INTRODUCING THE

EXOCHAIN™ NETWORK

EXOCHAIN is a blockchain-based platform that embraces adjudicated identity for legal protection within smart contracts. EXOCHAIN's EXO™ protocol use token establishes a framework for delivering patient-centric healthcare with systems-based, safe, clinical research.

Authors:
Konrad Rauscher, Bob Stewart, Anthony Buonomo

July 2018

The following pages describe EXOCHAIN's vision for the digital world's first identity rating system.

> The Internet reconfigures accessibility.
>
> - **Prof. Bill Dutton**, former director of the Oxford Internet Institute

> Computing is headed irreversibly into the realm of verified systems capable of complete security and transparency for the benefit of all.
>
> - **Bob Stewart**, EXOCHAIN founder

> EXOCHAIN reconfigures accessibility as being intrinsically tied to identity such that access is programmatically defined by the stakeholder(s) pertinent to every conceivable set of data.
>
> There exists an incipient need for ownership of identity to be redistributed back to the primary stakeholder(s) corresponding to each identity. The 'free-access' models, that extensively comprise the current digital services paradigm, in actuality undermine the self-sovereignty of end-users and increase the susceptibility of end-users to infringements upon the security and privacy of data associated with their personal identity.
>
> - **Konrad Rauscher**, EXOCHAIN engineer

Table of Contents

Note: the introduction section is intended for those new to blockchain paradigms and the Ethereum ecosystem.

Status Note

This is the second version of this document. The first version was published August 21st, 2017 in conjunction with an initial distribution amongst industry stakeholders. This second version is being published on December 31st, 2017, in tandem with the launch of EXOCHAIN's token presale.

The white paper will be maintained by EXOCHAIN. Subsequent versions are presently anticipated to contain the following enlargements:

- Value Chain Mapping and Token Economics
- Technical diagrams detailing service delivery architecture
- Expanded engagement w/ EXOCHAIN's value-added for regulatory compliance.
- Regulatory FDA and SEC compliance
- Future Markets
- . . .

Executive Summary

Over the course of the second half of the 20th century and into the 21st, the primary driver for the digitization of interaction between human and non-human entities was a desire (on the part of governments, businesses, and individuals alike) to acquire a competitive edge. A desire to develop and deploy technology expanded capacities and increased productivity *as quickly as possible* led to unprecedented economic growth and human advancement. However, participants in the digital world have been increasingly paying a cost (in such forms as privacy compromises, data theft, dampened resiliency of services, undermined data integrity, and subverted data sovereignty) in the aftermath of a race towards functionality and capacities that did not adequately incorporate a consideration for the implications and security *of,* and human nature's relation *to,* such technologies.

Identity enables us to keep track of entities (people, corporations, machines, etc), and their relationships. In a world with complex interrelationships between billions of entities, private, untamperable, and secure identity management is essential. Unfortunately, the designers of digital systems have thus far failed to (1) adequately consider external effects, and (2) to accurately distinguish personally-identifiable-information (PII) from non-PII. Due to these failings digital systems easily compromise real-world identities. Moreover, when these interconnected systems are built without a core understanding of identity, human dignity may be inadvertently compromised through denial of self-expression, the placing of individuals in

harm's way, and the unintentional oppression of those who most need self-determination.[5] Subsequently, the fear which many harbor concerning the entities that track them--be they individuals, governments, or corporations--is justified.

The time is ripe for the construction of a new identity ecosystem due to the convergence of four factors: **[1, New Technology]** The introduction of the first blockchain-based network protocol (Ethereum), and subsequent access to blockchain features that are uniquely suited for identity management. We now exist in a development, familiarization, and adoption phase that is antecedent to the widespread rise and usage of blockchain-based technologies. **[2, Risk]** The ever-increasing value tied to digital identities means that the intrinsic flaws in current treatments and understandings of digital identities are becoming ever more costly. **[3, Market Norms]** End-users lack adequate sovereignty in determining how the data corresponding to their identity is used by corporations and others, particularly those that provide services vital for digitally-active agents. **[4, Future Technology]** Now that we are at the threshold of an Internet of Things, we need a new identity paradigm for when humans ubiquitously interact with inanimate and artificially intelligent objects.

Through a re-evaluation digital identity that utilizes some of the latest developments in networked computation (the blockchain-based protocol platform Ethereum, among others), the EXOCHAIN network will encompass a cost-of-compliance reducing framework for all regulated industries that allows end-users to reclaim sovereignty of their data. By tackling the issues affecting clinical research quality as a first use case, EXOCHAIN will demonstrate these capabilities, as well as its unique capacity to function as a catalyst for trust between entities. In the context of clinical research, this means allowing for trusted adjudications and attestations, patients to trust that their data will be better protected (through data sovereignty), and clinical researchers to have greater trust in the integrity of data.

EXOCHAIN will also deploy 0dentity, the first methodology for evaluating and subsequently scoring the extent to which a digital identity has been established. This score is dynamic in nature, such that interactions within, as well as those connected to the EXOCHAIN network will be reflected by 0dentity instantiations on a live basis. This ecosystem will simplify, secure, and add transparency to interactions between entities, allowing transactions between parties to take place on an ad hoc, and automatic basis. Because transactions within the EXOCHAIN blockchain function are recorded in a transparent manner, users are protected through historically and more clearly represented terms of engagement.

By rejecting anonymity and embracing identity, organizations interfaced via EXOCHAIN can be protected with acceptable know-your-client types of regulatory compliance requirements. Through EXOCHAIN's tokenized protocol, participants (including patients and healthcare professionals) who engage in self-adjudication will benefit from access to seamless release

[5] Andrieu, Joe. 'Rebooting the Web of Trust.' *GitHub.com*, Fall 2017.

authority, redundancy reduction, programmatic permission designations, and personal data protection through zero-knowledge-proof attestations.

An Introduction to Smart Contracts

Glossary of Key Terms & Explanation of Concepts

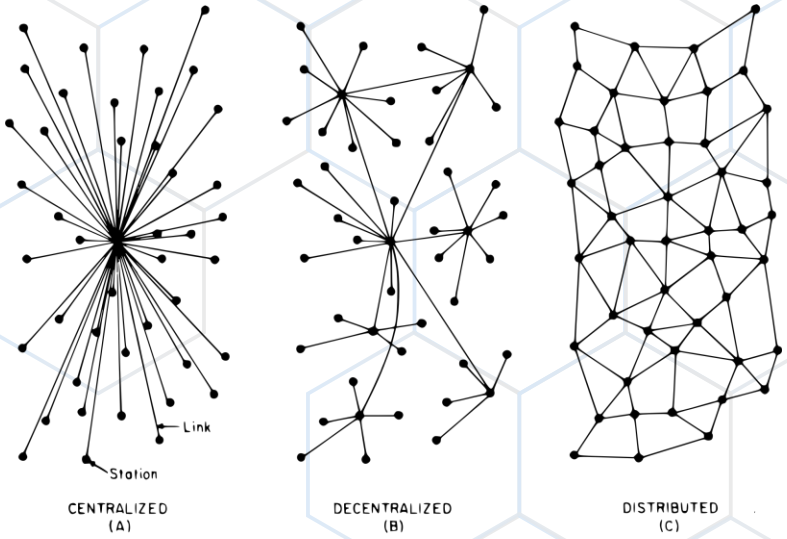


FIG. 1 — Centralized, Decentralized and Distributed Networks

Blockchain is, simply put, a database. Less simply, it is also a peer-to-peer (P2P) *distributed* ledger technology that enables transparent transactions and consensus systems. At this point, the term is semantically entangled with multiple concepts: a ledger, a technology, an application of a technology, and a new way of doing business. The first instantiation of a blockchain-based technology to achieve household name status is Bitcoin, a digital currency that does not rely on a central authority (such as the Federal Reserve) to clear financial transactions.

Analogy: In the 1980s, spreadsheets were first used to create ledgers of financial transactions (check registers, balance statements, etc.). Fast-forward to today, and spreadsheets can be used to create full-blown applications that track inventory, catalog assets, and create predictive charts. The same can be said of blockchain: first it was used to create a ledger of financial transactions (Bitcoin), and now it is being experimented with to track shipping documents, clinical studies, and drugs through the supply chain.

Blockchain technology has its own vocabulary for structures and behaviors (blocks, nodes, hash values, Merkle trees, etc.), much as spreadsheets have their own (rows, columns, pivot tables, functions, macros, etc.). Remember when you first used spreadsheets: rows, columns, functions, and macros were confusing. There seemed to be multiple ways of getting something done (function, macro, visual basic), and each required a new level of knowledge. Given a little exploration, each new way unlocked a larger world of flexibility and possibilities. As we are at the beginning of the evolution of blockchain technology, many companies and coalitions are experimenting with and

improving the underlying capabilities. There are differences in the vocabularies associated with each Blockchain "brand," just as VisiCalc, Lotus 1-2-3, and Microsoft Excel each provided the same functionality in a slightly different way using their own vocabulary.[6]

How Blockchain Works

Technical:

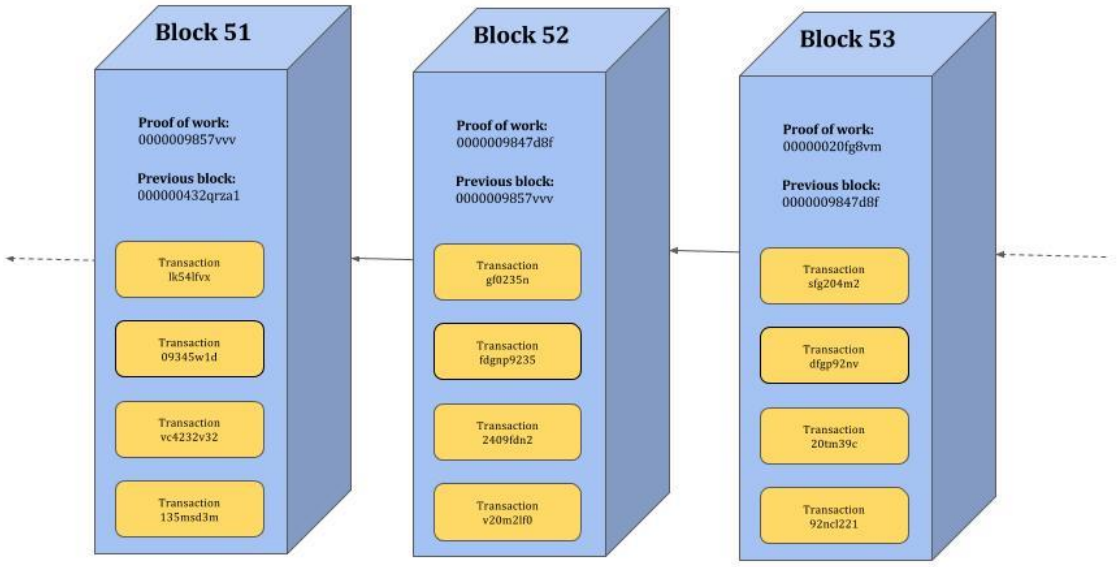
Although blockchain platforms differ, they typically share a common approach — creating a ledger of digital transactions between parties that are distributed among many computers, which are called nodes. Blockchains are constructed to make data resistant to corruption by allowing the nodes to form a consensus about which data is legitimate and therefore allowed on the blockchain. The data itself is organized into a series of chronologically grouped transactions, or blocks, which are digitally signed. The hash value (any function that can be used to map data of arbitrary size to data of fixed size) of the previous block of data is included in the current block. All this adds up to a stable data set in which the author (person, system, or company) cannot deny they contributed their data (called nonrepudiation), and the data is protected from nefarious activity. Blockchains use consensus mechanisms and other security features (such as digital signatures, encryption, hash values, etc.) to accomplish this.[7]

Analogy:

To understand how several people are able to keep their copies of the database in sync with everyone else, imagine there are ten individuals in a network. Everyone is sitting with an empty file folder and an empty page in front of them. Whenever anyone does something important in the network, like a transfer of funds, they announce it to everyone in the network. Everyone makes a note of the announcement on their pages until the page is filled. When it does, everyone has to seal the contents of the page by solving a mathematical puzzle. Solving the mathematical puzzle ensures that everyone's page had same contents and that they can never be modified. Whoever does it first, gets rewarded (with some amount of cryptocurrency). Once the page is sealed, the page is added to the file folder, a new page is brought out and the process continues forever. As time passes, these pages (blocks) that contain important records (transactions) are added to the folder (chain), thus forming the database (blockchain). [8]

---

[6] Celeste, Bob. 'Is Blockchain The Solution To Drug Traceability?' *Pharmaceutical Online*, July 2017.
[7] Ibid.
[8] Mamoria, Mohit. 'WTF is Ethereum?' *Hackernoon*, Aug. 2017.



Abstraction of a blockchain section

The desired outcome of this complex framework is a secure environment in which transactions can be stored, data is protected, and access to data is made flexible through programmatically defined transactions. The key features obtained are: [1] Once data is stored in the database, it can never be modified or deleted. Every record on a blockchain is permanent. [2] No single individual or organization maintains the database; any conceivable number of individuals and/or machines do, and every participant has a copy of the database with themselves.[9]

Note: EXOCHAIN users will not be tasked with mathematical puzzles. The blockchain upon which EXOCHAIN will run will be be maintained via the Ethereum network, which manages such mining tasks.

Protocol

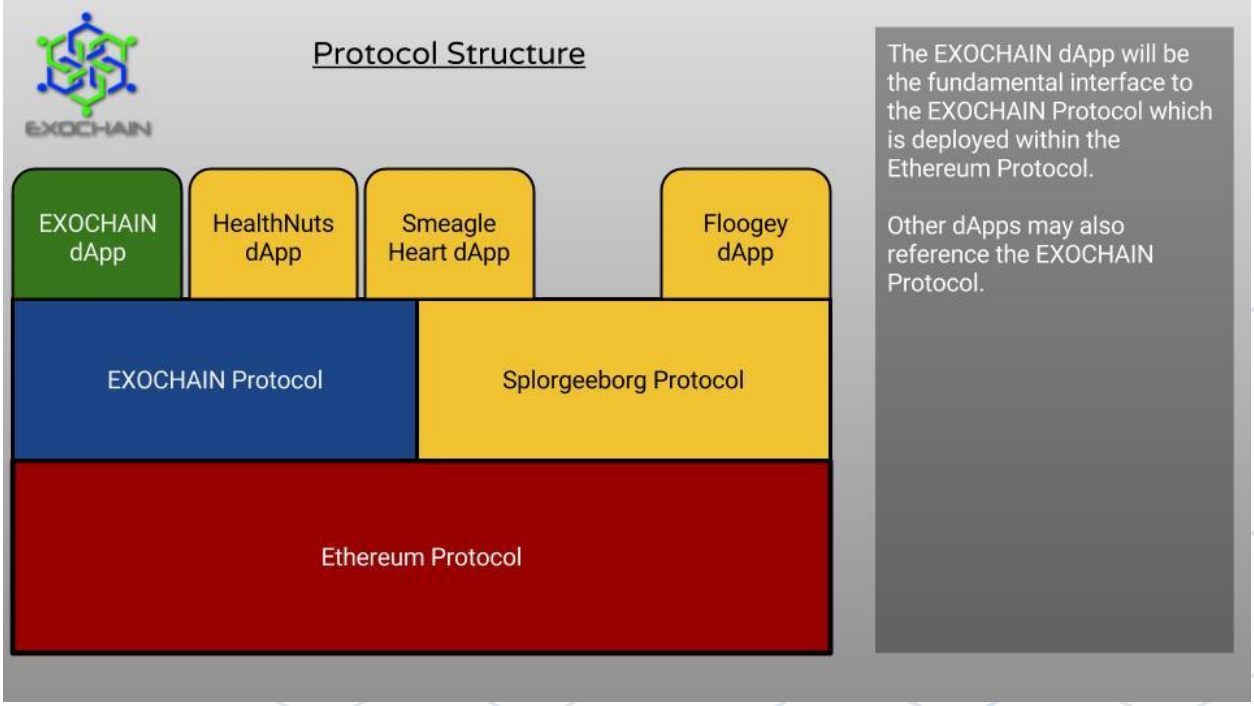
Technical:

In blockchain parelence, *protocol* typically refers to the set of rules that maintain distributed consensus across a peer-to-peer network. One protocol corresponds to one blockchain and usually one token as well.

Analogy:

Language as a protocol involving consensus on the meaning of words and word structures, in a manner that allows for more complex agreements to take place.

[9] Ibid.



Two varieties of protocols and their respective purposes:

[1] Crypto-economic Protocols[10]
establish financial incentives that propel a network of rational economic agents to coordinate behavior towards the completion of a process. Crypto-economic protocols are generally built upon Network Protocols such as Ethereum. They allow for the encoding of and adherence to agreed rules of access and data quality between companies, companies and customers, and companies and regulators.
Example: EXOCHAIN
Real-world parallel: Using the network protocol of language, Bob is able to act within a given economic paradigm, such as capitalism.

[2] Network Protocols[11]
facilitate communication between nodes; provide value through the interoperability that a standardised platform provides.
Example: Ethereum,
Real-world parallel: languages in general

Ethereum
is a blockchain-based, open-software, network protocol which enables developers to build and deploy decentralized applications (dApps). Ethereum markets itself as a "blockchain app

[10] e.g. decentralized oracle protocol
See Buterin, Vitalik. 'Ethereum and Oracles.' *Ethereum.org*, July 2014.
[11] i.e. transaction protocols
See Warren, Will. 'The difference between App Coins and Protocol Tokens.' *0xproject.com,* Feb. 2017.

platform" and continues to create a building-block set of features that can be used to establish secure information transfer between parties using internet-based communications. The immutability of data (data cannot be altered or deleted) and clarity of programmatically defined access are two of the main features lauded by Blockchain enthusiasts.

Accounts
are the basic unit or object in Ethereum. The blockchain tracks the state of every account. There are two types of accounts:[12]

> [1] Externally Owned Accounts [EOA], controlled by human users, and
>
> [2] Contract Accounts, which are controlled by their internal "smart-contract" code and can be activated by an Externally Owned Account. Contract Accounts are also capable of interaction with other contracts on an automatic and condition-determined basis.

Note:

> "Contracts" in Ethereum should not be seen as something that should be "fulfilled" or "complied with"; rather, they are more like "autonomous agents" that live inside of the Ethereum execution environment, always executing a specific piece of code when "invoked" by a message or transaction, and having direct control over their own ether balance and their own key/value store to keep track of persistent variables.[13]

Ethereum Smart Contracts
Are a conduit for both network and crypto-economic protocols. These blocks of logic are deployed to an environment where network and consensus mechanisms are managed by the Ethereum client and where Ethereum's peer-to-peer network can access the functionality of the contract. They also allow developers to create complex financial incentives, are capable of controlling digital assets, and implementing monetary policies.[14] Smart contracts are determined by code in a Contract Account which will be activated when an Externally Owned Account sends a transaction to the Contract Account. Smart Contracts are comprised of at most four components: [1] A Nonce (counter used to make sure reach transaction occurs only once) [2] Ether Balance [3] Contract Code [4] Storage.

Distributed / decentralized Applications [dApps]
Are full stack applications built on top of a network protocol such as Ethereum. A crypto-economic protocol and corresponding blockchain comprises the back-end, whilst a web interface

[12] See "Account Types, Gas, and Transactions' on the *Ethereum Homestead*.
[13] Ibid.
[14]See Warren, Will. 'The difference between App Coins and Protocol Tokens.' *0xproject.com,* Feb. 2017.

to protocol functions makes up the front-end. The decentralized nature of dApps stems from the manner in which the completion of processing occurs.

Applications vs. [tokenized] Protocols Distinction
Distributed applications create value by facilitating access to protocols, with end users paying transaction fees in the form of tokens for this access.

Tokens
Tokens can encapsulate access to functionality rather than function as equity when they have intrinsic utility and are non-dilutive to the company. A token sale (Initial Token Offering, or ITO) is better conceived of as a Kickstarter sale of pre-paid API (Application Programming Interface) keys, not (Initial Coin Offering, or ICO) equity crowdfunding.[15]

Transactions
Transactions are signed data packets that contain messages sent from account to account. They are comprised of the following data fields: [1] Recipient [2] Signature [3] Amount of Token(s) transferred [4] Data. When stored on distributed ledgers, they are ascribed time stamps.

Benefits of Decentralized Networks
With no central point of failure and secured using cryptography, distributed applications are well protected, robust and highly scalable.

History

The previous generation of digital protocols (HTTP, SMTP, TCP/IP, etc.) provided immense value. They are the foundation of the Internet and subsequently all technologies and services built on top of the Internet. However, the majority of this value was captured at the application level, primarily through the aggregation of data. The Internet stack, in terms of how value is *distributed*, is comprised of 'thin' protocols and 'fat' applications.[16] Before recent ambitious and forward-thinking applications of blockchain technology, investors operated on the expectation that investment in applications could result in relatively high returns, whilst direct investment in protocol technologies was understood to produce comparatively low returns.

Within the blockchain application stack, this value relationship between the protocol and application levels is reversed. The majority of value concentrates at the shared protocol level whilst only a fraction of this value distributes at the application layer. This Gestalt shift seems to be evidenced by Bitcoin and Ethereum, with ~$250B and ~$85B (as of the end of 2017) respective market caps and valuations of the largest companies built on top of these systems

[15] See 'Kickstarter vs Equity Crowdfunding' on *Seedinvest.com*, Sept. 2016
[16] Monegro, Joel. 'Fat Protocols.' *usv.com,* Aug. 2016.

being only a few hundred million at best.[17] This dynamic can be explained in part by what is referred to as the 'shared data level.'

Shared data level

With the replication and storage of user data across an open and decentralized network as opposed to individual applications that control access to disparate parcels of information, barriers to entry are reduced and the stage is set for a more competitive and vibrant ecosystem of products. In a framework that contains several competing, non-cooperating services which are interoperable with each other by virtue of building their services on top of the same open protocols, the market necessitates ingenuity in terms of cycle-time reduction, costs reduction, better quality products, and radical ideas.

Observations and Implications for the Future

Because of emerging trends, we will likely observe the following significant outcomes:

[1] Tokens mean instant custody without intermediaries
Because token holders need only hold private keys to guarantee custody, it changes our notion of property rights. For tokens, the final arbiter of who possesses what property is not a national court system but an international blockchain. While there will be contentious edge cases to work through, overtime blockchains will begin to provide "rule-of-law-as-a-service" as an international, programmable simplification of the litigation paradigm.

[2] An unbundling of data silos such as Facebook and LinkedIn will occur.
The ownership of data and associated power to monetize that data will transition from large companies to users.[18]

[3] Publishing the source code for software will be increasingly required for security reasons.
Running closed-source, black box software will be viewed as a security hazard.[19]

[4] The impending prevalence of tokenized feature access
Tokens for access to features that protocols provide will become as ubiquitous as software license and terms of service, such that tokens must be possessed for access to decentralized computing.

[5] Concerted and cross-industry effort to introduce network effects
'Systems thinking' has transformed multiple regulated enterprises – transportation, shipping, manufacturing, communications, food services and information technology, for example.

---

[17] Ibid.
[18] Maneeb, Ali. 'The next wave of computing.' *Medium.com*, Aug. 2017.
[19] Ibid.

However, the fields of biomedical product development, healthcare, and health research have yet to leverage a significant portion of the potential that the economies of scale and power of network effects harbor for these fields.

Distributed ledger networks are expected to change the manner in which we relate to our digital identities in several ways. This first of which is that an unbundling of data repositories such as Facebook and LinkedIn will occur. Because highly-customizable transaction protocols will endow end-users with ownership of their data, the associated power to monetize that data will transition from large companies to end-users. Second, publishing the source code for software will be increasingly required for security and quality-assurance reasons. Running closed-source, black box software will be viewed as a hazard, because code can't be verified by a community and end-users must resign themselves to trusting in the integrity of the stated functionality of software. A white-box approach such as a publicly defined smart-contract interface addresses both of these concerns. An additional expectation is that distributed ledger networks will increase standardization and interoperability of digital transactions. Because smart contracts exhibit strong network effects,[20] transactions for specific functionalities or behaviors are expected to converge towards a specific set of protocols, such that a standard set of functions will naturally develop for interactions involving identity validation, for example. One of the benefits of such standardization is that claims, attestations, and transaction data within such a paradigm are more meaningful, because they involve known, standardized processes. Finally, distributed- ledger networks are also expected to improve the computer network ecosystem by changing the incentivization structure of software developers. Because developers of distributed-ledger protocols, generally accrue wealth from greater participation in (and subsequently higher valuation of) the network they create, they are incentivized to attract users to their system by offering the best alternative to all other options (conventional or otherwise). This incentivization paradigm, coupled with the immutability of the code published as a smart contract, means that organizations who create transactional networks are both motivated to let end-users retain self-sovereignty over their data, and also incapable of changing code or data policy at a later point to access the value intrinsic in usage-data. Because the code corresponding to all functionality is immutable as well as publicly accessible, the integrity and safety of a protocol can be evaluated by the smart contract community, and end-users know that policies regarding the treatment of their transactions will not be modified in the future.

Proofs, Claims, and Attestations

Internet identity generally starts by establishing an initial identifier with an identity provider using some form of proof (credit card, mobile phone…). These identifiers are generally bound to the organization (bank, retailer) providing the credentials and authorizing transactions. This means that an individual needs to establish identities with every organization they would like to have a trusted relationship with. This is like "renting an identity" since the identity and at least some rights associated with the identity are bound to a specific identity provider or relying party

[20] 'Metcalfe's law' *Wikipedia.com.*

(like a bank or retailer). But a new identity needs to be established and maintained for every digital relationship an individual has with an organization. This is expensive for businesses and hard to manage for individuals.[21]

Fundamental Requirements of Digital Identity System

As articulated by Dmitry Khovratovich and Jason Law in a paper[22] that discusses digital identity

To be competitive with traditional paper credentials, a digital identity system is expected to contain the following features:

Compatibility. Credentials issued by different issuers can be combined for a single presentation by User who is required to prove several attributes simultaneously.
Unforgeability. A malicious User is unable to present a credential not issued by a legitimate Issuer.
Scalability. A system must handle hundreds of issuers and billions of Users, such as an international passport system. It might also be required to handle high levels of concurrency.
Performance / Low latency. Verification of credentials must be almost instant and not require broadband network connectivity per credential, even if it is issued by a previously unknown Issuer. Credentials can be stored and processed easily by the User even if offline.
Revocation. An Issuer can revoke any credential such that a User and any Verifiers can know within a reasonable amount of time that credential was revoked.

The following features are those considered impossible or difficult to implement in a paper identity system and thus represent the value-added of a digital identity system:

Minimal dependencies. Aside from an earlier issuance, an Issuer should not be involved during the preparation and presentation of proofs, and the verification of credentials, including proof of revocation.
Privacy / Anonymity. The real identity of a User can be kept secret from Verifiers who do not need it.
Unlinkability. Different presentations of the same credential cannot be linked together.
Selective Disclosure. Any subset of attributes embedded in a credential can be kept secret from Verifiers.

[21] Rowe, Gary. 'Blockchain-based Identity meets the Sovrin Foundation.' *LinkedIn.com*, Apr. 2017.
[22] Andrieu, Joe. 'Rebooting the Web of Trust.' *GitHub.com*, Fall 2017.

Availability. Rules triggering actions to limit or extend availability or access to any subset of credential data.

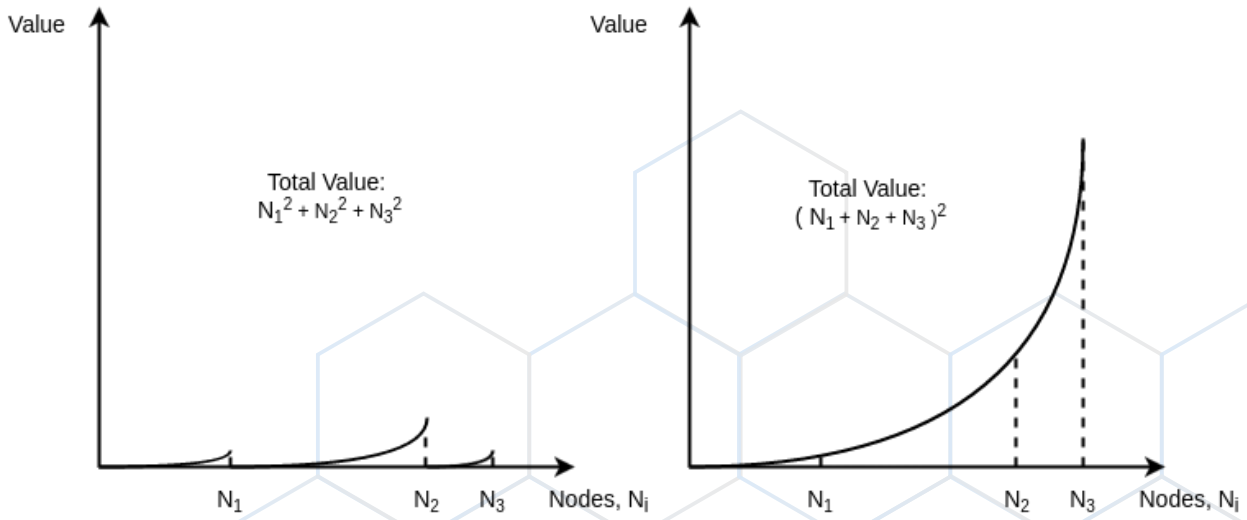
Although digital identity systems have the capacity for features unattainable by a paper credentials system, few of the features possible only in a digital identity system have yet to attain a ubiquitous level of incorporation into identity techniques, as technology that would make said functionality feasible, such as distributed-ledger protocols have only been introduced recently. Because of the programmatically definable behavior allowed in network protocols (such as Ethereum), it is has become feasible for digital identity systems to attain their full potential.

Two additional identity-pertinent techniques that have yet to be widely adopted are Zero Knowledge Proofs and 'once-and-done' attestations. Zero Knowledge Proofs[23] are attestations provided to support claims such that they do not reveal any additional information beyond the validity of a claim. An example of a Zero- Knowledge Proof could entail the following: [1] an individual submits a birth-certificate for review by a third- party. [2] The third-party adjudicates the submitted document as being valid. [3] The same individual is asked to prove that they are above the age of 21. [4] Rather than the individual using their birth certificate as supporting proof for the claim of being over 21, the previously referenced third-party can simply attest that the individual is indeed over the age of 21. This significance of the third-party attestation is that it does not provide any additional information (birth date, birth location, etc.) beyond the truth of the claim of being over 21. This example also exhibits the concept of a 'once-and-done' attestation. Instead of having to prove a claim each time a request for such a proof is made, a proof can be adjudicated once by a trusted third party such that the validity of a claim can be attested for through reference to a single validity evaluation. This process possesses significant potential for reducing the redundancy of digital proofs and has yet to be widely adopted by digital identity frameworks.

Chicken and Egg Dilemma

Denizens of the digital age have an intuitive sense of the value introduced by network effects from their engagement with such services as Facebook. However very few users of these services experienced the chicken-and-egg dilemma that were faced by early adopters. Because the value of the platform or network (social or otherwise) corresponds to the number of members in the network, and early adopters have little incentive to join a system with few users, the majority of networks that accrue value from membership never attain what is often referred to as 'critical mass'.

[23] See 'Zero Knowledge Proofs: An illustrated primer' by Mathew Green on *cryptographyengineering.com*



Formally, Metcalfe's Law defines the value of a network as being the total number of nodes it connects. This not only underscores the chicken-and-egg dilemma, but also the fact that redundant networks can severely dampen network effects by fragmenting a network, resulting in worse outcomes for all involved. Such dampening has been observed when token sales are improperly used a means to get around SEC securities regulations as a quick and easy method to crowdfund a project, as opposed to offering tokens that provide access to the functionality and utility value created by a protocol.

Fundamental Issues with the Current Digital Identity Paradigm

One issue with the digital paradigm of today is the federation of identity. Internet identity generally starts by establishing an initial identifier with an identity provider using some form of proof (credit card, mobile phone, etc.). These identifiers are generally bound to the organization (bank, retailer) providing the credentials and authorizing transactions. This means that an individual needs to establish identities with every organization they would like to have a trusted relationship with. This is like "renting an identity" since the identity and at least some rights associated with the identity are bound to a specific identity provider or relying party (like a bank or retailer). However a new identity needs to be established and maintained for every digital relationship an individual has with an organization. This is expensive for businesses and hard to manage for individuals.[24]

Another issue is how 'free-access' models are prone to stripping end users of sovereignty over their data. Entities like Facebook and Alphabet offer a swath of services at no monetary cost. However value is extracted from end-users in the form of usage data, to be stored in data

[24] Rowe, Gary. 'Blockchain-based Identity meets the Sovrin Foundation.' *LinkedIn.com*, Apr. 2017.

repositories. Companies don't do a very good job of revealing to consumers what information they hold and how much money they make from it. Such data is generally not publicly available.[25] Over the course of this process, end-users are relinquished of self-sovereignty of their data, because they lose control over what aspects of their data can be accessed, who can access that data, how their data is used, and how long the data can exist. The information accrued by such companies endows great power: Google can see what people search for, Facebook what they share, and Amazon what they buy.[26] This 'All-seeing view' is a concerning development that arguably represents the most extreme degree of power held by private institutions. Accordingly, there exists an incipient need for ownership of identity to be redistributed back to the primary stakeholder(s) corresponding to each identity. The 'free-access' models, that extensively comprise the current digital services paradigm, in actuality undermine the self-sovereignty of end-users and increase the susceptibility of end-users to infringements upon the security and privacy of data associated with their personal identity.

The key implement used to strip end-users of self-sovereignty over their data is Shrinkwrap. Like the wrapping paper hastily torn away on Christmas morning, Terms of Service (ToS) and End User License Agreements (EULAs) are hastily overcome, without examination. These contracts allow service and product providers to define 'terms of engagement.' However, end-users have very little leverage or allowance for specification of agreement; they are merely presented with the option of agreeing and being able to use the service or product or not agreeing, an option that would almost certainly entail severe inconvenience on the part of the end-user, and may even be impossible in many cases.[27] Further, most shrink-wrap consist of many thousands of words, many of which can be categorized as highly-technical legalese. Not only is the overwhelming majority of Shrinkwrap hastily ripped off with a click of 'I Agree', even if they were to be read, extreme readability gaps have been observed to exist between the projected average readability level of user-bases of given products and the calculated readability level of the shrinkwrap corresponding to that product, such that an end-user would understand very little of what they had just spent several hours reading, even if they had read it.[28] Finally, the significance of the preceding observations is elevated by the fact that shrink-wrap have been known to contain nefarious clauses, from asserting complicity to all future versions of a Shrinkwrap to attempting to prevent critical speech about a product or company.[29]

[25] 'The world's most valuable resource is no longer oil, but data.' *The Economist*, May 2017.
[26] Ibid.
[27] Rauscher, Konrad. 'The digital shrink wrap dilemma.' *Third Worldwide Cybersecurity Summit*, Oct. 2012.
[28] Ibid.
[29] Ibid.

EXOCHAIN

EXOCHAIN aims to create an identity infrastructure that drives clinical research quality [as a first use case], effectiveness and efficiency, while reducing liability and cost.

Towards this end, EXOCHAIN will create the first digital framework for scoring one's identity, which utilizes 0dentity, a simultaneous identity-sovereignty score.

This protectable ecosystem will simplify, secure, and add transparency to interactions between entities, allowing transactions between parties to take place on an ad hoc, and automatic basis.

Because transactions within the EXOCHAIN blockchain are recorded in a transparent manner, users are protected through historically and more clearly represented terms of engagement.[30]

By rejecting anonymity and embracing identity, organizations interfaced with via EXOCHAIN are protected with know-your-customer compliance.

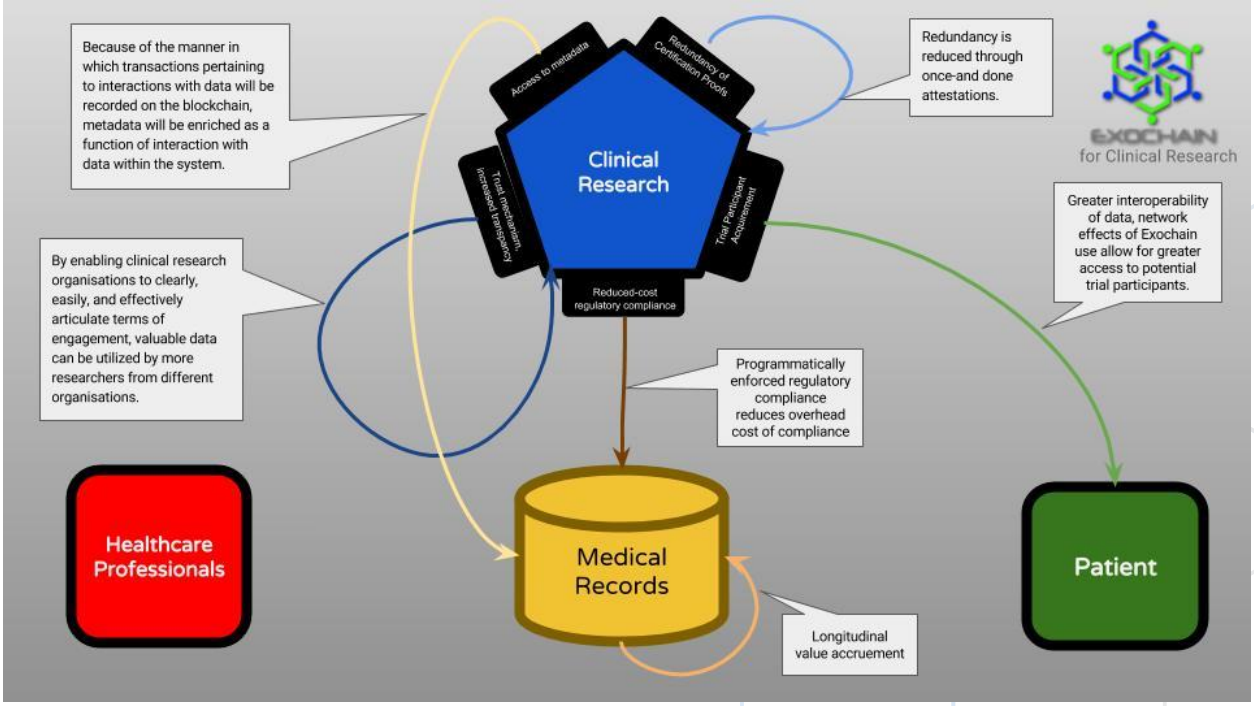
Through EXOCHAIN's tokenized protocol, participants (including patients and healthcare professionals) who engage in self-adjudication will benefit from access to seamless release authority, redundancy reduction, programmatic permission designations, and personal data protection through zero-knowledge-proof attestations.[31]

EXOCHAIN has transcended the Chicken and Egg Dilemma through a contractually exclusive partnership with the 1.3 million member ACRES BlueCloud network, by which the EXOCHAIN network will commence, on day one, with over 1.3 million healthcare professionals representing over 50,000 healthcare provider organizations in conjunction with over 125 ACRES allied industry partners.

The following pages articulate how EXOCHAIN redefines the relation among clinical stakeholders including payers, providers, and patients, among others.

[30] Steptoe & Johnson LLP. 'The Enforceability of Smart Contracts.' *Lexology.com*, May 2017.
[31] 'Zero Knowldge Proof' *Wikipedia.com*

Clinical Research



Issue: High overhead costs of regulatory compliance in general.

EXOCHAIN's solution:
Many clinical research organizations, including smaller ones, often find it difficult to meet the high-hurdle overhead of full regulatory compliance and are hampered and taxed by the need to deploy systems that are generally prohibitively expensive without the benefits of economies of scale as enjoyed by larger organizations. Because full-feature participation in the EXOCHAIN ecosystem requires establishment of identity through EXOCHAIN's adjudication framework and identity score, regulatory compliance is simplified through extensive and automated validation of data integrity. Authorization is verified and ensures regulatory compliant access to medical records.

Issue: Extraordinarily low participation in clinical trials - 4% globally & under 3% for cancer in the US. [32] [33]

[32] US Food & Drug Administration. '2015-2016 Global Participation in Clinical Trials Report.' *fda.gov,* July 2017.
[33] 'Transforming Clinical Research in the United States: Challenges and Opportunities: Workshop Summary.' *Institute of Medicine (US) Forum on Drug Discovery, Development, and Translation,* 2010.

EXOCHAIN's solution:
Although a significant component of this low participation rate is explained by the strenuous conditions used to select participants for clinical trials, EXOCHAIN can improve participation rates by providing clinical researchers with access to better methods for determining potential volunteers (i.e. an interface to a database of verified and attribute-rich patient record instances). By increasing the access clinical researchers have to categorized, feature-rich, and adjudicated patients who have programmatically defined the extent to -- and the manner in which -- patient records can be engaged with and patients contacted, the overhead involved in acquiring trial participants is dramatically reduced. Patient access and acquisition is the first in a series of critical steps leading to generating "clean data" -- data that is evaluable according to scientific and regulatory terms.

Issue: Research systems lack a trusted mechanism to track IP in collaborative research. Because of this, clinical research organizations express highly risk-averse behavior that diminishes collaboration between organizations and reduces the productivity and impact of clinical researchers themselves. Entire swaths of useful data are kept inaccessible from other research organizations due to fears regarding IP, protecting value of investments, etc.

EXOCHAIN's solution:
Adjudicated user identities enable agreements and transactions with legal standing. Risk is further mitigated by ensuring that transactions within smart-contracts can be jurisdictionally enforced, and, when required, delivered as evidence in support of contract enforcement or regulatory compliance litigation. By enabling clinical research organizations to clearly, easily, and effectively articulate terms of engagement, valuable data can be utilized by more researchers from different organizations.

Issue: Redundancy of certification proofs

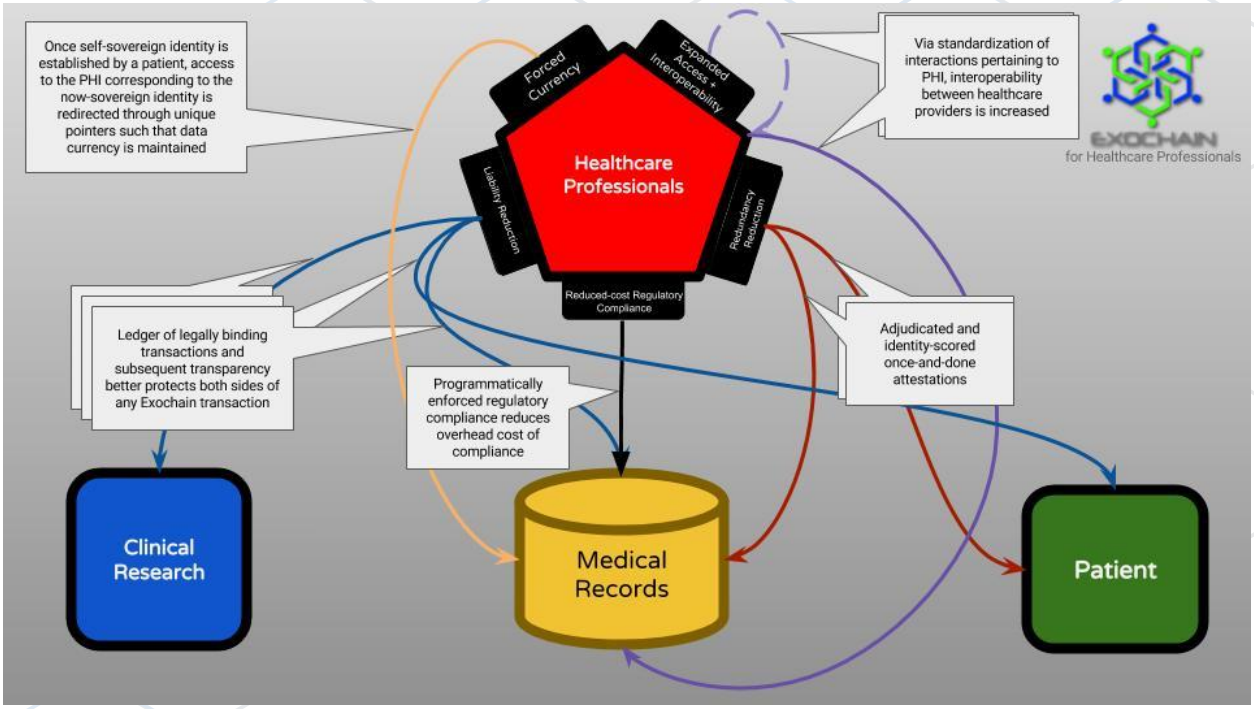
EXOCHAIN's solution:
Redundancy is reduced through once-and done attestations. For example, rather than completing the same form on a per-request basis, a form can be completed once and EXOCHAIN can provide attestations that the form was completed and is current. The number of such attestations recorded on the EXOCHAIN ledger can be thought of as a function of time, the number of users in the EXOCHAIN network, and activeness of said users. These attestations are truth statements, such that the greater number of attestations recorded on EXOCHAIN's ledger, the more truth that exists within the network and can be referenced in decision making.

EXOCHAIN feature:
Longitudinal value accruement. Because of the manner in which transactions pertaining to interactions with data will be recorded on the blockchain, metadata will be enriched as a function of interaction with data within the system. This can be thought of as a network effect by which the value of all data in the system increases as the data is engaged with. For example,

the pertinence of a set of records for a specific field of research can be realized and subsequently represented to those involved in the same field.

EXOCHAIN feature:
Programmatically-definable transactions and agreements. For example, programmatically enforced double-blind relation to data can be achieved through the EXOCHAIN protocol such that double-blind status automatically ceases after certain conditions have met, such as the completion of the study or an allocated passage of time.

Healthcare professionals



Issue: Redundant proofs

EXOCHAIN's solution:
Adjudicated and identity-scored once-and-done attestations.

Issue: Segmentation of record networks complicates and mitigates inter-network interoperability, resulting in data access issues that affect quality of care. A lack of interoperability between healthcare providers costs 150,000 lives and $18.6 billion per year, according to the Premier Healthcare Alliance.[34] [35]

[34] Rana, Aditya. 'Is Blockchain The Solution For Healthcare?' *dataeconomy.com*, March. 2017.
[35] Minegain, Bernie. 'Data-sharing initiative reduces deaths.' *Healthcare IT News*, March 2013.

EXOCHAIN's solution:
Disparate network transcendence through standardization by way of a transparent and flexible protocol defines how inter-entity (healthcare professionals, clinical researchers, and patients) interaction occurs.

Example:
Patients coming from the Veterans Affairs system being able to seamlessly release their records to doctors and then subsequently again to referred specialists outside the VA system.

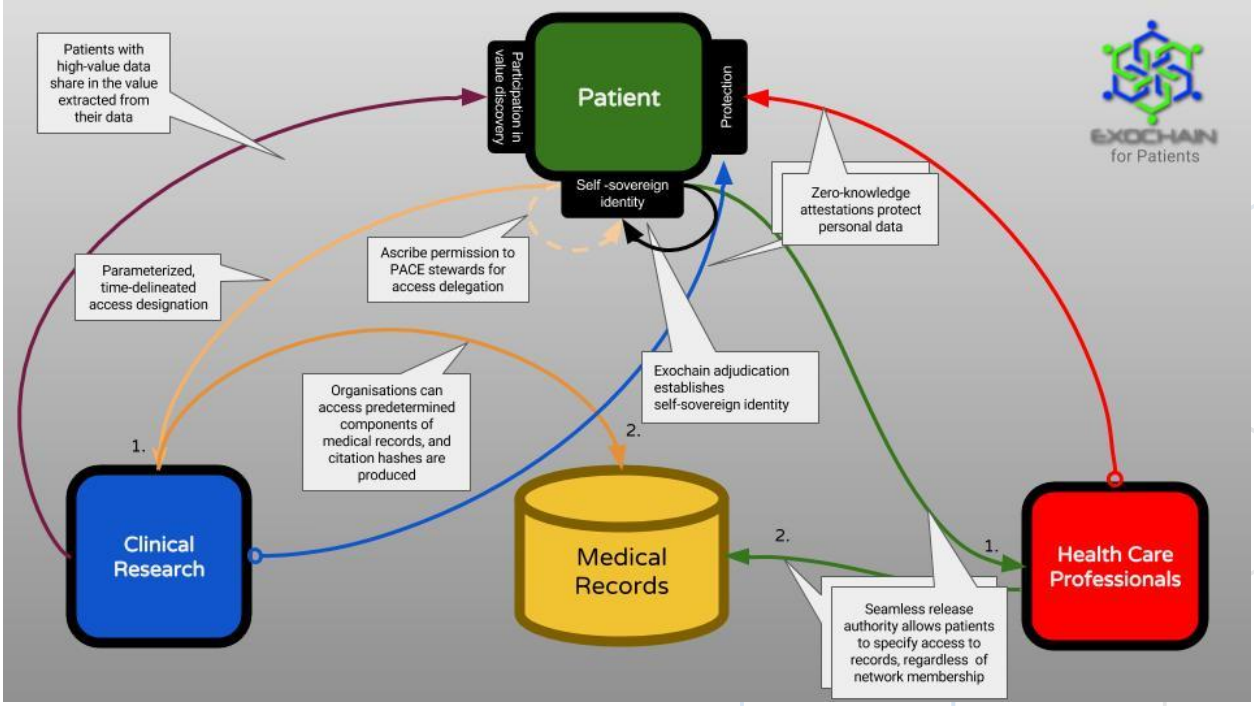
Issue: Version management difficulty coupled with tendencies towards dis-synchronization result in a system where medical data can easily become 'stale' and healthcare professionals suffer from having to engage with data administration activities with gross opportunity cost.

> *"We've turned many physicians and other providers into data entry clerks and it detracts … from their productivity but it detracts greatly from their ability to provide quality care"*
>
> - Tom Price, Fmr. United States Secretary of Health and Human Services.

EXOCHAIN's solution:
Introduction of an object-oriented approach to interaction with personal medical records. By redirecting access to personal healthcare record objects (an abstraction of personal medical record data that encapsulates all the PHI of a person) through unique pointers, data currency is maintained. Such a redefinition of the access process allows for the paradigm to shift from doctors and medical professionals facing a specific set of documents on a per-case basis towards one where patients provide modulated, time-delimited access.

EXOCHAIN feature:
Easier PHI regulatory compliance. Because full-feature participation in the EXOCHAIN ecosystem requires establishment of identity through EXOCHAIN's adjudication framework and identity score, regulatory compliance is simplified through extensive and automated validation of data integrity. Authorization is verified and ensures regulatory compliant access to medical records.

PATIENTS



Issue: Centralization of power and wealth by entities who charge compromises to end-user self-sovereignty, data security, and data privacy for access to valuable services. These compromises are then leveraged to extract value from end-user data (personal, meta, usage, or otherwise). This occurs without end-users enjoying any benefit from an extraction of value from a resource that would not exist without them. Not only does such a dynamic represent unfair value distribution practices, but poorly incentivizes early participation in systems where network effects determine the value of participation in the network.

EXOCHAIN's solution:
Democratize the manner in which value is extracted to data through the creation of a levelled playing field in which end-users are empowered to achieve self-sovereignty through an EXOCHAIN identity score. Doing so can define the terms of engagement with their data. It also allows users to see a share of the potentially extremely high-impact value that they are providing (such as rare genetic profiles). This would be accomplished through the terms of engagement to which all assessors of data agree.

Issue: *Obstacles to participation in clinical research and thus experimental, potentially life saving treatments.*

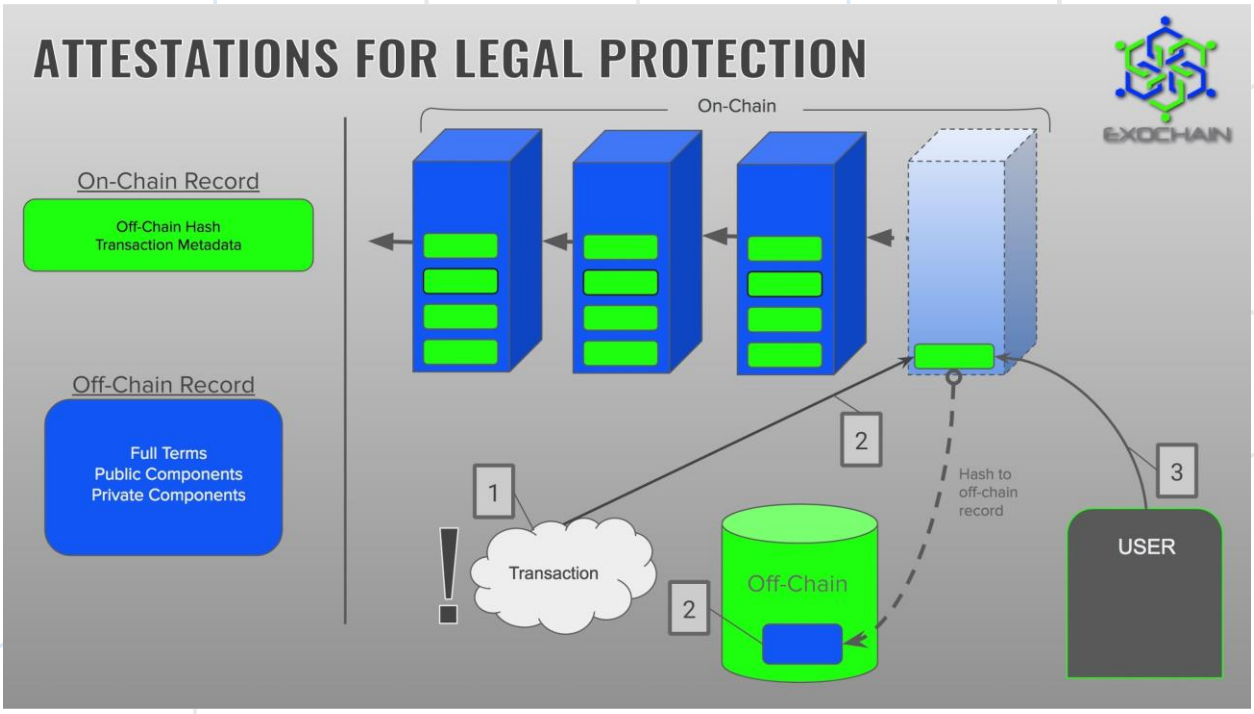
EXOCHAIN's solution:
Increase the visibility and engagement of patients to, with -- and for -- clinical research entities, while reducing the overhead (cost of regulatory compliance, liabilities, etc.) per patient involved in a clinical trial would be a significant part of any such value proposition.

EXOCHAIN feature: End-user participation in value discovery.

EXOCHAIN feature: Personal data protection is achieved through such mechanisms as zero-knowledge attestations.

EXOCHAIN feature: Self-sovereign identity that allows for parameterized data access designations w/ time delineation and seamless release authority.

Example Process Flows



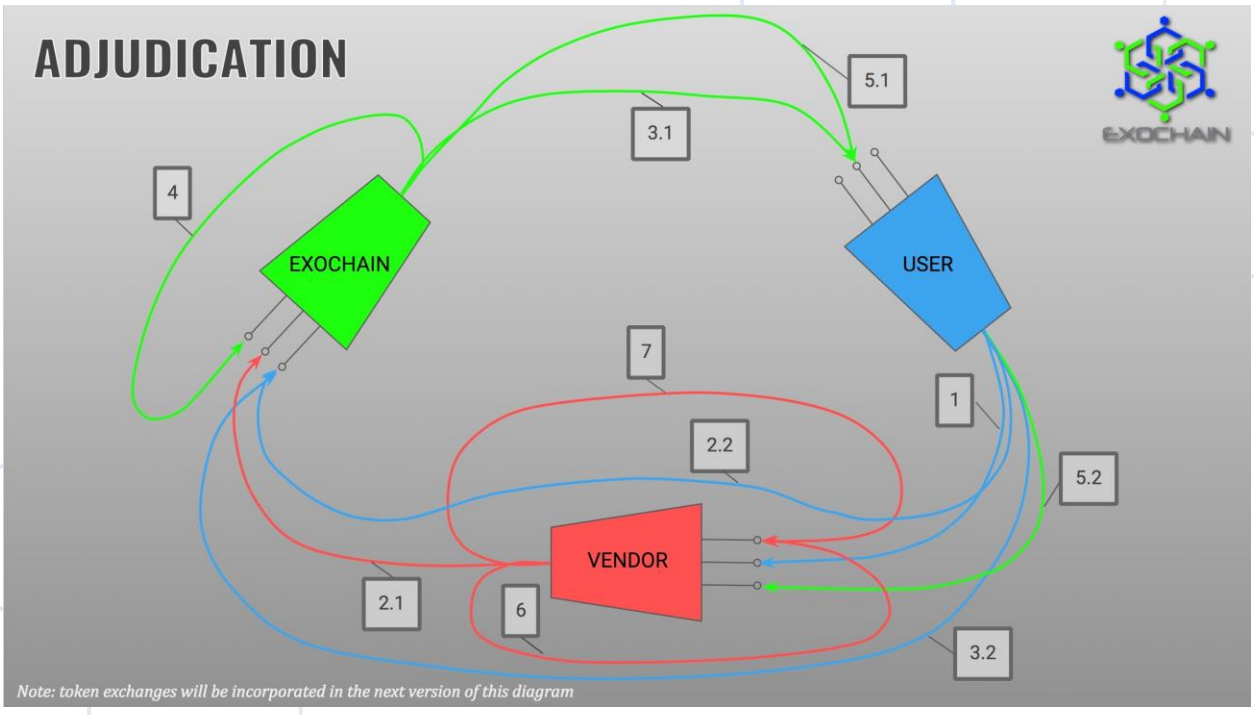
Attestations for Legal Protection Process Flow

1. Transaction occurs
2. Transaction recorded, both on-leger and off-ledger

- On-ledger record:
  - Metadata about the transaction
    - parties involved in transaction (identified by unique key / address)
      - This address will correspond to an individual or entity register with EXOCHAIN
    - Type of transaction

        - Timestamp of transaction
    - A hash (address) that corresponds to an off-chain transaction data object
- Off ledger:
    - The transaction data object referenced by the on-chain hash
    - Includes:
        - Full Terms of transaction
        - components of the transaction specified as public
    - Can include:
        - components of the transaction specified as private that can only be accessed with the proper key, which can be provided by either one or both of the parties involved in the transaction, or once a set of conditions have been met (time-delimited release for double blind trial, for example.)
            - This key can be requested from the entity(s) possessing the key

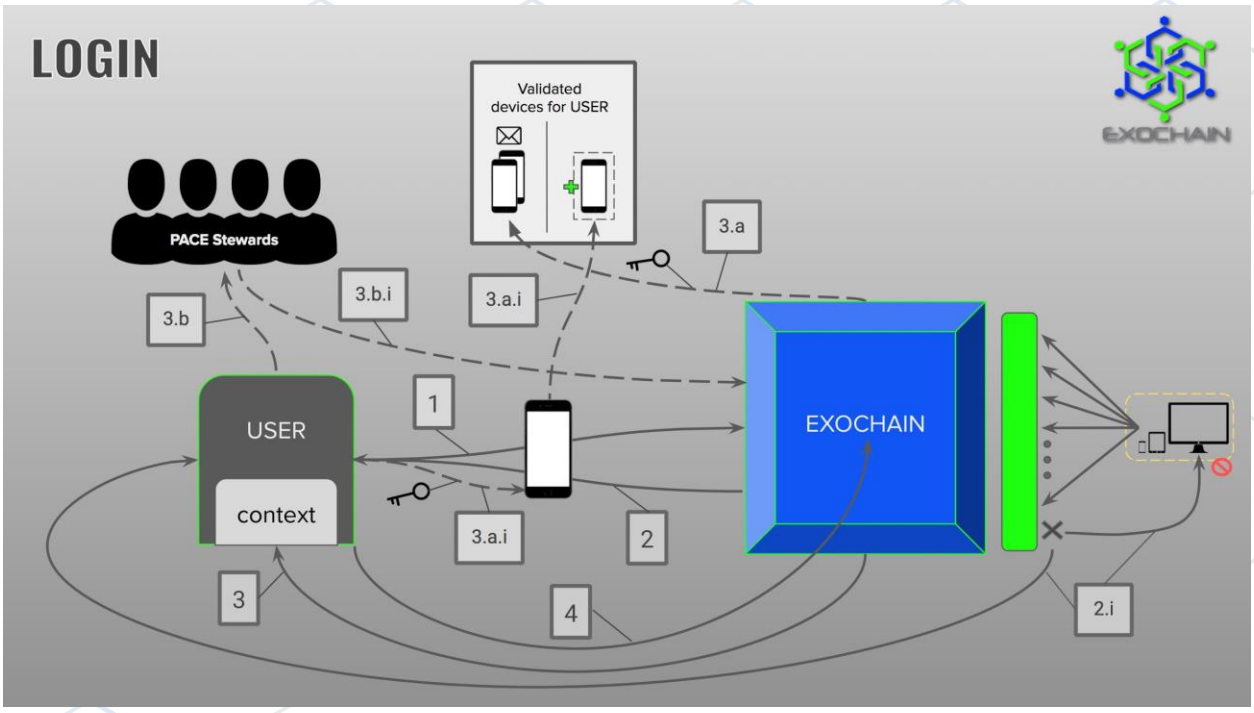
3. Record of transaction can be referenced later; those involved in the transaction are protected through a clearly and historically represented (that the transaction occurred and occurred before or after other transactions) record of the terms of engagement involved in the transaction



Adjudication Process Flow

1. USER authenticates with VENDOR using VENDOR's chosen mechanism
2. If USER successfully authenticates with VENDOR, informative components of VENDOR's authentication outcome are passed to EXOCHAIN **[2.1]** and the USER is redirected to the EXOCHAIN site **[2.2]**

3. EXOCHAIN evaluates the USER's security context (device, location, etc.) **[3.1]** and leads the USER through additional authentication factor flows as necessary **[3.2]**
    a. Conditions for additional authentication factor flows entail: unprecedented device, location, unknown email, etc
4. EXOCHAIN adjudication algorithms process the results of said authentication mechanisms and incorporates them into 0dentity score [an 0dentity score is instantiated at this point if one did not exist for USER]
5. EXOCHAIN redirects **[5.1]** browser back to VENDOR site **[5.2]**, with accompanying encrypted 0dentity information
6. VENDOR evaluates 0dentity score
7. VENDOR instantiates session



Log-in Process Flow

1. USER navigates to and is subsequently presented with login page
2. USER enters login information
    a. IF login credentials are correct, proceed to **[3]**
    b. ELSE If USER incorrectly enters login information, error message presented
        i. Mechanism for per-device lockout from additional login attempts and notification of USER via trusted means of communication (validated devices, validated email, etc.) IF *X* incorrect attempts from a given device.
3. EXOCHAIN evaluates the USER's context (device, location, etc.)

a. IF unprecedented device, then EXO generates OTP (one-time password), sends to other OTP-validated device or email, and prompts user to enter OTP on unprecedented device
    i. Once OTP is successfully submitted this formerly unprecedented device becomes precedented
b. ELSE IF unprecedented device AND no access to validated device or email, PACE-method[36] can be used to request access via established stewards corresponding to that identity
    i. Once PACE Stewards receive the request, they communicate their approval / rejection of the request to EXOCHAIN; if approval, proceed to **[4]**

4. IF validation steps are completed in **[3]**, USER redirected to Account Overview / Hub page

Trademarks and Partnerships

0dentity™

EXOCHAIN™'s digital identity score will possess the following features:

Signature: 0dentity's functionality as a signature will follow standard cryptographic procedures through use of a public-private key pair.

Dynamic score: Identity is not static because the set of recorded information corresponding to an identity is ever-changing. 0dentity is updated as these factors change. Additionally, given the extent to which a digital identity can be deemed as established and secured would be damaged in the case of abnormal or compromising behavior corresponding to said identity, an 0dentity score has the capacity to fall given such activity. If an 0dentity score continues to fall, the access and capabilities endowed by having and 0dentity score above a set of thresholds (one such threshold could determine whether an individual can access their personal healthcare records, for example) are quickly reduced as an 0dentity score falls below consecutive thresholds. The converse also holds; an 0dentity score (or, more specifically, a component or weight that comprises an 0dentity score) would increase (and the set of capabilities it bestows expands), once it has been established that control has been regained.

Service-dependent: A given domain will value different components of identity. A service may utilize specific aspects of 0dentity when determining its trust in the 0dentity holder.

[36] PACE stand for Primary Alternate Contingency Emergency. PACE stewards can be thought of as 'trustees' of a given digital identity. EXOCHAIN will require its users to specify four such stewards.

Minimal release: Many services only require a specific degree of information. For example, services that require an attestation of and individual being over the age of eighteen. An interaction with the corresponding 0dentity instantiation could provide such verification without revealing additional information data (i.e birth date, name, etc).

BlueCloud®

EXOCHAIN has vanquished the chicken-and-egg dilemma (as discussed in the introduction) through its partnership with the BlueCloud network. Through this partnership, EXOCHAIN's LYNK blockchain protocol is in the process of being developed and deployed as the exclusive global standard for login adjudication for all of the over 1.3 million registered medical professionals who are currently enrolled in the BlueCloud network. The BlueCloud network is comprised of well over 50,000 industry stakeholder organizations and represents pharmaceutical drug discovery companies, hospitals, contract research organizations, and universities, all of which must verify and secure the identity of patients and professionals participating in FDA-regulated clinical trials.

ACRES®

The EXOCHAIN LYNK protocol is also the exclusive standard used by the non-profit Alliance for Clinical Research Excellence and Safety [ACRES Global] in their objective of safely accelerating clinical research. Their ascribed standard-status of the EXOCHAIN LYNK protocol is a recognition of the potential that the protocol possesses for providing [1] easier, faster, and immutable transaction processing and [2] a mechanism for a seamless medical record release authority that allows for the safe application of medical data towards research for cures.

EXO Token

Chains (EXO- or otherwise) are comprised of links. The value of the chain is determined by quality and manner of connections between links, as well as the number of links comprising the chain.

This analogy is relevant for the EXOCHAIN ecosystem; users in network increase the value of the entire chain (value accruement through network effects.) The EXO token will endow users access the functionality provided by the EXOCHAIN protocol in a manner that covers the costs of: computation on a per-transaction level (i.e. gas payments due to Ethereum), development, network enlargement, data storage, etc.

Going Forward

The ultimate implementation of the features laid out in the preceding pages may be subject to pivots or alternative framings as the complex and yet-evolving nature of the subject matter necessitates a degree of flexibility, such that the best design is the one arrived at. The process flows as presently envisioned involve many components (in the case of the diagrams, 'arrows')

that presently exist as planned development efforts. A set of priorities will be ascribed to implement these functionalities such that a balance is struck between [1] rapidly introducing high-value services to members of the EXOCHAIN network and quickly [2] ensuring comprehensive security and resiliency throughout all layers of the product. In the near future, EXOCHAIN will further integrate with the BlueCloud® network becoming both integral and exclusive to their onboarding, subsequent login, and industry-specific SaaS app store licensing processes.

Comparative Analysis of EXOCHAIN and several other relevant Entities in the Identity / Healthcare Space

General Comment

The most differentiating aspect of EXOCHAIN relative to the attempts at engaging with healthcare and identity IT presented below is that EXOCHAIN possesses both a fully developed use-case and signed partnership agreements for this specific use-case. This means network effects-- *fast*.

SelfKey

Being built over distributed ledger technology, the SelfKey service is oriented around keeping regulators satisfied with Smart verification procedures, while providing businesses with a smoother and more efficient 'know-your-client' process. Users of SelfKey are conceived of as being able to own the 'keys" to their personal data and identity certificates. Therefore, identity owners are the only ones who get to select what aspects of their information are to be shared, with whom, and under what terms. Because of the immutability of data on a SelfKey ledger, such data is expected to serve as a solid provenance for audits and regulatory checks.

Have: Conceptual model that incorporates the value-add of identity attestations.
Lack: Demonstrated or articulated strategy to beat the chicken & egg dilemma; no targeted application (e.g. healthcare), no key partnerships to rapidly develop network effects.

Civic

In general terms, is a system conceived of effectively shifting the paradigm from proof via reference of access PII to attestations of ownership, such that a credit card number would not

be useful unless an attestation exists that the credit card number belongs to the person who wants to use it. Not much detail is provided, however, regarding how this would be implemented on a technical level.

Weakness: Built on top of the rootstock (RSK) system, a layer on top of bitcoin created to service smart contracts. Because bitcoin was not built with consideration for smart contracts from the ground up, the RSK smart contract functionality is not fully integrated into the system. Consequently, RSK sacrifices security[37] by relying upon merge-mining to execute a two-way peg with Bitcoin.

Shortcoming: According to Civic's white paper, there is no engagement with issues surrounding regulatory compliance (redundancy, high overhead costs, etc.)

uPort

Is a mobile-capable identity framework for secure digital interactions. Built on Ethereum, the application consists of three main components: a set of smart contracts, developer libraries, and a mobile app. uPort enables self-sovereign identity, because uPort identities are fully owned and controlled by the creator. A uPort identity can digitaly sign and verify a claim, action, or transaction and can be cryptographically linked to off-chain data stores (i.e. they are self-sovereign).

Shortcoming: More of a utility protocol; not attempting to create an ecosystem and relatively not much to be gained in terms of network effects.

Health Nexus

Health Nexus framework for an ecosystem with a governing consortium implemented through a smart contract and data storage capabilities. Created by Simply Vital Health (SVH), the product has been dubbed as a 'healthcare operating system' by SVH.

Shortcomings: [1] Simply Vital Health is relying on third-party developers to create the application layers (i.e. Pharmaceutical tracking, Data Accesability and Sharing, Insurance payments and reimbursements, Transparency, etc.). [2] Simply Vital Health refers to *ConnectingCare*, a blockchain-based product aimed towards transitioning providers to value

[37] Voyiatzis, Artemios G., and Edgar Weippl. "Merged Mining: Curse or Cure?." *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, September 14-15, 2017, Proceedings*. Vol. 10436. Springer, 2017.

based care, as 'indisputable proof of the viability of Health Nexus and gives an exciting glimpse at what will be built on Health Nexus in future.' However, *ConnectingCare* was only launched in July of 2017 and has yet to transcend pilots with a few key clients. [3] Health Nexus enables a governing consortium, comprised of healthcare industry leaders, to manage blockchain operations, including certifying compliant nodes, and proposing and voting on protocol level updates. Because additional executive users may be inducted with a 60% approval from the other consortium members, the model is susceptible to a dilution in integrity over time. As consecutive 'bad apples' are approved to join the consortium, the number of 'good' consortium members required to be convinced, err in judgement, or otherwise act in a way that would lead to the induction of more 'bad apples' decreases. This is particularly the case if the 'bad apples' collude to attain control.

Conclusion

> I have a dream for the Web [in which computers] become capable of analyzing all the data on the Web – the content, links, and transactions between people and computers. A "Semantic Web", which makes this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines. The "intelligent agents" people have touted for ages will finally materialize.[38]
>
> - Sir Tim Berners-Lee, implementer of first successful HTTP-based communication

Although Tim Berners-Lee conceived of his 'semantic web' as the enabler of machines talking to machines such that they handle the mechanisms that comprise our daily lives, we are at the convergence of developments that not only allows for the construction of a more effective paradigm but necessitates the deployment of such a paradigm. These developments include the arrival of new technologies such as Ethereum, poignant distortions that have emerged in the digital world costly and dangerous flaws that are intrinsic to previous technologies, and the ubiquitous use of digital identities.

As a first use case, EXOCHAIN, utilizing bleeding-edge digital transaction methods, is poised to connect patients, healthcare providers, and clinical researchers in a secure environment. Because of EXOCHAIN, clinical researchers and healthcare professionals will benefit from reduced overhead of regulatory compliance and lessened redundancy of certification proofs. Patients will be better-off from the establishment of Self-sovereignty for their PHI. This means participation in value discovery, improved access to PHI, and increased privacy and augmented protection of data.

[38] Berners-Lee, Tim; Fischetti, Mark. 'Weaving the Web.' Chapter 12, 1999.

All EXOCHAIN users will enjoy the benefits of disparate network transcendence through standardization of access via a tokenized protocol framework: secure medical record portability and a seamless release authority.