Making Blockchain REAL for business

CASE STUDY: Health Information Exchange (HIE)

Background

SECURITY THREAT

The blooming threat to PHI security is all over the places, building up a pile of inconvenient questions regarding HIE.

Case Study Client Industry:
Healthcare & Life Sciences

Applicable Industries:
- Healthcare
- Pharmaceutical
- Life Sciences

Business Use Case

✓ How can healthcare organizations control patients' private data transfer to other caregivers in a trusted way? Some providers can't even guarantee PHI security within their own organization, let alone its journey to other institutions. EXAMPLE: A patient with diabetes travels around the country, catches a cold and gets admitted to the hospital outside their network because of severe headaches and blurred vision coming with fever

✓ How can the hospital access PHI, find out more about the patient's diabetes history, analyze the patient's health data in general and treat this hyperglycemia episode together with a cold?

CHAINNINJA PROVIDES THE ANSWERS

Challenges

Hindering Healthcare IT

HIE

CHALLENGES

Data Security & Privacy & Operational

Sensitive Interactions

PHI

MUST BE ASSURED

Challenges

MULTIPLE REASONS PHI MUST BE ASSURED

- ✓ No uniform architectures & standards to ensure trusted access to PHI and PII (personally identifiable information) & safe data exchange between all stakeholders, including patients
- ✓ Hinders patient engagement due to patients' limited ownership of their health data, hurts care cooperation between providers from different networks, and also back-pedals population health management since caregivers can't effectively exchange their insights in a secure way
- ✓ Major issues related to privacy and security include:
    - ✓ Hacking attacks
    - ✓ Data integrity and availability
    - ✓ Trust and access control
    - ✓ Confidentiality of PHI and PII
- ✓ Nonrepudiation
- ✓ Compliance with HIPAA and other privacy regulations

PATIENT ENGAGEMENT ISSUES

- ✓ Poorly trackable clinical outcomes
- ✓ Fragmented efforts in population health management
- ✓ Inconsistent disease management

Solution

ChainNinja built a "Chain of Trust" where we have created a new health information exchange framework and solved related problems

We have defined blockchain as a distributed record of peer-to-peer transactions composed of interlinked transaction blocks in a digital ledger. It is a system with no central authority, where each participant can store, exchange and view information without pre-existing trust.

Each blockchain network participant has a secret private key and a public key that acts as a visible identifier. This pair of keys is cryptographically linked so that identification is possible only in one direction by using the private key that unlocks a participant's profile.

Due to identity permission layers, patients can limit data access and then share relevant parts of their personal information with particular providers within their care network.   A potential attacker will not be able to crack a single patient's private key to access PHI. Instead, the hacker would need to steal each user's private key to obtain valuable identifiable information.

Taking this further, banks that positively identify a fraudulent transaction could distribute details of that transaction globally to all connected banks, thus preventing the opportunity for further fraud.

All providers within one blockchain can keep their own copy of the health care ledger. If the block is to be adjusted, 51% of network participants have to approve the change, as every copy of this blockchain should be updated to reflect the change. This feature improves security and helps to limit the risk of a malicious activity since all changes are broadcasted within the network and distributed ledgers provide safeguard copies against hacks or tampering attempts.

4 WAYS THIS BLOCKCHAIN – BASED DATA PLATFORM CAN BENEFIT HEALTHCARE PROVIDERS AND HEALTH SYSTEM

✓ Friction in data exchanges are reduced
✓ The quality of care is improved
✓ Health literacy in patients is increased
✓ Data Security is Enhanced

SMART CONTRACTS

BENEFITS

Patients get suspicious about recording and sharing their social and health data. Health data including Identity, genetic or biometric data is accumulated from various settings. Patients need to feel they own their data.

Helps providers to gain patients' trust since individuals will be able to track everything that happens with their information. Here, trust means better visibility in a patient's health status outside the clinical setting and between appointments.

In population health management, providers use blockchain to progress in clinical research, patient safety event reporting, adverse event identification, public health reporting and precision medicine. Through the blockchain transaction layer, organizations can access sets of standardized, non-patient identifiable data. These data sets are then analyzed with cognitive computing, machine learning and analytics.

Smart contracts serve as a gateway to store standardized information, which all network participants can immediately access thanks to API-oriented architecture.
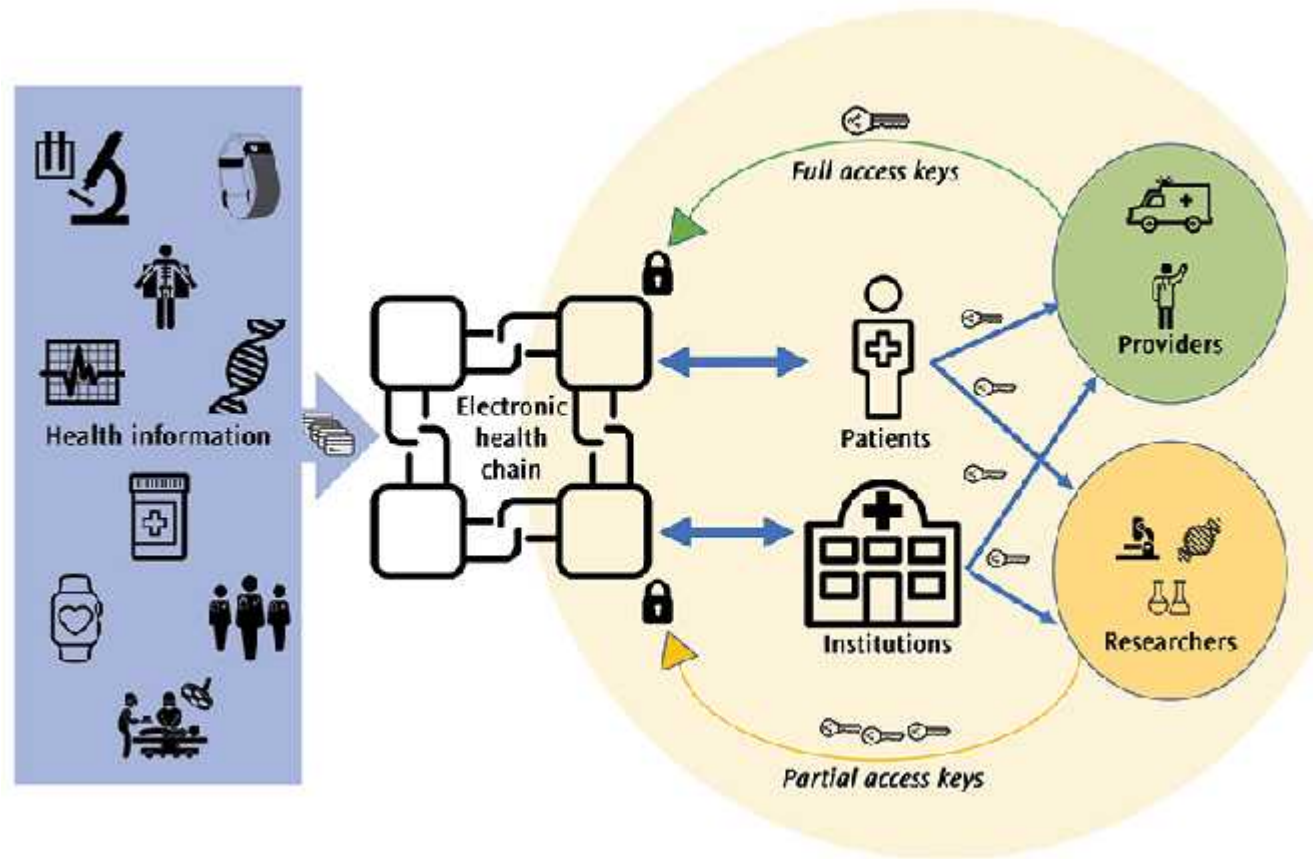
This architecture allows for seamless integration with each organization's existing systems, so providers can focus on their internal systems.

Blockchain also helps with frictionless connectivity since it's supported by smart contracts and consistent authorization to access health data
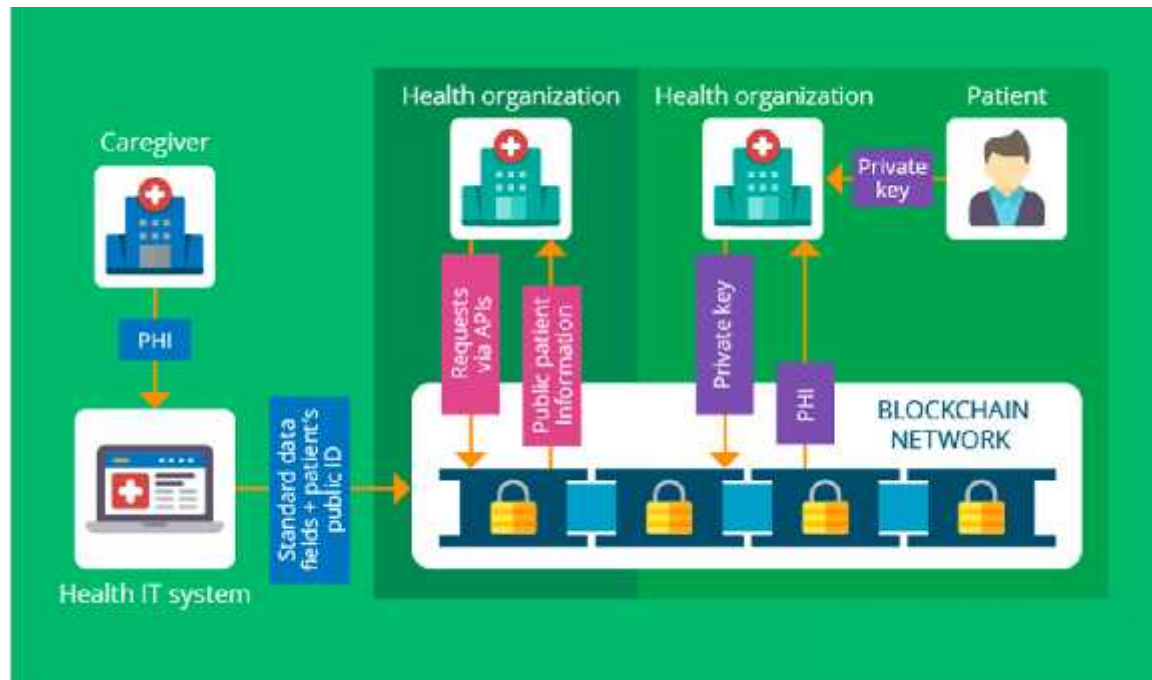
Logical

Technical

ChainNinja = Results

✓ Custom End to End Solutions
✓ Specialized Blockchains
✓ Collaborative, Agile and Efficient
✓ Open Platform and Open Governance
✓ Regulatory Compliance
✓ Coexistence with Adjacent Systems

Sanjay Kumar, CTO provides strategy and architecture consulting, business use cases applicability assessment, Blockchain tools selection, developing PoCs using open source frameworks for both public and private Blockchain platforms.