Neuro-Ledger® and Sustainability

Peter Waher

Trust Anchor Group AB, Blekholmstorget 30F, Stockholm, Sweden
peter.waher@trustanchorgroup.com

Abstract. This short paper describes the sustainability benefits of using a new type of Distributed Ledger named the Neuro-Ledger®, for persistent, distributed and auditable storage.

Keywords: Distributed Ledger Technology, DLT, Persistence, Sustainability.

1 Introduction

It has long been known that blockchain technologies raise serious concerns with regards to privacy, scalability and energy consumption. Furthermore, inherent in the design and choice of a single algorithm for the duration of a block-chain raises longevity and security concerns. The Neuro-Ledger® solves many of these issues[1] by introducing a new type of digital ledger, that is not based on a block chain, and is therefore not susceptible to the vulnerabilities built into such an architecture. This paper focuses on the Sustainability aspects of using the Neuro-Ledger®

2 Degenerative chains

A blockchain using Proof-of-Work (PoW) in its consensus algorithm, will degrade over time. As new computer hardware is made available, they can execute a proof-of-work quicker than older machines. This requires adjustments to be made to the proof-of-work algorithm, to assure it is still as difficult to generate new blocks as earlier. Otherwise, in time, malicious entities will be able to hijack a blockchain, simply because they can generate vast amounts of new blocks. As proof-of-work becomes more complex, older machines will no longer be able to compete generating new blocks. To stay operational over time, performing the same tasks as before, operators need to constantly upgrade hardware in their blockchain solutions, even if complexity does not increase. Performance therefore degrades over time, by design, as technology evolves. New inventions in the computer hardware field, will not benefit blockchain solutions, as they will drive an increase in complexity for the proof-of-work, rather than allow nodes to perform more constructive tasks. This is contrary to the definition and very essence of sustainability. Sustainable solutions cannot be based on solutions requiring proof-of-work.

[1] See Neuro-Ledger™, Executive Summary, p. 1, 2019-10-11.

Information waste

Since deleting blocks in a chain is not possible (regardless of consensus algorithm), the amount of unused information waste in a block-chain increases over time. This further reduces the efficiency of the system as time progresses. The percentage of useful information in a blockchain compared to the overall amount of information processed is reduced the longer the system operates. Apart from being a problem when processing personal data, it is also contrary to sustainability requirements, which requires systems to only process necessary information. Why acquire hardware to process information that is no longer necessary to process?

Energy consumption

As a consequence of the degenerative nature of block-chain solutions (double degenerative nature, in the case of proof-of-work-based block-chains), high performance computing is required to protect the network and process information over time, as solutions grow. This consumes a lot of energy. This energy is principally wasted in unproductive and/or unnecessary work. The proof-of-work does not generate value, so consuming vast amounts of physical energy as a means to protect an otherwise unprotected blockchain is a great waste. If the goal is to create future-proof systems that are also sustainable, using proof-of-work-based blockchains is counter-productive.

3 Alternatives

Several alternatives to the problem of PoW in consensus algorithms of blockchain have been proposed. These include replacing PoW with a proof-of-stake (PoS) instead. But such a solution is not a general solution for many of the other vulnerabilities listed earlier. It is also only applicable to blockchains where there is a clear measurable stake (such as coin-based blockchains). PoS cannot be applied to a general DLT, which just acts as a distributed ledger of immutable information that can be validated and audited.

No chains

Employing a consensus algorithm to establish a single chain in a blockchain is a consequence of designing a blockchain for distrusted networks. In the general case however, there is no need for links to the previous block, establishing a chain of blocks, in a trust-based environment[2]. Why should one node be affected by unrelated

[2] In a trust-based environment, every participant has a well-defined identity, protected by cryptographic signatures. Each node can freely issue blocks from its own domain. Recipients, trusting the identity, and having access privileges, can access blocks, and information inside. It is always clear who is the issuer of a block, and everyone can validate the corresponding signatures.

operations taking place on another node? There is no need to compete in a trusted network. Therefore, there is no need for a consensus algorithm, and no need for chains, unless required specifically by an application. Instead, the Neuro-Ledger® implements a big, distributed set of blocks, which may, or may not be related, based on their contents. Blocks can still be linked (in multiple co-existing chains), if required, or ordered in time, up to clock differences between nodes, as they are time stamped. Not using chains has the following benefits:

- Blocks can be deleted, without affecting information in other blocks.
- Information in a Neuro-Ledger® can be removed when it is no longer needed, complying with important privacy requirements. Blocks have a Time-to-Live, or TTL, or best-before date.
- A propagation mechanism in the protocol makes sure changes made on the source is propagated across the network.

Strong cryptographic signatures instead of PoW or PoS

Instead of spending time on fruitless proofs (of work or stake), Neuro-Ledger® uses strong asymmetric ciphers to create strong signatures for each block, protecting both the integrity of the contents of the block, as well as the identity of the creator of the block. It is much quicker and easier to create such signatures, and validate such signatures, than to execute the proofs used in blockchain implementations. Furthermore, ciphers used can vary over time, or across node, complying with cryptographic best-practices. It makes it possible to phase out ciphers in a timely fashion, in favor of new modern ciphers.

4 Summary

Using blockchain-based ledgers is dangerous for many reasons. It is also unsustainable. Very few use cases actually require the use of a blockchain. What is desired, are the general qualities in a Distributed Ledger. The Neuro-Ledger® is a new type of Distributed Ledger, that is better suited for processing information, including sensitive and private information, over time. It does not suffer from the same vulnerabilities as traditional blockchains. For more information, see footnote 1.