Health Nexus

Lucas Hendren and Katherine Kuzmeskas

Version 1.0

Abstract

Health Nexus is a blockchain-oriented distributed system handling data transfer, payments, and storage specifically designed for Health Care. Because of the sensitive nature and requirements of healthcare, existing blockchain distributed systems are not adequate for healthcare. The goal of Health Nexus is to create a blockchain system that can pass the stringent requirements of healthcare by ensuring better data integrity, encryption, and by providing a validation system to ensure the miners running this network are compliant entities. Health Nexus uses a Distributed Hash Table combined with an Ethereum base Blockchain to provide, among many other features, an ability for frictionless data sharing and access to new revenue streams. This is accomplished via an upgrade to data integrity and security system and the addition of an executive governance system for node validation.

Healthcare is under major financial distress, particularly in the United States. Strongly contributing factors are the inability to efficiently share data, the lack of transparency, and therefore the lack of effective care coordination. However, healthcare in the United States, specifically, is experiencing an unprecedented opportunity through federal legislation to benefit from and embrace technology that reduces the friction around transparency and data sharing. Globally, other countries are also feeling the impact caused by the inefficiencies around poor care coordination. By allowing healthcare data to be securely shared in real time and for applications to be automated, healthcare costs can be significantly lowered by improving communication, data analytics, research, and ultimately, patient care. With steeply increasing healthcare costs, a secure solution for transparency and cost savings can have a massive impact on society.

This whitepaper has been prepared solely for the purpose of informing potential contributors to Health Nexus with respect to a proposed technical implementation of, and architecture for, Health Nexus. This whitepaper is non-binding in all respects and does not create any legal obligation of any kind on any person (including SimplyVital). The ultimate implementation of Health Nexus is dependent upon several factors and risks outside of the control of SimplyVital, including regulatory risks, contributor participation, the adoption of blockchain technology and the continued use and adoption of the Ethereum network. Nothing in this whitepaper or otherwise shall require SimplyVital to take any steps to develop or otherwise implement Health Nexus. SimplyVital reserves the right to abandon Health Nexus at any time and to change the implementation of Health Nexus contemplated by this whitepaper at any time. Prospective users of Health Nexus and other contributors to Health Nexus are advised to contribute and/or participate at their own risk and without reliance on any statement contained in this whitepaper.

Table of Contents

Overview

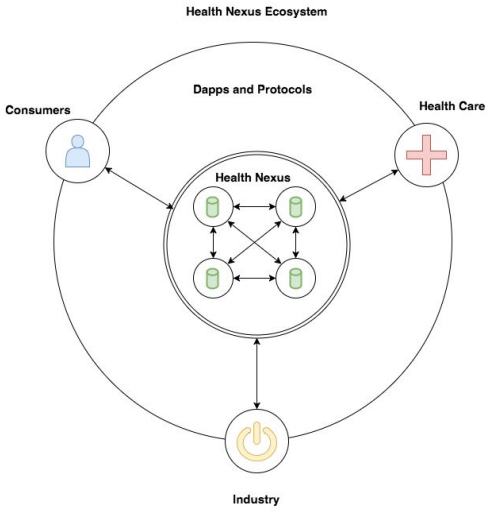
Healthcare is experiencing an unprecedented opportunity to benefit from and embrace technology that reduces the friction around transparency and data sharing. In an effort to reduce the rising costs of healthcare, the Federal government, through the Centers for Medicare and Medicaid Services (CMS) and private payers, are forcing a shift into Value Based Care from Fee for Service. In Fee For Service (FFS), providers are reimbursed for each procedure they do (here forward inclusive of: physicians and nurses). This can easily lead to misaligned practices that favor volume of care (procedures) over quality of care. To combat this increasing concern, which has impacted the steep rise of healthcare data, over the next 3 years $300 billion of healthcare payments, private and public, will be tied to Value Based Care programs. Value Based Care (VBC) programs, converse to FFS, reimburse providers based on the quality outcomes of patient health. This aligns incentives across the care continuum to focus on ensuring that patients receive the right care at the right time and an appropriate level of care.

Value Based Care is a true paradigm shift and a tipping point in healthcare. Never before have providers from different clinical affiliations been required to coordinate care in such a manner, and follow their patients outside of their four walls. Therefore, success in Value Based Care relies on trust, accessibility and immutability of shared data, and transparency — a perfect checklist for utilizing blockchain technology. It is widely documented that communication between providers is poor, and the effectiveness and financially sustainability of Value Based Care relies on effective coordination and communication between providers. It has been demonstrated that 30% of malpractice suits are due to communication failures; Accenture demonstrated that hospitals waste $12B per year due to poor communication; and communication between EMRs is non-existent because companies can lose market share by sharing certain data. Providers are relying on disparate Electronic Medical Record technology (each facility has a different EMR set up), faxing, phone conversations, and Excel spreadsheets resulting in an inefficient and disjointed process for provider communication. In addition, providers in VBC programs do receive data for analysis, but data can be 3–12 months behind, resulting in the need to make strategic decisions on only historical data, instead of in near real time.

The shift into Value Based Care is a significant transition, although the idea and desire to share healthcare data between providers is not new. Nearly 10 years ago, in 2009, the American Recovery and Reinvestment Act (ARRA) included the Health Information Technology for Economic and Clinical Health (HITECH) Act to promote “the electronic movement and use of health information among organizations using nationally recognized interoperability standards.” The Office of the National Coordination for Health Information Technology (ONC) in the U.S. Department of Health and Human Services received $564 million from the HITECH Act with the intention to develop and deploy health information exchanges (HIEs) across the nation. Although all 56 states and territories applied for and received funding for strategic development and implementation of HIEs, the majority of HIEs failed because they were not able to attain financial stability due to providers not participating. Providers did not participate because the value of simply sending data to a warehouse, with no strategic insight provided from the data, is

extremely low; providers sought insight and ease of use of the HIEs. Because there was no value in sharing data, providers found data sharing to be threatening to their market share, unaware of how their data was actually being used. Countless articles and healthcare leaders learned from this outcome that interoperability, or sharing of healthcare data, is a business issue not a technology issue. This means that there needs to be true financial incentive to share medical information. Value Based Care provides the financial incentive. A myriad of VBC programs require efficient care coordination and communication among providers, and also specifically require data sharing, thus the strong financial incentive. The ascendance of VBC positions healthcare for adoption of a technology that lessens the burden around coordination and data sharing.

Enter SimplyVital Health. Our goal is to transform Value Based Care using blockchain technology. Our system will provide a thriving ecosystem for creating a healthcare marketplace and the opportunity for sharing of healthcare data, with the goal of reducing the friction around and to increase the financial upside for providers participating in effective coordination. This marketplace can include apps for every piece of the care continuum such as healthcare facilities, insurance agencies, pharmaceutical companies, and research institutions. Because of the accessibility of the marketplace, applications can be written for local scale or globally.



Example application layers that can be implemented on a local or global scale:

- Clinical Quality Metrics (CQMs)
    - Automatic distribution of updated CQMs from the Federal government and payers, which change annually.
    - Automatic reporting on CQMs. Physician practices spend over $15.4 billion annually reporting clinical quality measures, a cost due to inefficiencies.
- Transparency
    - Access to deidentified data for facility and provider benchmarking locally, regionally, and nationally in near real time. Current data from CMS, for example, is 2 years behind. This ties with CQMs and Value Based Care programs such as MACRA.

- Insurance payments and reimbursements
    - Ability to create new and expand upon existing Value Based Care reimbursement programs such as Bundled Payments. Bundled Payments can have a massive impact on driving down cost and improving quality care. But, the processes are arcane and inefficient. A shared ledger and transparency can pave the way for new models.
    - Ability to financially gainshare with the entire care continuum. CMS has made it legal to share savings from the surgeon all the way down to the patient. A complex process that can be easily automated via smart contracts.
- Pharmaceutical tracking
    - Prescription and HLTHication purchase and tracking locally, nationally, and globally
    - Enabling a nationwide Prescription Drug Monitoring Program. Currently 49 states have a PDMP but access to data out of state is not accessible. Utilizing blockchain technology safely and securely stores this information, which is a well documented concern within these systems.
- Data Accessibility and Sharing
    - Ability for healthcare providers, facilities, researchers, pharmaceutical companies, and patients to sell their data in ways tied to positive economic externalities merged with positive outcomes at mass scale. This is a massive industry with a few major players, such as LexisNexis. Right now, only companies such as LexisNexis profits. Meanwhile, healthcare spend billions of dollars re-purchasing this data. Case in point, Pfizer spends $12MM annually purchasing healthcare data.
- Digital Insurance/Futures App [Securing the Assets of Decentralized Applications using Financial Derivatives]**
    - A marketplace to provide insurance to take care of your decentralized application in an effort to provide additional security. A UMass Amherst professor researching blockchain security has suggested and written about such a protocol.[1]

Existing SimplyVital Health Platform

Our current product, ConnectingCare, is designed to introduce blockchain technology to healthcare. The platform provides one of the most secure Health Insurance Portability and Accountability Act (HIPAA) protocols, and was one of the first working blockchain application in healthcare. As a practical and realistic foray into blockchain in healthcare, ConnectingCare uses a proprietary API call to create a receipt of activity in the SV platform that is stored on the blockchain. Tracking activity in healthcare technology platforms is a requirement of HIPAA. Securing this information on the blockchain ensures that this data is always available, accessible, and immutable. With providers being required to work together and share data like never before, security and trust is paramount.

Intentionally, the ConnectingCare platform as it exists today is a standalone business model in the Health Nexus model. We are using ConnectingCare to prove that blockchain technology can greatly improve healthcare, while also acquiring partners throughout which we can build out our modern blockchain system. The drawback of this system is in its simplicity, though intentional. The capabilities of blockchain technology is much that we can not use it to govern access to data or any of the capabilities related to smart contracts. Again, strategic and practical, blockchain adoption in healthcare will likely be tiered and phased. As such, SV has protected itself from this reality by executing a phased development and implementation process.

Healthcare providers will be provided with multiple ways to increase their revenue stream through the data and services they can provide through the Health Nexus system, in addition to using their already existing software to mine and run the system. It is anticipated that physician revenues will decrease $106B and hospitals $250B by 2030. With such gravity in narrowing margins, providers must look beyond typical cost saving processes to remain financially viable.

Related Projects

Insight and knowledge derived from our team's experience in healthcare, interviews with healthcare professionals actively working in the field, and thorough research of other blockchain initiatives are what drove our decision to create our own healthcare blockchain ecosystem. It became quite clear that a dedicated, permissioned blockchain ecosystem would be far superior in adoption than other solutions. Below, we describe our research on the alternative solutions that we explored and are continuing to follow.

The Enterprise Ethereum Alliance (EEA) has garnered attention and followers, and we plan to continue following the alliance closely, identifying partnership opportunities in the future. For now, there are two main drivers for why we will build our system in parallel to monitoring the EEA: first, they are a standard, not a product, and we are primarily interested in getting this system built to fulfill healthcare's needs and in users' hands so that we can continue to iterate off of the MVP and start a phased adoption; second, they have a limited number of healthcare providers on their system and we want to ensure our system is built around the needs of healthcare and not another industry. While we support the alliance, we do not believe it is the right time to join.

Another project is Hyperledger's Fabric. While they are more healthcare focused than the EEA, they still have a limited number of healthcare members and we are worried that healthcare won't have as much input as the other industries, and the result will be a system more tailored to the requirements of the financial industry. In addition, while it is designed to be modular, there are certain capabilities that Hyperledger's Fabric currently does not have, such as governance and data storage, and we would need to build those out. We also would prefer to go with an Ethereum-based system due to it having already undergone user testing and proof of concepts, and thus having a longer track record. As such, we will also follow Fabric's development for the time but will not plan on using it for Health Nexus.

The next project we are watching is Quorum. Quorum purposes a very interesting solution for enterprise blockchains that shows promise; however, some of the same issues arise involving a lack of healthcare focus and user testing. Another concern is that we do not believe nodes will need private states to track at this time. By utilizing a key-pair system and validation service, we believe this will leave this part unnecessary and will just add in an additional level of overhead. We will monitor the project due to its interesting proposals but do not plan on utilizing it at this time.

The final project we are keeping track of is Patientory. Patientory is interesting and there are similarities in our blockchain, but also key differences. The first and largest one is our governance protocol. By insuring a more stable method of upgrading the network we are hoping this system proves to be more stable. In addition, our node validation service will provide a more trustless environment for healthcare. This service is also different than Patientory's foundation, in that our consortium is much more decentralized and is more like a governing body than a single entity. The next major difference is our intention to include data storage down the line, which could lead to major cost savings on the behalf of the provider. The last major difference is that we are providing day-one usability to token owners as outlined in the roadmap during phase one.

Design

Health Nexus is a dual system platform utilizing a Blockchain protocol for transactions, identity and smart contracts, and with a distributed hash table (DHT) for data storage, managed by a governance system. The Blockchain protocol will be based off of the Ethereum network, and will start with proof of stake [2] (i.e., Casper) and govern the data storage sites. There are other consensus mechanisms that we are investigating that will be researched in conjunction with the development of the system and may be adopted after a vote via the governance protocol at a later time. Health Nexus implements several major modifications to the Ethereum protocol, such as: the ability to store identity on the network, a government system that allows for upgrading and validation, and interactions that are built in to allow for communication with the DHT. The DHT will also use a new system to verify valid storage and miner nodes, keeping track of identity and data access, and negotiate cost of storage through the Blockchain protocol. The currency of our system, Health Cash, will be what funds the miners and data silos. The currency can also be used to activate smart contracts or trade for keys. The goal of this design is to create a blockchain system that can pass the requirements of healthcare by ensuring better data integrity and providing a validation system to ensure the miners running this network are compliant entities. In the following sections we will go through the details of the blockchain system, the decentralized database, the governance system, and finally, system specifics.

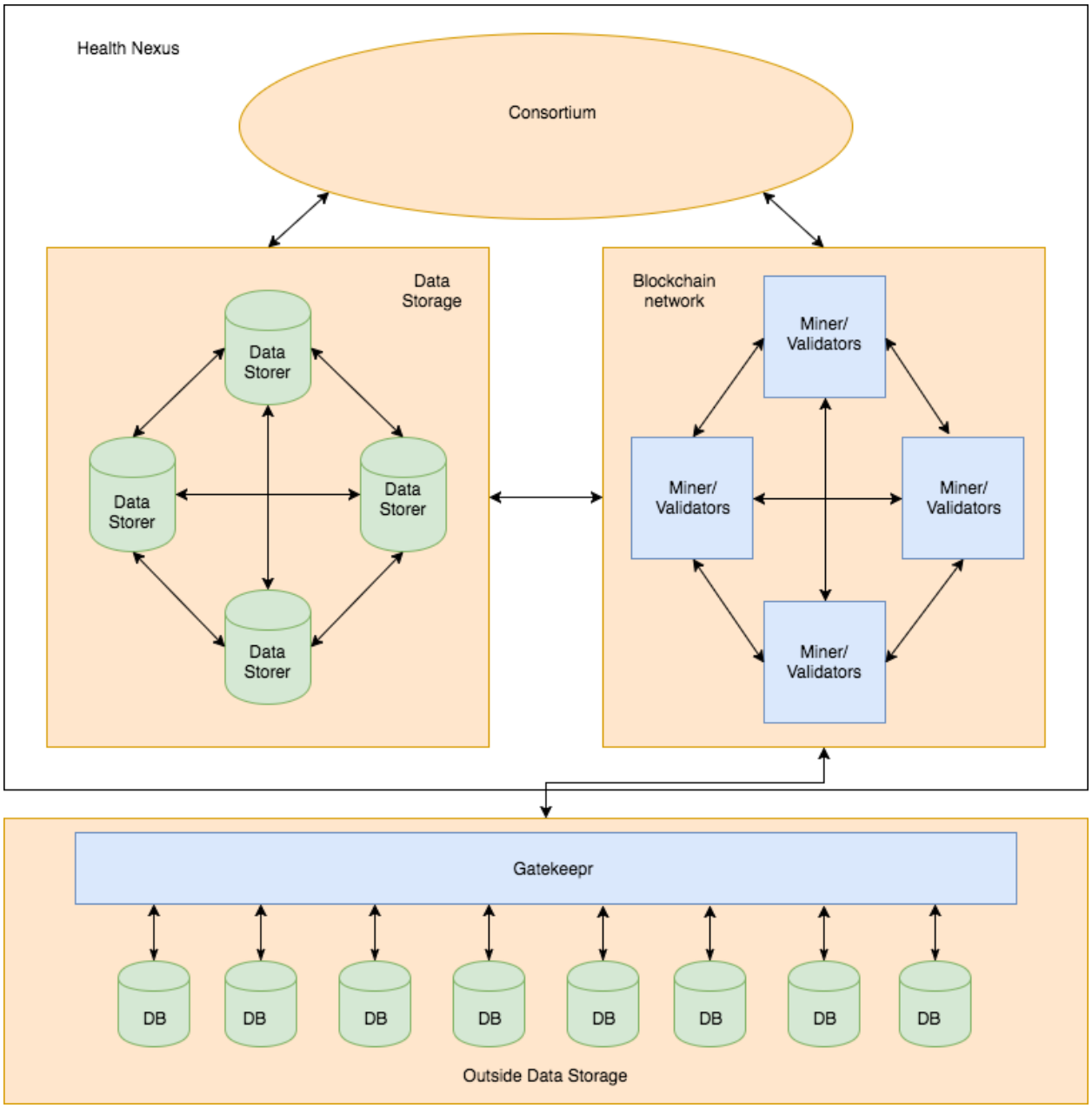


Figure 1: Diagram of Health Nexus system

In addition, we will be providing day-one usability in the form of a smart contract market place. This marketplace will allow for the creation, management, buying, selling, and sharing of permissioned keys that will allow access to off-chain data. This design will allow users to to use our tokens to manage their data via the blockchain on day one and provide a Proof of Concept tool for hospitals. Later on, we will perform a 1-to-1 conversion to Health Cash 2.0, which is presented in more detail in the road map.

Token

There are several benefits to establishing a new token. Due to the strict regulations around privacy and security in the industry, healthcare processes and data sharing capabilities will need to be run on a dedicated Blockchain system. As such, there would be several interoperability issues if another currency is used. Other currencies, like Ether, would not be able to function appropriately with a HIPAA-compliant system and Healthcare to achieve its maximum value due to its openness and lack of governance.

With a focus on security at the core, this token will also be able to:

1. Reward miners/validators and data storage devices that run our ecosystem;
2. Provide an extra incentive for early adopters of the platform;
3. Provide a transaction currency that allows one the ability to buy and sell medical data in real time and take part in the previously mentioned medical application system;

As such, people will need the token to be able to transfer permissioned keys giving access to off-chain data, access smart contracts and data storage space which will involve the selling of the token. The token will be used by the people involved in the transaction and used to pay node fees for running the network. The only way to earn tokens, without buying or trading for them, would be to operate a node on the network and receive payments from running the network.

As mentioned previously a percentage of these tokens will be set aside for to help accelerate adoption by already existing entities. To entice health care providers to adopt our platform, we are using a similar system that Paypal and GUP successfully used, which will include a referral program.

Governance

HIPAA compliance and the extra security needed by hospitals requires a new governance model. This new governance model requires special privileges to be granted to the governing consortium in the form of executive user IDs, which will be in the form of tokens. This will create a permissioned blockchain [3] with high security and public access to transact keys, tokens, smart contracts. These user IDs will allow these users to give out other special user privileges, also in the form of executive tokens. Any base account can trade tokens, activate and add smart contracts and add data and keys to the system; however, the only users who can allow new nodes to join the Blockchain service, join the data storage service, or push updates, are the entities with executive IDs.

To ensure a robust network with no middlemen, there are several ways to attain executive ID to join the governing consortium. Initially, SimplyVital Health and any major partners who have volunteered to perform this mission will have their executive IDs seeded in the genesis block. After that there are several primary ways:

1. An existing consortium member may issue you an ID, given there is 60% approval from the other consortium members
2. An existing consortium member may propose a new member, and the validators and consortium members, approve of it with a simple majority and no quorum
3. Validators may propose new consortium members and, with a simple majority

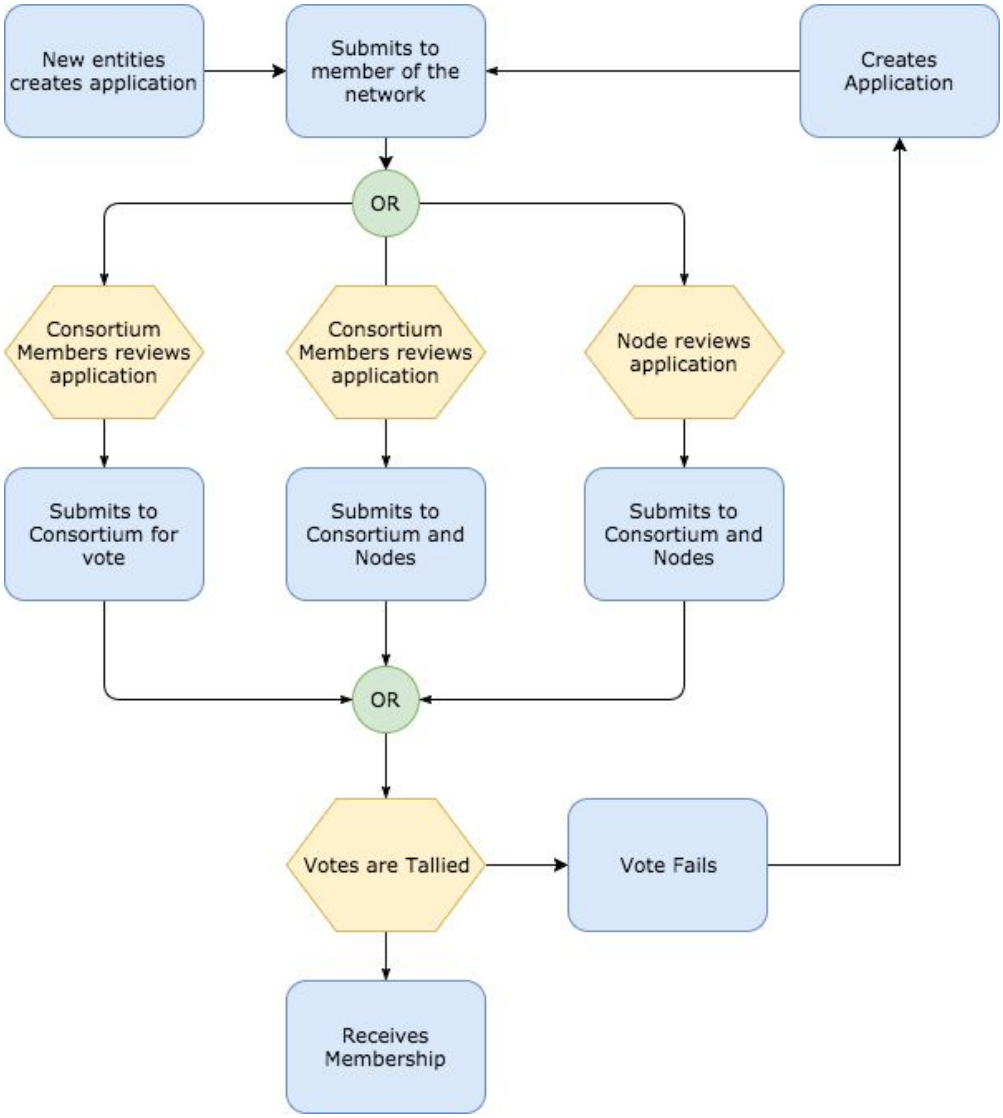


Figure 2: Workflow for becoming a member of the Health Nexus Consortium

In addition, an executive ID may be taken away. They may be taken away when either a stakeholder or consortium member submits a proposal and a certain percentage of the consortium vote and a certain percentage of the stakeholders with 51% of quorum.

Private health care providers will likely not be comfortable with either storing their data in public servers or allowing public servers to perform these computations. As such, the governing consortium will provide a verification/audit service. This verification service will involve the

governing consortium checking that the entities running servers are currently HIPAA certified and that the entities are active administrators checking for their nodes. In case there is a breach, the consortium can quickly push an update to fix the breach and in addition since the data is not directly stored on the blockchain but on an encrypted database, the data will be fine. Once certified they will be issued a Provider ID, which will allow them to create a miner node and a data storage node, and in addition create more provider IDs attached to their entities. Meanwhile the governing consortium will keep track of these healthcare entities and ensure that they are meeting compliances. Should a provider fail the compliance check their key will either be allowed to expire or the entity that granted them the key may take it back. In addition, in case of a large breach, other members can vote to have the permission taken away with a 60% positive vote. While there are several other models we have considered, including public servers or having a GNT inspired validation system, this system will need to be run on a Permissioned Blockchain, which our governance model will allow for. This need is due to current HIPAA requirements and the current status of the providers. It will remain open to the public to use, but only validated entities will be allowed to operate it.

For updating, all update changes will be proposed by the governing consortium who will have to have their special executive ID in their wallet to propose a change. These changes will take place over an election cycle that will last a certain number of blocks. This time length can be change in future updates. During this period, the update process is broken up into four periods. In the first periods, updates are proposed to the network and stakeholders are allowed to vote on for approval. In the second period, the update with the most approval will go to vote again with the votes either being a yay, nay, or abstain. During the third quarter, if the vote was approved the updated protocol replaces the protocol in testing. Finally, after running for the entire third session, the update is voted on one last time before being pushed forward. There are a few things that should be noted: This system will currently not require any quorum for the majority of the decisions. That is due to the potential lack of responsiveness on behalf of the network in non-tech related fields. Quorum will be further looked into, and may be added later. Should nothing be approved during the second period, the first period immediately restarts. Additionally, in cases of emergency, should the governing consortium find a critical bug or malicious code, the governing consortium can immediately push an update with a positive vote of 60%. This is the current method, and is due to the critical nature of the data being provided. This may change during testing or via an update.

One potential issue with this system is that a consortium member could try to add miners to the system to try to seize control through a 51% attack. To defend against this attack, should a consortium member try to add more than a certain percentage of new miners to a network, then there will be a vote of approval from among the consortium members to grant that increase.

The governing consortium is not a middleman and all individuals will be allowed to interact with the chain; however, due to the sensitive nature of this system the governing consortium will be needed to help maintain the system and provide verification. As such the governing consortium may either individually charge fees for verification and update purpose solely to the miners, who will be making a profit off of mining these blocks.

As will be mentioned in future plans. Further down the line, when this is more established with more industry adoption, we will look closely at other models more similar to Tezos or GNT. Currently, we will stick with our current model to drive further industry adoption.

Smart Contract Blockchain

Our Health Nexus Blockchain protocol and token is based on the Ethereum protocol, which is an open source Blockchain with distributed computing for smart contracts. Smart contracts are state-based, immutable programs stored on the chain, which can guarantee the contract's actions.

We have added a few modifications on top of Ethereum. First, similar to our data storage nodes (which are detailed in following sections), miners/validators will be certified ahead of time and will be sent a special node ID to their node address to certify them. The next difference from Ethereum is the ability of the user to transfer our token, Health Cash, along with several other types of data like permissioned key pairs for data access. The user will be able to store their public identification keys, and any other keys they generated, to access or edit their data. These keys allow access to their data through the use of special gatekeepers that will either be a special authentication server, which sits in front of the data, or the blockchain system itself if a distributed data storage system is proven effective. A user will also be able to store the key used to certify miners/validators and data storage nodes, these keys will given out by the governing consortium and will act as a whitelist, as further detailed in the governance section.

This whitelisting system is specifically designed to meet the requirements of HIPAA compliance. The whitelist exists to focus on healthcare security compliance. Due to ongoing research by others including MedRec [4], which goes in depth to this key system, we have strong reason to believe that this approach will aid compliance with HIPAA regulation and be able to be quickly adopted by healthcare.

The last major difference is that a user will be able to store a contract state for their data storage node if they are a Health Nexus data storage center, as further detailed in the data storage section. In the upcoming sections we will discuss these specifications in more technical detail as well as touch on other main aspects of our Blockchain technology. It is important to note that this will be a large fork of the existing Ethereum project. Tendermint or Parity could be a stepping stone, so we are investigating these as possibilities.

Accounts

In Health Nexus, like Ethereum, our state on the blockchain is made up of objects. We have the 4 fields mentioned in Ethereum which are the nonce, crypto currency balance, contract code, and storage. In addition, we will have a key storage section along with a valid miner/storer ID and an executive ID. These will allow users to keep track of their identities and their ability to

mine or store data. Health Cash (HLTH) is the fuel of this network, and is used to pay transaction fees, fuel smart contracts, and provide liquidity to medical data and identities stored in the system. In addition, there are two contracts with which a user will interact: the first is similar to its counterpart on the Ethereum network, the other is a data storage contract, which will use its contract field to handle the data storage account in a safe and migratable manner.

Messages and Transactions

Within the Health Nexus system, transactions on the blockchain protocol will function very similarly to the Ethereum network with a recipient, signature, amount of HLTH, optional data field, STARTGAS, and GASPRICE.

Messages are also very similar to their Ethereum-based counterpart and contains the same fields, which include the sender, recipient, amount of ether, optional data field, and STARTGAS value, are sendable only as contracts, and exist only in the execution environment.

In addition, we are looking into either adding in an identity field for trading identities or keeping that in the optional data field for Message and Transactions.

Distributed Consensus

Our system will start out by utilizing proof of stake. We will continue to assess further updates to our system based on methods listed in the future section, which will include systems using proof of burn and proof of authority, based on available resources with dedicate time at phase 5.

Data Storage

Our database system utilizes a Distributed Hash table to manage a specially modified Kademlia table to securely store data [5] with it being based on the system explained in Storj [6]. In this section, we describe in more detail our data storage section with our intention being to start with a system based off Storj and make changes to make it useable by healthcare. When phase 4 is reached, we will release a supplemental white paper that will detail the system and necessary changes. We will write a supplemental white paper because our development of our distributed data storage system will be further in our development plan and new techniques may have emerged by then.

Signature for Data Storage

For nodes to send messages back and forth to each other, much like S/Kademlia, they have to sign their messages. When joining the network, a node creates an ECDSA key pair, a public and private key, with the Node ID corresponding to a hash of the public key. This Node ID also corresponds to its Health Nexus wallet address. Its public key will also be assigned to this address in the wallets identity system. A node will sign every message before sending the message out, and the retrieving nodes will verify that message in turn by checking the wallet address for a storage node token. This upgrade greatly increases the security of the system by helping to prevent eclipse attacks and ensuring only verified miners can take part. It also allows an individual to make requests to individual storage nodes for specific security situations.

Data Storage Contracts

The storage of data is negotiated via state channels and stored via smart contracts on the Blockchain. These contracts will be standardized with the same API and function calls, and will hold basic data necessary for all aspects of the relationship between the data store and the user. Both sides should store this information, and we will plan on allowing them to store this on the Blockchain to provide continuous auditing.

There will be an automated publisher and subscriber market place for this system. This system will be built in by modifying the Kademlia DHT. A partially filled contract for every node will be stored as a smart contract attached to the node's wallet ID. This partially filled contract contains all the information on the data storage provider and what they are charging. This value can also be easily updated by the data storage provider by pushing to their smart contract on their chain. As such, when the DHT is being formed or updated the lookup code for the partially filled out smart contract is added. For a user to find and negotiate this contract they can proceed through the DHT table while pinging the blockchain network for information on the smart contract. When a contract with the appropriate parameters is found, the user may either accept the contract and route the appropriate payment to the contract to be given to the wallet address or may counter offer a second set of parameters for the contract for the database owner to decide on. The database owner may then either accept, decline, or continue the negotiation via the negotiating mechanisms. Once the contract is decided, the contract is finalized and activated giving the user the ability to use the given storage space. This is a newer system and we believe that it will provide both better latency and a better data storage market place than the currently used Quasar method [7], which utilizes Bloom filters [8]. In addition, this method will allow for two other useful features: it will be much easier for a user or service provider to quickly sample the network to see what the current price for data storage is, which will be very important to a hospital center; and will allow a user to directly contact a single data node if they choose to without having to do a DHT look up. This will allow users with sensitive data to seek out specific data storage providers that could provide them more secure databases.

We will start off by using the existing system, based off StorJ [6], then work on this new approach. An additional service may also come later. Since all the miners' contracts are located on the blockchain and associated with a certain data storer permissioning ID, a

consortium member or user could create a market place by constantly reading through the chain and checking on the current statuses.

We will also look at combining Quasar with this method and updating Quasar with a Bloom filter replacement. The combined form will feature a Quasar Bloom filter within the DHT for each node, and each node will update the filters corresponding to its neighbors as its updating its table and then update its own filter. In addition, we will look at subbing the filter out with other potential filters which include Pagh et al. [9], Cache-Hash-Space-Efficient Bloom Filters [10], and cuckoo filters [11] during phase 5. We will start with cuckoo filters since there is already an open source and easy-to-adopt version available.We will have a better idea of which to adopt as we do efficiency testing to assess which is the best method.

Payments

While in general the payment method for this system isn't set in stone and is up to the individual users, we are assuming users will use Health Cash (HLTH) for transfer and payments. There are several other ways to configure for payments. A user can request that audits or partial audits be paired with their payments to ensure proper storage by submitting said request to a member of the governing consortium who has agreed to the service. To help secure that, future areas of research will be done to create permissioned keys for performing audits to insure compliance. In addition, we will be looking into state channels, as previously mentioned, in the future. State channels would allow the user and data storage to communicate and handle payments directly lowering the amount of stress put on this Health Nexus.

Process for Storing Data

Steps	**Description**
1	Proceed Through DHT
2	Either find contract through Blockchain lookup or basic data provided on DHT
3	Message the blockchain address with valid contract data based on the information provided
4	Either Address accepts, responds with a counter offer sending you to the previous step, or rejects in which case you proceed back to step 1
5	If accepted, you're given permission to store data
6	Proceed through the process of encrypting, sharding and storing data
7	Either pay directly every time through the chain or setup a micropayments channel to be handled at the end of a predetermined amount of time

8	Message the blockchain for partial and full audits at leisure

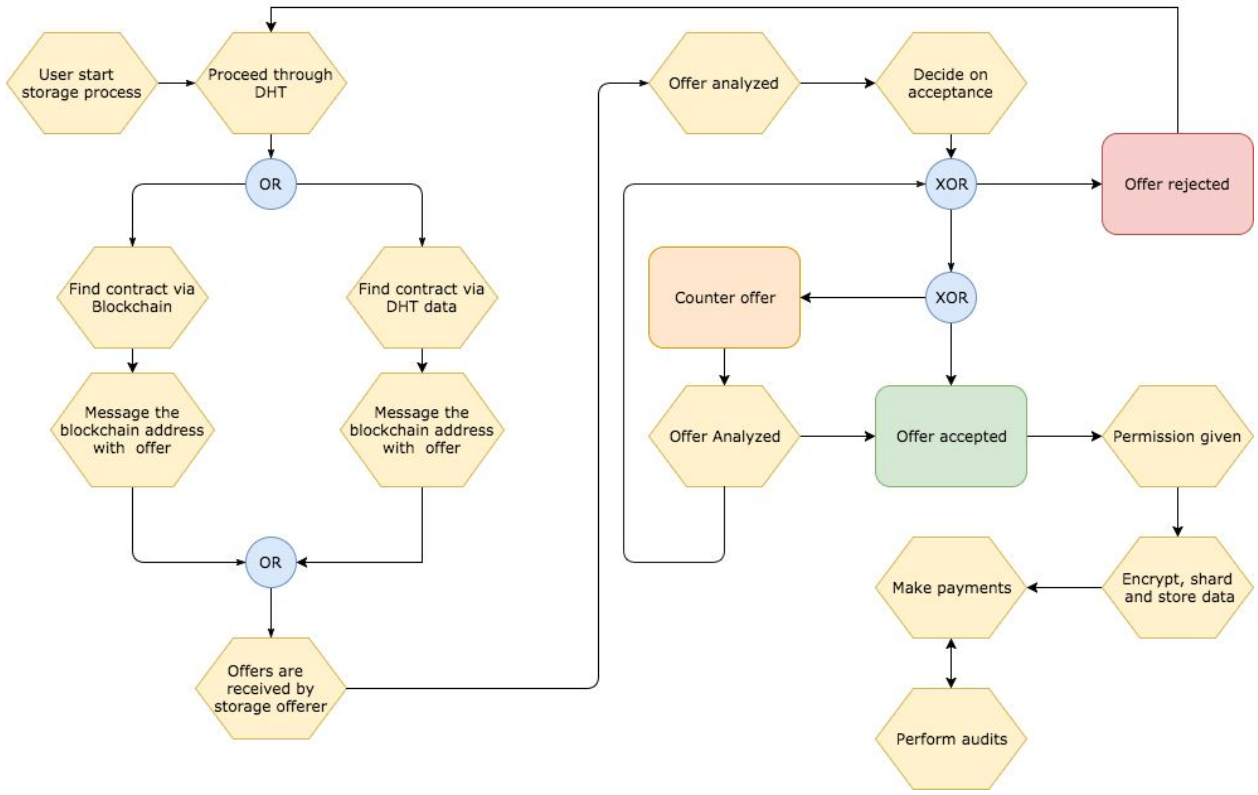


Figure 4: Table and diagram for the process of storing data

Redundancy

In addition to the built in redundancy systems, we will be continuing to trial new error correction codes, such as Bose–Chaudhuri–Hocquenghem (BCH) and should they be found to be reliable, will either replace the old method or be added as an option to switch to. While we will start with the same Reed-Solomon [12] protocol as StorJ does. In addition, we will be continuing to trial new error correction coding like BCH and should they be found to be reliable, will either replace the old method or be added as an option to switch to.

Insurance

We are also working on creating an insurance contract templates to allow people to have contract insurance, or creating a mandatory insurance section for smart contracts and data storage. This strategy will provide an extra level of security that could help provide further legitimacy for health care, and will be based on “Securing the Assets of Decentralized Applications using Financial Derivatives” [1].

Database

In the first phase, levelDB will be used to store the data of blocks. LevelDB is a key-value store. Several useful features include long-term support and high performing reads. The main reason for Health Nexus using levelDB initially is due to its compact size and its successful track record of working with the Bitcoin core and geth client. This most likely will not be efficient enough and other systems will be immediately looked into.

As such, a few improvements will be pursued and tested during the outlined roadmap. The first being the creation of smaller levelDB instances that are created ad hoc for precise database usage. The second would be using LMDB, which is more efficient than levelDB, less prone to corruption, and has been trialed in Monero.

CryptoGraphic Hash Function
SHA256

Encryption
AES-256

Licensing
Apache License, Version 2.0
We have come to this licensing after working with our lawyers and partners. This license will provide both the right mix of open source capabilities with protections allowing for both the open source community and health care entities to take part.

Key System

Currently users will create new keys via ECDSA key pair creation that will be added to their Health Nexus wallet. When added, using their first key, they will be able to permission and delete these keys with their private wallet key.

Road Map

The road map of our system is designed in phases, allowing for continuous development and stand alone business cases. The code will be viewable on github. In addition each milestone shall have research done beforehand, with the results published in a white paper.

It is important to note several things about the stages: We would like for each phase to be able to stand alone and generate value without requiring the next phases to take place. This is designed due to the strict security restrictions and late-adopter practice in healthcare. Thus if something goes wrong with one of the phases, the distributed system can still continue to function and provide value. The schedule and roadmap will also be updated for new developments and unforeseen events. Every stage will have additional functionality.

The goal is to accomplish this road map in 4 years. The first phase will be finished and available by the token sale. The next 3 stages we are estimating a year to complete for each. Once all these stages are complete, while there are future plans as described in the Future Areas of Research section, we plan on the community and consortium leading further growth and development with us continue to contribute to for an additional year. After words we will work on additional research and open source UI tools. The status of our network can also be tracked via this github repository.

Phase 1

Our first stage will be deploying an ERC 20 Token that will allow users to store keys/URLs on the Ethereum Blockchain. In addition to the keys/URLs, additional data including permissioning will be included. The created key will also be able to

- Create children keys
- Manage children keys
- Be bought, sold and shared
- Store access for outside data storage

Using these keys, a person can give a permissioned key to another user. That user can then access the URL attached to the key for data. The server at the URL endpoint can check the signature of the message and the key on the blockchain to insure its a valid user before giving out access, which will function as the gatekeeper we earlier mentioned. This will allow users to store, track, and manage permissioned access on the blockchain and in addition it will give healthcare a product to trial out into the future. This is designed to insure day one capabilities as we continue to flesh out our system further and is based on research done by Medrec[4].

Phase 2

Our second stage will be building our initial Blockchain ecosystem. Our initial ecosystem will have the built in governance solution, currency transaction, and the ability to run smart contracts. Users at this stage can

- trade their currency;
- run HIPAA compliant smart contracts;
- generate their own apps;
- and basic UI and CLI.

As such, users can generate their own apps, allowing them to build health data marketplaces, apps that allow one to interact with pharmacies, and for automated insurance markets. This stage will also be fully released on github when we have several partners in the governing consortium.

Phase 3

The next phase will be adding in the ability to create and store keys and the creation of the consortium and network. As such this stage will allow for:

- The transferring of health care data through keys that could correspond to either a url or a password for a different system.

- A developer SDK.
- A Health Cash web client and Provider dashboard.
- The conversion of the initial ERC20 token 1 to 1 for HLTH 2.0 on the new blockchain.

The consortium members and network will also be expanded and fully created at this point. We attend to have a working consortium prior to the end of this stage and once we have large consortium, the network will go fully public. We are waiting for this stage to fill the consortium and go public for two reasons. Firstly, once the consortium is created it will be much more difficult to guide the creation of the platform. Secondly, in order to insure legal compliance we must ensure a large network of miners and consortium members prior to launch.

Phase 4

The final stage will involve the secure data storage layer. This will require the most trust from healthcare providers and is the most theoretical, as such it is being scheduled last. This will allow hospitals to securely store their data and share their data in real time on Health Nexus without allowing access to their current system via keys and will allow for real time data analytics. This phase could take longer than projected as that we will have to work in depth with healthcare providers to insure HIPAA compliance; however, we have allocated extra time for its design and have insured the steps before it can constitute a valid blockchain in case of delays.

Phase 5

Going into the future, after we have finished the portions outlined we will be planning on the overall consortium and open source community to continue to drive future developments. SimplyVital Health will continue to contribute but at this point we will have given most of our ability to drive the system to the consortium and view the consortium and open source community to be a better driver. If we reach are hard cap we will continue to work on the system based on the areas mentioned in future research for another year after the last phase. Based on ongoing development and research we may escalate these to our existing road map earlier; however, if not we will look into them at this phase.

Future Areas of Research

When the roadmap is complete ,we will step away from the continued development of this blockchain system. Our plan is to let the community and fellow consortium members continue upgrading the system in the future to insure its long term decentralization. That is not to say we will not continue to contribute and we plan on working on these contributions fully for an additional year if we receive max fundings. We may also get to some of these earlier than planned, we primarily are including these in the future section because most of these are still in the theory phase and we do not want to make promises we can not implement. In the proceeding sections are areas we are interested in doing further research and implementation on after the road map has been completed. A report or white paper will be released before any major area of research is implemented to further flesh out the design.

Contract Code Execution

After the road map is complete, we will look into slight changes to the protocol to handle potential downside of a Turing-complete script, which is that the number of potential steps for a script is unbounded. We will specifically be looking into how Tezos purposes dealing with this problem [13]. To solve this issue, a cap on the maximum number steps for a contract to run on a single transaction will be issued. This cap will be updateable through the governance system in the future. If a contract needs more steps, prior to an update, it may simply continue the contract by performing it in multiple transactions. This will help to prevent denial-of-service attacks via CPU usage.

Proof of Authority

In proof of authority, certain nodes are granted the ability to contribute blocks and nodes vote on which block to be added to the chain. With the extra level of trust on this permissioned system this consensus protocol will have a higher chance of success. That being said it does not currently have a proven track record, as such more research and testing will have to be done. In addition this change would not take place till after the full distributed system is launched that way it may be put to a vote to the governing consortium to insure the solution is supported by the community..

Oracles

Oracles can be used to push data to the blockchain and we are very interested in integrating them into our system. This would be incredibly useful technology to integrate into this system and the healthcare industry is already interested in this ability.

Public servers and databases

We plan on researching the HIPAA compliance involved in making the system entirely public and taking away the executive branch's ability to govern what miners and data storers are on the system. We will work with our healthcare partners to see if this is possible, but this is far down the road and unlikely.

Reputation or Validation system

Looking at other systems, it may be possible to add in a validation system, where any user can hop on as a data storage system, but they can build a reputation or be validated by other entities to build trustworthiness. This in turn could replace the executive branch’s ability to add in data storage centers via tokens but would also in phase 5 or beyond.

Quorum-Voting

Currently there is no Quorum required for the votes, this is due to potential voters not being able to be counted on showing up. We plan to consider and include Quorum, however, first we will gather validation from the testing phase to ensure if instituted, the miners, can be relied on to vote.

Parity algorithm

While we are using Reed–Solomon for parity right now, we will investigate other parity algorithms to try to ensure the best system is used, this includes investigating Bose–Chaudhuri–Hocquenghem(BCH) codes.

LMDB

The Lightning Memory-Mapped Database is a B+ Tree that is similar to Berkeley DB and is a high performance key-value store. It out performs levelDB in all read and batch write operations and in additional is significantly more reliable in data integrity then levelDB. As such we plan to do research into replacing levelDB with LMDB.

State Channels

When performing a transaction, the only people who need to know about the transaction are the ones who perform it. As such, state channels allow users to initiate a state on the blockchain, in our case through a smart contract, and proceed to simply send signed updates to each other to confirm. This allows much greater latency on our network by removing the a large number of transactions from having to be settled and just putting the final state. As such we will be doing further research to ensure state channels can properly function.

Attacks

We have dedicate a specific section to attacks due to the sensitive nature of healthcare. Specifically healthcare focused cyber attacks have risen 320% from 2015 to 2016. We are going over recent examples and new techniques that our system will provide on top of current blockchain fixes.

Ransomware

As shown via WannaCry, ransom ware can be a massive problem for the modern healthcare ecosystem. By storing their data and apps on secure, redundant and immutable systems,

health care can prevent an attack like this from happening. Should their personal machines get taken down they can just simply access this system through other secure devices and continue to operate. As such Health Nexus is uniquely suited to deal with this issue.

Identity hijacking

Identity hijacking, which is where a node's ID is stolen, is prevented by requiring all the Node IDs to be public key hashes and requiring all messages to be signed. This approach will prevent a malicious agent from impersonating any other node.

Sybil Attacks

In a Sybil attack, the malicious entity gains a large amount of influence on the system by creating a large number of fake nodes. Along with traditional mechanism that come from using a Kademlia system to defend against this, the added identity protection should also help to mitigate the risks to this attack.

Eclipse Attacks

In an Eclipse attack a malicious entity tries to surround our node with their malicious nodes in order to ensure all outbound connections go through the fraudulent entities. In order to deal with this, every data storage node uses a public hash key from the blockchain. This means for an entity to perform an eclipse attack they would have to continuously until it finds the three closes hash ids and most defend its position which is preventively difficult and also gets more difficult as the system grows. This system provides an additional defense, they would need to generate existing hash keys to gain access to the correct privilege token, otherwise the given node will not respond to it.

Hostage Bytes

This is a storage specific attack where a fraudulent farm holds your data hostage. The standard way to take care of this would be to mirror your files. This system provides additional protection, because the miners and data storers are vetted, a fraudulent entity can have their privileges revoked by the executive branch.

Frequently Asked Questions

1. Why build an entirely new platform, instead of building on top of that already exists?

    a. To clarify we are not starting entirely from scratch. We will be forking an existing branch of the Ethereum Network to start. In addition none of the existing platforms have the capabilities need for healthcare
2. Why not just build on top of a platform that already has a permissioned ledger with private transactions?
    a. There are several reasons for this. While there are a few permissioned ledgers we are looking at that have previously been mentioned as a starting point. Most of these were not built with healthcare input and are still fairly untested when compared to the main branch of Ethereum. This leads us to make this decision to start from one of the aforementioned branches based on reliability and certain features we believe are necessary.
3. Why use blockchain at all?
    a. The reason for blockchain is not a technical reason, it is because of trust. Health Care needs an auditable and trustless system to truly allow data sharing, buying and selling.
4. What is the current state of product by SV?
    a. We have our current blockchain product in production and have our first customers. It currently creates an audit trail of transactions and provides an analytics platform on that

References

[1] George Bissias, Brian Levine, Nikunj Kapadia. Securing the Assets of Decentralized Applications using Financial Derivatives (2017). https://arxiv.org/abs/1701.03945.

[2] Vitalik Buterin. Slasher: A punitive proof-of-stake algorithm (2014). https://blog.ethereum.org/2014/01/15/ slasher-a-punitive-proof-of-stake-algorithm/.

[3] Hashed Health. DECENTRALIZED HEALTH NETWORKS. https://hashedhealth.com/decentralized-health-networks/, 2017.

[4] Thiago Vieira Joe Paradiso Andrew Lippman Ariel Ekblaw Asaf Azaria. MedRec (2016). www.pubpub.org/pub/medrec.

[5] P. Maymounkov, D. Mazieres. Kademlia: A peer-to-peer information system. based on the xor metric (2002). https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf.

[6] Shawn Wilkinson, Tome Boshevski, Tome Boshevski, James Prestwich, Gordon Hall, Patrick Gerbes, Philip Hutchins, Chris Pollard. Storj A Peer-to-Peer Cloud Storage Network (2016). https://storj.io/storj.pdf.

[7] G. Hall. Kad quasar, (2016). https://github.com/kadtools/kad-quasar.

[8] B. Bloom. Space/time trade-offs in hash coding with allowable errors, (1970). http://dmod.eu/deca/ft gateway.cfm.pdf.

[9] A. Pagh, R. Pagh, and S. S. Rao. An optimal bloom filter replacement. In Proc. ASM-SIAM Symposium on Discrete Algorithms, SODA (2005).

[10] Putze, F.; Sanders, P.; Singler, J. "Cache-, Hash- and Space-Efficient Bloom Filters", in Demetrescu, Camil, *Experimental Algorithms, 6th International Workshop, WEA 2007* (PDF), Lecture Notes in Computer Science, **4525**, Springer-Verlag, Lecture Notes in Computer Science 4525, pp. 108–121, ISBN 978-3-540-72844-3, doi:10.1007/978-3-540-72845-0 (2007).

[11] Fan, Bin; Andersen, Dave G.; Kaminsky, Michael; Mitzenmacher, Michael D. "Cuckoo filter: Practically better than Bloom", *Proc. 10th ACM Int. Conf. Emerging*

Networking Experiments and Technologies (CoNEXT '14), pp. 75–88,doi:10.1145/2674005.2674994 (2014).

[12] J. S. Plank. A tutorial on reed-solomon coding for fault-tolerance in raid-like systems, (1996). http://web.eecs.utk.edu/~plank/plank/papers/CS-96-332.pdf.

[13] L.M Goodman. Tezos — a self-amending crypto-ledger White paper. https://www.tezos.com/static/papers/white_paper.pdf, 2014.

