Challenges of Trustable AI and Added-Value on Health
B. Séroussi et al. (Eds.)
© 2022 European Federation for Medical Informatics (EFMI) and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).
doi:10.3233/SHTI220479

Non-Fungible Tokens as a Mechanism for Representing Patient Consent

James CUNNINGHAM[a,1], Nigel DAVIES[b], Sarah DEVANEY[c], Søren HOLM[c], Mike HARDING[b], Victoria NEUMANN[b] and John AINSWORTH[a]
[a] *Division of Informatics, Imaging and Data Sciences, Health EResearch Centre, Manchester Academic Health Science Centre, University of Manchester, Manchester, United Kingdom*
[b] *Department of Computing and Communications, Lancaster University, Lancaster, United Kingdom*
[c] *CSEP, Department of Law, School of Social Sciences, The University of Manchester, Manchester, United Kingdom*

Abstract. In recent years we have seen the adoption of distributed ledger technology (DLT), originally the mechanism underpinning the operation of the Bitcoin crypto currency, across a wider range of technology sectors including healthcare. DLT allows for the design of informatics systems with the properties of immutability, security, and decentralization. One recent innovation in the space has been the specification and development of Non-Fungible Tokens (NFTs). NFTs are decentralized DLT-based records that represent ownership of a unique digital asset. The predominant current use case for NFTs has been in the representation and sale of digital artwork, however the features offered by NFTs, unique-ness, immutability, transferability, and verifiability, are directly applicable to the design of health informatics systems. In this paper we explore these properties and describe a reference architecture for using NFTs as a means of representing and transferring records of patient's consent for medical data use.

Keywords. blockchain, health information technology, distributed ledger technologies, digital health

1. Introduction

Distributed Ledger Technology (DLT), or blockchain, is the core innovation of the Bitcoin digital currency, created by the pseudonymous Satoshi Nakamoto as a decentralized, trustless, and pseudonymous alternative to traditional fiat currencies [1]. DLT is the mechanism by which distributed nodes in a peer-to-peer network can achieve consensus as to a canonical sequence of transactions that have been processed by the network, even where there exist nodes within that network acting maliciously – a solution to the so-called Byzantine Generals problem [2]. Based around public key cryptography [3] DLT allows for the creation of digital networks with the properties of immutability, security, decentralization, and trustless-ness [4]. This technology has seen adoption across a range of industries including the energy sector [5], smart cities [6], government [7] and transport [8]. In healthcare DLT has seen use in a wide range of healthcare

[1] Corresponding Author, James Cunningham; E-mail: James.A.Cunningham@manchester.ac.uk.

applications such as vaccination coordination [9], medical record access [10], access to healthcare service marketplaces [11] and pharmaceutical supply chain management [12]. In all such instances, the key properties of DLT around security, data permanence and lack of central control, are being leveraged to enhance both institutional and public trust in the systems being developed and to provide guarantees around the security and integrity of sensitive medical data [11]. The core features of DLT have been extended with the adoption and implementation of smart contracts [13], executable specifications of instructions that can manipulate data held on a blockchain. The predominant use case of smart contracts has been the creation of digital tokens – fungible, ownable and tradable as-sets represented by a record within a smart contract of the quantity of the token owned network participant. These tokens are utilized for a range of purposes such as, for example, being sold for funding in exchange for an ownership stake in an enterprise, the representation of weighted voting rights in some form of governance mechanism or simply as currencies in and of themselves [14]. More recently we have seen the use and adoption of Non-Fungible Tokens (NFTs). Contrasted to standard tokens NFTs are used to represent a unique, rather than homogenous and fungible, asset, for example an item of digital artwork, whilst sharing the properties of ownership and tradability with ERC20 tokens [15]. The predominant use of NFTs has in-deed been within digital artwork, where the creators of artworks can embed and transfer ownership rights to digital art works/ This ability to imbue uniqueness onto inherently reproducible digital resources can be seen as the key innovation of NFTs. Other examples of NFTs include applications within the internet of things, to represent assets within land registries and ownership digital assets within online gaming. In healthcare specifically NFTs have been utilized as a potential governance mechanism for the governance of genomic data sets [15]. This paper explores the use of NFTs in the healthcare space, in particular the representation of consent for data re-use.

2. Methods

NFTs are implemented as coded specifications of smart contracts hosted on blockchain infrastructure. The pre-dominant implementation of NFTs is on the Ethereum blockchain, where NFTs are implemented against the ERC-721 standard. This defines NFTs as being smart contracts that record the following information for a given asset that is to be represented by the NFT: A record of the owner of the NFT; An optional quantity representing the quantity of the asset held by the corresponding owner; Functions for transferring the ownership of the NFT, and for delegating the ability to transfer ownership to third parties; A URI recording the location of the digital asset represented by the NFT.NFTs define a **unique** representation of a digital asset, that is, whilst the representation of the asset itself may be duplicated, there is only a single canonical representation of that asset as recorded by the underlying NFT. They are **verifiable**; given reference to an NFT, there is a defined method of deciding whether the representation being referenced is the same one as originally created by the originator of that NFT. They are **transferable**, meaning they are owned by the holder of a single private key and that **ownership** property can be transferred to the owner of a different private key. They exhibit **immutability**, in that information recorded about an NFT, including its current state and the history of its ownership cannot be deleted or changed in any way. These properties have broad applicability across applications in the health informatics domain. **Uniqueness** – references to medical data, and in particular records

of the associated rights to use that data should be singular items which cannot and should not be copied within the bounds of a system. The property of unique-ness allows such items to be represented without reliance on a centralized, potentially fallible data bases. **Verifiability** – it is crucial that the provenance and legitimacy of digital artifacts within healthcare systems is accounted for, Cryptographic verifiability can ensure that this property is met. **Transferability** – ownership of digital medical records, the rights to access those records and metadata about the use of those records can all be individually owned and transferable instances within healthcare applications. Immutability – the ability to audit medical systems to ensure regulatory compliance and to allow patients to verify legitimate use of their data is automatically accounted for by the property of immutability.

3. Results

We produced an architecture and reference implementation of a system for transmitting the consent of multiple data subjects to use their data for research purposes and to allow legitimate consumers of such data to apply these consents to obtain data from medical data providers. Once these consents have been obtained and used for a specified purpose then they are no longer able to be used to obtain further data. This system uses NFTs as the mechanism for recording and transmitting these bundles of consents between data consumers and data providers in such a way that the system does not need to rely on a trusted third party to verify the legitimacy of these consents. The system is designed to enable data subjects to record signed records of consent that permit Data Consumers to request medical data from Data Providers in line with the consents that have been given by the subjects to which that data pertains. Further: Consent should be obtainable independently of any entity other than the data subject who pro-vided that consent; Once obtained, consent can be used to legitimately obtain data by presenting it to a data provider which acts as the guardian of a data subject's medical data; There should be a permanently auditable record of which consents have been used by who for what purposes; No entity should be able to prevent or revoke the application of a consent to obtain data out-side of the data subject and the data provider. The high-level architecture of the system is illustrated in Figure 1, a description of the individual components of the system is given in the following sections.

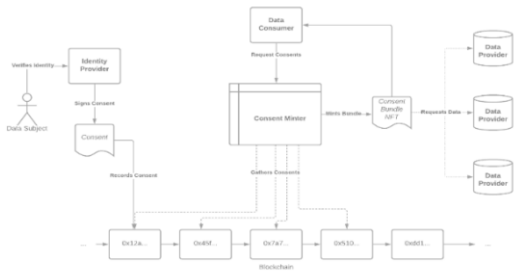

Figure 1. System Architecture.

Data Subject: an individual who has the rights to consent to the use of medical data for a given purpose. Within the system the role of a data subject is to verify their identity with an Identity Provider, allowing them access to the functionality of the system.

Identity Provider: the component responsible for verifying the identity of data subjects. An Identity Provider transmits and records signed records of Consent from Data Subjects.
Consent: an object consisting of a message, signed by an Identity Provider, which is written to the underlying blockchain through a smart contract, recording the following information: The signature of the Identity Provider issuing the consent; A pseudonymized identifier of the subject of the consent; A designation of the type of data the consent refers to; A designation of the purpose of use which is being consented for.
Data Consumer: entities within the system that wish to request data from Data Providers. Data Consumers can request data about sub-jects by providing references to recorded consents for the use of data to Data Providers in the form of Consent Bundles.
Consent Minter: Once consents have been gathered from data subjects and recorded, Data Consumers can call a Consent Minter smart contract which mints a unique NFT that references a series of recorded consents that have been issued for a given purpose.
Consent Bundle NFT: A Consent Bundle is an NFT representing a group of consents for a given purpose. The bundle can be passed directly from a Data Consumer to a Data Provider alongside a request for data to demonstrate the legitimacy of that request. Alternatively Consent Bundles can be passed or exchanged between data consumers or reserved for use at a later data. Once used to obtain data the NFT can be marked by the Data Provider as having been used. This can allow other data providers to base their decision to release data against that NFT on its previous use or can be 'burned' by the Data Provider, preventing its future use.
Data Provider: Data Providers are the entities within the system that are responsible for the storage of medical data and the transmission of that data to Data Consumers. They are responsible for verifying the identity of the Data Con-sumer making the request for data to ensure the legiti-macy of that request, and for consuming and processing the Consent Bundle object used to verify the legitimacy of an incoming request. The system was implemented on top of the Ethereum network. Since deployments and interactions with smart contracts on the network incur a so-called gas fee, pay-able in the Ethereum cryptocurrency, we deployed the system onto one of the Ethereum test networks, where obtaining the 'currency' used for gas payments is free. Smart contracts were written using version 0.8.0 of the Solidity programming language and the non-blockchain specific portions of the system were written in a mixture of the Go programming language and JavaScript, particularly utilizing the Web3.0 Ethereum libraries.

4. Discussion

We have looked at a reference implementation of a system whereby consented bundles of rights to access healthcare data are represented as NFTs and can be passed between parties without the knowledge of either the issuer or consumer of those rights. When those rights are exercised to access data those rights then expire. Whilst such a system could be implemented using a traditional informatics architecture, the ability to transfer privately, securely, and freely such rights around before access, and to do so outside of the knowledge and control any centralized entity are features unique to an DLT-based NFT solution. Whether these properties are necessary or even desirable in the context of an eHealth application will be dependent on the specific environment in which the system is implemented and will need to account for ethico-legal considerations. However, as with all healthcare systems, public perception and trust can be crucial factors in determining the ultimate success of a given application. The ability to transfer trust away

from a single entity into a system wide implementation may enhance both the perception of trust in the system and serve to mitigate the fallout from misuse or failure of the system away from a single entity thereby encouraging adoption. NFTs can provide a mechanism by which implementations of health informatics architectures can remove centralized sources of trust where it is deemed necessary. Where this is seen as beneficial and a desirable property NFTs provide an efficient and so-far unique means of doing so. NFTs represent a means of imparting uniqueness on digital assets and allow such assets to be owned and transferred as singular items (contrasted even with other blockchain-based approaches to managing patient consent), whilst preventing their duplication. To allow this in an informatics infrastructure that does not rely on the single entity or trusted third party to provide such functionality is a function unique to NFTs. Within medical informatics applications the properties provided by NFTs can potentially be used in situations that require the exchange and execution of unique one-time rights in situations where trust in the overall system will be enhanced by removal of reliance on a single component of the system. Moving forward we would conclude that NFTs can play a significant role in the development of eHealth applications.

References

[1] Nakamoto S. "A peer-to-peer electronic cash system." Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf 4 (2008).
[2] Lamport L, Shostak R, and Pease M. "The Byzantine generals problem." In Concurrency: the Works of Leslie Lamport, (2019) pp. 203-226.
[3] Salomaa A. Public-key cryptography. (2013)
[4] de Leon DC, Stalick AQ, Jillepalli AA, Haney MA, Sheldon FT. Blockchain: properties and misconceptions. Asia Pacific Journal of Innovation and Entrepreneurship. 2017 Dec 4.
[5] Mihaylov M, Jurado S, Avellana N, Van Moffaert K, de Abril IM, Nowé A. NRGcoin: Virtual currency for trading of renewable energy in smart grids. In11th International conference on the European energy market (EEM14) 2014 May 28 (pp. 1-6). IEEE.
[6] Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. In2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS) 2016 Dec 12 (pp. 1392-1393). IEEE.
[7] Atzori M. Blockchain technology and decentralized governance: Is the state still necessary?. Available at SSRN 2709713. 2015 Dec 1.
[8] Yuan Y, Wang FY. Towards blockchain-based intelligent transportation systems. In2016 IEEE 19th international conference on intelligent transportation systems (ITSC) 2016 Nov 1 (pp. 2663-2668). IEEE.
[9] Williams-Grut O. Estonia is using the technology behind bitcoin to secure 1 million health records. Bus Insid. 2016.
[10] Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In2016 2nd international conference on open and big data (OBD) 2016 Aug 22 (pp. 25-30). IEEE.
[11] Leeming G, Cunningham J, Ainsworth J. A ledger of me: personalizing healthcare using blockchain technology. Frontiers in medicine. 2019 Jul 24;6:171.
[12] Mattke J, Hund A, Maier C, Weitzel T. How an Enterprise Blockchain Application in the US Pharmaceuticals Supply Chain is Saving Lives. MIS Quarterly Executive. 2019 Dec 1;18(4).
[13] Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper. 2014 Apr;151(2014):1-32..
[14] Victor F, Lüders BK. Measuring ethereum-based erc20 token networks. InInternational Conference on Financial Cryptography and Data Security 2019 Feb 18 (pp. 113-129). Springer, Cham.
[15] Wang Q, Li R, Wang Q, Chen S. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447. 2021 May 16.
[16] Uribe D, Waters G. Privacy laws, genomic data and non-fungible tokens. The Journal of The British Blockchain Association. 2020 May 30:13164.