Use of Blockchain in Health IT and Health-related Research

Using off-chain (kreateIoT) with a public blockchain to achieve patient privacy, security, scalability and interoperability of Electronic Healthcare Records

(Sirish Bajpai, Raj Sharma)

The meaningful use program was established under the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and it's widely accepted that the Act as a policy was a success. Through Electronic Health Records (EHR) certification, the program aims to improve healthcare quality, safety, efficiency and reduce health disparities. Additionally, the program drives providers to engage patients and families, improve care coordination and maintain health information and security. HITECH was designed to ultimately improve clinical outcomes, improve population health, increase transparency, empower patients and make more data available for research. However, interoperability remains a monumental challenge that needs to be confronted while keeping security and privacy concerns in mind. Electronic health records that exist are typically maintained in on-site repositories powered by physical servers or on an IT cloud. This centralized healthcare data creates a heightened vulnerability for security breaches, one where hackers can easily gain unauthorized access into systems loaded with private patient information.

The electronic health record problems at its core are 'what happened when' and 'who has access to that information' problems. While these are the types of issues that lend themselves well to blockchain technology, the difficulty comes in striking a balance between privacy and transparency, all within a sea of multitude of software systems that were not designed to be interoperable or allow sharing of data.

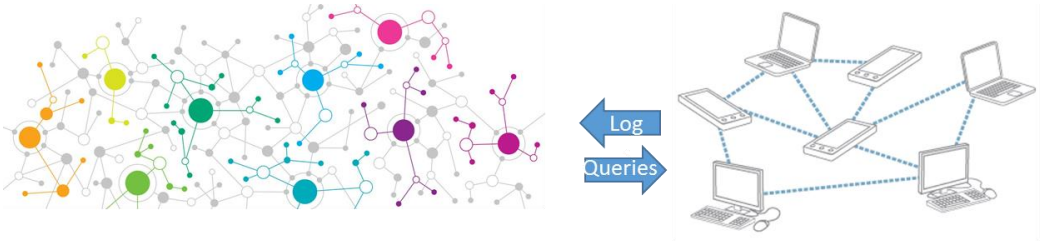
By Scott Adams

In order to further meet the objectives of HITECH, what is necessary is a peer-to-peer network enabling providers, payers and patients access to healthcare data to run translations, normalizations, and computations on data while keeping the data completely private. The public nature of a blockchain guarantees transparency over how applications work and leaves

an irrefutable record of activities, providing strong incentives for honest behavior. However, the intense verification and public nature of the blockchain limits potential use cases in healthcare. Modern healthcare applications use huge amounts of data and run extensive translations, normalizations and analysis on healthcare data. In their current design, public blockchains cannot handle privacy and are not well-suited for heavy translations and computations.

Since their inception blockchain inspired technologies have evolved and can be divided into two: fully decentralized permission-less ledgers such as Bitcoin and Ethereum, and semi-centralized permissioned ledgers such as Ripple. It would seem that there is an inherent trade-off between having a pseudo-anonymous system, where no one is trusted and all information must remain public, and having a somewhat centralized system with trusted nodes that can verify true underlying identities. With an off-chain technology linked to a blockchain, this trade-off can be avoided while the network remains fully decentralized.

In this paper, kreateIoT proposes an internet application with a decentralized architecture, where no single party has absolute power and control. This end-to-end decentralized healthcare app is developed using private computations, which are further partitioned to on-chain and off-chain execution. Off-chain code returns results privately, while sending logs of translations performed to a public blockchain. This blockchain adaptation for EHRs creates a network infrastructure of providers, payers and patients, where providers create an EHR as a blockchain asset, patients own the asset, and authorized parties can access or modify it (with patient's consent).



Public Blockchain e.g. Ethereum
- Native currency e.g. Ether
- Distributed ledger
- Proof of Stake
- Public and secure
- Network of nodes

kreateIoT Off-chain
- Native asset issuance
- Healthcare record translations
- Proof of Translation
- Private and secure
- Network of smartphones and computers

Any access or modification to the EHR will be recorded in the public blockchain while patients can share their private data with providers, payers and researchers with cryptographic guarantees regarding their privacy. An external blockchain such as Ethereum can be utilized as

the controller of the network to manage access control, manage identities, and serve as a tamper-proof log of events.

Privacy and Security

kreateIoT is a decentralized off-chain computation platform for healthcare with guaranteed privacy. The goal is to enable 'privacy by design' for end-to-end decentralized healthcare applications, without a trusted third party. The key to doing this is the ability to run translations, normalizations, and computations on data, without having access to the raw data itself. kreateIoT's computational model is based on a highly optimized version of secure multi-party computation (MPC), guaranteed by a verifiable secret-sharing scheme. Using MPC, healthcare data queries and translations are computed in a distributed way.

Instead of having all the data in one place, kreateIoT off-chain encrypts data by breaking it up into several components, and by randomly segregating it to hundreds of smartphones and servers in the network. Protected Health Information (PHI) is split among different nodes, and they compute translations and formatting functions together without leaking information to other nodes, while ensuring correct execution. Hence, no single party ever has access to any patient's health data in its entirety; instead, every node has an incomplete and meaningless piece of the total data set. Each node runs calculations on its assigned block of data, until the user merges the results to decrypt a block.

During computations and translations, for temporary storage of healthcare data, kreateIoT uses a distributed off-chain hash-table for holding secret-shared data that is accessible through a public blockchain such as Ethereum. Private data is encrypted on the client-side before storage and access-control protocols are programmed into the public blockchain, which stores references to the data but not the data itself. Each node in kreateIoT's distributed off-chain has a distinct view of its shares of encrypted data only so that the computation and the translation process is guaranteed to be privacy-preserving and fault tolerant.

User Control

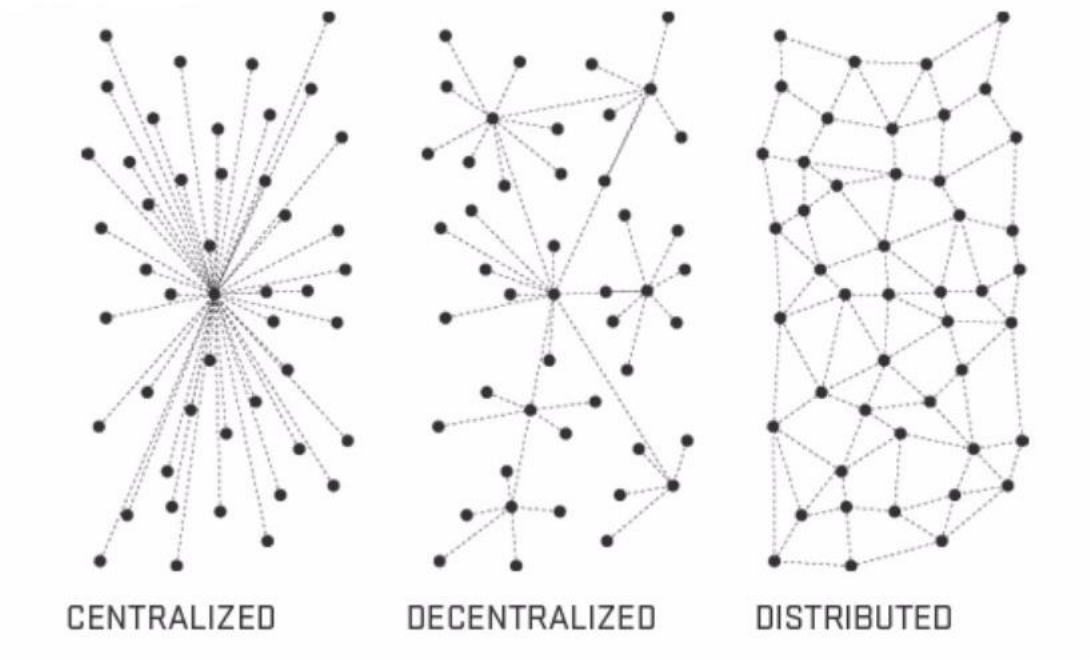
Individuals manage information from their own electronic devices such as smartphones or tablets, and share that information seamlessly across multiple electronic platforms as appropriate. With kreateIoT, users can effectively add to the chain, cryptographically signed permission slips giving other entities rights to access their stored data in particular ways. Healthcare providers, Health Information Exchanges (HIE), insurance companies, and researchers can use kreateIoT to query health data, but the individual will have the power to give permission to third parties to run queries and computations and the power to revoke that at will.

Scalability

kreateIoT off-chain is designed to connect to an existing blockchain such as Ethereum and off-load private and intensive computations from Ethereum to itself. Unlike public blockchains,

which cannot scale to clearing many complex translations and transactions, computations and data storage in kreateIoT are not replicated by every node in the network. Only a small subset of randomly chosen nodes perform each computation over different parts of the data. The decreased requirements of storage and computing power means that even users' smartphones can participate as nodes in a multi-party computation model. To keep track of who owns what data and where any given data's pieces have been distributed, kreateIoT stores that metadata in the Ethereum blockchain. kreateIoT's own off-chain computational network is used to run heavy and publicly verifiable computations, while all the transactions are facilitated by the Ethereum blockchain which enforces access-control based on digital signatures and programmable permissions.

So code is executed both on the public blockchain (public parts) and on kreateIoT (private or computationally intensive parts). kreateIoT's execution ensures both privacy and correctness, whereas the Ethereum blockchain alone can only ensure correctness. Proofs of correct execution are stored on Ethereum blockchain and can be audited. Note that code execution in Ethereum blockchain is decentralized but not distributed, so every node redundantly executes the same code and maintains the same public state. In kreateIoT, the computational work is efficiently distributed across a network of smartphones and servers which have agreed to participate in the 'dynamic translation' process (more on 'Translators' later).



Traditional Ethereum, Bitcoin kreateIoT

For scalability, and to maximize the computational power of the network, kreateIoT uses a network reduction technique, where a random subset of the entire network is selected to perform a computation for translation. The random process preferentially selects nodes based

on load-balancing requirements and accumulated reputation, as is measured by their publicly validated actions.

Interoperability

Despite well-documented benefits of patient medical records systems in terms of quality of care delivered to patients, interoperability efforts are occurring slowly. The implications of this are far-reaching, negatively impacting clinical, fiscal and operational healthcare performance. This is why a new solution that supports the entire care continuum based on blockchain's record-keeping properties is required. Electronic health information needs to be available for appropriate use at the right time in solving major challenges such as providing more effective care and informing and accelerating scientific research. While there is some progress in establishing standards and services to support health information exchange and interoperability, it is not the norm that electronic health information is shared beyond groups of health care providers who subscribe to specific services or organizations. This frequently means that a patient's electronic health information is not shared across organizational, vendor and geographic boundaries. Electronic health information is also not sufficiently standardized to allow seamless interoperability, as it is still inconsistently expressed with vocabulary, structure, and format, thereby limiting the potential uses of the information to improve healthcare.

In case of kreateIoT off-chain, instead of relying on 'interoperability standards' for healthcare data, we allow individuals to dynamically request translation services from the off-chain network using their mobile devices, while incentivizing network members to deliver the service the user needs so as to effectively share her healthcare records with entities of her choice. The network members, which could be HIE servers and members' smartphones, would not only deliver the virtual infrastructure for communication (like for bitcoin), they would also play a major role in translating among different message formats such as HL-7, CCDA, and FHIR. Additionally, the electronic health information would be normalized to allow seamless interoperability and expression with respect to vocabulary, structure, and format. Instead of using Miners to create blockchain features, kreateIoT network members or nodes (referred to as 'Translators' in kreateIoT network) translate message formats and enable communication, while also producing a version of immutability in the resulting transaction log. In Bitcoin, Miners do the work of securing the Blockchain via hashing blocks against difficulty targets. In kreateIoT, Translators enable communication via suggesting message formats which they deduce from previous communication and translation patterns.

Use Case

Let's look at a use case which takes kreateIoT off-chain features such as privacy, security, user control, scalability, and interoperability and makes them available to Bob who interacts with various aspects of the current healthcare system in his journey as a patient.

①

Bob is approaching his mid-fifties and becoming more and more health conscious; something he never worried about in his younger days.

Bob has started using Wearables and also uses certain Home Medical Equipment (HME) such as a CPAP machine.

Bob is aware that he has access to a lot of his Personal Health Records (PHRs) online; he even accesses his health information from time to time and knows about the Blue Button initiative too. He has also come across several apps that promise to consolidate his PHRs in one place.

However, Bob is overwhelmed and frustrated because his PHRs are scattered all over the place. He is tired of remembering user ids and passwords for all the different web sites that hold his health records, even though he understands that this is necessary for his privacy and security.

Even though Bob knows he has access to his PHR, he doesn't feel he is in charge of his own health records. He feels a total loss of control and ownership.

②

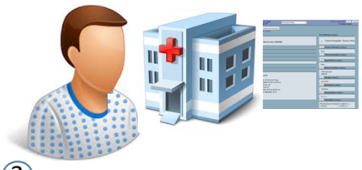
Bob downloads this new app on his phone that not only consolidates all his PHRs on his phone, but also rewards him whenever he authorizes a company or an organization to use any part of his health records for research or marketing purposes.

Bob also knows that various Electronic Health Records Systems (EHRs) in use today do not interoperate with each other, so he also opts to let his phone participate in doing translations among different health record formats (such as HL7, CDA, CCD and FHIR). He knows that his PHR will be private and secure and he will also be rewarded for letting his phone participate in these translations when its idle.

Now Bob maintains a health wallet on his phone which contains all his health records; some formatted and normalized while others in raw data form.

Whenever Bob sees any care giver he makes it a point to ask for his health records in electronic format. He knows that his doctors and other care givers have to provide this data electronically in order to qualify for meaningful use.

Bob is also connected electronically with his local Pharmacy and all his prescriptions and his pharmacy records also get downloaded in the health wallet on his phone.



③

While on the way to work, Bob feels a bit lightheaded, but after his workout that was often the case. He didn't think much about it. After he arrived at his office, he collapsed and had to be admitted to the Hospital.

It turned out that Bob had a minor stroke. After a few days in the Hospital and a few weeks at the rehab facility, life seemed to be returning to normal. He was back at work, but he knew he had an appointment with his Primary Care Physician that was coming up.

In preparation for his visit, Bob logs on to the patient portal of the Hospital and the rehab facility's EHR systems and downloads all his recent health data on his phone.

Bob was so happy that he didn't have to carry a brief case full of sheets of paper containing notes and charts and test results like he had seen his parents do when he accompanied them for their Doctors' visits.

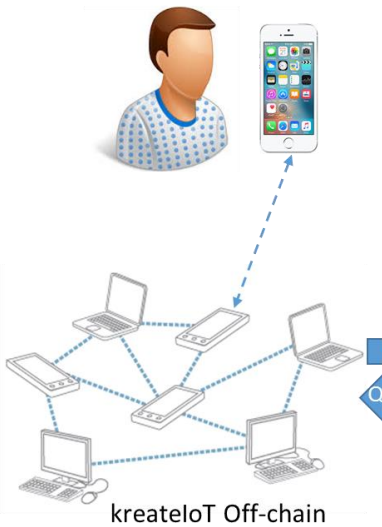
④ When Bob reaches his Primary Physician Dr. Alice's office and tries to share the data he has downloaded from the Hospital EHR system with Dr. Alice's EMR system, he realizes that the two systems are not compatible. To add to his annoyance, he is not able to share the records from the rehab facility with Dr. Alice either.

Bob remembers that he can use the app on his phone to do the translation and share his recent Hospital data with Dr. Alice.

Bob fires up the app on his phone and waits for the results…

⑥ Within seconds the translation results arrive on Bob's phone, who then uploads the data to Dr. Alice's EMR system.

If Dr. Alice's EMR system is also a participant in kreateIoT off-chain, Bob can ask for the results to be shared directly with her EMR system in a secure way.



kreateIoT Off-chain

Public Blockchain e.g. Ethereum

⑤ The app on Bob's phone requests kreateIoT off-chain to do the translation and forwards a quantum of his EHR data to kreateIoT for translation and normalization.

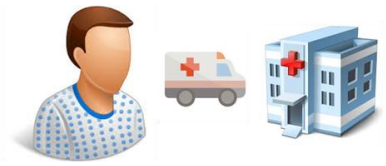
The kreateIoT off-chain breaks up the EHR data into shares, discovers other phones nearby which have signed up to be Translators, and distributes the Translation workload to a random selection of phones using a secret sharing scheme.

Each randomly selected node runs computations on its assigned block of data, until the results are sent and merged back to decrypt a block of translated data on Bob's phone.

⑦ kreateIoT logs the result of the translation and the exchange of data between Bob and Dr. Alice on the Ethereum blockchain, thereby creating an immutable record of the transaction (but without storing any of the healthcare data on the public blockchain).

kreateIoT's machine learning capabilities note the mechanics of the translation and the systems involved in the translation, and stores this knowledge for future translations.

The resultant effect of a system such as the one created by kreateIoT would be to minimize or eliminate the need for mandating EHR companies to implement new universal standards. Data interoperability continues to be an issue for both healthcare providers and technology vendors. Collecting it, storing it, normalizing it, tracing its lineage as well as its compliance and governance are all necessary so providers can harness technology innovations to glean insights that enhance patient care. The constant friction between EHR companies and market forces to open up their systems and share data with other healthcare players needs to be reduced or eliminated. kreateIoT removes the need for a trusted third party while enabling autonomous control of personal data; thereby reducing friction between EHR companies and other players.



Remember how Bob felt lightheaded on his way to work and then had a minor stroke in his office and had to be rushed to the Hospital? Well, this is what had happened.

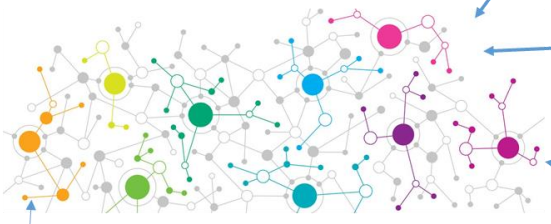
Co-workers scrambled to call 911, EMTs arrived and rushed Bob to the Hospital in an Ambulance. On the way, using biometrics for verification, EMTs scanned Bob's phone for his identifier. Bob had a profile setup previously with help from his Primary Care Physician, had included rules, and identified family members that could approve access to his medical records in case of an emergency.

Bob had four family members listed, including his wife Jane. The EMT announced and requested access to Bob's medical records on the Ethereum blockchain. Within minutes, Jane had verified access and the EMT was able to access Bob's medical records. This enabled the EMTs to provide more specific care, considering his pre-existing conditions.

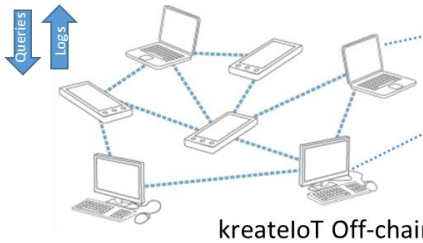
Bob had an electronic medical record on his phone that was accessible on a blockchain network, globally, by any provider and payer after authorization is provided.

Insurance Companies

Public Blockchain e.g. Ethereum



Healthcare Research



kreateIoT Off-chain

Health Information Exchanges (HIE) can have nodes that are part of kreateIoT off-chain and contribute computing power for translations and normalizations. HIEs can also request patient data from Ethereum blockchain.

Whenever there is a need for translating records from one format to another or from one EHR system to another, the translation work is handed off to kreateIoT off-chain. Translations would be performed in a secure way on the kreateIoT off-chain. The results can then be shared with care providers, payers and researchers under Bob's control and authorization. The exchanges would be recorded on the Ethereum blockchain as an immutable record of the transaction.

With new advances in technology, value alignment is found at the intersection of wearable tech and integration of medical records. kreateIoT places personal and patient information into the hands of the individual. Data from Doctor visits, EHRs, sleep patterns, heart rate, glucose, and other IoT devices (wearables and Home Medical Equipment) are all stored on individual's phone and made accessible to other authorized parties using the blockchain. As long as patients

are aware and have access to their data that is residing in various systems, patients will be able to make the choice of who they share this data with, instead of being at the mercy of technology vendors.

The goal is to enable a marketplace where patients can opt to sell the rights to use their encrypted health and medical data in bulk computations and statistics without giving raw access to the underlying data itself. The marketplace would eliminate tremendous amounts of friction, lower cost of customer acquisition and offer a new way to generate health credits or income stream for patients. Primary care providers would be able to select effective medications for patients with certain conditions based on their genetic profiles and results of comparative effectiveness research. Individuals, care providers, public health and researchers will be able to contribute information and learn from information shared across the health IT ecosystem.

Conclusion

In this paper, we have described a way of building a composite blockchain from two different blockchains – Ethereum and kreateIoT. The underlying mathematics of both algorithms differ significantly. Hashing is based on Cryptography while Machine Learning is Algebraic. The result is a system that doesn't rely on standards (instead, it uses Machine Learning to learn differences in health information formats and their contexts based on successful and failed negotiations). Such a system could lead the way to dissolving quasi-monopolistic information silos by connecting both large and small players into a large enough communicating network. Combining this off-chain Machine Intelligence Proof of Translation with existing blockchain technology such as Ethereum delivers a version of immutability; a necessary step to allow an open and un-permissioned eco system, even though there are legitimate reasons to restrict access to sensitive parts of such networks. When off-chain kreateIoT network is used with a blockchain such as Ethereum we achieve interoperability, privacy, security, scalability and immutability of records. This way we achieve what HITECH was designed to ultimately improve: clinical outcomes, improved population health, increased transparency, empowered patients and more research data.

Table 1: A comparison between Bitcoin implementation and kreateIoT implementation

	Bitcoin Implementation	kreateIoT Implementation
Computing Power: Use the computing power of a large distributed system	Miner's hashing power	Predictive machine learning capabilities
Incentives: Cryptocurrency reward for completing an atom of work	Rewards for hashing block headers	Rewards for translating and normalizing healthcare records on demand
Consensus: Establish consensus in a distributed (immutable) system	Immutable transactions	Common and agreed machine terminology
Disintermediation of trusted middleman: Disintermediating of instance that oversees both sides and acts as mediators between participants	Banks, Credit Card companies, PayPal	Interoperability Gateways (technology, vendors)

Table 2: A comparison between Ethereum Proof of Stake and kreateIoT Proof of Translation

	Ethereum Proof of Stake	kreateIoT Proof of Translation
Purpose	Create an immutable Blockchain for contracts	Create common message formats to allow machines to communicate
Work to be performed	Find a value for the nonce that results in a block header hash that is less than the difficulty target	Find a format/content which sender and receiver approve
Deterministic?	Yes, for any input (arbitrary length) e.g. SHA 256 will always produce the same fixed length output	Almost always. The variability will be in the usability of the translated data
Predictable timeframe?	Yes, statistically	For most messages 'yes' statistically, but there could be non-translatable messages
Can it fail?	Statistically not	Yes, sender and receiver could never reach an agreed message format (format/content)
Money supply	Ether	New? Ether?
Hard to find solutions?	Yes, depending on difficulty target	Will generally get easier with the learning effect of the network. There can always be very hard or untranslatable messages
Easy to verify solution?	Yes, feature of hash function	Partially, sender and receiver have to agree and sign the message, which can be verified. Deciding if a translation is useful is subjective
Workload difficulty adjusting over time?	No	Yes, network learning effect implies that translations will get easier. There can always be very hard or untranslatable messages
Difficulty of winning reward	Increasing (money supply decreasing and workload difficulty unchanged)	Over time lesser need to do translations because of machine learning but there will be more data available for analytics which could generate rewards for patients
Payer	Mining Reward: Ether Transaction Fee: Sender of Ether	Translation Reward: New? Ether? Transaction Fee: Insurance companies, Researchers
Cheating possible?	No	Unlikely
Immutability?	Yes	'Weak immutability' per default as sender and receiver need to agree to changes. 'Strong immutability' in combination with existing proof of stake

Acknowledgements:

- Nitin Gupta – Blockchain, Distributed Database and Technology Advisor to kreateIoT
- Enigma: Decentralized Computation Platform with Guaranteed Privacy - Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland
- Babelchain Machine Communication Proof of Understanding - Benedikt Herudek