Scrybe: Blockchain Ledger for Clinical Trials

(2018-035)

Scrybe incorporates a Lightweight Mining Algorithm which ensures data integrity, and non-repudiation making it a strong solution for securely storing clinical trial data

Market Overview

Scrybe utilizes Lightweight Mining (LWM) which always the algorithm to depart from the resource-intensive and time-consuming verification approaches that cryptocurrencies use when expanding the blockchain. The clinical trials market size is expected to reach 68.9 billion by 2026, growing with a CAGR of 5.7%. Digitization is rapidly be adapted by securely maintaining patient data record which lowers cost and reduces process errors. Ensuring that trial data is securely stored is essential to meet stringent regulations from governing bodies like the FDA. Scrybe also prevents malicious manipulation of data and is not dependent on local policy. This allows auditors to verify the integrity of the stored data, and the data integrity and non-repudiation are guaranteed.

Technical Summary

Scrybe has two main components: blocks and transitions. Blocks are added to the blockchain by authorized miners. Transactions can reference previous transactions, providing a chain of custody, or they can be genesis events, which register the acquisition of new data. Both patient information and permissions are collected and stored on a local server controlled by the medical institution. Using non-sensitive meta-data, a transaction is created on the secure server and a permanent universal resource locator (PURL) is created pointing to the data. The transaction is signed and submitted to miners. These miners add the transaction to a block which is then added to the blockchain where it can be broadcast to other miners for verification. Raw data is collected and stored locally on a secure server. This process is repeated as more information is generated and subsequently associated with the original transaction. This allows auditors and researchers to access the findings of other teams by viewing transaction records within the blockchain complete with signature for data verification.

Application

Clinical trials, information security, data management

Development Stage

Ready for Licensing

Advantages

- All data is digitally signed ensuring integrity and allowing it to be tracked
- Improved energy efficiency and lower cost
- Can tolerate a larger percentage of malicious actors

App Type	Country	Serial No.	Patent No.	CURF Ref. No.	Inventors
	United States		NA	2018-035	Dr. Richard Brooks, Dr. Tony Skjellum, Dr. Lu Yu

About the Inventors

Dr. Richard Brooks

Professor of Electrical and Computer Engineering at Clemson University

Dr. Brooks has in the past been PI on research programs funded by the Air Force Office of Scientific Research, National Science Foundation, Department of Energy, National Institute of Standards, Army Research Office, Office of Naval Research and BMW Corporation. His network security research projects have included funding from NSF (analyzing wired and wireless denial of service vulnerabilities), DoE (authentication and authorization of exa-scale storage systems), BMW Corporation (controlling dissemination of intellectual property), and the US State Department (creating anonymous communications tools for civil society groups). It frequently looks at attacks that disable security measures by working at a different level of the protocol stack.

For more information on this technology contact:

curf@clemson.edu
Please put technology ID in subject line of email.