THE SOLID REALM

Distributed recording of owner-transferable user-defined data

“Digital Property”

By Nyneve Software, LLC
info@nynevesoftware.com

What happens if you design a public blockchain technology that is philosophically geared for

BUSINESS FIRST

Then, right from the beginning…

1. Overcome hurdles that business have with existing blockchain technology
2. Provide a clear vision and reference examples that favor GDP vs. electricity spent
3. Inherently accommodate The Law and Regulatory Compliance

And … START by supporting Visa, Mastercard, ACH; Terms, Conditions, and BUSINESS Contracts

“Private”, “Consortium”, “Public”
In blockchain terminology – all at the same time

In The Solid Realm, various kinds of computer node networks interoperate because…

- The end-user “wallet architecture” is in control
- This is not an ledger for coin-wallet balances
- This is multi-petabyte BLOB/CLOB-referencing “title” engine with optional block consensus

AND OWNER-CHAIN CRYPTOGRAPHY

Paper – as an analogy

Paper can be photocopied and stored in multiple filing cabinets

If on the paper, it says which filing cabinets it is stored in…

Then every copy of the paper references every other copy

The filing cabinets are free to stand-alone, or to band together for consensus

When you transfer title to the paper,
simply check all filing cabinets and cabinet systems
that are referenced on the paper itself

CONTROL

Where to file ownership of paper next is, fundamentally, up to the END-USER

…**and** any **particular application** associated with the particular paper

Will the Police Officer honor a Driver's License from another country ?

That is not the job of the blockchain or node network to decide, but to support!

You Hold-Title to something, and you can prove it by the strength of multiple independent filing cabinets and filing cabinet systems

FREEDOM

Take your paper with you

If a particular filing cabinet or system of filing cabinets (node network) makes you sad take your paper with you and file it somewhere else

No other blockchain methodology is – in the end – “by the individual people” and not the Node Consortium. Blockchains typically have to FORK EVERYTHING to fix one thing.

THE CUSTOMER IS ALWAYS RIGHT

Try telling another blockchain to fork-off
your individual property and see what happens

LAW

Ability to “fork” individual paper

A court order can be accommodated by “filing cabinets” and “systems of filing cabinets” so as to individually address single transactions or the entire history of a single “paper”, again, without ‘forking the entire blockchain’.

THE CUSTOMER IS ALWAYS RIGHT

Except when…

HOW DOES IT WORK? – PART I

Allow us to now shamelessly introduce our hardware

If you see how we use The Solid Realm blockchain software technology, you will have a ready grasp of the design details to follow

…and hopefully you will be impressed by the hardware we are promoting!

Our choice for hardware

Solid Armor

The Hardware Wallet of ZERO Connectivity

Off-line only, not even USB connectivity

Fully audit all I/O and cryptography as it happens

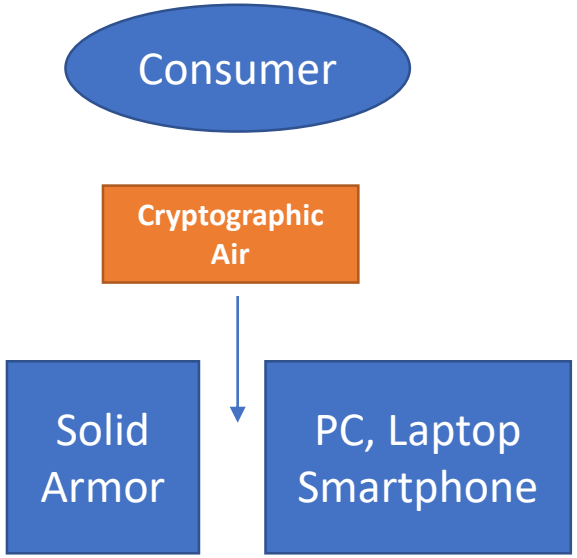
Solid Armory

An entire line of protocol isolation networking solutions in use by the military and critical infrastructure

27 Patents

15 year Solid History

Solid Armor Hardware Wallet Features



No chips for wifi, Bluetooth, cellular, GPS and no USB

Typical QR Code scan and presentation of stored wallet public key capability (to meet common practice)

Sign crypto-coin transactions inside Solid Armor, never exposing private keys to any other device (ever)

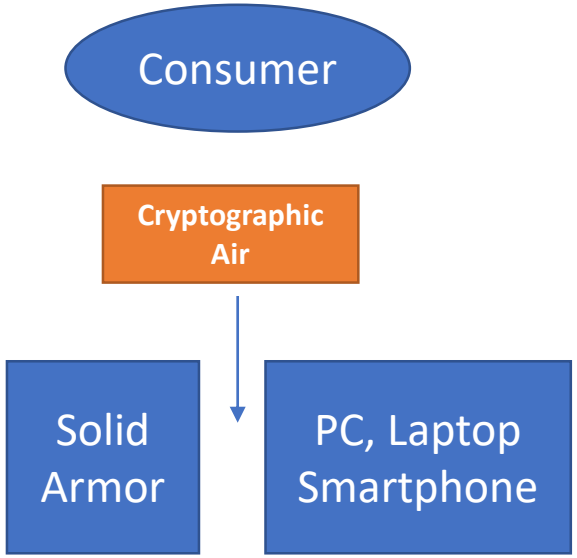
End-to-end secure Visa/MC “checkout” with participating services.

Partially secure web forms (bypass your PC screen and keyboard - or those of other device(s)) with any web site

Fully end-to-end secure web forms processing with participating services

All cryptography is available for display to the user to verify and audit all QR Code traffic, every step

Solid Armor Hardware Wallet Features - continued



Always off-line, NEVER on-line device for MyEtherWallet

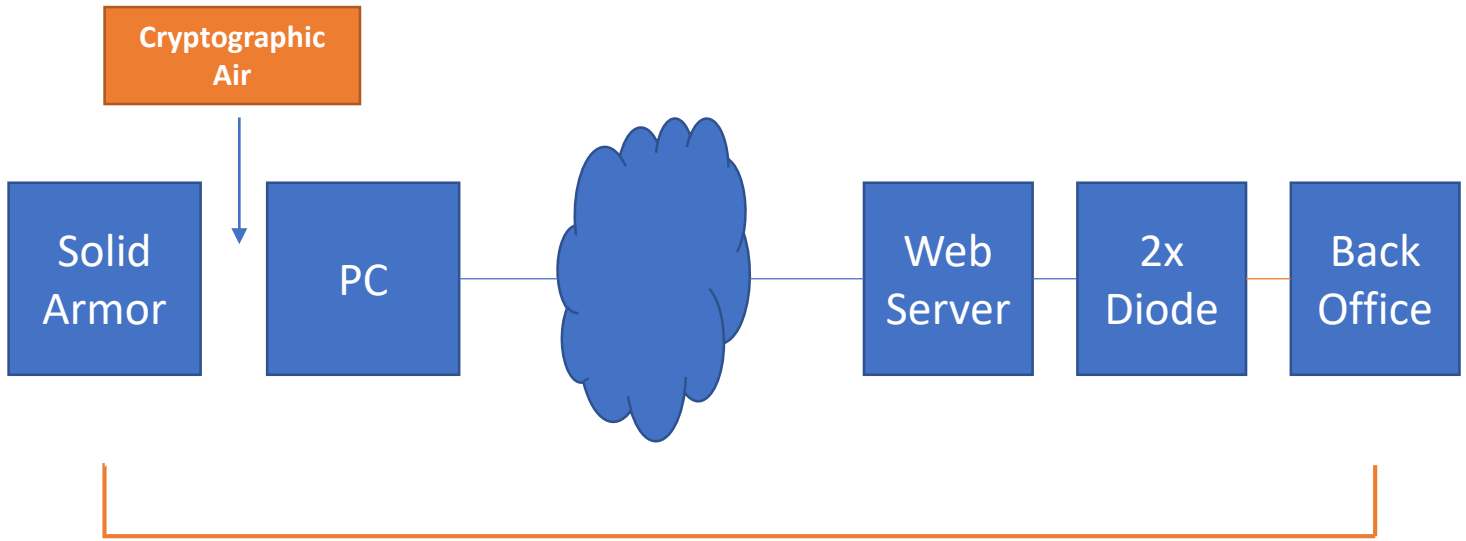
In-person private-key exchange. Later send secure messages through *any* medium, email, print on paper, etc.,

Downloadable and updatable Javascript applications
(a multiple QR Code Process)

Javascript isolation from QR Code display and processing

Reseller and whitelabel

The “pretty good” credit/debit card transaction

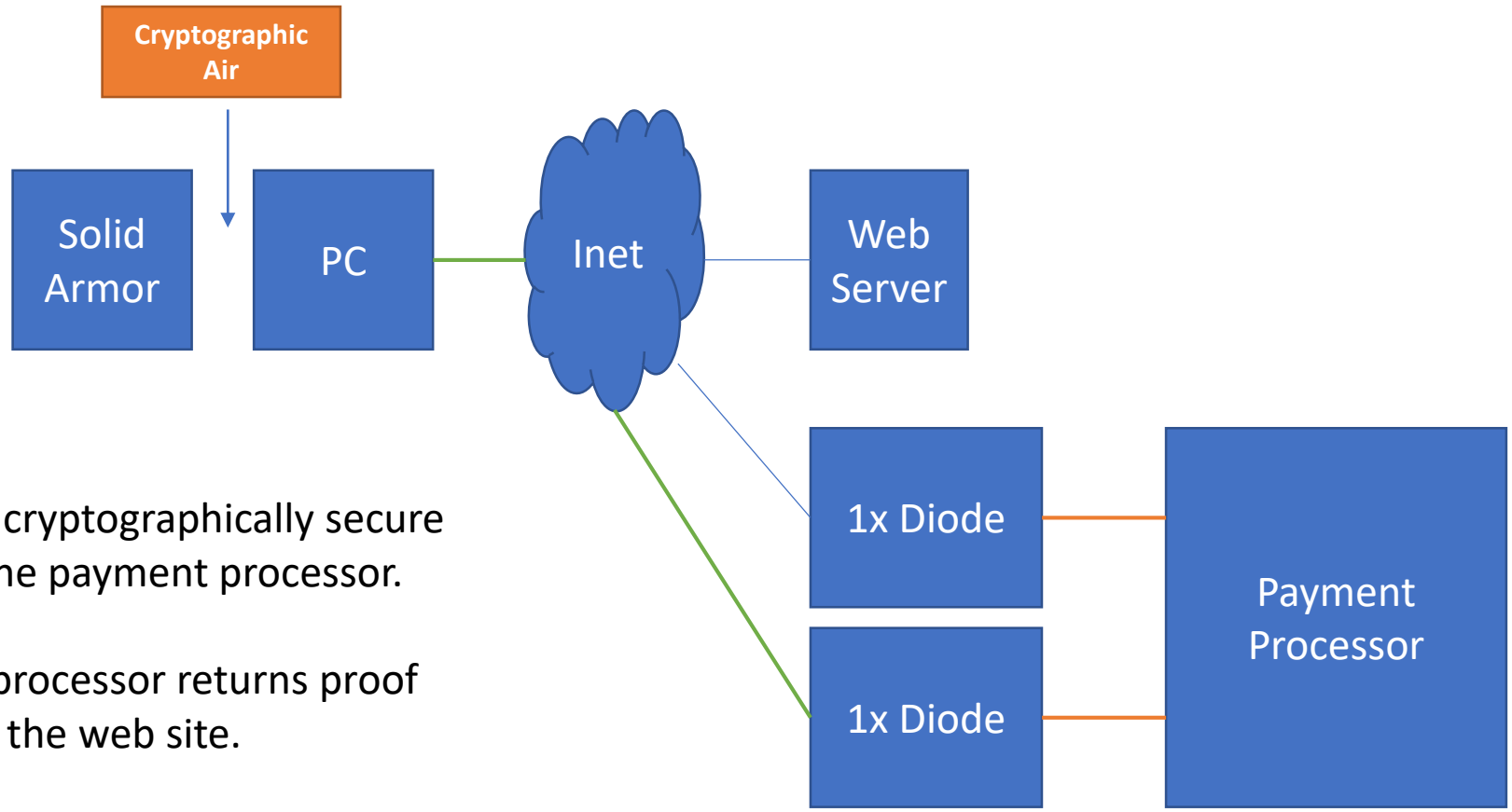


Solid Armor and the Back Office are effectively non-networking hardware

The transaction cryptography is end-to-end

No ”man-in-the-keyboard” or in the browser, no “man-in-the-back-office”

The ideal credit/debit card transaction



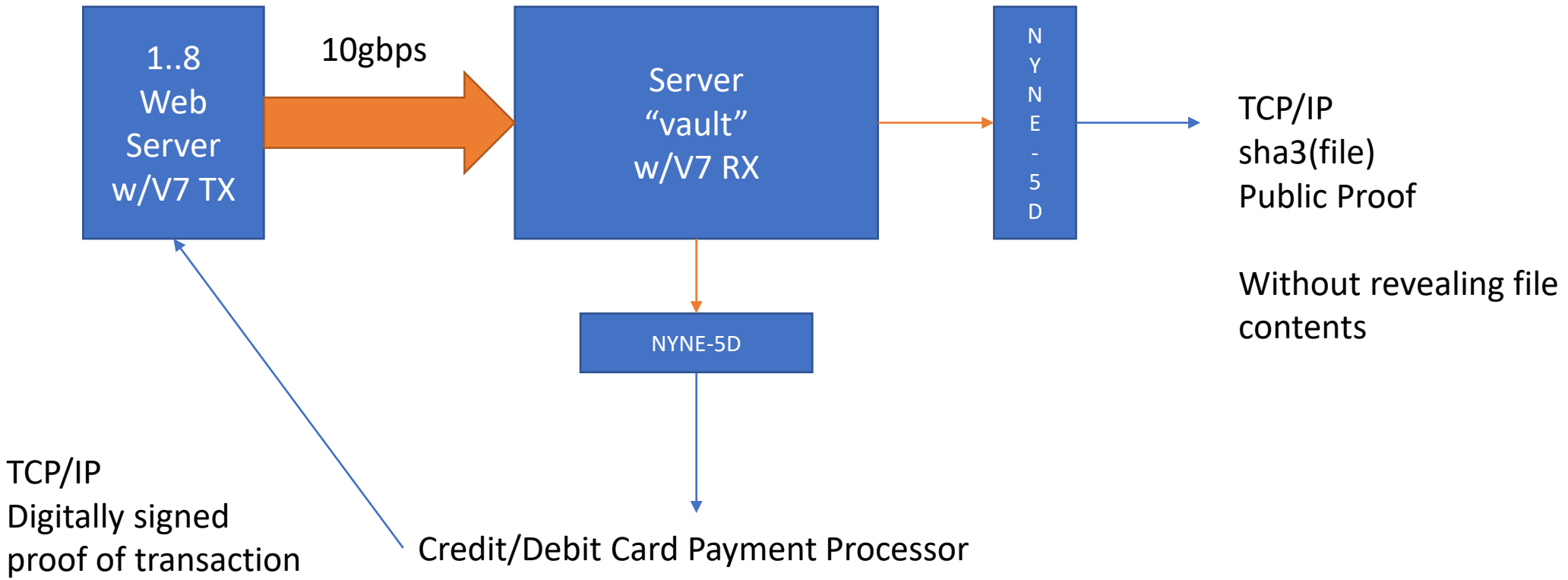
Solid Armor is cryptographically secure directly with the payment processor.

The payment processor returns proof of payment to the web site.

Only the payment processor and Solid Armor have custody of private card data

Business Service: front-end use-case – Digital File Proof

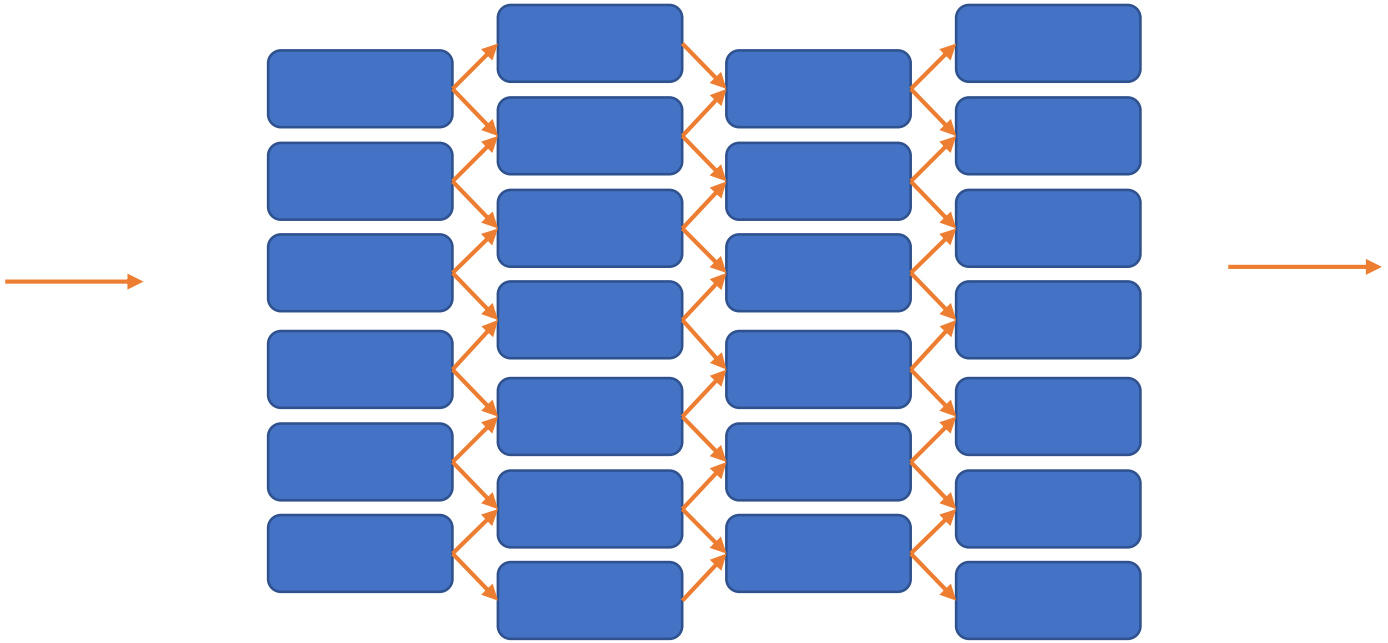
“The blockchain of custody”



Physically unidirectional node network topology

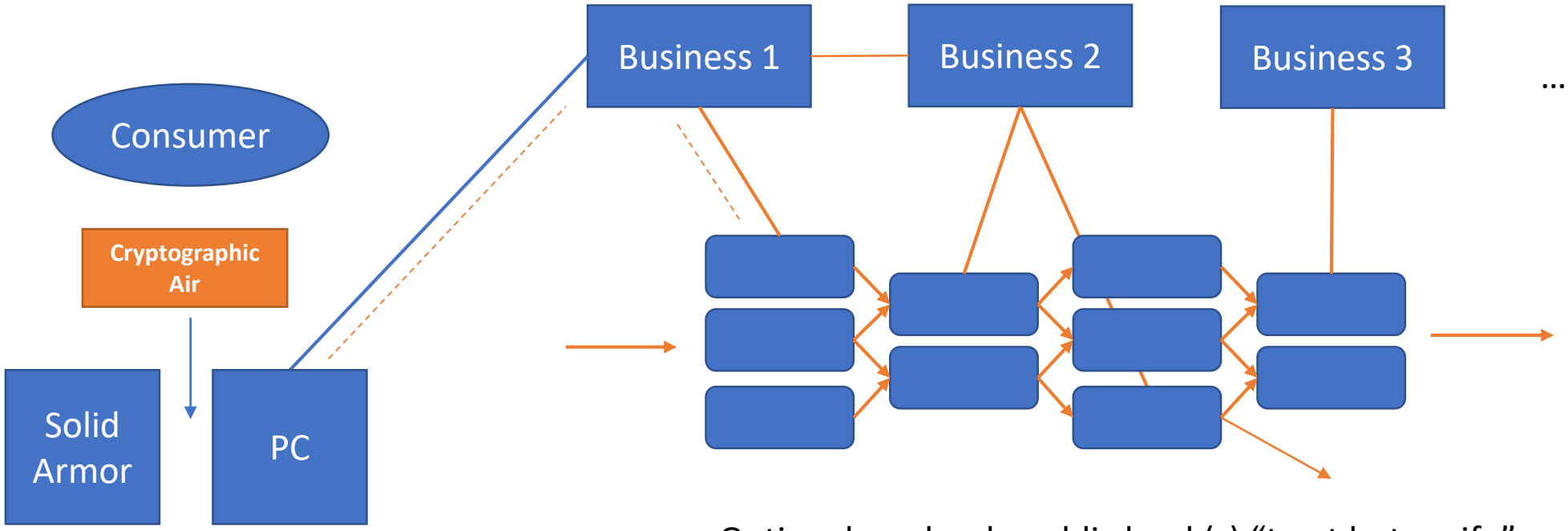
“A physical blockchain” Diode-in, Diode-out

Shown with minimal fan out



Controlled entry to node member blockchain
Physical Anti-spam/anti-flood – and public option to read-only any node

Business-consortium “jet-stream” blockchain
Physical isolation from public spam/flood/lag



Optional read-only public hook(s) “trust but verify”
Optional sub-domain of public Digital Property address space

Ultra-high speed, business-contractual service level, minimal node-count, maximal bandwidth
“Ethereum actually in the ether” – for example – it is not just our blockchain that can use Solid Armory hardware.

HOW DOES IT WORK? – PART II

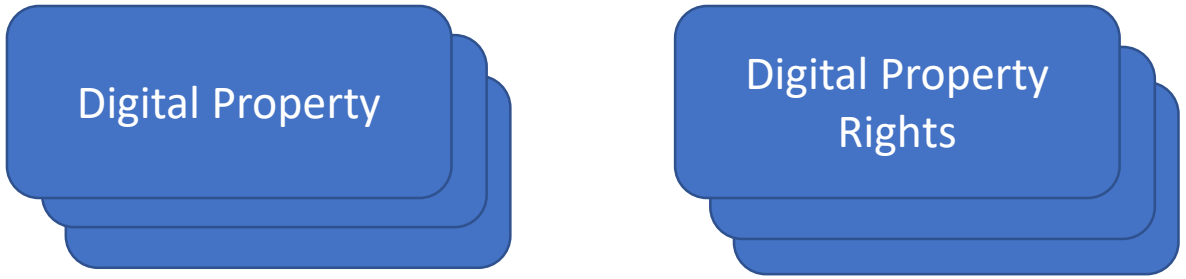
Base level data types of The Solid Realm

- Digital Property
- Digital Property Rights
- Multiple Semi-autonomous Block Ledgers

[Digital Property + Rights] Logical Address Space
340,282,366,920,938,000,000,000,000,000,000,000,000

A SOLID REALM WALLET IS A CONTAINER
of digital properties and digital property rights

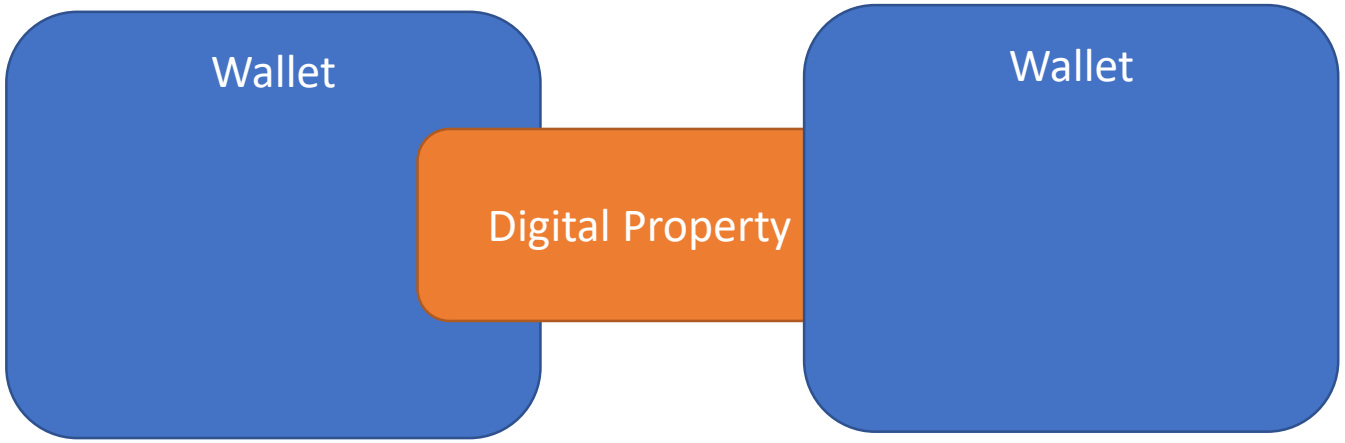
The user owns the wallet, the node network(s) have copies of the property proof



NO WALLET REPRESENTATION ON-CHAIN

Only the digital property proof is on-chain

Wallet applications exchange property secrets between wallet applications



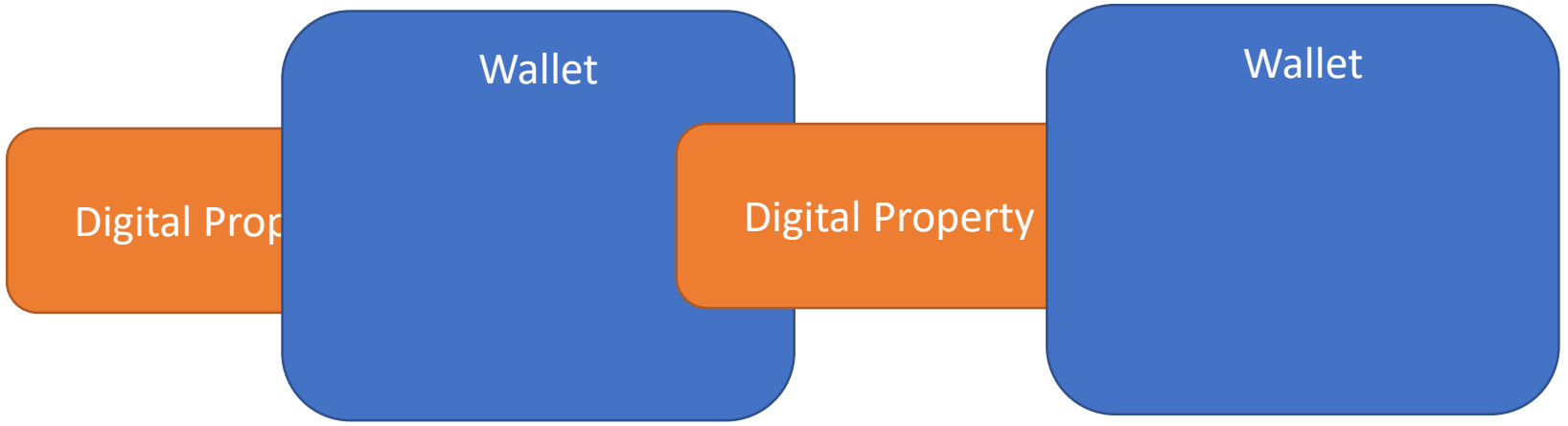
The new owner records new public unlock secrets of the property onto the chain
This maintains a unique public record of one owner of the digital property

# of sequential off-chain transactions before recording

This is an end-user application choice

Not a blockchain node-network rule

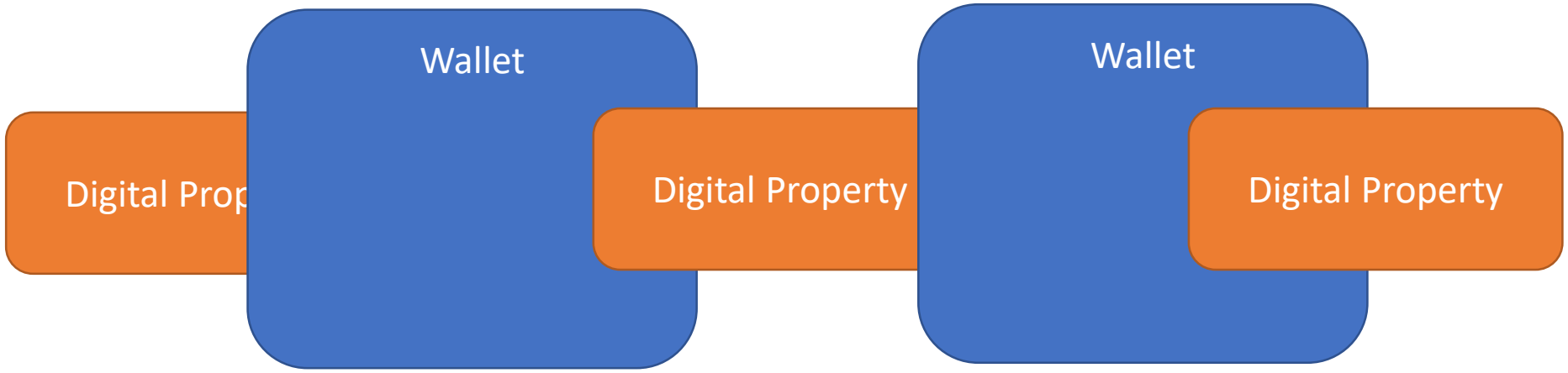
Wallet applications exchange property secrets between wallet applications



The new owner records new public unlock secrets of the property onto the chain
This maintains a unique public record of one owner of the digital property

Digital Property has more freedom than coin-ledgers

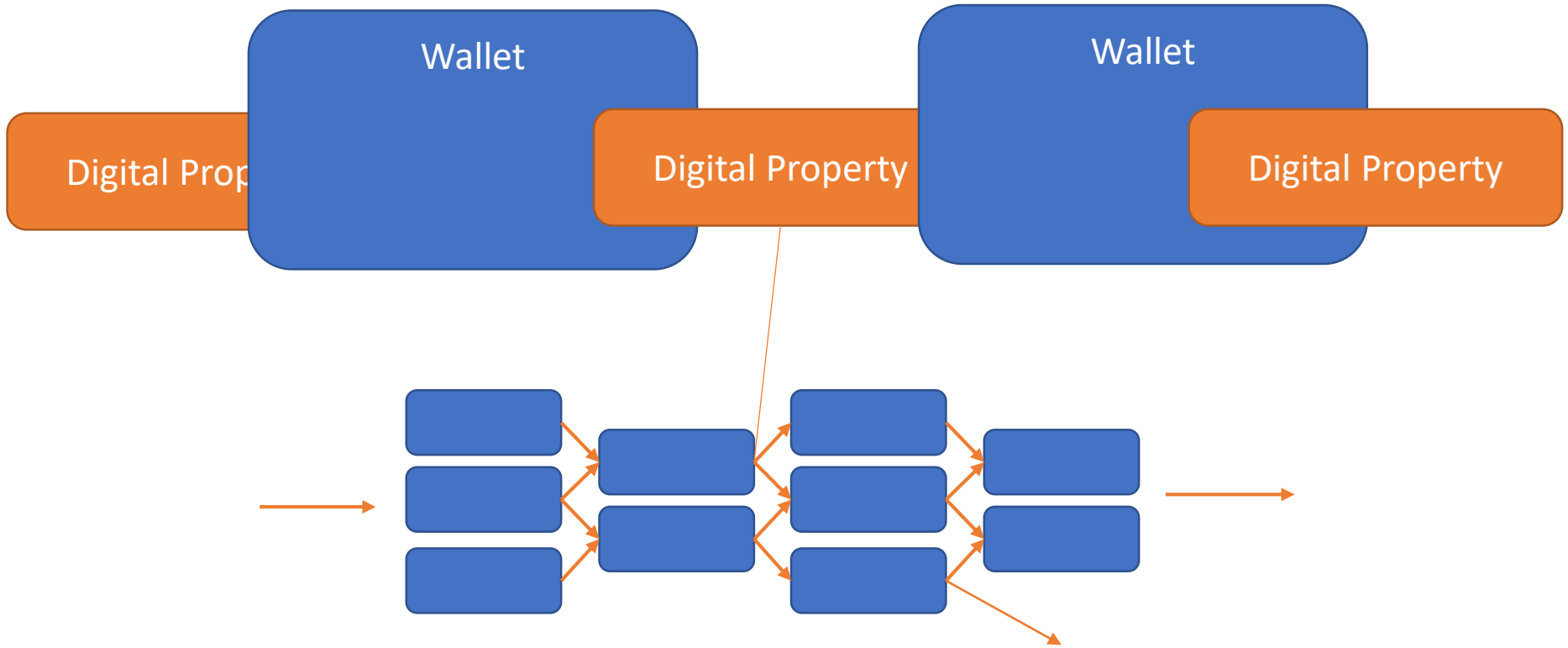
Wallet applications exchange property secrets between wallet applications



The new owner records new public unlock secrets of the property onto the chain
This maintains a unique public record of one owner of the digital property

The node network(s) are application touchstones

Real-world application complexity ultimately exceeds any blockchain



Exploring a transfer – for comparison purposes – of a paper bitcoin

A paper bitcoin contains both the **public key** and the **private key** of a bitcoin wallet

Just because someone hands you a paper bitcoin does not mean that they do not retain a copy

Exploring a transfer – for comparison purposes – of a paper bitcoin

In order for you to know that you are the only one with the Bitcoin$ now, you have to transfer the bitcoin out of the paper Bitcoin address(es) into a new Bitcoin wallet address that **only you know**

A Digital Property - Cast (as a Master Transaction Token)

Shopping Cart Order # 423423
Bill-to: …
Ship-to: …
Pay with Encapsulated Paper Bitcoin Wallet #1 … ~$4.95
Pay with Encapsulated Paper Bitcoin Wallet #2 … ~$32.78

Only the sha3(this above, peppered) lives on the blockchain

A Digital Property - Cast - as a Master Transaction Token

Digital Property is a secure cryptographic wrapper for ANY BLOB/CLOB.

Product doesn’t ship unless the BTC is successfully transferred out of each paper wallet.

The vendor’s life is simplified and **payment may be augmented and ensured with credit/debit card.**

A Digital Property - Cast - as a Master Transaction Token

Traditional business does not need the presumed transaction anonymity aspects of BTC. **It needs the receipts!**

Prepared-in-advance “paper” BTC wallet(s) did not invoke recording/gas fees on consumer’s part.

Digital Property Structure in Client Wallet(s)

- Property ID
- RecordedSequence#
- Previous Pepper
- Next Pepper
- Server Side Previous Unlock
- Server Side Next Unlock

Pepper denies any previous or future owner from attempted tampering with history

The client wallet defines next unlock for the server

Structure is flexible to contain additional payload

WHAT IS IN A SOLID REALM BLOCKCHAIN NODE

"DTD"
Document Type Declarations
For { address range }

Node Registration

Node-Signed
Ledger(s)

Digital Property Proof
123 Bytes per Property per Version

340,282,366,920,938,000,000,000,000,000,000,000,000 [128bit Digital Property Address Range]

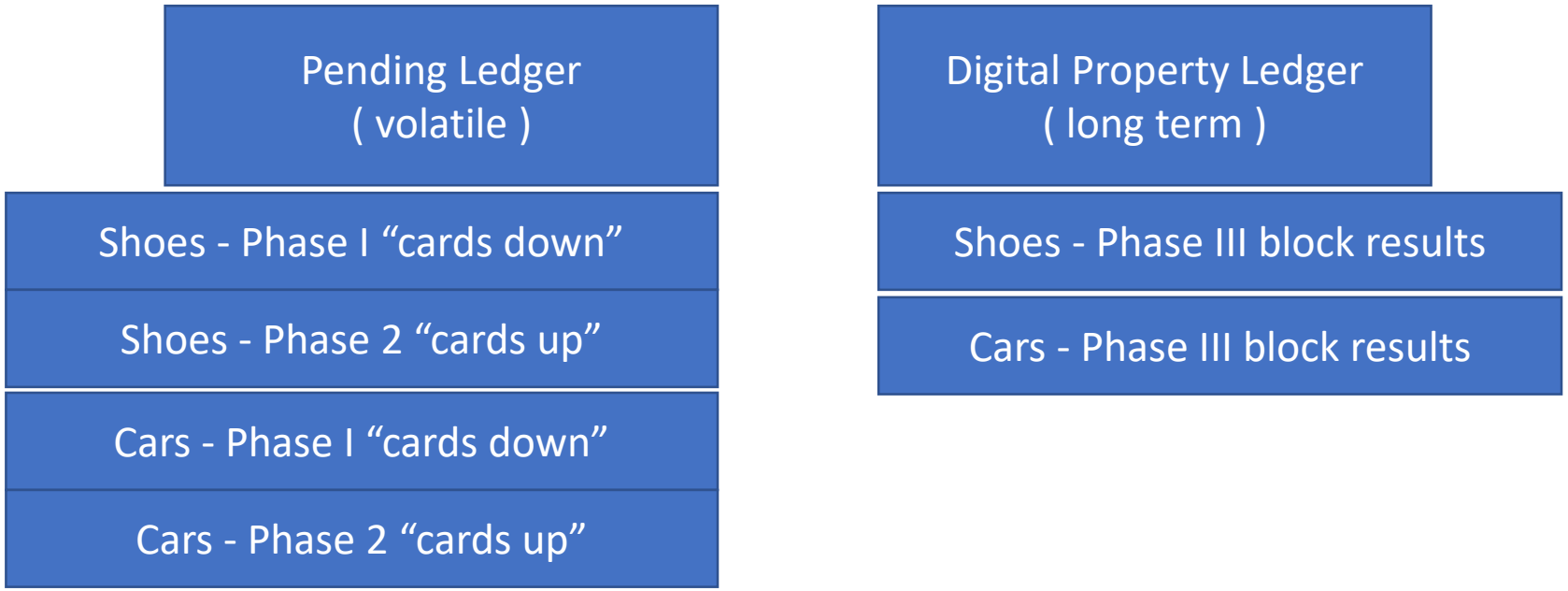
THERE ARE 3 BASE DATA TYPES

Everything works off of these

- Digital Property
  - Digital Property
  - Digital Property Rights
  - DTD
  - Node Registration
- Pending Ledger (volatile)
  - Phase I “cards down”
  - Phase 2 “cards up”
- Digital Property Ledger (long term)
  - Phase III block results

FREE MARKET OF BLOCKMAKING

Nodes subscribe to DTDs to make blocks for



How much Proof is Enough Proof ? Maybe 20,000 nodes is enough and you don’t need 150,000 all repeating the consensus. The Solid Realm Wallet makes this much tighter.

“PROOF OF RECORDING” - method
Wallets issue recordings in two phases

Nodes have to assemble two cryptographic halves of a new digital property version in order to participate in making a block for the associated DTD

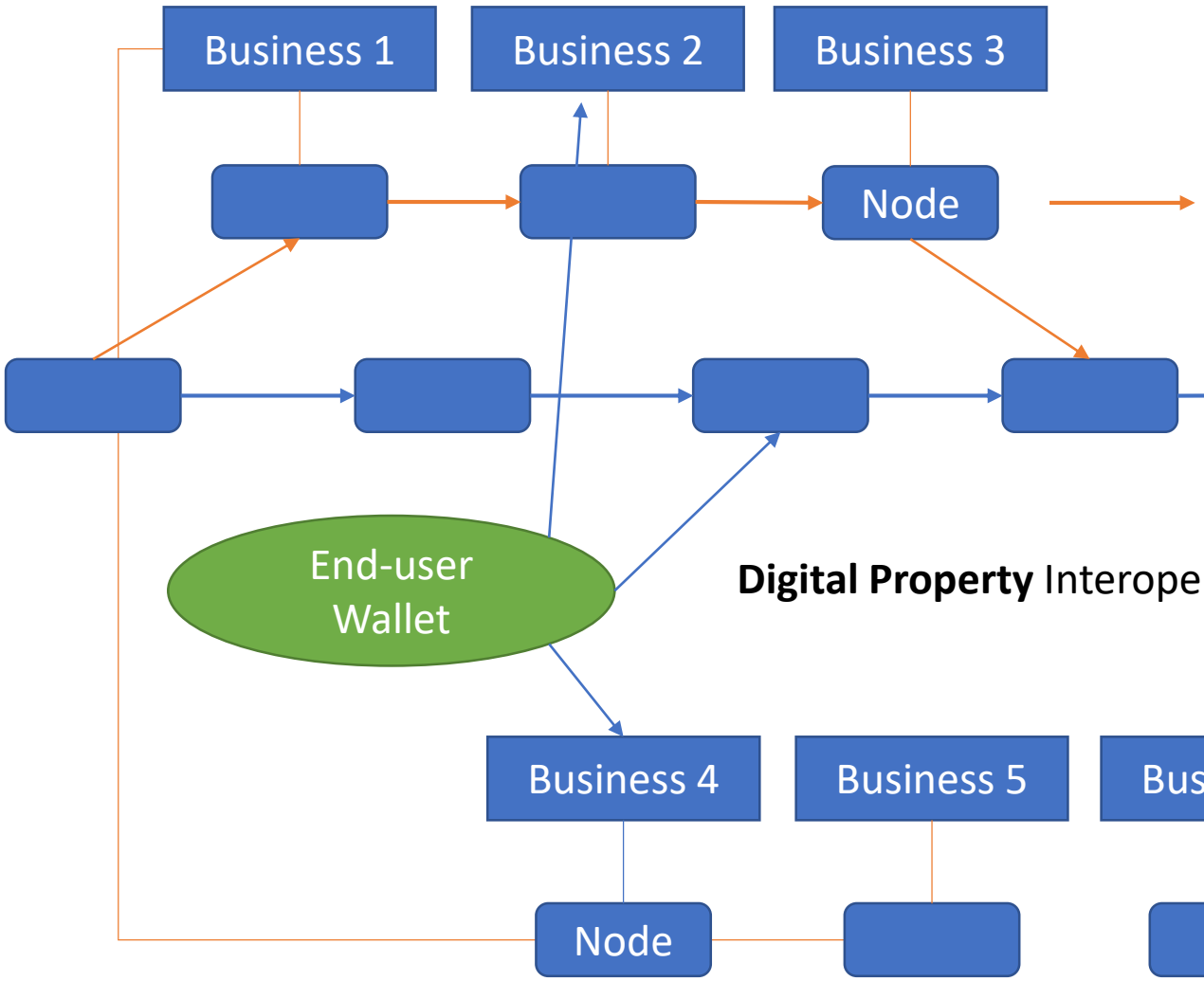
This results in “proof” of “yes I have the digital property and it checks out and I am not just repeating a consensus value.”

This is not a (so far to date 2018) “coin ledger balance” mechanics, it is a “replicate individual digital properties” mechanics.

Nodes make entire blocks for DTDs, but the properties themselves can contain their own individual histories (application configurable) [1 previous – minimum].

Simultaneous ‘On-chain… chain’, and ‘Off-chain… chain’.

The “cool” factor



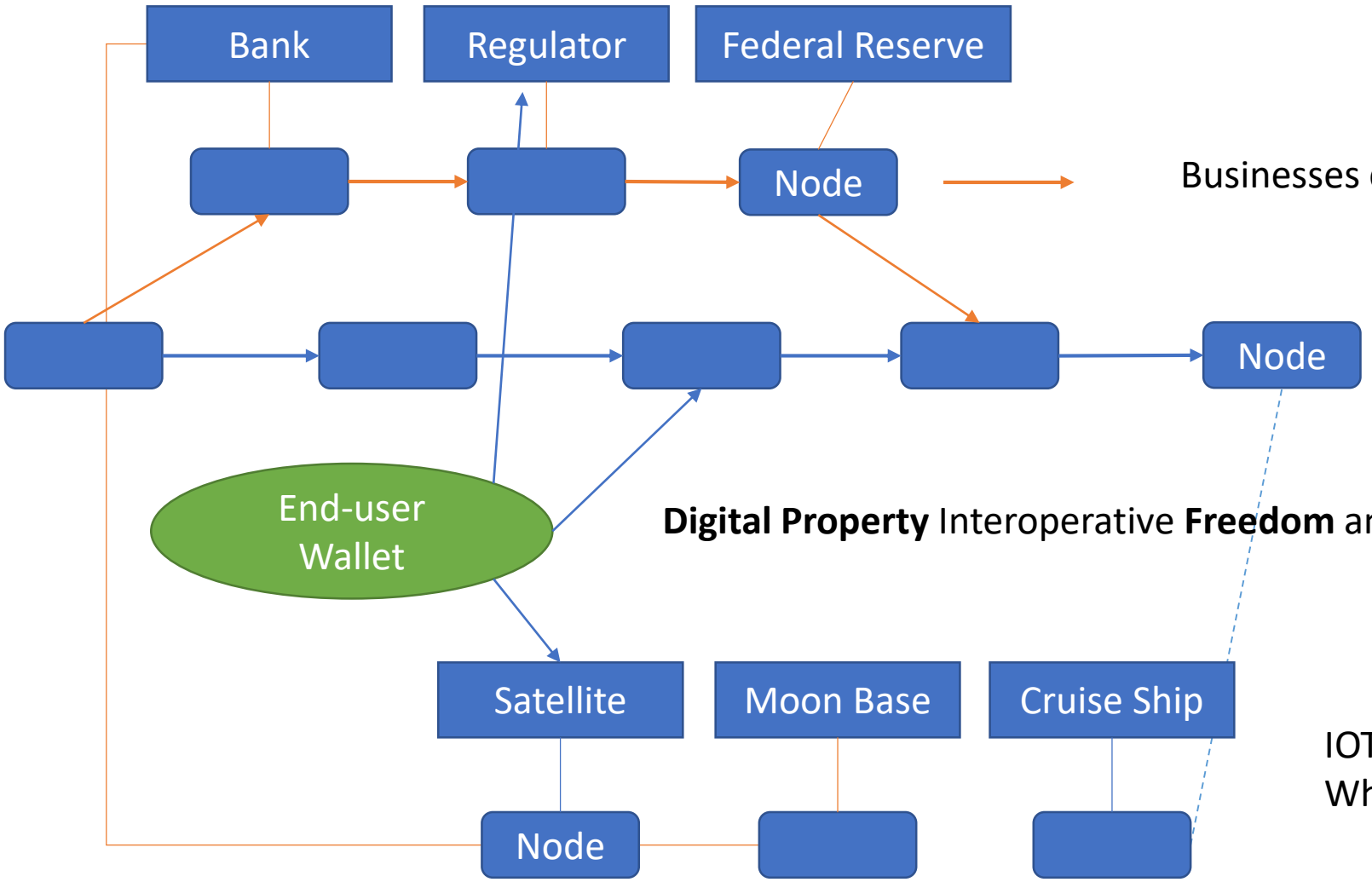
Semi-private high speed **consortium**
Network isolation “secure” hardware
“Fast-Lane”

Public node network **“backbone”**

Digital Property Interoperative **Freedom** and **“Immortality”**

Stand-alone **Private** Services
Zero to intermittent to full public net connectivity

Evolutionary vs. Revolutionary



Businesses come and go

Ledgers by themselves paint into a corner

Digital Property Interoperative **Freedom** and **“Immortality”**

IOT – What is a “thing”
Where is a “thing”

Summary and Jargon Index

PHYSICAL “Fast Lanes”
LOGICAL “Fast Lanes”
“Proof of recording”
Stand-alone-node participation
Immortal User-Controlled Digital Property
On-chain chain parallel with **Off-chain chain**
Simultaneously Public, Consortium, and Private Ecosystem
Dial-your-proof-strength
Multi-Node Injection