

Veracity Technology Spearhead

Enabling end-to-end veracity within value exchange ecosystems

Supporting rules-as-code using NFTs stored on a private blockchain

Hayden McAlister University of Otago
Stephen Cranefield University of Otago
David Evers University of Otago

Background

Blockchain is presented as a decentralised technology to support the interactions of people and organisations. A key benefit of blockchain systems is that they can facilitate building computer systems that involve multiple parties cooperating, yet do not need to deploy these systems in a centrally controlled manner.

This project employs a particular open source blockchain technology, Hyperledger Fabric. Compared to the blockchain that cryptocurrencies such as bitcoin and Ethereum use, Hyperledger Fabric is known as a 'closed', 'private', or 'permissioned' blockchain, meaning that the set of participants collaborating to store the blockchain is controlled.

The project prototypes a platform on which a system was built to track stakeholders' interactions within a human organ allocation use case. The software uses a "rules-as-code" design, in which there is a clear link between the human-readable specifications of regulation and its implementation in code. The blockchain system verifies both the state of interactions and the rules that are being checked within the use case.

Relevance of findings to Aotearoa New Zealand

On blockchain, given that Aotearoa New Zealand involves a large number of small interacting commercial organisations, closed blockchains are an appealing way to reduce the administrative difficulty in setting up software that needs to be reliable, but still operate in an efficient manner, when interconnecting independent parties that have a mutual record-keeping objective.

Regarding rules-as-code, the small scale of Aotearoa New Zealand is a benefit for exploring such systems: some existing local successes in deploying rules-as-code have come from being able to form small teams whose members span expertise in many areas, including technical ones.

Main research findings

Our prototype demonstrates a means to link an existing data storage and rule checking system with a closed blockchain. The blockchain allows the authenticity of the rule checking system's inferences to be verified. Persistent cryptographic records are maintained that indicate how input and output data, and the rules themselves, are being changed over time.

The unique cryptographic records stored on the blockchain are a form of Non-Fungible Token (NFT): a digital identifier used to identify ownership and to track provenance over time. NFTs require associated software that manages their ownership. In open blockchains this software is implemented using new, inherently risky smart contract programming languages.

Our prototype demonstrated that instead, more typical types of programming could be used to manage our system's digital records. Further, the record-keeping consensus mechanism in the blockchain is not a performance bottleneck, and increased resilience of record storage can be facilitated easily by adding more server computers into the underlying blockchain.

A web-based interactive notebook was used to provide a user interface through which events relevant to the interactions between parties could be recorded, and consequent rule-based inferences could be queried.

In order to effect highly reproducible, automated software deployment, our prototype was developed using software container technology. The source code for our work is publicly available on GitHub and has already been successfully deployed within subsequent research work.

See: <https://github.com/veracitylab/SWIPL-Notebook-Blockchain-Filehashing>

