SURETEK INFOSOFT *CASE STUDY*

VERIFIABLE NURSING CREDENTIALS ON BLOCKCHAIN PLATFORM

CLIENT PROFILE

Our client is an emerging Decentralized Autonomous Organization dealing in Virtual Healthcare. They are developing a blockchain based virtual care network platform. They strongly advocate bringing blockchain to the healthcare industry and nursing profession in particular.

BUSINESS CHALLENGE

Healthcare is at a crisis globally, with global demand for medical services outpacing the ability to verify the health records of physicians. Every healthcare organization uses a "credentialing" process to ensure that each of its affiliated physicians and other clinicians are competent and worthy of trust that patients put in them. In a way, credentialing is a process used by hospitals to avoid misconduct.

Healthcare complexity can be reduced using the application of blockchain technology to medical licensing records. The client realizing the potential of blockchain implementation and started to develop a secure blockchain based verification system which helps validating the records of the physicians.

SURETEK SOLUTION

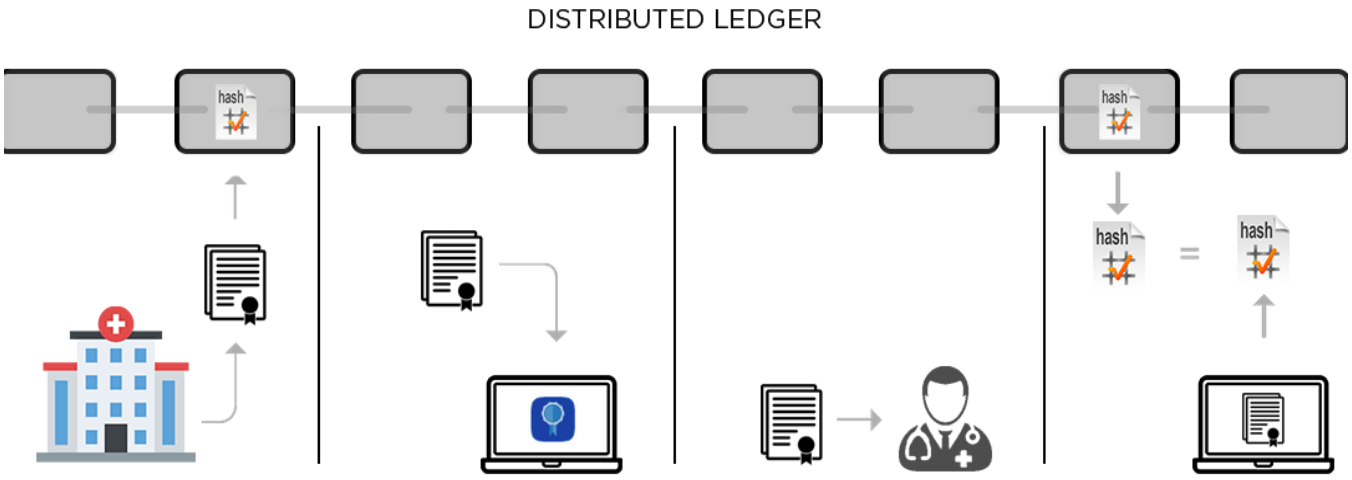
Suretek proposed a way to create a safe and secure system of storing physicians credentials built upon a distributive ledger known as the blockchain.

Blockchain is well-matched for credentialing. Every piece of documentation supplied by the physician, and every verification action performed by the hospital credentialing office, are viewed as transactions to be entered in the permanent ledger.

SURETEK'S CONTRIBUTION

- Development of mobile and web application using the blockchain technology in the backend.
- Implemented private distributed data network using the IPFS protocol.
- Verification process of licenses using third party API – Nursys.
- Utilizing digital signatures/hash values on blockchain-based data which allows access only when authorized.
- Embedding a combination of a hash signature of the document which is stored in a separate, mutable data system (IPFS).
- Developed the oracle services which were further utilized by Smart Contracts.

- Employing Consensus decision making, where all parties agree to the validity of transaction and commit it to the blockchain workflow helping secure the transactional data.
- Harboring Asymmetric encryption to encrypt the transactional files using the public key of the recipient allowing only the intended officials to access the data records.
- Implemented proxy re-encryption algorithm using NuCypher KMS for encryption and decryption.
- Developed the smart contracts for issuing tokens and rewards.



TECHNOLOGIES USED

NuCypher KMS, pyUmbral, PHP (Laravel), iOS and Android development platform, Python, IPFS, Qtum, NurSys QuickConfirm API