SOLID REALM

—

The business blockchain

Nyneve Software, LLC

10107 Brantley Bend
Austin, TX 78748

512-909-2206
info@nynevesoftware.com

Solid Realm, The Business Blockchain

Abstract

The Solid Realm is a blockchain software architecture design. It overcomes many hurdles businesses encounter with current blockchain technology. The focus is to provide and maintain clear vision and reference examples that favor GDP vs. electricity spent, that is, "provide real-world-work". Part of the idea of "real world work" are Matters of Law, Regulatory Compliance, and inherent features supporting traditional business transaction types.

Introduction

Let's get down to business. As an entity, wouldn't it be nice to be able to readily accept end-to-end, secure consumer transactions that require:

- A "shopping cart checkout"
- Multiple and differing cryptocurrency attached payments
- Backed up by a credit/debit card

all in one "click"

Would it helpful if this transaction were PCI compliant from a Secure-Vault directly to a Secure-Vault with no remote compromise?

This type of transaction and transaction history are the basis for the design of The Solid Realm blockchain.

The world of failure-by-design

- There is no level of Secure Hosting for Server-Side technologies, which prevent the end user from being the weakest link.

  The end-user needs something of their own that can be relied upon, without staffing full-time IT Security Experts, just to secure their web browser every time they use it.

- There is no rational expectation of an end-user having a "secure smartphone".

  Almost on a daily-basis we are bombarded with new "zero-day" exploits of hardware itself, such as CPU's, SDR's, and Networking Appliances, such as Routers and Firewalls.

  Also, we see entire product lines fail when their Root Certificates are compromised, giving hackers a back door to the entire world.

- There is no rational expectation of a "secure hardware wallet" for cryptocurrency transactions, if the design requires it to network or to plug-in to any other computing device.

  The STUXNET virus destroyed a uranium centrifuge complex because a USB device was plugged into a computer.

Business at the mercy of blowing winds

- Many blockchain and cryptocurrencies have emerged without regard for "Service Level Agreements".

- The idea of an "immutable ledger" risks mass exodus of hobbyists for greener pastures or newer technologies.

- The idea of "free" exchange of cryptocurrency is anything but free. Blockchains are in business after all. Transactions are costly.

- Cryptocurrencies are often great examples of taxation without representation. The 'gas' transaction fees do not go toward improving the infrastructure. We pay more to transact faster, but why are the roads not getting any better?

- Cryptographic exchange services, or "gas stations along the highway", transact business off-chain to meet consumer performance demands. The blockchains themselves cannot handle the volume.

Extreme losses and extreme measures

There are numerous and on-going examples of cryptocurrency losses due to theft and misconfiguration totaling hundreds of millions in dollar-equivalent value; and on-going credit/debit card fraud to the tune of $billions.

The greatest common denominator in all this comes down to the ultimate insecurity of the transactions that are taking place.

A parking-lot hack of a retail vendor's wireless internet interface to a credit card processor is no different than an on-line shopper's browser getting hacked via any number of means.

The completed end-to-end security for transactions generally does not exist.

This is true for both Cryptocurrencies and Credit/Debit card transactions.

People who are serious about security for their cryptocurrency transactions have computers that are always off-line. The problem is that data has to be transferred from an off-line computer to an on-line computer using "dirty needles", i.e., USB sticks that can transmit viruses, as mentioned earlier.

We all know what the solution is

Encryption and decryption activities must take place on devices that are never connected to anything. The kind of hardware that nobody can see you typing a message before it is encrypted; or see what you received, after you decrypt it.

The Solid Realm blockchain exists because this kind of technology is now rapidly emerging.

It may come as a surprise, but end-to-end secure hardware has been in existence for over 15 years.

- It protects the military.

- It protects the nation's critical infrastructure.

- It is available to the public.

Let's take a quick look

What can you do if the blockchain design is "owner-transferable digital property" instead of coin-ledger-balances and network-bound "smart contracts".
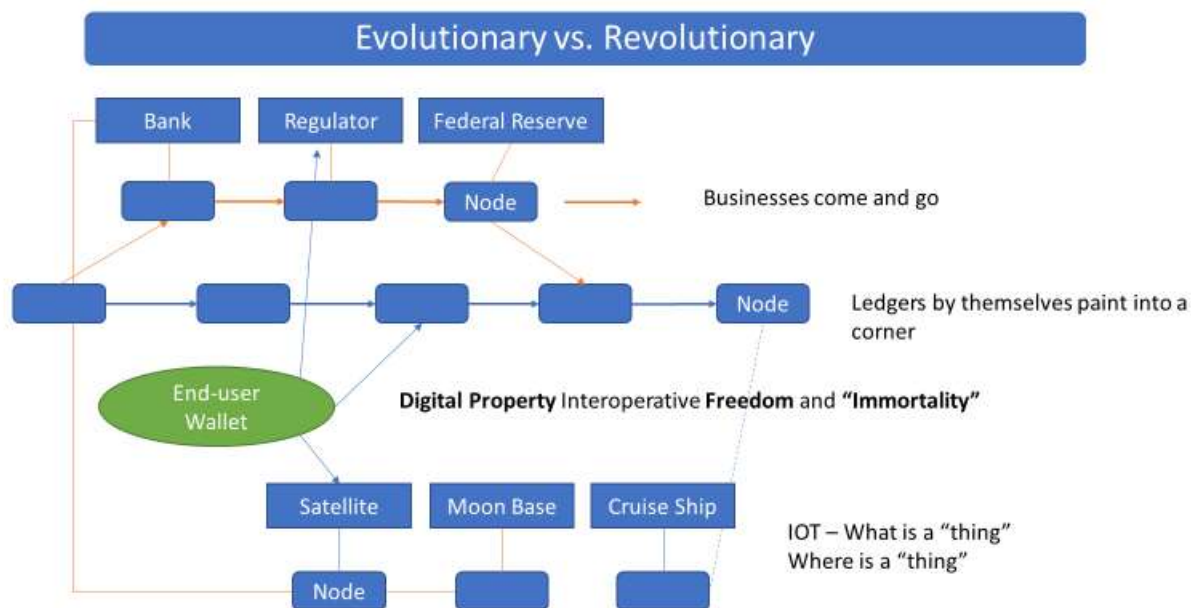
- Businesses are free to establish high speed service levels
- The public can semi-independently "police the police"
- Businesses can stand-alone without being connected 24/7
- The end-user is entirely in control of their own "digital property"

A network of relationships

Whereas many blockchain technologies purport anonymity in transactions, The Solid Realm is a network of relationships controlled by the end-user.

The Solid Realm is good at Owner-Transferable Digital Property. This is a very powerful capability of its own right.

By comparison, what did you buy with your cryptocurrency transaction? A movie-ticket? The Solid Realm is designed to contain the movie-ticket.

A network of end-to-end secure transaction wrappers

A typical cryptocurrency transaction does not contain the "Purchase Order", "Invoice", or "Receipt". The Solid Realm works with end-to-end secure transactions, and supports complete document models.

"This is my order, my payment(s), and my instructions" – all at once. "Thank you for your order, here is your receipt".

By default, everybody gets private "proof-of-existence".

If you present the transaction details, you can prove them on the blockchain. If you just look at the blockchain, you have no idea what it represents.

What is so different from everything else?

The Solid Realm blockchain is designed to run in the presence of secure hardware, both in the hands of the end-user and in the secure hosting facilities of businesses.

This is achieved by having both an Internal Blockchain, inside of "digital properties", and an external traditional-looking blockchain where a vast node-network competes for "the truth".

The fundamental design required to do this allows "digital property" to be "immortal digital property" capable of injecting itself into newly emerging technology and discarding the old.

An individual business has the option of having a single stand-alone node that does not ever connect to a global node network. "A movie theatre tearing a ticket stub in-person".

The hardware platforms allow for the convenient and business friendly inclusion of Credit/Debit card transactions entirely in-stride and augmenting the non-exclusive use of popular cryptocurrencies.

Businesses may establish "fast lanes", high bandwidth, high throughput, for private and consortium use without fully disconnecting from "the public no-trust" of traditional blockchain philosophy.

The Solid Realm is a helping hand for all cryptocurrencies by engaging the security, performance, and flexibility that traditional business requires; thereby providing the economic "real-world" B2C traction necessary to move the entire world forward with all cryptocurrencies.