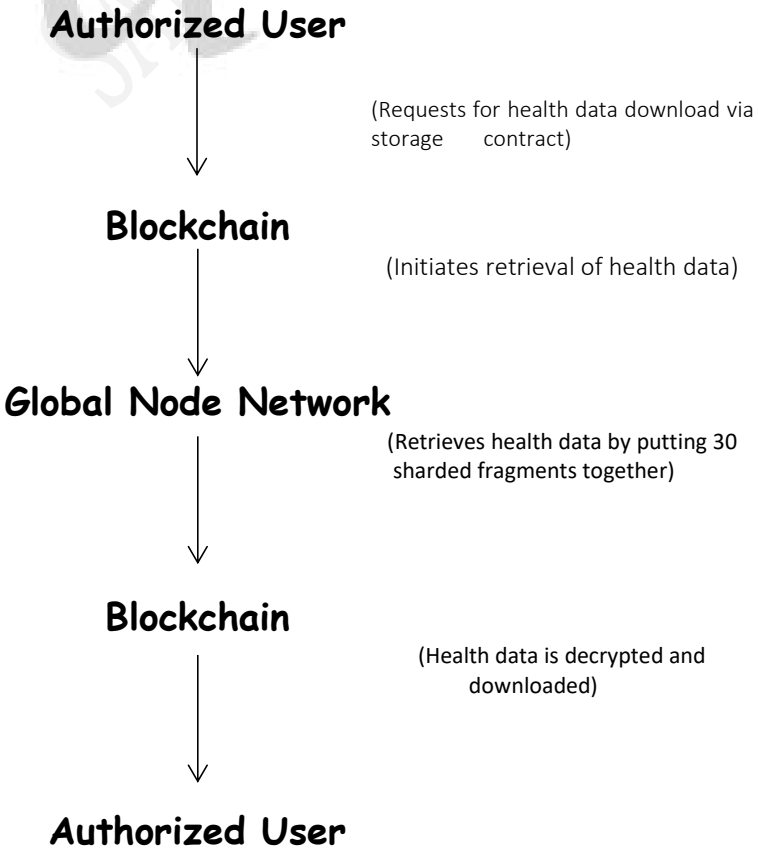
i. Database engine: A key-value store database.
ii. Consensus engine: To be used by validators for nodes to remain synchronized.
iii. Nodes: To provide decentralized storage space for clients and execute network changes for a fee.
iv. Native token: Would be available via centralized and decentralized exchanges for subscription to storage plan, node operator rewards and staking.
v. Client library/ DApp: User interface to access DhdBank.
vi. Client proxy: For clients to trust the response by DhdBank network.
vii. Zones: Database zone that would provide the storage capacity for the network.
Peg zone that would enable interoperability with other networks.
Hub zone that would link the Database and Peg zones.

Users would have access to the decentralized health data bank via a user-friendly DApp to securely upload, manage and retrieve health data. Data would be securely uploaded or downloaded with AES-256 end-to-end encryption after a confirmed storage contract on the DhdBank network.

When uploading data, an end-to-end encryption occurs automatically while the data is then be broken down into 80 fragments and stored on different nodes on the network using Sharding Protocol. The Sharding Protocol would ensure the scalability and security of the network while speeding up the network storage transactions.



When downloading data, a confirmed storage contract would initiate the download process by putting together 30 fragments of the data on the network, which are decrypted on the DApp for the user.



Advantages of DhdBank over Traditional Storage systems

I. No central point of failure, usually open to system hack.
II. Low cost of storage.
III. Scalable with global coverage.
IV. Secure.
V. Fast.
VI. Durable

Impact of DhdBank on Patient Care

In a world being transformed by digital technology, health care is an information enterprise. A seamless flow of information between digital health care professionals and infrastructure encompasses and leverages digital technology in transforming patient care and maximizing health care outcomes. The DhdBank technology would result to:

i. Improved patient care.
ii. Improved diagnostics and patient care outcome.
iii. Increased patient participation in care giving.
iv. Security of patient data.
v. Ease of access to specialists for review and successful treatment.
vi. Reduced errors arising from paper manual.
vii. Time efficiency during medical consultation and clinical visits.
viii. Reduced cost for medical facilities.
ix. An overall efficiency, productivity and convenience in patient care.

Conclusion

In a world revolving around digital information, the emergence of decentralized health data storage would bring convenience, efficiency and satisfaction in patient care. DhdBank would enable storage contracts which are a form of agreement between a client and a storage provider.
These encrypted health data would be stored on a node network and can be managed and retrieved by the client or authorized user anytime within the storage contract duration.

References

Adam & Matt et al., (2014) *Enabling Blockchain Innovations with Pegged Sidechains.*

Bitcoin Developer Guide *https://bitcoin.org/en/developer-guide*

Gregory Maxwell *Proof of Storage to make distributed resource consumption costly.* https://bitcointalk.org/index.php?topic=310323.0

Ha Trinh (2020) *The four big challenges to data management in health care* https://www.google.com/amp/s/blog.fpt-software.com/the-four-big-challenges-to-data-management-in-healthcare%3fhs_amp=true

Hovav & Brent (2008) *Compact Proofs of Retrievability*, Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90-107.

R.C. Merkle (1980)*Protocols for public key cryptosystems,* In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

Satoshi Nakamoto (2008*) Bitcoin: A Peer-to-Peer Electronic Cash System.*

Suzanne & Spliter et al.,(2018) *2018 Verizon Data Breach Investigations Report* https://www.researchgate.net/publication/324455350

V. Rashmi, Nihar B. Shah & P. Vijay Kumar (2009) *Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction.*