Neuro-Payment Architecture

Executive Summary

Peter Waher

Trust Anchor Group AB
peter.waher@trustanchorgroup.com

Abstract. TAG Neurons can be interconnected into federated networks and provide an architecture for interoperability across domains. One of the key features of the TAG Neuron® is its integration with payment services, and its capacity to provide online and offline automatable and programmable payment services to machines and users. This paper provides an overview of this architecture, as well as available services, and how they can be used to provide smart financial services.

Keywords: Interoperability, Payments, Automation, eDaler, Marketplace.

1 Introduction

The TAG Neuron® is a key infrastructure component that permits the creation of globally scalable, decentralized and interoperable networks for the next-generation smart society. This includes interoperation between humans and humans (H2H), humans and machines (H2M) and machines to machines (M2M). It includes privacy protection, exchange of confidential and protected information, as well as digital identities, legally binding smart contracts, tokenization, automation, including payment automation as well as support for online and offline payments, conditional payments, programmable payments, micro-payments, etc. The TAG Neuron® interconnects the Web, with the Internet of Things, and next-generation Financial Services and distributed services.

The TAG Neuron® architecture is described in a series of white papers focusing on different aspects: The use of Digital identities in Smart Societies is described in *Identity Architecture for Smart Societies*[1]. This includes how digital identities are crucial to comply with *Know your Customer* (KyC) requirements, and how the architecture makes sure users are protected by giving them sovereignty over their identities, and who has access to them.

The next-generation distributed ledger technology (DLT) Neuro-Ledger®, on which the TAG Neuron® is built, is described in *Neuro-Ledger, Executive Summary*[2]. The paper describes inherent problems in traditional block-chain technologies, and why they are not suitable for use in smart societies, or for sensitive or personal information, and how the Neuro-Ledger® solves these issues. The Neuro-Ledger® is further described in *Neuro-Ledger and Sustainability*[3], which focuses on the environ-

mental impact of the Neuro-Ledger® in comparison with traditional block-chain technologies.

Tokens on the Neuro-Ledger® are called *Neuro-Features*™, and they are described in *Neuro-Features, Executive Summary*[4]. Neuro-Features™ support both simple tokens, as well as programmable tokens with associated state-machines for automation. The latter play an important part in the creation of programmable payments. The paper also describes how to create smart contracts, that are also contracts in a legal sense, and how this is used to tokenize physical assets. The digitalization of legal claims is also an important aspect of programmable payments.

The current paper focuses on the payment service abstraction layer made available by the TAG Neuron®, and how they can be used to integrate existing payment and financial services to the TAG Neuron® network. As soon as such services have been integrated, they can be used by services running on the TAG Neuron® network, including human users via *Neuro-Access* App[5] (or derivative), automated agents or external services via the *Agent API*[6], or Neuro-Feature™ tokens, hosting programmable payment logic in a context defined by legally binding smart contracts.

2 Federation

Before we can understand how payments are performed from one entity to another, we must first understand how entities interact in the Neuron® network. Each entity connects to the network via an *account*. This account resides with a *service provider*, that acts on a *domain*. The entity needs to prove it has access to the account, by authenticating itself with the service provider, during the connection phase. The actual mechanism used during authentication, is negotiated between the entity and the service provider, and may differ across the network and over time, as authentication mechanisms get obsoleted and replaced by newer mechanisms.

Once connected, the entity can exchange information with any other entity on the network, regardless of which service provider each of the entities are connected to. This is possible because the service providers themselves *interoperate* in a standardized[7] manner. Fig. 1 illustrates how different entities (clients named C_i) connected to different service providers (operating on domains D_j) still can exchange messages between each other. This principle of interoperation is called *Federation* and is the key to the success of the Internet, and globally scalable Internet Technologies such as *e-mail* and *Instant Messaging*. For this role as intermediary helping entities in the network to interconnect securely, the Neurons are also called *brokers*.

3 eDaler®

eDaler® is the means to digitally represent value in the TAG Neuron® network, and more specifically, the transfer of value. Before an entity can get access to eDaler®, it needs to have an approved *digital identity* assigned to the account. This

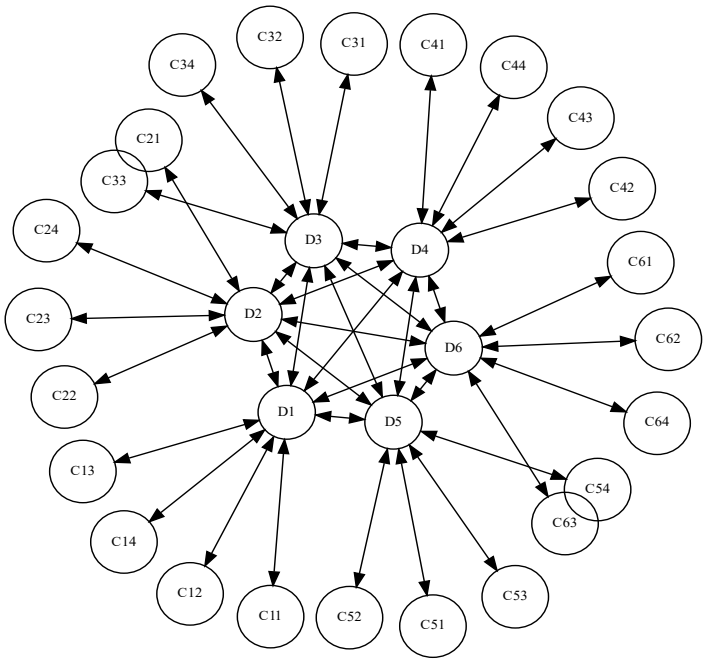

Fig. 1. Federated, globally scalable network

digital identity serves multiple purposes. It provides the entity with a *private key*, which can be used to sign information, and the service provider (and the rest of the network) with its corresponding *public key*, which is used to validate signatures, to make sure claims originate with the entity, and is some fraudulent actor. The digital identity also contains sufficient *personal information* for the service provider to comply with *Know your Customer* (KyC) requirements available within its domain of operation. As these requirements may vary from country to country, region to region, state to state or between companies or organizations, the federated nature of the TAG Neuron® network simplifies the process, as it may implement different rules in different domains. The interoperable nature of the network will allow such participants to interoperate anyway, even if configurations in different domains vary. Once such KyC requirements are satisfied, the service provider will be able to provide the entity with *financial services*, including payment services. This includes, providing the account with the corresponding digital identity, with one or more digital eDaler® *wallets*. An eDaler® wallet, contains a balance, and associated *currency*, as well as transaction history. The eDaler® is not a currency itself. It is a legally binding claim that the service provider makes to the entity, within the financial legal framework the service provider operates in, that the balance in wallet, represents the same amount of units of currency, as is defined by the wallet. It is the *liability* the service provider has on account of the entity.

4 Financial Service Abstraction Layer

Each TAG Neuron® has a *Financial Service Abstract Layer* (called *Paiwise™*) and can host its own set of services. This makes it possible for each service provider to adapt to the financial framework in its own domain of operation, and still interoperate with other service providers in the federated network. The financial service abstraction layer defines interfaces for the following types of services:

- *Buy eDaler®* – The service allows an entity to buy eDaler®, i.e. pay using FIAT or other currency, and get eDaler® in return. Implementing this interface makes it possible to let users in the corresponding domain to pay using card, directly from bank account, or via credits, etc.
- *Sell eDaler®* – An entity can sell an amount of eDaler® in its wallet and get FIAT or other currency in return. These services make it possible for users to convert their eDaler® to money in their bank account, for instance.
- *Web Payment®* – Permits web pages hosted on the Neuron® to charge for services directly, without using eDaler®, via web checkouts.
- *Currency Converter* – Helps Neurons establish exchange rates when transferring eDaler® from one currency to another.
- *Identity Authenticator* – Analyzes and can approve or reject digital identity applications, automatically, semi-automatically or manually. This makes it possible to customize the KyC-process for the legal context in each domain.
- *Peer Review Service* – Can perform reviews of digital identity applications to certify the validity of digital identity applications or parts of digital identity applications. These kinds of services can simplify the peer review process, where such are used to approve digital identity applications.

5 Micro payments and payment flows

By using eDaler® as the digital medium by which value is transferred in financial services, implementations become much simpler: Instead of implementing the entire flow, and what financial services to use in each end, the user can select the service provider to use for payment (buying eDaler®), then transfer the eDaler® to the appropriate account or accounts, and then let the entity in charge of that account (or entities in charge of the accounts) to choose how and when to convert the eDaler® to money. By using eDaler®, there is also no limit on the amounts to use in the transfers. You don't have to worry about bank fees in the transactions of eDaler® either. While there may be commission fees, depending on what service providers are used, there are no fixed fees or gas fees involved in eDaler® transactions. This makes it possible to implement *micro transactions* and *payment flows* using eDaler®. For example, you can charge fractions of cents, and accumulate micro payments into larger sums over

time, and convert the accumulated funds to FIAT when the amounts dictate it makes sense to pay bank fees for the purpose.

6 eDaler® operations

All eDaler® operations are encoded into URIs using the URI scheme `edaler`. eDaler® operations that can be encoded into URIs include:

- *Transfer* – Transfers an amount of eDaler® from one account on one Neuron® to another account on another Neuron®. The eDaler® is transferred when *anyone* sends the URI to the Neuron® network, and the URI passes all associated validation tests. The sender needs to sign the transfer using its digital identity. In its simplest form, an eDaler® transfer represents a *peer-to-peer payment*, optionally combined with buying and selling eDaler® before and after the transfer.
- *Request Payment* – A user can request eDaler® payment from another, by creating an eDaler® URI for the purpose. The request is sent, and the potential sender can sign the request to initiate a transfer.
- *Create* – A service provider can generate eDaler® to any account on the Neuron®, being liable to return the amount to the user if the user chooses to. The eDaler® is generated when the user to receive the eDaler® sends the URI to its Neuron® that created the eDaler®. The recipient needs to sign the request with its digital identity.
- *Destroy* – A service provider can destroy eDaler® from any account (with approval of the user) on the Neuron®. The user of the account that will get its eDaler® destroyed, needs to sign the request with its digital identity.

Personal payments and payments *in blanco*

All eDaler® are cryptographically signed by the liable party, using the digital identity associated with the account to which the corresponding wallet belongs. The beneficiary of the operation can be either implicitly or explicitly defined. If the beneficiary is explicitly defined in the URI, it does not matter what entity submits the URI to the network; the stated beneficiary will receive any eDaler® resulting from the transfer, from the liable party. If the beneficiary is not explicitly defined in the URI, the entity that submits the URI to the network, will become the beneficiary implicitly, simply for submitting the URI to the network. Such URIs make it possible to create payments *in blanco*, paid to whomever submits the URIs to the network.

Messages, Encryption and Privacy

All eDaler® URIs can be encoded with a message to the beneficiary. This message can also be used for logging purposes and for the liable party to keep track of the

purpose of the transaction. If the beneficiary of a transaction is known, the message can be *encrypted* using the public key of the recipient. (URIs encoding payments *in blanco* cannot be encrypted.) Encrypting messages is the recommended form of protecting the privacy of users in the network. For security, transparency and auditability reasons, the service provider will log eDaler® URIs processed. Encrypting messages in transactions assures private information is not made available to people and systems that should not have access to such information.

Offline payments

As all eDaler® transactions are encoded into URIs, and URIs constitute a well-known Internet standard[8], they are very easy to transmit. They can be transmitting online using the TAG Neuron® network itself using the underlying XMPP protocol, or via e-Mail or Instant Messaging (chat) or any number of applications or methods. They can also be transmitted using any number of methods available that do not require an online connection, such as using optical QR codes, near-field radio, or even handwritten notes. URIs are very simple to process and transmit. And each contains the information necessary to validate and process the transaction once the URI gets to the TAG Neuron® network. This makes eDaler® suitable as a mechanism to implement digital offline payments. Even if Internet connectivity does not exist, entities can exchange URIs containing the necessary information to know who each other are, and that the payment can be processed at a later stage.

Conditional payments

An eDaler® transfer URI can be encoded with a smart contract reference. This assures a transaction is only accepted by Neurons, if the corresponding smart contract is in a *signed* state. This makes it possible to encode payments that rely on the compliance of conditions encoded in a contract. If this contract is signed by a third party (for instance), a buyer can send a payment to a seller, on the condition that the seller performs a task or sends goods according to a contract. The seller cannot consume the eDaler® until the contract is signed, for example, representing the successful delivery of the goods, or performance of the corresponding task. The Buyer can assure the seller, that the seller will receive the payment, by sending a conditional payment. The Buyer is at the same time assured that the actual payment is not processed until the agreed upon terms are complied with.

Validations

For an eDaler® URI to be successfully processed a series of validations are performed on the URI. All must pass before a transaction can be performed. If the validation rules fail, the URI can be attempted at a later stage (such as when a conditional payment URI is submitted before the condition contract has been signed). The rules include checks that accounts exist, digital identities exist, signatures are valid, condi-

tional requirements are met, funds are available in wallets, currencies match, or are converted according to approved indices, and necessary agreements exist between domains, or within the hierarchy of neurons.

Neuron® hierarchy

Neurons can interact directly in a federated sense. For certain interactions this interconnectivity may be inefficient. Examples include the ability to know if a Neuron® is well-known or not, or if there exists an agreement for transfer of funds between domains. In such cases, Neuron® hierarchy can be used. Neurons (a.k.a. *Brokers*) are arranged in a tree-structure, each Neuron® having a *parent* Neuron®. The parent Neuron® distributes software updates to child Neurons. They also act as an authority and can help find paths in a trusted network of Neurons. The top-most Neuron® is a *Trust Anchor* (a.k.a. *Root Broker*) in the network of Neurons. The Trust Anchor is its own parent; it acts as a root for the tree that branches out from its child Neurons. While it may be inefficient to find contractual agreements between all Neurons in a global federated network, a *path of agreements* can be found, by utilizing the tree structure of the Neuron® hierarchy. This path can then be used to perform a transaction between the Neurons acting as endpoints of the path. Fig 2 illustrates how Neurons are organized in a tree-like hierarchy.

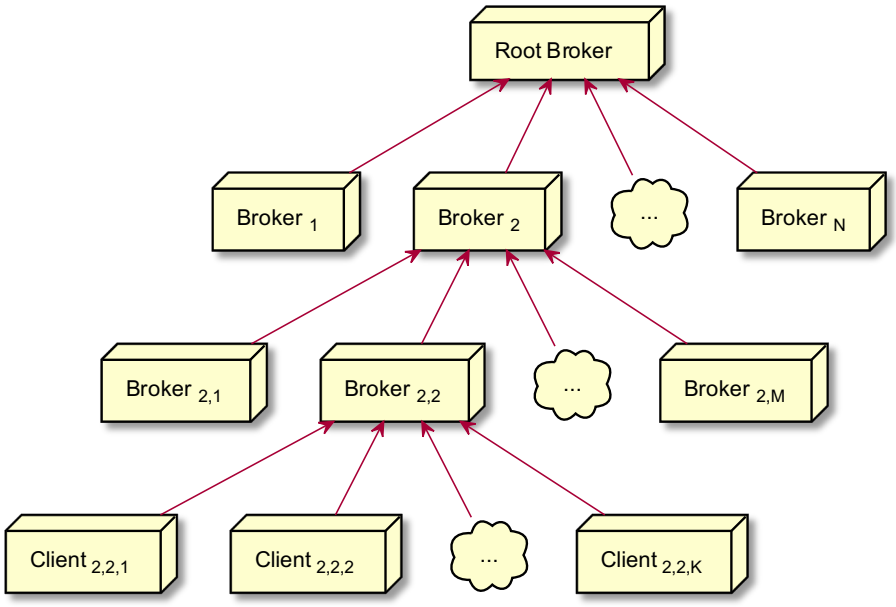

Fig. 2. Neuron® hierarchy

Role of Neuro-Ledger®

The Distributed Ledger on which the TAG Neuron® network is based, is not the principal source for validating and authorizing transactions using eDaler®. There are many reasons for this, the main being that different domains may not want to share ledgers. They may contain confidential, personal or sensitive information that they do not want to share with their competitors, or even openly. Instead, validated digital identities with public keys and digital signatures are used to authorize transactions. The Distributed Ledger (or Ledgers) involved *observe* all that happens within their domains of influence, and record events for security, transparency and auditability purposes. The ledgers can also act as a buffer for resilience and security, but there is no requirement for domains to share all information with all other nodes on the Internet. Trusted nodes can choose to share selected collections of information between trusted nodes, at the discretion of each domain. They can also choose to share different collections with different nodes. This principle is called *local governance*, and permits the creation of *heterogeneous networks,* where small, weak or resource-constrained actors can interoperate with large, strong or virtually limitless actors, on a level playing field.

7 Contractual payments

Each transaction of eDaler® needs to be digitally signed by the liable party transmitting eDaler®. This signature can be explicitly done, on the eDaler® URI itself, or implicitly done, as part of a signature of a *smart contract* of which the liable party is part. This makes it possible to encode contractual payments, that are performed as soon as all parties in a contract have signed the contract, and the contract becomes *signed*. The Paiwise™ Payment Instructions XML[9] schema allows entities to create smart contracts that can buy, sell and transfer eDaler® using smart contracts. Contractual *payment distributions* among parties in a contract is a simple example.

8 Usage payments

Apart from being an interoperability broker, the TAG Neuron® interfaces any type of connected device (or Thing), tying together the *Internet of Things* with the world of *Financial Services*. For this reason, the TAG Neuron® also referred to as an *IoT Broker*, or *"The IoT Broker"*[10]. In this aspect, the TAG Neuron® provides things with several important services: A Thing Registry (for discovery and ownership claims), Decision Support (help with answering what things can do), Provisioning (access rights, who can access and do what) and Ownership (who is the legal owner of a thing). This provisioning can be determined by smart contracts. This means it is possible for an owner of a device to provide a smart contract that defines that who-ever agrees to its terms (which may include payment instructions), are allowed access. This permits the creation of cyber-physical systems where users automatically pay for access to devices based on usage, in a completely automated manner.

9 Programmable payments

The TAG Neuron® permits entities to create tokens called *Neuro-Features*™ on the Neuron®. Such Neuro-Features are created using smart contracts[11]. These tokens may create a *state machine* that can execute logic in accordance with the definitions in the smart contract[12]. Since this logic is governed by the signatures of the parts of the contract, the state-machine can execute eDaler®-operations in the name of the signatories. Since the state-machine operates over time, it can be used to implement advanced programmable payment constructs, such as rule or event-based payments, escrow payments, micro-loan arrangements, crowdfunding projects, payments in accordance with compliance of plans and milestones, tokenization projects with programmable return on investment, etc.

10 Marketplace with automated auctions

To facilitate trade on the TAG Neuron® network, each Neuron® also contains an online marketplace and auction service. The Neuron® as *Trust Provider* acts as an automated *auctioneer*. The entire auction flow is also managed via smart contracts[13]. Entities can *consign* anything for sale to the auctioneer via a smart contract. Entities that need anything, can publish their interest to purchase via another type of consignment to the auctioneer, also via a smart contract. In both cases, anyone can place *offers* to the auctioneer, either to purchase something for sale, or sell something to someone interested in the purchase. Each consignment comes with *time limits* and rules of how to evaluate offers. Offers can be evaluated on *price*, effectively optimizing the transaction based on price. They can also be evaluated by *score*, allowing bids to be evaluated on other parameters, available as tags in the offer smart contracts. This makes it possible to optimize on delivery time, environmental certification, quality, etc. Apart from time limits, and rules for evaluation of offers, consignments also have initial bids, as well as accept bids. Accept bids result in immediate acceptance of the offer, even if the time limit has not expired. If no accept bid has been provided, the best offer, according to the rules available in the consignment contract, is executed, and corresponding payments are automatically executed. If payments cannot be executed, due to lack of funds, the best bid is automatically disqualified, and the next best bid is executed, etc., until a successful bid is found. If no suitable offer is found, the consignment fails and is terminated. If a token or similar object with an ownership is consigned to the auctioneer, the ownership of the token is also automatically transferred, as the consignment concludes with a successful bid being executed.

Automated marketplaces using auctions is the principal tool for optimization in Industry 4.0-type applications.

[1] Identity Architecture for Smart Societies, 2023-03-21, https://lab.tagroot.io/Documentation/TagID/Identity%20Architecture%20for%20Smart%20Societies.pdf

[2] Neuro-Ledger, Executive Summary, 2019-10-11, https://lab.tagroot.io/Documentation/NeuroLedger/Neuro-Ledger,%20Executive%20Summary.pdf

[3] Neuro-Ledger® and Sustainability, 2021-08-24, https://lab.tagroot.io/Documentation/NeuroLedger/Neuro-Ledger%20and%20Sustainability.pdf

[4] Neuro-Features™, Executive Summary, 2021-11-11, https://lab.tagroot.io/Documentation/NeuroFeatures/Neuro-Features,%20Executive%20Summary.pdf

[5] Neuro-Access can be downloaded on Android and iOS.
Android: https://play.google.com/store/apps/details?id=com.tag.NeuroAccess
iOS: https://apps.apple.com/be/app/neuro-access/id6446863270

[6] Agent API: https://lab.tagroot.io/Documentation/Neuron/Agent.md

[7] The protocol used to interoperate across domains, is called XMPP. It is standardized by the Internet Engineering Task Force (IETF), in RFC 6120, 6121 and 6122. You can read more on https://xmpp.org/

[8] URIs are standardized by the IETF in RFC 3986.

[9] Paiwise™ Payment Instructions XML Schema: https://paiwise.tagroot.io/Schema/PaymentInstructions.xsd

[10] For more information on how the TAG Neuron® can act as an IoT Broker and provision ownership and payments on usage, see: https://cybercity.online/

[11] Neuro-Feature™ XML Schema: https://paiwise.tagroot.io/Schema/NeuroFeatures.xsd

[12] Neuro-Feature™ State-Machine XML Schema: https://paiwise.tagroot.io/Schema/StateMachines.xsd

[13] TAG Marketplace XML schema: https://paiwise.tagroot.io/Schema/Marketplace.xsd