Notarius Electronicus

How to create trust in open smart city networks

Peter Waher

Trust Anchor Group AB
peter.waher@trustanchorgroup.com

Abstract. There are different strategies to create decentralized open networks that are secure at the same time. Some are based on distrust and often rely on costly algorithms such as Proof of Work or Proof of Stake to prove actor's intentions are not malicious, followed by a consensus method that determines the true state of the network. Other methods rely on trust, trust relationships, digital identities or identifiers and digital signatures to prove claims made. This paper describes the use of a "Notarius Electronicus" as a digital representation of a "Notarius Publicus" used in the real world, as a means to create Trust in an open digital network, digitally mirroring how we have created Trust in our open analog societies for millennia.

Keywords: Interoperation, Decentralization, Trust, XMPP, Trust-Provider, Neuro-Ledger, Neuro-Foundation

1 Introduction

The Internet was built as a decentralized open network. Anyone could connect to the network and interoperate. In the beginning it was not realized to what extent malicious actors would attempt to use the Internet for fraud, or purely destructive purposes. For this reason, most Internet technologies lack sufficient protection mechanisms allowing for the creation of Open and Secure networks. Instead, closed networks or services have been created, with limited or no interoperability. Closed networks are easier to secure, as identities can be provided to all actors from a central point, and validation is therefore relatively straight-forward. Closed, centralized networks also benefit larger companies, who have limited interest in interoperability, and want to control, protect and grow their share in the market, rather than permitting or promoting access to competing services for their end users.

It is possible, however, to create open decentralized digital networks that are also secure. To see how, we first take a look at how this problem has been solved historically, in our analog world.

2 Notarius Publicus

In antiquity, and in later medieval and renaissance societies based on Roman Law, similar problems existed. As relatively open societies were created, a mechanism to provide trust was necessary. The role of a Notarius Publicus was introduced. They were infused with trust by the society, both by leaders, and by citizens, and could provide, as a service, a means to project this trust to other members of society. This projection of trust took the form of simple acts of validating transactions, documents and signatures, as well as taking notes and recording public events.

By allowing the notary, as an independent third party, to officially validate each end of a transaction, they could project the trust society had in these functionaries to the parties of an agreement. As long as all parties in an agreement trusted a notary, they could trust each other if the notary would validate the basic claims made by each participant. Similarly, and in a larger context, if a large society had faith in a set of public notaries, all distinguished and recognized in society, and as long as these notaries could trust each other, they could by extension provide a *federated* service where people could form agreements, even if using different notaries, as long as their respective notaries could attest to the standing of each one, and the notaries involved each trusted each other.

The public notary function was, and still is, an important service that allows for agreements to be made between actors who do not know each other directly. This service becomes increasingly important in societies that have a high level of distrust in general. While its citizens might instinctively dislike the requirement to use a public notary to arrange an agreement, due to the time it requires, the benefits outweigh the discomfort. There is a tremendous opportunity however, for digital solutions in this space to optimize the process. But to do this correctly, we first must understand the problems a digital solution must solve.

3 Digital Threats to Trust in the Society

In the current digital revolution several distributed technologies have emerged that challenge the traditional trust model developed in societies based on Roman Law. As mentioned earlier, the Internet was originally developed without much consideration to security threats, and therefore intrinsically lacks important tools for threat mitigation. For this reason, most Internet technologies must solve security threats individually, each one doomed to repeat the mistakes already solved by earlier technologies. Cybersecurity has been forced to be treated in a reactive manner, rather than proactive. Vulnerabilities are treated, if at all, after a threat has manifested itself in each technology separately. There is no mechanism on the Internet that can help technologies to reach agreements securely, in a way similar to how notaries in analog societies help their citizens. Each technology must defend itself and often fail. Furthermore, services cannot normally collaborate and defend each other. Knowledge gained by one system cannot be used by other systems automatically. Instead, each participant must repeat the mistakes earlier technologies have already experienced and solved.

The beneficiaries from this architecture are hackers, fraudsters, intelligence agencies and those that plan or execute cyber-warfare, and also the global technology giants. These giants have been able to create centralized infrastructures permitting their clients a seemingly half-secure presence on the Internet, but at a huge cost of diminishing privacy, net-neutrality and interoperability.

To counter this centralization effort, several decentralized efforts exist. The idea has been to create an infrastructure where parts can negotiate between themselves directly without the approval of centralized giants, be they companies, banks or government authorities. This is a serious mistake. By omitting the vital trust function of a digital notary, they suffer similar problems and worse as thoroughly documented already by more than six decades of experience since the invention of the Internet. By permitting everyone access to sensitive data, they also create immense privacy problems[1]. By failing to value the intrinsic value of the notary function in creating trust in an otherwise untrusted or untrustworthy network, these technologies will repeat the mistakes made by their predecessors, as evidenced by the huge amount of fraud committed on these networks during the last years. Fortunately, there are alternatives to choose from.

4 Decentralized Alternatives

Fortunately, there are other emerging decentralized technologies available, that solve the issues presented so far. Communication protocols such as XMPP[2], standardized at the highest Internet level by the IETF, allow participants across the globe to communicate with each other securely, freely, openly, extensively and without centralized processing and potential eavesdropping, regardless of network topology.

Other decentralization efforts based on distributed ledgers, such as the Neuro-Ledger®, offer decentralized storage and processing of information in a distributed ledger that is both secure and protects privacy. It does this by amending a traditional blockchain with features that solve the issues presented[3]. It also permits distributed services to share open intelligence of threats, in order to collaborate to make the network more secure[4]. By separating the communication layer and ledger layer, very sensitive information can be processed on the ledger[5].

[1] 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.

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

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

[4] Open Threat Intelligence using Neuro-Ledger, Executive Summary, 2024-08-27, https://neuro-foundation.io/Papers/Open%20Threat%20Intelligence%20using%20Neuro-Ledger.pdf

[5] Interoperability of Medical Records on the Neuro-Ledger, Executive Summary, 2024-08-29, https://neuro-foundation.io/Papers/Interoperability%20of%20Medical%20Records%20on%20the%20Neuro-Ledger.pdf

The Neuro-Ledger mirrors the analog trust architecture provided by Roman Law, by introducing a new actor in the Internetwork, the *Trust Provider*, which is a digital representation of the functions that a Notarius Publicus has in the physical world. The Trust Provider using digital signatures, validates identity applications, approves smart contract proposals and any form of agreement or transaction in the network, ensuring integrity between human-readable claims and machine-readable counterparts. As it is built on-top of the XMPP network, it is already from the on-set globally scalable, and federated, permitting real-time communication between parties regardless of network topology, protecting privacy of its participants, and permitting each domain to govern its own policies and content (so-called local governance), for maximum interoperability. As this Trust Provider taken on similar functions and responsibilities as the Notarius Publicus, we will call it a *Notarius Electronicus*, as a homage to its analog counterpart.

5 Notarius Electronicus

The Notarius Electronicus is a digital representation of the Notarius Publicus in the decentralized network created by the Neuro-Ledger. Each participant can apply for a digital identity, and if the Notarius Electronicus validates it, the identity is infused with trust. Everyone in the network that can trust the Notarius Electronicus, can therefore also trust its validation of a digital identity, and in turn, any signature it has made. Since the Neuro-Ledger is federated by nature, the set of trusted Notarius Electronicus available, each one operating on its own domain, creates a federated trusted network, over which digital agreements can be made, and over which digital payments can be performed, manually or automatically[6]. As the Notarius Electronicus performs an exceptionally valuable service in the network, it is important to protect its role, so that it can finance its operations, and maintain the trust given it by the society. The Neuron-Ledger® not only protects and digitally mirrors the role of the notary in the network, but it also ensures and protects the economic basis that underpins the correct functioning of the operation, by allowing a commission- or fee-based digital economy to be created around the notary function. Therefore, the Neuro-Ledger allows the Trust Provider, or Electronic Notary, to be compensated for each validation and signature, ensuring that its current analog form can be efficiently digitized. The benefits of the digitalization of the notary function include an increase in productivity in the society, as agreements take seconds to complete, instead of hours or days, while at the same time protecting the vital role of the notary. Furthermore, the new Electronic Notary becomes a vital part of an open and secure digital smart society, just as the Public Notary has been a vital part of an open and secure analog society. This increases the importance of the role, and opens new opportunities, for ensuring secure interoperation across all levels of a digital smart society[7].

[6] Neuro-Payment Architecture, Executive Summary, 2024-05-20, https://neuro-foundation.io/Papers/Neuro-Payment%20architecture.pdf

[7] Neuro-Features™, Executive Summary, 2021-11-11, https://neuro-foundation.io/Papers/Neuro-Features,%20Executive%20Summary.pdf

6 Identifiers, Signatures and Identities

A common misunderstanding is to confuse the concepts of digital *identifier*, digital *signature* and digital *identity*. A digital identifier is a unique string associated with something. It can be a cryptographic *public key* for instance, or a unique string associated with a public key. A digital signature is a proof that the signatory has the corresponding *private key*, but only if the private key is really kept private. Centralized stores of keys can never be seen as proofs of ownership of a private key. And proof of having the private key is not proof of the identity supposedly associated with the identifier. A digital identity is much more than a digital identifier that can perform digital signatures.

The concept of identity requires a context. In modern society, a person's identity often consists of first, middle and last names, a national personal number and citizenship. It can also contain other information, such as address, civil state or sex. It can contain photos and biometric information. In the general case, it is a set of claims about the individual or entity being identified that *society* has chosen to accept as statements that uniquely identifies the person or entity in that society. All this information, not just a small subset such as name and personal number, are important attributes that are part of an identity. This is especially important when arranging agreements between parties, allowing each party to gain access to all these items of information about each other. A digital identity cannot be created by a person itself, as a person cannot validate its own claims. A person can at most create a digital identifier.

Another important aspect of an identity is that the claims are *validated*. They must also be validated by someone everyone can *trust*. This is exactly the role a Notarius Electronicus fills: Being the validator of such identity claims. By performing such a service, a Notarius Electronicus can create a proper digital identity from a digital identifier, a validated set of claims and a digital signature of the claims. Without such a role, a proper digital identity that can be used to form agreements cannot be created.

Once it is clear how an infrastructure for a smart society, including digital identities is to be created, there is one this to consider: Who should be allowed to control the technology?

7 The Neuro-Foundation

Most humans and organizations are loyal to the entities that pay their bills. This is the underlying reason why free software from large corporations cannot be trusted. Large companies producing "free" software are not loyal or concerned with the interests of the users of such software, but rather, see the users as the commercial products being commercialized. They use the information they collect about their users and monetize it. This monetization can take different forms. Companies can resell the information, or help oppressive governments monitor or censor their citizens, inform politicians what people think and conversely, be paid to influence how people think, and so on. The habit of relying on free software is one of the most important underlying factors for the limitations of privacy on the Internet today. People expecting software to be free, often do not realize that in doing so, like Pinocchio, they themselves become the product. In order to build a digital framework for an open and free smart society with proper digital human rights, it is therefore important not to rely on undisclosed interests and free software. Instead, the infrastructure must be developed and financed by the users and beneficiaries of the infrastructure itself, lest other interests take control of the information for their undisclosed purposes.

For this purpose, the Neuro-Foundation is being formed. 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®. The Neuron is an infrastructure component that facilitates the creation of open, interoperable, and yet secure networks over the Internet. It hosts the Neuro-Ledger, and a communication infrastructure for things such as self-sovereign digital identities, legally binding smart contracts, tokenization of physical assets, and programmable payments.

As part of a process where the Neuron-based technology is accepted by larger operators world-wide, much of the technologies are being moved to the Neuro-Foundation[8], 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. This includes the Neuro-Ledger. Commercial use of the software, however, requires a commercial license with the Neuro-Foundation. The reason for this is to help finance the maintenance and development of the Neuro-based technologies, without having to resort to funds from sources that would otherwise restrict its development or impede its protection of the digital human rights the technology protects.

8 Conclusion

The Public Notary function in societies based on Roman Law, is an intrinsic and valuable function that creates Trust in an otherwise untrusted environment. By digitizing the Public Notary, creating an Electronic Notary with similar functionality, it is possible to create open and interoperable digital societies (smart societies) that are also secure. To do this, it is vital to protect the interests of the Trust Providers, or the Electronic Notaries, the actors who infuse and project Trust into the digital network. By doing so, actors that do not know or trust each other, can still reach meaningful agreements and generate digital transactions based on such agreements, creating a fully functioning digital economy. Any process that would work in an analog society based on Public Notaries, can be digitized, automated and optimized, using an equivalent digital infrastructure of Electronic Notaries.

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