Interoperability of Medical Records on the Neuro-Ledger

Executive Summary

Peter Waher, Mateo Florez

Trust Anchor Group AB
peter.waher@trustanchorgroup.com
mateo@trustanchorgroup.com

Abstract. This paper describes how the Neuro-Ledger® can be used to create an open, interoperable, and yet secure, infrastructure for the exchange of medical health records and related information between service providers and stakeholders in a flexible and extensible manner, while at the same time complying with standards and regulations regarding cybersecurity, privacy, and interoperability. Furthermore, a mechanism where health information can be monetized is presented, giving people an opportunity to be reimbursed for sharing their health information, for example, in the form of anonymized or pseudonymized information shared with research organizations and companies, all using a zero-configuration infrastructure, allowing stakeholders to make agreements without manual interaction with operators of technical infrastructure.

Keywords: Neuro-Ledger, DLT, Interoperability, Privacy, Cyber-Security, Medical Records, HL7, IEEE 2933, EHDS.

1 Introduction

Regardless of how health services are organized in different nations, there is increasing pressure to access private medical records and related health information from people. There are many reasons for this, such as mobility, international cooperation, travel, and research automation. A concrete example is health insurance companies, banks and financial institutions that want to better model insurance policies to estimate risks. Reversely, it is in the people's interest to be able to select health service providers themselves, allowing the service providers access to their history, regardless of where they have lived or worked before. Creating central repositories for such information is not feasible or of interest due to privacy and cybersecurity concerns. And if such a repository is not global, it would have limitations, boundaries of its own, and it would only be a matter of time before requirements to interoperate across such boundaries would require an even larger and more centralized repository to be formed. Instead of a centralized approach, a globally scalable, decentralized, federated, and interoperable model is preferred, where stakeholders can interact with each other, without previous permission from central authorities (so-called local governance) and where people are owners of their information and can control who can

© Neuro-Foundation 2024

access it, and for what purposes. However, to do so, a new type of technical infrastructure is required, one that allows people and organizations to make agreements on which automatic processes and communication can be based. For agreements to be made, a method to properly identify actors is needed, in a way that works in a legal context. Furthermore, programable payments and payment distributions must be supported, adhering to signed agreements, and a system for defining information ownership must be established.

2 The Role of the Neuron® in Interoperation

To solve the challenges of interoperation in a smart and open society, the Neuron® was created. It is the basis for creating a globally scalable, federated, open, and secure network. It helps participants connect and exchange information securely, regardless of the domain to which they are connected. Each domain can be locally governed, and interoperation across domains is still possible. The basis for global, federated interoperation, is the XMPP protocol[1]. It is standardized by the Internet Engineering Task Force (IETF) and is the basis for many communication-related software on the Internet, most notably Instant Messaging applications, but also other types of applications, including Internet of Things[2]. The applications have multiple things in common: Real-time communication over the Internet, in a secure manner that protects confidentiality and privacy. Apart from providing users with XMPP connectivity and instant messaging and communicating in real-time with connected devices, the Neuron® also provides users with means to create legal self-sovereign identities[3], smart contracts (including legal agreements) and tokens (transparent applications defining ownership)[4], to perform instant payments, programmable payments and conditional payments, as well as trade between parties using automated auctions[5].

3 The Role of the Neuro-Ledger® in Interoperation

As soon as a system starts operating in a legal context, there is a need for transparency and auditability. Due to the private and sensitive nature of the information processed by the Neurons, typically distributed ledgers such as blockchain cannot provide transparency to the stakeholders. A blockchain would reveal too much information to participants, and stakeholders would lose control (ownership) of the information placed there, as there is no control on whom can access it[6]. For this reason, the Neuro-Ledger® was introduced. All legal transactions processed by a Neuron® are recorded on the Neuro-Ledger®, to assure not only transparency and auditability, but also compliance with privacy regulations (like the GDPR) and protect confidentiality and ownership of information.

The Neuro-Ledger® is a next-generation distributed ledger (DLT) that solves many of the inherent problems of traditional blockchain-based distributed ledgers. Instead of blocks chained together, blocks are standalone, and the distributed ledger is federated and distributed. As with the Neuron® itself, this means that all domains are free (using principles of local governance) to generate any blocks they choose to, and

then to distribute them according to principles set forth by cooperating domains. Any domain can interoperate and cooperate in any exchange of information agreed upon.

4 Interoperation of Sensitive Information

The Neuro-Ledger® is not the principal interface for the interoperation of sensitive information. This is done by the Neuron® itself. Each participating Neuron® has its own ledger, annotating everything that happens within its domain of influence. Just like a company can have its own ledger for its own bookkeeping, it does not need to share its ledger with other companies when it does business (and it should not, or it would not be able to keep its trade secrets). It only needs to share the ledger with actors that require access to it, such as subsidiaries, partners, auditors, authorities, and more. Likewise, Neurons interoperate in real-time with each other, without the need to share ledgers. Each Neuron® participating in a transaction notes a record in its ledger from its point of view.

The Neuro-Ledgers themselves can also interoperate to share blocks, or collections of blocks. Typically, the flow of blocks is based on criteria different from that of sensitive information between Neurons. Neurons share information for interoperability purposes to provide distributed services. This is done at a very fine-grained level: Only information authorized by their owners is shared with properly authenticated parties. Neuro-Ledgers share blocks for resilience, redundancy, or for cooperative work and data synchronization across domains (data mirroring). While blocks are ordered into collections, and different collections can be shared differently, they can still contain multiple items of information in each block. It is thus not a sufficiently fine-grained entity on which to base interoperation of sensitive information. So, while the flow of blocks generated by different ledgers can still be shared between participants, such as subsidiaries, auditors, authorities, partners, and more, they are shared for different purposes compared to the information shared by the Neurons. Information shared between Neuro-Ledgers is always shared in accordance with data protection agreements between the domains. Sensitive information shared between Neurons is always shared in accordance with contracts between participants, or by consent of their owners. This separation of responsibilities between the Neuron® and the Neuro-Ledger® allows them to provide resilient and distributed interoperation of very sensitive information, while at the same time protect the privacy, integrity, and auditability of the information and its operations. For more information about the Neuro-Ledger®, and how it solves the above-mentioned problems, see the *Neuro-Ledger, Executive Summary*[7]

5 Smart Contracts as the basis for Interoperation

Traditional services on the Internet exchange information using so-called *web services*. While there are many types of web services, they are sometimes collectively referred to as *web 2.0*. (Web 1.0, while not being called 1.0 at the time, consisted of information published and maintained on web servers by the service providers them-

selves; Web 2.0 allowed the users to provide the content being published.) While the use of web services has many benefits, there are many drawbacks as well: There are millions of web services, all doing specific tasks, all different. This makes interoperability a massive challenge as the number of APIs that need to be supported grows. There is also no traceability, transparency, and legal responsibility built into the concept of a web service or a web service call. While services may provide some form of traceability, by the use of logs, they are built on top of such web services and are not integral parts of the actual interoperation.

A new type of web is being created, where data is linked, semantic processing is distributed, and transactions are based on transparent agreements made on distributed ledgers. A smart contract, on the Neuro-Ledger® is an object that contains machine-instructions that can be processed and executed. It also contains localized human-readable text, describing the contents of the smart contract to human observers, and a mechanism and validation process that protects the integrity of both. A smart contract has well-defined roles that must be filled and signed before the contract becomes *legally binding*. Instead of calling a web service to request a service, a smart contract with the required information is signed by all parties. Once the contract has received sufficient signatures and becomes *legally binding*, its instructions are processed, and necessary information transmitted. This may include payment instructions, which enable automatic reimbursement and payment distributions for access to information.

More information about *Legal Identities*[8] and *Smart Contracts*[9] is available on the Neuro-Foundation website (see references below), and the *Neuro-Features, Executive Summary* white paper.

6 Trust Providers and Trust-based Computing

All signatories digitally sign a smart contract, including the Neuron®, that validates the process. The Neuron® here acts as a *Trust Provider*, an electronic notary observing the process, validating the signatures and identities of signatories, providing trust to the network and the transaction, and recording the process in its Neuro-Ledger®. The Trust Provider can also enforce the legal context of the operations it permits within its domain. It also protects access to the information, ensuring only authorized parties can access it. If participants can trust the Trust Provider involved, they can also trust the claims made by the signatories. The role of the Trust Provider here is like that of a Certificate Authority in X.509, but extended to cover digital identities, smart contracts, and digital signatures in real-time (as well as payment integration, auctions, and other services).

Using the Neuro-Ledger® in interoperation between parties adds *Trust* to the exchange. This type of exchange is called *Trust-based Computing*, which differs from exchanges based on distrust (such as blockchain), where all information must be obfuscated and anonymized, unless indelible privacy intrusions are created. Another way to increase *trust* in the network is to use *Certifiers* when signing contracts. Certifiers are third parties that attest to the validity of the claims in the contract. Using well-known certifiers significantly increases trust in the network. While they may

require commission, programmable payments make it easy to distribute monetary flows automatically and accordingly. The Neuro-Ledger® and Neuron® also make sure information is exchanged in an end-to-end encrypted manner where necessary. It is, therefore, an excellent choice to achieve compliance with new international standards such as the IEEE 2933 on *Clinical IoT Data and Device Interoperability with TIPPSS*[10], where TIPPSS stands for Trust, Identity, Privacy, Protection, Safety, Security, or international regulations such as the European Health Data Space EHDS[11].

7 Interoperable Information

To be able to do all the tasks mentioned in earlier sections, the Neuron® needs to be able to present information in a unique and unambiguous manner. This is done using a *canonical* and *normal* form of XML. This guarantees that anyone with access to the information gets the same binary representation of the information, regardless of how it was communicated. This is a requirement to be able to validate digital signatures. XML was also chosen because it is extensible, well-known, and well-defined, and its syntax can be validated using a well-known Internet standard called XML Schema. XML is human-readable, making it easier for developers to understand, troubleshoot issues, and maintain transparency. Even non-technical individuals can grasp its basic structure. XML can also be communicated easily over XMPP, the primary communication protocol the Neuron® uses to interoperate with other entities over the federated network. XMPP is also based on XML.

So, anything that can be semantically encoded using well-defined XML, with XML schemas downloadable from the Internet for validation purposes, can be encoded into a smart contract on a Neuro-Ledger®. This includes a wide variety of information already standardized, such as Health Data based on the international Health Level 7 standard v3 and beyond[12], as well as any semantic information[13], sensor data[14] or control operations[15], and much more. This greatly facilitates the interoperability of such information in already well-known formats.

Apart from the XML that goes into a smart contract, any binary information encoded using a well-known Internet Content-Type recognized by the Neuron® can also be attached to the smart contract. This feature enables the interoperation of information not described as XML, such as images, video, sound, and other documents supported and accepted by Neuron® overseeing the construction of the contract. Attaching such information to a smart contract gives it the same privacy and access protections as the smart contract itself.

8 Automated processing of sensitive information

Apart from legal digital identities and smart contracts, the Neuron® allows developers to tokenize digital or physical assets using a technology called *Neuro-Features*™. Medical records are an excellent example of digital assets that can be. Tokenizing an asset allows for automated trade and processing of the information, such as anonymization and pseudonymization of information, according to a program

inside the token. The program is a *state-machine* with well-known states that can manage its assets and interact with the outside world according to rules defined by the token. Tokens are created using smart contracts. All trade is performed using smart contracts. Furthermore, using tokens to protect personal health records has multiple benefits: It allows interested parties (such as research organizations) access the information or parts of the information (such as anonymized information) if they agree to specific terms set by the owner of such token. The terms can, for example, include monetary compensation, and details about what types of information can be accessed. Basing anonymization or pseudonymization on tokens makes the process transparent, ensuring proper information processing. Since interoperation with tokens is automatable, agreements and remunerations can efficiently be made, even if the number of individuals is large and individual amounts small (so called *micro-transactions*). Processing, is by default, distributed. There is no need to collect and process the sensitive information centrally. Information can be processed close to the person, with only the anonymized or pseudonymized information transmitted to where it will be further processed. This type of process also allows the organization requesting access to the information, to get into *direct contact* with the person owning the information, making interaction more personal, increasing *Trust*.

9 Digital Sensor Twins

Another use case for tokenized assets is tokenizing sensor data, creating a digital sensor data twin. Letting the token access and store sensor data and protect it allows the owner to authorize who accesses the sensor data and under what conditions. There might also be different requirements for different use cases or users, such as distinguishing access to sensors (or actuators) by friends and family, from health service workers, including emergency services, research organizations, insurance companies, and more. Some could have privileged real-time access to all data, while others only have restricted access. The complexities of managing different versions and arrangements are simplified by distributing the logic to tokens that reside close to the data owner. Each token can execute independently in its local environment.

10 Agent API

To communicate in the federated Neuron® network, parties communicate XMPP. Libraries in the form of nugets exist for this purpose[16]. An HTTP-based RESTful Agent API also exists for each Neuron®. It allows agents to interact with the Neuron® network without knowing XMPP. Connectivity is properly authenticated, and each agent can associate the account with a *digital legal identity* and create and sign *smart contracts*. Since all operations in Web 3.0 are reduced to the management of legal identities and smart contracts, the Agent API is straightforward and versatile. The same API can be used for almost any task in the Neuron® network.

11 The Neuro-Foundation

The Neuro-Ledger® was originally developed by Peter Waher, and the Trust Anchor Group, a Swedish company (of which Peter is a founder) developing the Neuron®. As part of a process where the Neuron-based technology is accepted by larger operators world-wide, much of the technologies are (at the time of writing) being moved to the Neuro-Foundation[17]. Neuro-Foundation is a not-for-profit organization supported by its member organizations and commercial licenses of its software. As a part of this move, source code is also made freely accessible open source. The Neuro-Ledger® is, therefore, free to use for non-commercial purposes. Commercial use requires a commercial license with the Neuro-Foundation, to help finance the maintenance and development of the Neuro-based technologies.

---

[1] XMPP Standards Foundation: https://xmpp.org/

[2] IoT Harmonization using XMPP: https://neuro-foundation.io/Papers/IoT%20Harmonization%20using%20XMPP.pdf

[3] Identity Architecture for Smart Societies: https://neuro-foundation.io/Papers/Identity%20Architecture%20for%20Smart%20Societies.pdf

[4] Neuro-Features, Executive Summary: https://neuro-foundation.io/Papers/Neuro-Features,%20Executive%20Summary.pdf

[5] Neuro-Payment architecture: https://neuro-foundation.io/Papers/Neuro-Payment%20architecture.pdf

[6] European Parliamentary Research Service (EPRS), Panel for the Future of Science and Technology, "Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?", PE634.445 – July 2019.

[7] Neuro-Ledger, Executive Summary, 2019-10-11, https://neuro-foundation.io/Papers/Neuro-Ledger,%20Executive%20Summary.pdf

[8] On legal identities: https://neuro-foundation.io/LegalIdentities.md

[9] On smart contracts: https://neuro-foundation.io/SmartContracts.md

[10] IEEE 2933 Working Group: https://sagroups.ieee.org/2933/

[11] European Health Data Space EHDS: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197

[12] Health-Level 7 (HL7): https://www.hl7.org/

[13] Resource Description Framework (RDF): https://www.w3.org/RDF/

[14] On sensor data: https://neuro-foundation.io/SensorData.md

[15] On control parameters: https://neuro-foundation.io/ControlParameters.md

[16] XMPP-related nugets: https://neuro-foundation.io/Implementations.md

[17] The Neuro-Foundation: https://neuro-foundation.io/