Neuro-Features™

Executive Summary

Peter Waher

Trust Anchor Group AB
peter.waher@trustanchorgroup.com

Abstract. This paper describes *Neuro-Features*™, a TAG Technology that can be used to monetize digital or physical assets, by creating Non-Fungible Tokens or Asset-backed Tokens. By using *e-Daler*® and *Paiwise*™ technologies, value creation, monitoring and auditing, as well as automated payments and trade can be used.

Keywords: Distributed Ledger Technology, DLT, NFT, Tokens, Paiwise, e-Daler.

1 Introduction

Monetization of digital resources is a hot topic today. A number of efforts exist to encode unique digital assets as *non-fungible tokens*, using different technologies including Distributed Ledgers and Smart Contracts. A similar approach can be used to monetize physical assets that are sometimes too small to be monetized using regular or manual approaches, or more inefficient to manage. Examples may include small parts of land, individual shares or options in companies, parts commonly owned assets such as vehicles, buildings, or of physical installations (solar panels, windmills, etc.) or small units of other types of assets (parts of animals, trees, fields, etc.). They can also be used to monetize temporary services or opportunities. Examples may include personal meetings, seats at events or restaurants, travel arrangements, parts of space in containers or other types of cargo services, parts of crops or yields, etc.

There are several efforts using "smart contracts" today that provide non-fungible tokens, or similar, using blockchain and "smart contracts". These implementations lack many of the necessary requirements placed on such tokens. This document outlines how Neuro-Features™ can be used to implement secure and legally binding Non-Fungible Tokens (NFTs) or Asset-backed Tokens instead. But first, an introduction to blockchain-based "smart contracts" is necessary, for the reader to understand why Neuro-Features™ offer a better solution to token-based assets.

2 “Smart Contracts”, that are not

There is a lot of interest in blockchain technology and smart contracts. But very few know what these technologies really are[1]. Some that do, have said that smart contracts, are neither smart, nor are they contracts. Even one of the co-founders of Ethereum, and one of the protagonists of the development of their so-called “smart contracts”, claim that he regrets the use of the term “smart contracts”, and that “persistent script” is a better term[2]. So, what are these so-called smart contracts, and how do they work, and how do they not work?

A blockchain persists information in a linked chain of blocks. Each block is cryptographically signed, and thus becomes immutable. The contents of a block cannot be changed, unless it be detected by other nodes in the distributed network of nodes comprising the blockchain, and the change is thus discarded. A blockchain is an example, of what is in more general terms known as a *Distributed Ledger*: It persists information in a way that is difficult to alter or delete. It runs on multiple machines, for resilience and accessibility reasons, and for this reason becomes very resilient to change (for practical purposes “impossible” with today’s technology).

A so-called “smart contract” in the blockchain world, is a piece of preprocessed (or compiled) machine instructions that is placed on the blockchain. It therefore becomes persistent, and impervious to change, as it too is cryptographically signed. It is also distributed across the nodes in the network. As these validate the signature of the “smart contract”, they can choose to execute the code. The code in turn, evaluates information on the blockchain, and each node therefore comes to the same conclusion, using the built-in consensus algorithm. It is clear from this description, that such a “smart contract” has very little to do with contractual agreements, and that “persistent script” is indeed a better name for the construct.

Following is a list of attributes that so called “smart contracts” in this sense lack:

- The are *not smart*, in the sense that they cannot adapt to changing circumstances.
- They are *not contracts*, or digital representations of contracts, or agreements, as humans traditionally use the term.
- There are *no parts* in a contract, *no roles* with different responsibilities, *no parameters* to adapt contracts.
- They are *not transparent*, as they are preprocessed or compiled, and meant for execution, not for reading, validation, or auditing by humans.
- There is *no integrity*; there is no verification step assuring the contract is consistent with law, regulations or policy). There is no responsible party in case something goes wrong. There is therefore no legal accountability of such “smart contracts”.

---

[1] For an introduction to block-chain and some of its shortcomings, as well as an introduction to Neuro-Ledger™, an alternative Distributed Ledger Technology, see Neuro-Ledger™, Executive Summary, 2019-10-11.

[2] https://twitter.com/VitalikButerin/status/1051160932699770882

- They are *not machine readable*, in the sense that they only contain machine instructions, not descriptive semantics on the contents of the contract. The meaning of the contract must be deduced, if possible.
- They are *limited in size*.
- They have *no life cycle*. Once persisted, it never vanishes.
- They *lack relevant privacy protection*: Contracts are accessible to everyone with access to the blocks. To protect sensitive information, private keys need to be used to encrypt data. If keys are lost, exposed information cannot be deleted or re-encrypted using other keys. For a comprehensive study on the problem of using blockchains with personal information, see [1].
- There is *no interoperability*. They cannot be used to model declarative or informative contracts such as signed financial statements, sworn statements, certificates, approved sensor data, etc.

3 Smart Contracts, that are

In order to create Asset-backed Tokens, with legally binding agreements, another type of smart contract is required. Neuro-Features™ use smart contracts as defined in IEEE P1451.99[3], which is a better digital representation of how contracts and agreements are made in the human society. These smart contracts are hosted by federated *neurons*, that interconnect in order to create a decentralized, interoperable network.

Each *Neuron*™ also runs a *Neuro-Ledger*™, a Distributed Ledger, not based on blockchain. It can be used for resilience, and auditing of information. But the *Neuro-Ledger*™ is not the principal interface for accessing smart contracts: The Neuron has an Interoperable communication interface, which is defined in IEEE P1451.99, and can be used to request access to the smart contracts or associated legal identities. This makes it possible to restrict access to the information, as access to the DLT is not required for accessing and validating the digital assets.

Following are some properties of these smart contracts:

- Contracts have both *machine-readable* and localizable *human-readable* information.
- Contracts are *transparent* and *interoperable*. They are defined using XML and validated using XML Schemas based on the corresponding namespaces (W3C standards). Machine-readable information encoded in the contract is not pre-processed or compiled, it may or may not be executed. The semantics of the machine-readable section is defined by the namespace of the corresponding XML, and what services are available on the corresponding *Neurons*.
- *Integrity* and *legality* of contracts is achieved by an approval process of parametrized contract templates. During this process, machine-readable and human-readable information is analyzed and compared, to assert they match. During this process, compliance with existing laws, rules and policies is also

[3] https://gitlab.com/IEEE-SA/XMPPI/IoT/-/blob/master/SmartContracts.md

asserted. Once approved, the template is signed by the *Trust Provider* responsible for the *Neuron*. When smart contracts are created, they are created from approved templates, where only parameters and parts are allowed to change (within the scope of validation rules defined in the template). This protects the *legal integrity* of automatically created smart contracts.

- Every change to the contract is signed by the *Trust Provider*, to guarantee the integrity of the change, and the current state of the object. Each change is logged as an event in the *Neuro-Ledger*™.
- Contracts have a *lifecycle*, with a duration, required archiving time and an optional archiving time. A contract can be deleted during the optional archiving time and is automatically deleted at the end of the optional archiving time, if not done so before.
- Contracts are signed by *parties*, having specific predefined *roles*. Each cryptographic signature is added to the contract. When the minimum required number of parts have signed with corresponding roles, the contract becomes *Signed*, or active. Only when a contract becomes signed, are the encoded instructions or information processed, and the duration of the contract counted.
- Contracts are *smart* and can adapt, depending on definition. They can be overridden by new contracts, or be revoked, if permitted in the definition, and parts agree thereto.
- Access to contracts can be restricted to parties with *authorized access only*.
- *Validation*, *resilience*, and *auditing* of contracts is done using the distributed *Neuro-Ledger*™. Access to the DLT is not required to interoperate and access contracts and legal identities. It is sufficient to have a legal identity in the network.
- Contracts are *not limited in size* for any practical purposes.
- Contracts can have *attachments* of any Internet Content-Type. Each attachment is cryptographically signed as well. Attachments may include documents, images, etc.

Smart Legally binding Contracts

A smart contract is created on a *domain*, governed by a *Trust Provider*. The *Trust Provider* on that domain controls the approval process of proposed contracts or templates. Each approved contract or template is also signed by the Trust Provider. By enforcing a policy where the legal integrity of templates and contracts is assured, together with the cryptographic security of signature algorithms used by the *Neuron*™ and *Neuro-Ledger*™, signed smart contracts are *legally binding* during the duration of the contract. All state changes (such as approval or signatures) are persisted in the distributed *Neuro-Ledger*™ and can therefore also be audited and validated, as well as the resilience of the information be assured.

State-of-the-art cryptography

State-of-the-art encryption and data protection is employed in the TAG *Neuron*™ and TAG *Neuro-Ledger*™. This means assets based on smart contracts are well-protected protected using methods that are replaced as old algorithms become obsolete and new algorithms replace them. Traditional block-chains have algorithms encoded into the very infrastructure, which makes algorithm-change practically impossible. Algorithm negotiation and evolution is build-in to TAG infrastructure products, to make sure information is always protected using state-of-the-art cryptography. Current level employs use of ed448/EdDSA, commonly known as *Goldilocks*[4], 224-bit strength cryptographic signatures as a minimum.

Sustainable and environmentally friendly

As the *Neuro-Ledger*™ is not based on blockchain, it lacks many of the drawbacks of a block-chain. Proof-of-Work (PoW), the principal consensus algorithm on an open blockchain requires a lot of processing power, and therefore also consumes a lot of energy. It solves a mathematical puzzle, only to demonstrate it has spent sufficient energy in order to not be a malicious actor that spams the network. PoW is otherwise completely unproductive. Its goal is to spend energy unproductively. This makes networks based on such technologies wasteful and unsustainable, at scale, by definition.

The *Neuro-Ledger*™ on the other hand, does not need a Proof-of-Work, as it is federated, and each generator proves its right to generate blocks on its domain using state-of-the-art cryptographic signatures using strong, well-authenticated digital identities of the corresponding domain. This makes the generation of blocks more scalable and much more energy efficient.

Examples

Examples of smart contracts that can be created using *Neuron*™ technology, that are difficult (or impossible) to create using blockchain technologies, include:

- Legally binding contracts and agreements between companies and systems, for automation.
- Human-readable contracts and sworn statements, such as notarial documents, with machine-readable information for integration with automated systems (Cyber-Physical Systems).
- Declarative agreements for automation, such as Data Protection Agreements for data exchange of personal or sensitive information.
- Consent-based contracts for privacy, require that only parts in the contract have access to the information, and that the contract can be revoked and forgotten.

[4] https://datatracker.ietf.org/doc/html/rfc8032

- Automated and legally binding contractual payments, including conditional payments that can be processed only on the fulfillment of legally binding obligations.
- Asset-backed tokens, and related contracts, that protect the ownership or lease of the physical assets forming the base of the digital instruments and their values.

4 e-Daler®

e-Daler® is a federated token-based instant payment technology built into the TAG *Neuron*™. It supports *cross-domain* instant payments, as well as offline payments. Transactions are logged in the *Neuro-Ledger*™ for traceability and auditability. Payments can also be made *offline*, making it possible to digitalize payment solutions in areas with limited or intermittent connectivity. Contractual payments can also be automated using Paiwise™, and included in general smart contracts, including *Neuro-Features*™. Access to an *e-Daler*® wallet can be given either through a TAG *Digital ID*™ or through the TAG *e-Daler*® nuget, for integration with systems and automated services.

Each *Trust Provider* defines the value of an e-Daler within its domain; typically, it is bound to the currency used by the *Trust Provider*. *Trust Providers* that trust each other can perform cross-domain transactions. Currency conversion can be performed, if a shared agreement exists for such, and an approved currency converter is used.

5 Neuro-Features™

Neuro-Features™ are digital instruments that can be used to implement *non-fungible tokens* (NFTs) and *asset-backed tokens*. They are represented by a sequence of smart contracts, that define the legality and related digital or physical asset defined by the instrument, as well as a unique *ownership* of the instrument. A *Neuro-Feature*™ has a lifecycle (which may be short, or very long), and a unique *owner* during its active life. Ownership can be transferred from the current owner, to the next. Each transfer is itself constituted by a smart contract. This transfer contract may include Paiwise™ payment instructions, which automatically transfer *e-Daler*® from the buyer to the seller, upon agreement. These payment instructions form an auditable trail and proof of the *value* of the digital or physical asset.

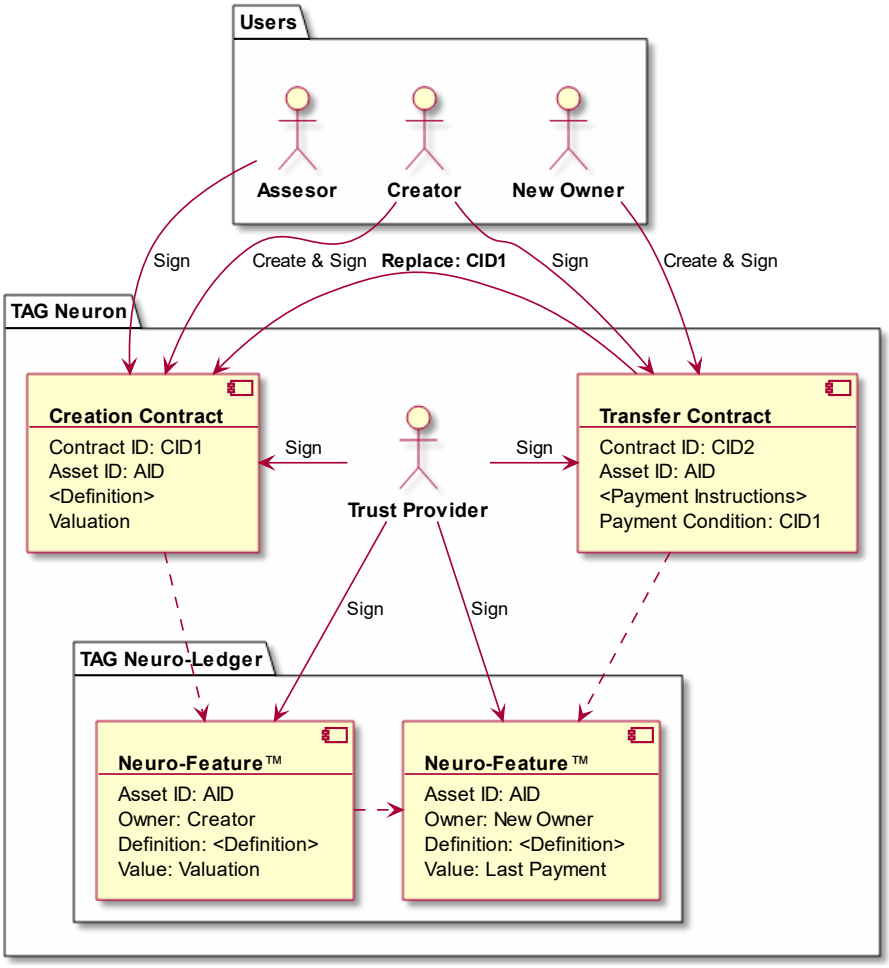
Neuro-Features™ can be used to create:

- Non-fungible Tokens
- Asset-based Tokens (based on land, real-estate, etc.)
- Ownership in production facilities with profit sharing (shares in company, power plant, manufacturing, etc.)
- Transferrable Leases
- Transport package in a Supply Chain, including intermodal logistics.

- Negotiable rights, such as emission rights
- Limited services (for example, seats at restaurant, theatre, event, travel, etc.)
- etc.

Collectively, these Neuro-Features™ can be seen as *cyber-physical assets*, which can be traded in *cyber-physical systems*.

Following is a simplified diagram on how a Neuro-Feature™ is created, and ownership transferred using smart contracts using TAG *Neuron*™ and TAG *Neuro-Ledger*™.



6 TAG Marketplace™

The TAG *Marketplace*™ is an online auction capability built on-top of the TAG *Neuron*™ and TAG *Neuro-Ledger*®, that uses *e-Daler*® for making transactions of

physical or electronic commodities in online auctions. It allows for Industry 4.0-type optimizations of supply chains, by providing an autonomous and automatable transaction layer between buyer and supplier. *Neuro-Features*™ can be traded in a TAG *Marketplace*™.

7 Summary

Using TAG *Neuro-Features*™ is a practical way to implement digital token-based assets that can be traded online, either by humans or autonomously by machines. These tokens can either be digital or have legally binding association with physical assets (thus becoming *cyber-physical assets*, that can be used and traded in *cyber-physical systems*).

To test the concept, contact Trust Anchor Group AB[5] to setup a Proof of Concept (PoC), or register your interest to participate in coming proof of concepts organized by our partners.

8 References

[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.

[5] https://www.trustanchorgroup.com/