



**DAL
IDENTITY**
Diverse Authentication Library

An Evolutionary Approach
to Securing Interoperable
Assets using Digital Twins

All Rights Reserved Q1 2024



"Everybody's concerned about security. Cybersecurity is just a word pointing to an obsession with digital automation. But what is security when it becomes the opposite of freedom? When it isn't really about liberating ourselves from danger or risk? This is the fundamental question we must ask ourselves. It is the only question we must answer right now."

- Anonymous (an Officer of the US Army Central CyberCommand)



"There is no Internet of Things without an Internet of Microservices that is fully secure. The latter simply cannot exist without the former. Therefore, microservices must have great utility, ease of use & be fully interoperable at the object level."

- Marcel Donges, CTO of DAL: Inventor of Web 4.0 & its interoperating software



GOING BACK TO FUNDAMENTALS

What we do in terms of security.



Real Identity Management

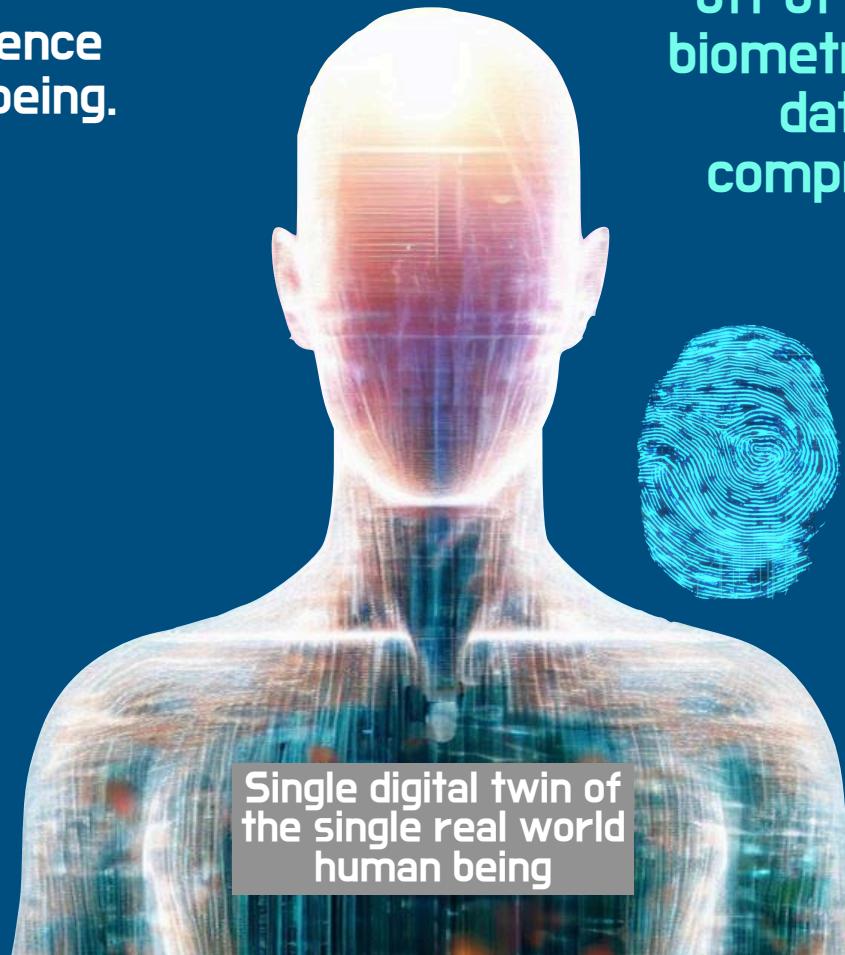


Real Digital Forensics

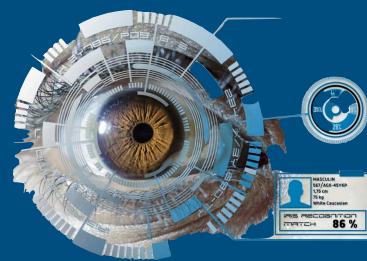


What is an identity?

It is a record proving the existence of a single, real world human being.



All of the data given off of the body, from biometrics to sensory data to forensics, comprise a person's real identity.



What are forensics?



Forensics are methods that combine science & law to produce evidentiary proof of human activities. They can be used to prevent crimes like fraud or civil abuses, in addition to submitting them for court decisions after crimes have already been committed.

Digital forensics are methods that provide an audit trail of human activities across devices that can prevent crimes or prove them ipso facto.



Why do forensics & identities matter?

Nearly 70% of all identities are fakes, whether they originate online or offline, leading to tens of trillions of dollars in losses every year.



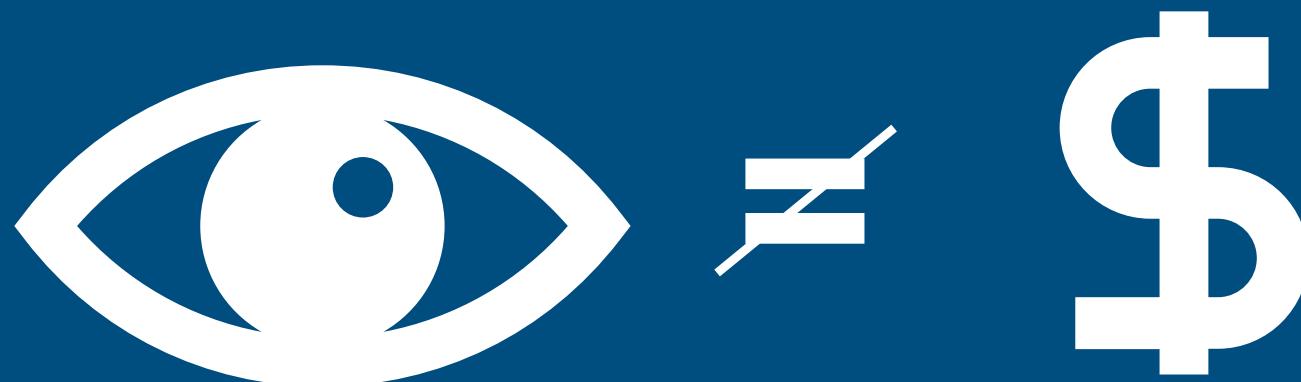
“Selfies” which use artificial intelligence are the worst contributor of identity theft!

We give real digital identities back to the individual with full forensics, thereby enabling them to own their data, monetize & manage it.



Why aren't they a digital standard?

Because corporations, institutions & governments still believe that it is more profitable to implement protocols for greater & greater control of economic activities without using forensic identities (a DAL Identity). **when the exact opposite is the case.**



How would the standard change?



So then what is Web 4.0?

It is a transformative technology paradigm that shifts the economic focus from standalone manufactured products to specialized microservices designed to meet specific economic needs.

Standalone Products



Needs-Based
Microservices



So then what does Web 4.0 actually do?

Web 4.0 bridges the currently separated worlds of The Web, The Metaverse and "Real World Things" so that people can envision & actualize newer, better realities.



WORLDWIDE WEB



METAVERSES



THE REAL WORLD



What functions characterize Web 4.0?

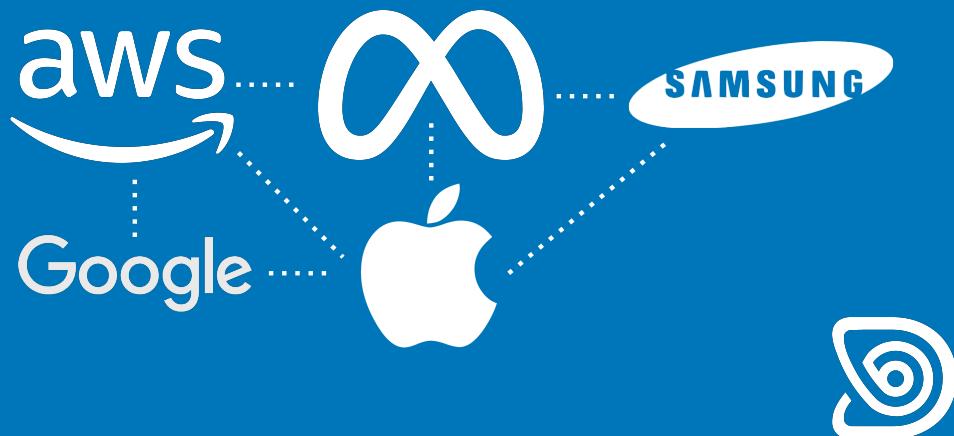
Like "Real World Things" you can grab, drag, drop, and use them in different contexts. You can grab them:

- with your hand
- your finger
- your mouse
- your VR-Controller

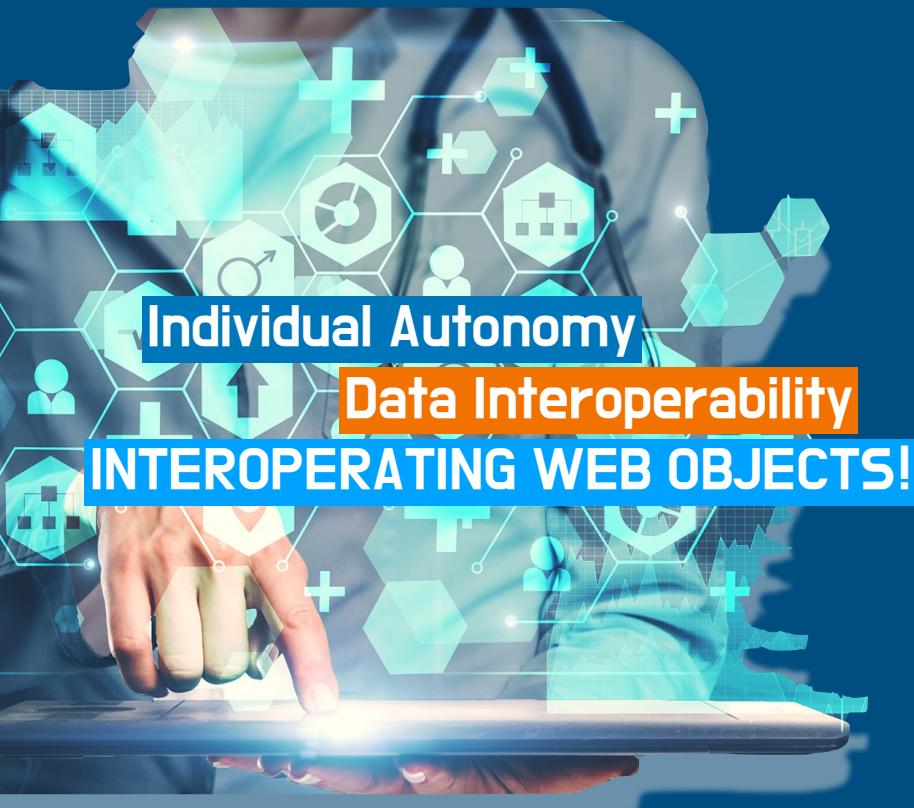


And move them in:

- between different Web Sites on different Web Domains.
- between different devices like Desktops, iPads, Phones, and VR/AR Glasses
- between different operating system technologies like Mac OS, android, iOS, Windows, Linux, Unix, ...
- between different vendors like Apple, Google, Samsung, Facebook/Meta, Amazon, Microsoft



What features characterize Web 4.0?



In Web 4.0, individuals can autonomously use or offer **microservices** without relying on third-party dependencies such as eCommerce providers (Amazon), search engines (Google), application providers (Apple), social networks (Facebook), or financial institutions (traditional banks or FinTech/Defi platforms).

This shift places greater control in the hands of individuals and at incredible scale because they have interoperability at the data level.



In other words...

Imagine that everybody has a self-driving car and building blocks they can use without an "authority" (3rd party) telling them what to do, or how to do it.

The cars and the building blocks are virtual simulations of you. They have all the necessary information they need to function & perform.

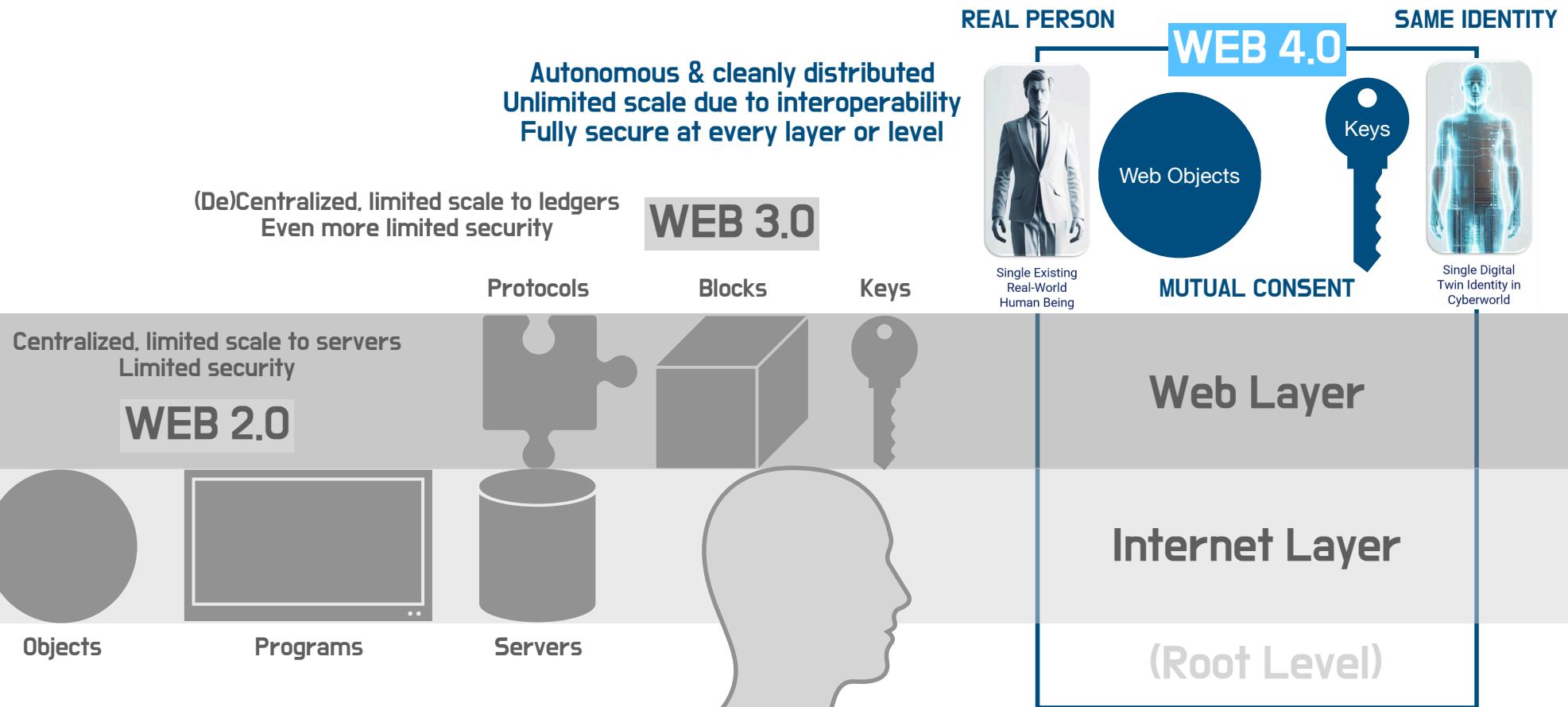
These functions become microservices that are performed between you & your peers. You both own the data, the services & the products you create together.

WELCOME TO WEB 4.0!



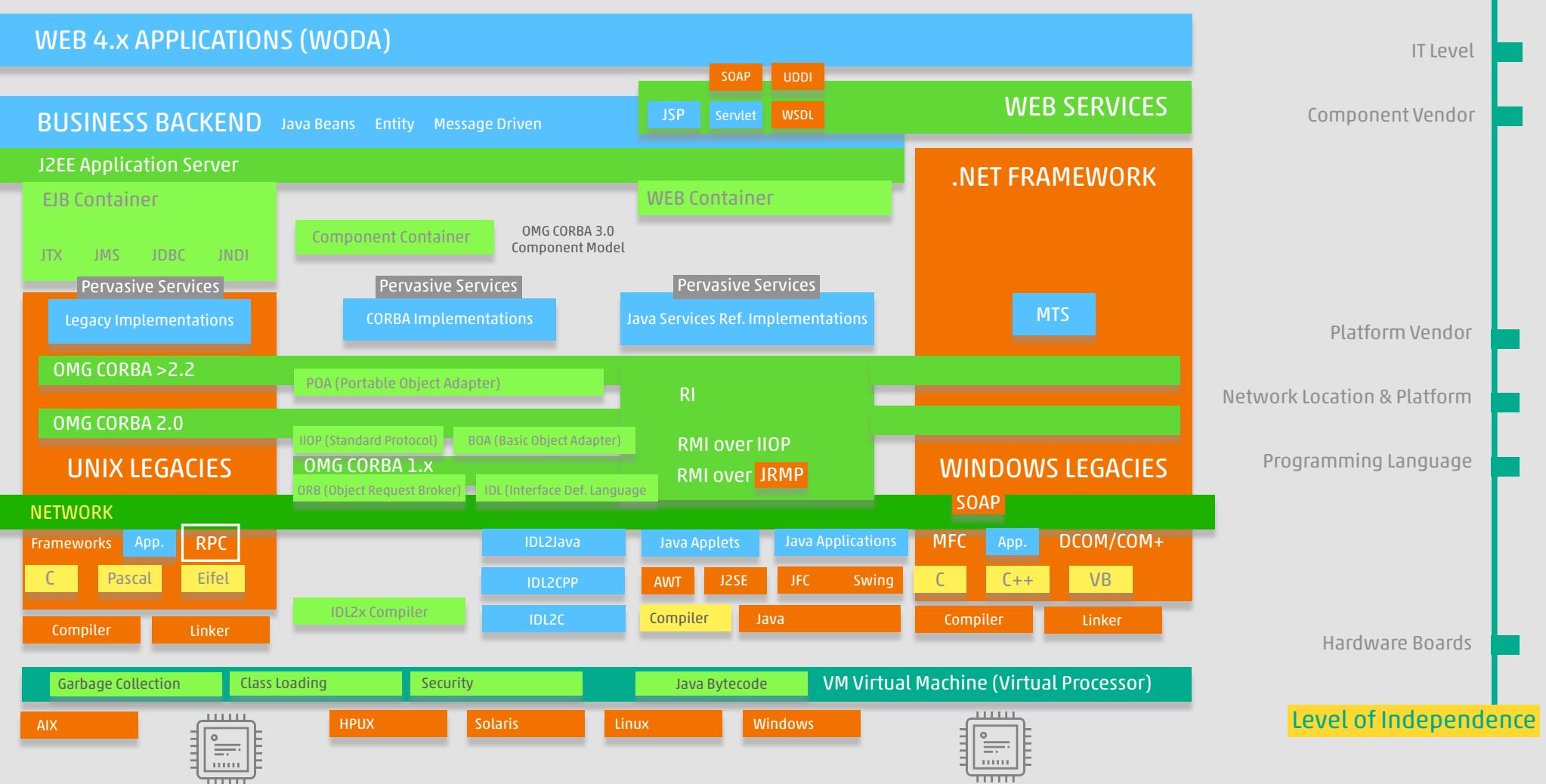
(LIVE DEMO RUNS HERE)

THE BASICS OF WEB 4.0 INFRASTRUCTURE & IDENTITY

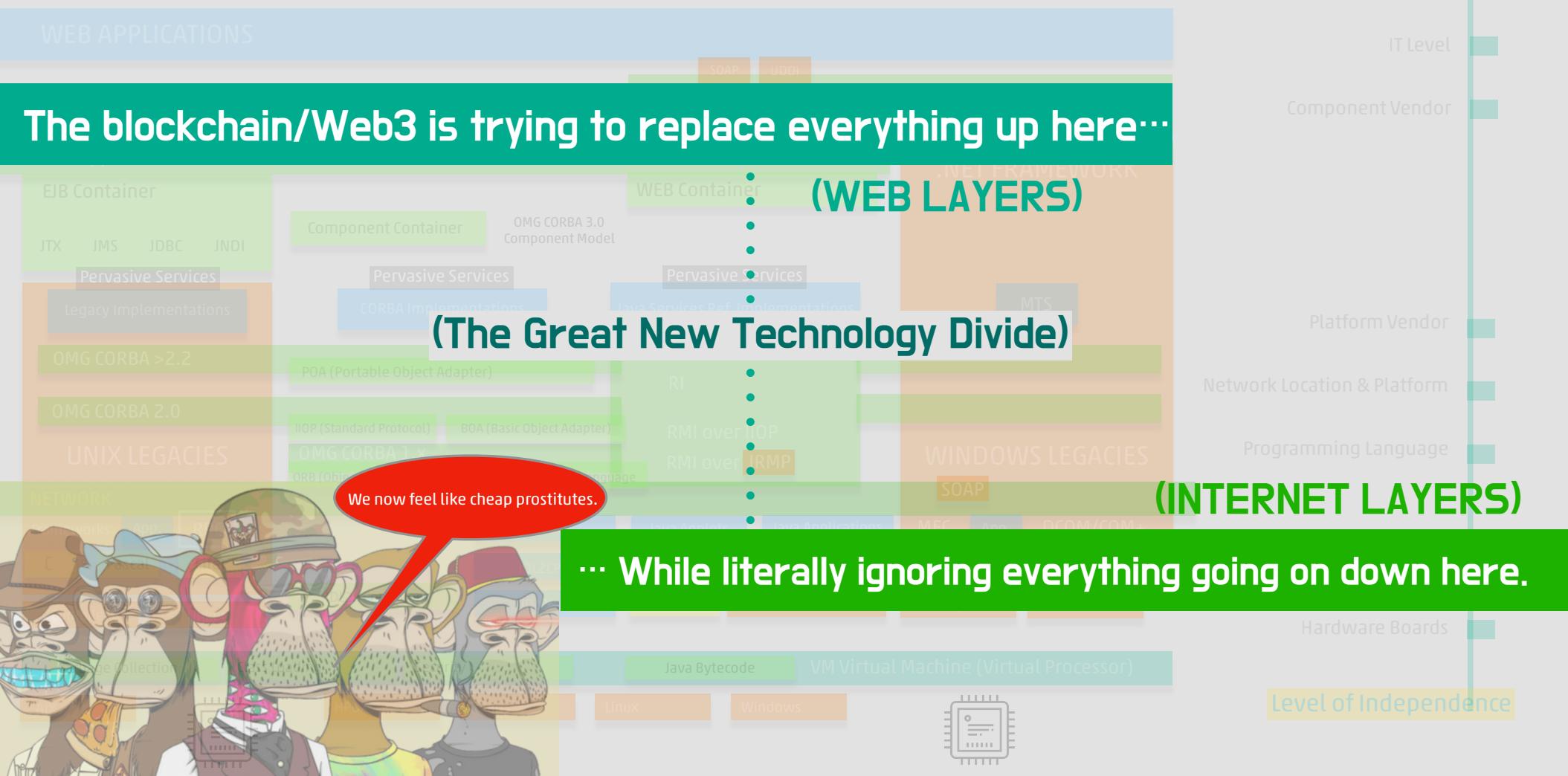


Web 2.0/Web 3.0 identities owned & managed by 3rd parties driving AI-generated synthetics or fakes

How technology infrastructure actually stacks up on the InterWebs.



How technology infrastructure actually stacks up on the InterWebs.



The web security problem, simplified.



Web protocols make the web
more & more insecure!

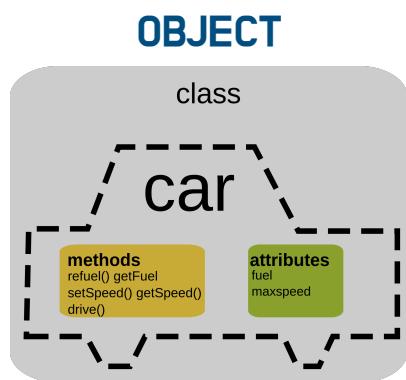


Web objects without protocols
make the web totally secure!



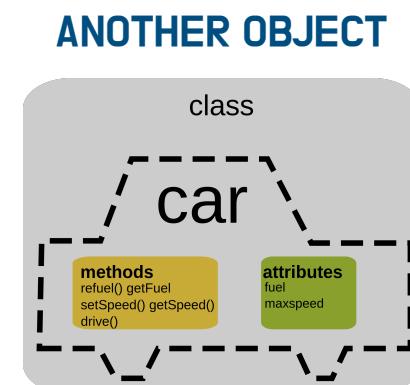
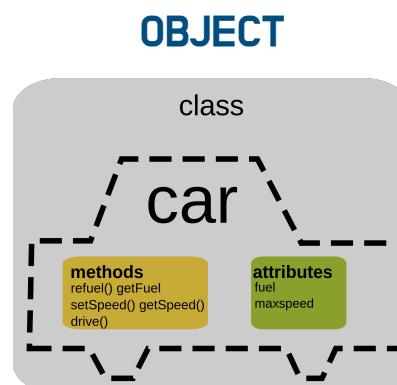
WEB PROTOCOLS VS. OBJECT-ORIENTED PROGRAMMING

Web Protocols



An object with accurate information is forced to make requests via protocols to share its data with different devices & databases along the web, thereby leaving it open to attack.

Object Orientation



Objects with accurate information request to share their data directly without any need for protocols, and if structured properly, leave no attack vectors open with that request.



TOTALLY UNNECESSARY!

The maze
of useless
& often
prohibitively
expensive
Web
Protocols

(This is
literally
Web 2.0 &
Web 3.0!)

- Provides standardized services such as virtual terminal, file and job transfer and operation

7

Layer 6: Presentation Layer

- Masks the differences of data formats between dissimilar systems
- Specifies architecture-independent data transfer format
- Encodes and decodes data; Encrypts and decrypts data; Compresses and decompresses data

6

Layer 5: Session Layer

- Manages user sessions and dialogues
- Controls establishment and termination of logical links between users
- Reports upper layer errors

5

Layer 4: Transport Layer

- Manages end-to-end message delivery in network
- Provides reliable and sequential packet delivery through error recovery and flow control mechanisms
- Provides connectionless oriented packet delivery

4

Layer 3: Network Layer

- Determines how data are transferred among network devices
- Routes packets according to unique network addresses
- Provides flow and congestion control to prevent network resource depletion

3

Layer 2: Data Link Layer

- Defines procedures for operating the communication link
- Provides framing and sequencing
- Detects and corrects received frame errors

2

Layer 1: Physical Layer

- Defines physical means of sending data over network devices
- Interfaces between network medium and devices
- Defines optical, electrical and mechanical characteristics

1

ANSI
American National Standards Institute
25 west 43rd Street, 4th FL
New York NY 10001 USA
Tel: 212-642-4000
www.ansi.org

ETSI
European Telecommunications Standards Institute
655 Route des Lucches
91190 Sophia Antipolis Cedex, France
Tel: 33 (0)4 92 94 42 00
www.etsi.org

FCC
Federal Communications Commission
445 12th Street SW
Washington DC 20584 USA
Tel: 888-225-5322
www.fcc.gov

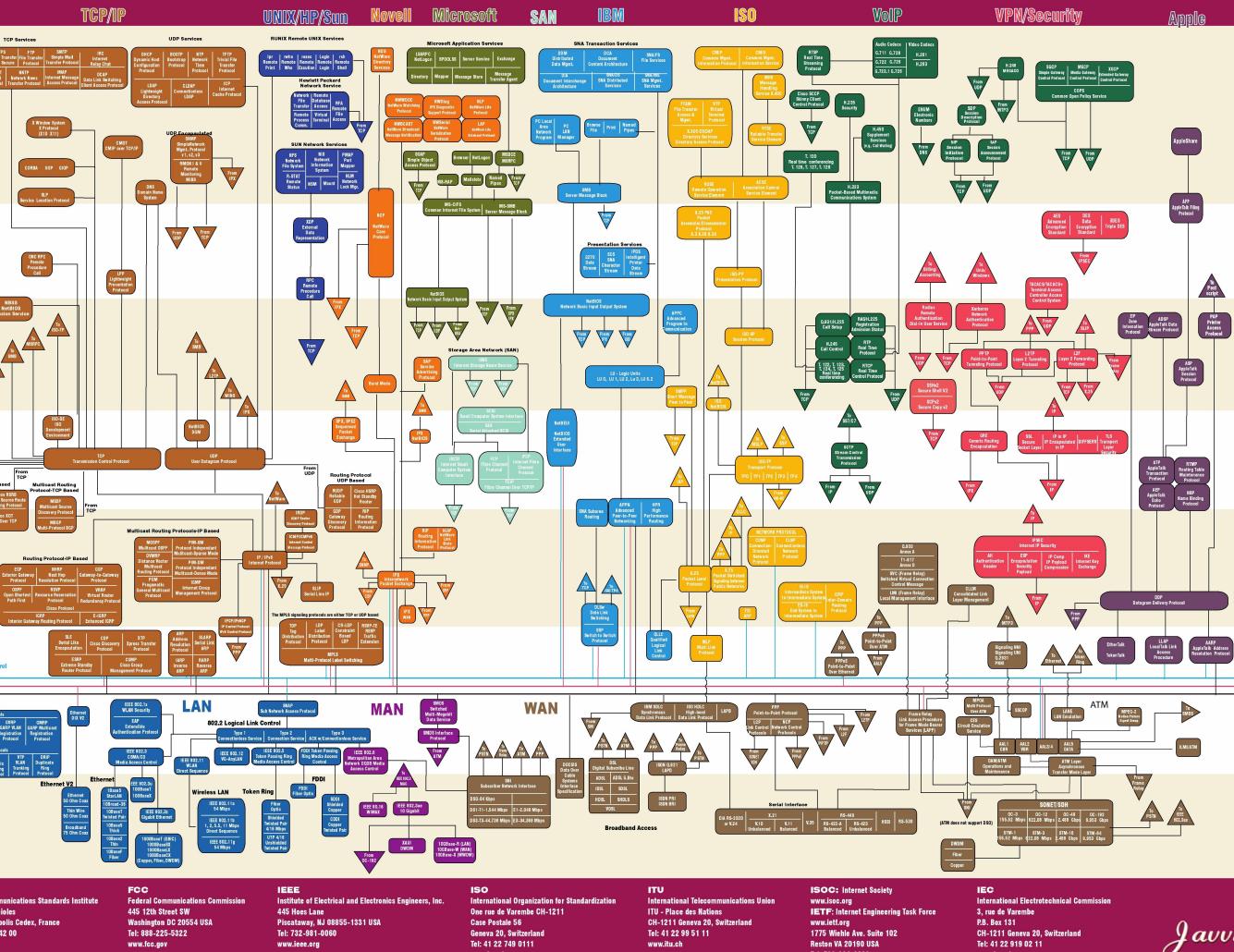
IEEE
Institute of Electrical and Electronics Engineers, Inc.
445 Hoes Lane
Piscataway NJ 08855-1331 USA
Tel: 732-981-0800
www.ieee.org

ISO
International Organization for Standardization
1, rue Maurice de Wailly CH-1211
Case Postale 56
Geneva 20, Switzerland
Tel: 41 22 749 0111
www.iso.ch

ITU
International Telecommunications Union
100, Avenue des Nations
CH-1211 Geneva 20, Switzerland
Tel: 41 22 99 51 11
www.itu.ch

ISOC: Internet Society
www.isoc.org
IETF: Internet Engineering Task Force
www.ietf.org
ITU: International Telecommunication Union
100, Avenue des Nations
CH-1211 Geneva 20, Switzerland
Tel: 41 22 99 51 11
www.ietf.org
IEC: International Electrotechnical Commission
2, rue de Varembe
CH-1211 Geneva 20, Switzerland
Tel: 41 22 919 02 11
www.iec.ch

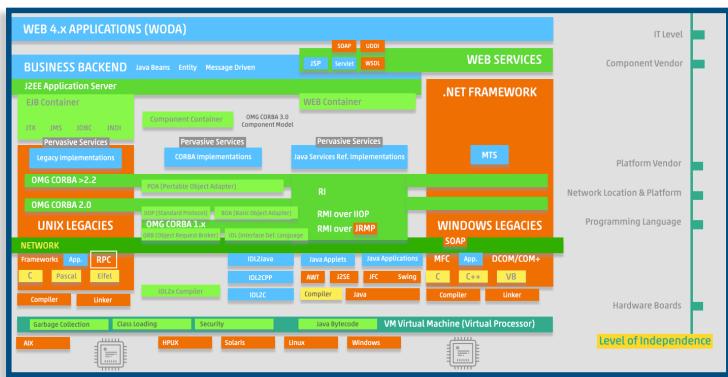
NETWORK COMMUNICATION PROTOCOLS MAP



Javin

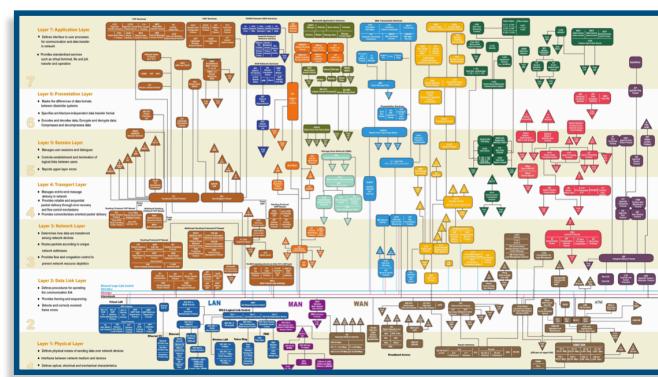
To sum it up:

THE ENTIRE INTERNET

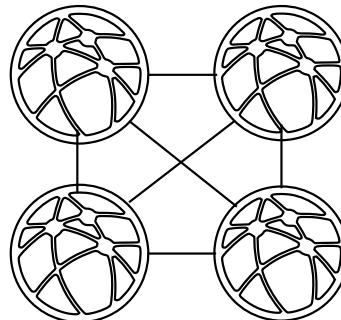


&

THE ENTIRE WEB



**Do not function
properly nor
securely without:**



INTEROPERABLE WEB OBJECTS!



OUR APPLIED SECURITY METHODS

Smart Network Security

Verified Trust between Digital Peers

**NO WEB
PROTOCOLS.
ONLY WEB
OBJECTS!**

The DAL Web 4.0 Platform

**Seamlessly interoperates
with any system on the
planet, connecting any
dataset anywhere**

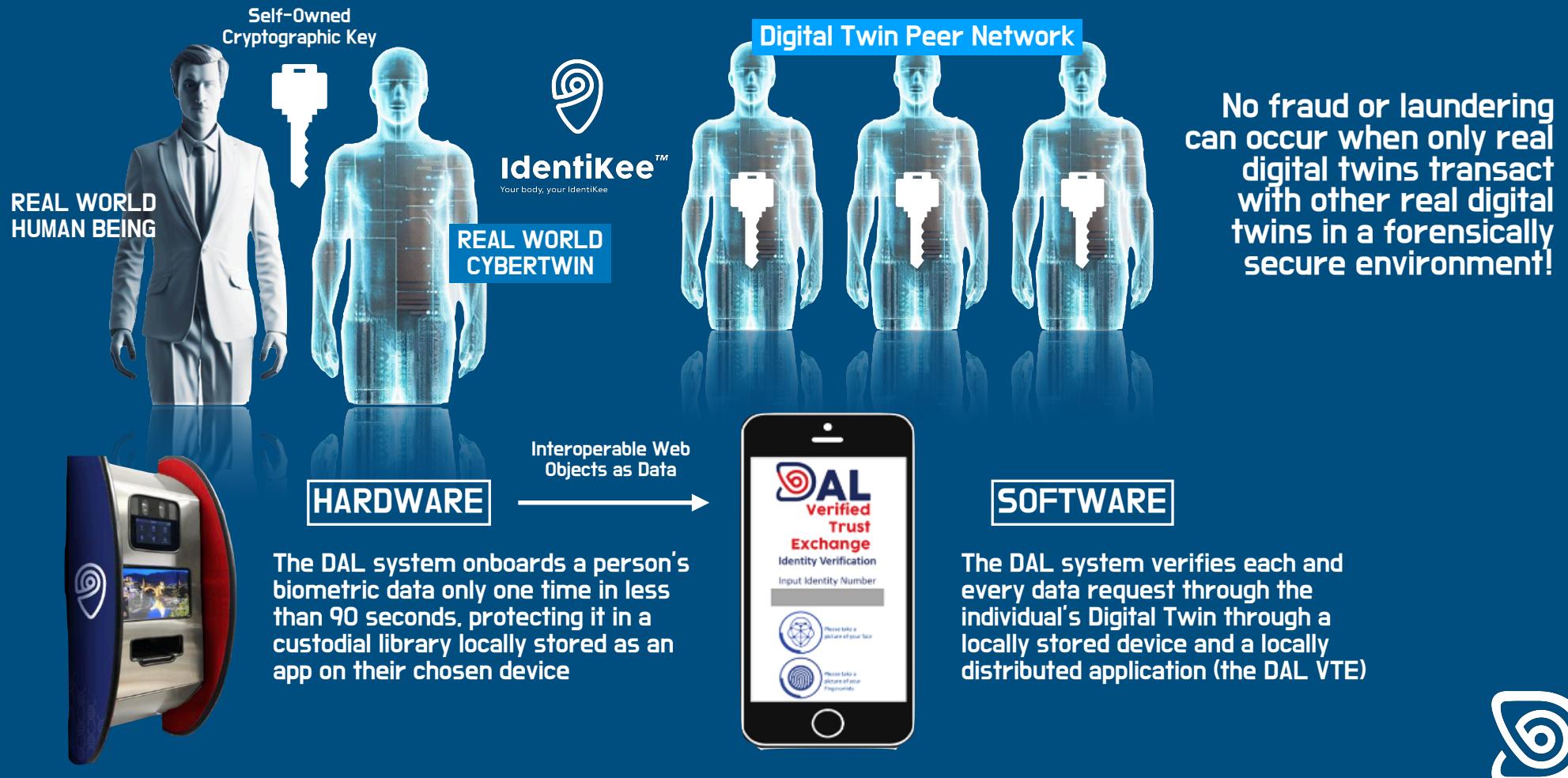
THE DAL IDENTITY

A single digital twin of the single real world human being, which is owned, managed & monetized by that same real human being, transacting with other real world human beings

FULL-SCALE FORENSIC DATACENTER SECURITY!

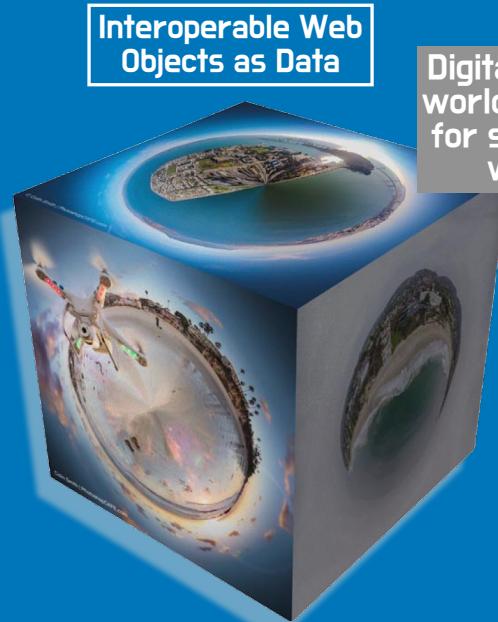


Smart Security (the DAL W4S Standard)



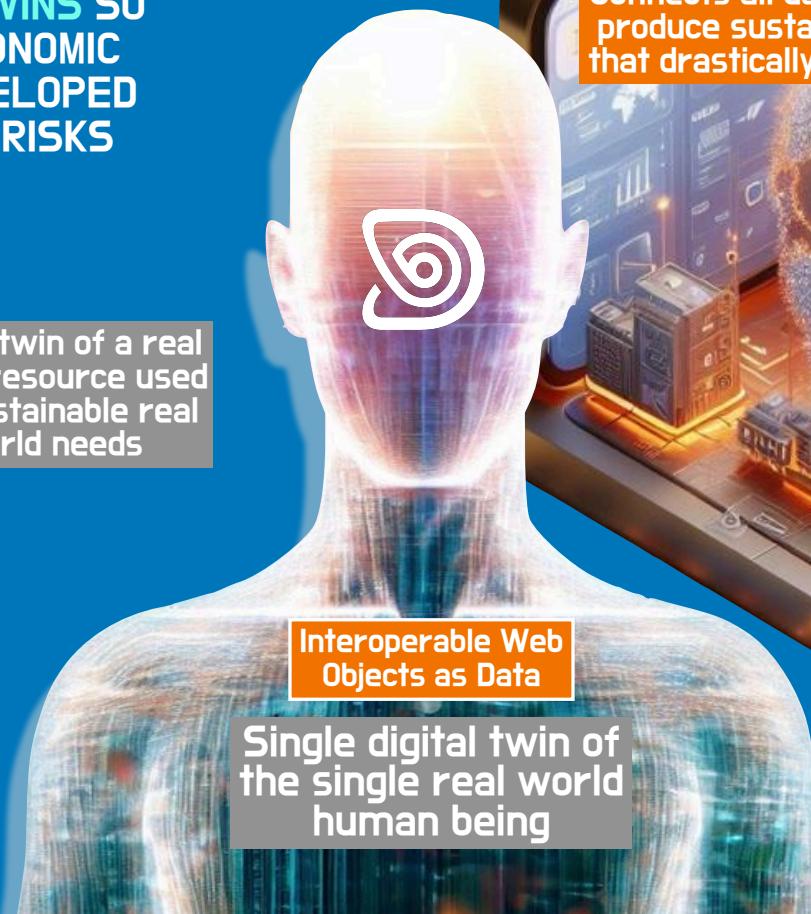
DAL Digital Twin Web4 Security

SIMULATING THE NATURAL WORLD WITH SECURE DIGITAL TWINS SO THAT BETTER SOCIOECONOMIC SCENARIOS CAN BE DEVELOPED WITHOUT TAKING HUGE RISKS



Interoperable Web Objects as Data

Digital twin of a real world resource used for sustainable real world needs



Single digital twin of the single real world human being

The DAL Web 4.0 Platform

Connects all data seamlessly between digital twins to produce sustainable outcomes & predictive analytics that drastically cut costs + create new profit centers.

UXAD CITY MANAGEMENT APP

THE LINE

Interoperable Web Objects as Data

Interoperable Web Objects as Data

Digital twin metaverse used for sustainable planning, development & governance

A collage of images and interfaces illustrating the DAL Web 4.0 Platform. It includes a smartphone displaying a digital twin interface, a large screen showing a 3D city model, a screenshot of a "CITY MANAGEMENT APP" showing "THE LINE" building, and a "UXAD" interface with a sidebar and a main view showing a digital twin of a city. Several callout boxes highlight "Interoperable Web Objects as Data" and "Digital twin metaverse used for sustainable planning, development & governance".

How we generate secure revenue with sustainable impact.

Example: The Mining Sector

STEP 1

Digital twins of mining workers are created to protect mining resources, manage responsible labor practices & implement proper environmental standards

COST-CUTTING



STEP 2

A digital twin METAVERSE of the entire mining operation is created for resource management, operational planning & economic modeling

NEW REVENUE STREAM CREATION

DAL



STEP 3

The DAL Platform connects all the data between the workers, the resources & the assets so that outside partners can transact with full accuracy as well as transparency

RECURRING REVENUE

DAL Platform

Producers + Market Makers



Commodities Exchanges



DAL

Delivery & Storage

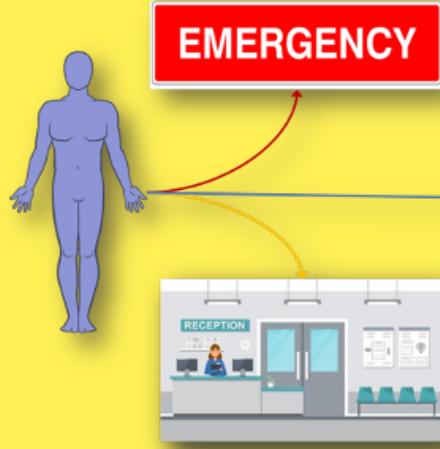


How we generate secure revenue with extreme efficiency.

Example: The Healthcare Sector

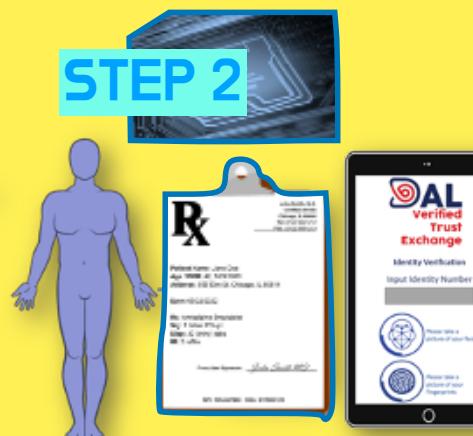
During an emergency room visit or a routine doctor's exam, **the patient uploads their biometric data in less than 90 seconds; that real human being's digital twin owns, manages & monetizes their own health data**, sharing that data with providers as well as insurance underwriters.

STEP 1



EMERGENCY

STEP 2



+ PHARMACY



STEP 3

SHARED DATA REVENUE

Primary

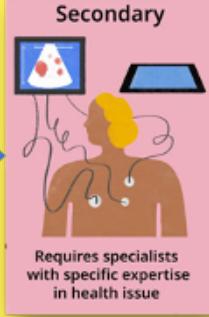
For illness, injury, acute medical problems, and referrals



SHARED DATA REVENUE

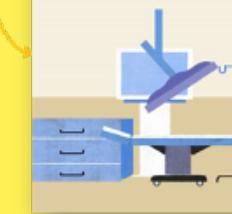
Secondary

Requires specialists with specific expertise in health issue



Tertiary

Requires highly specialized equipment and expertise

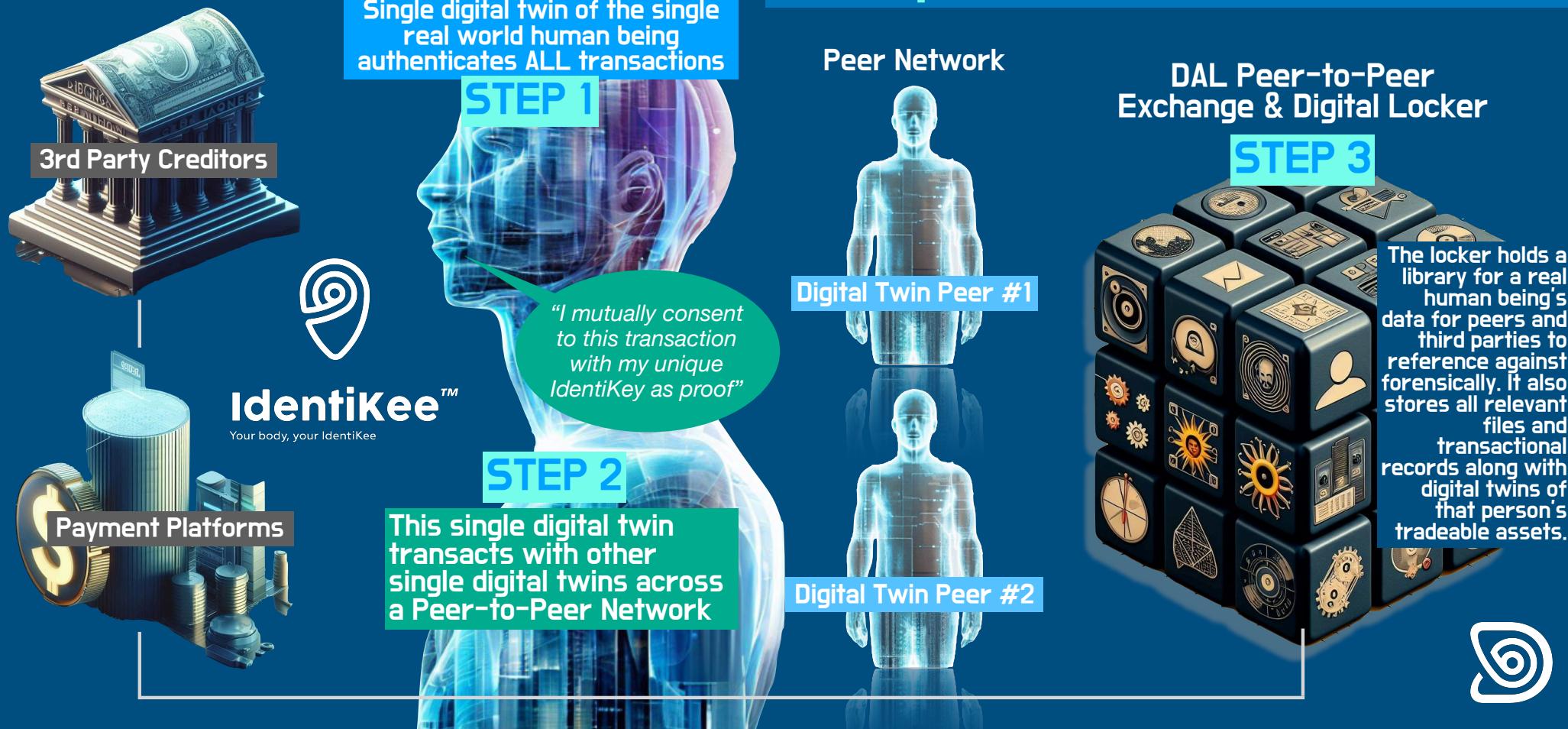


SHARED DATA REVENUE



How we generate secure revenue with positive peer impact.

Example: The Finance Sector



Asset-based tokenization.

1 Identity Token issued to the Person only Once



Personal Web Token

a Mutual Credit Token issued to
counterparties any number of times

UNIT OF ACCOUNT (Token version issued as a mutual credit)

Per request & mutual consent

a Cryptographic Key accompanying each issued Mutual Credit Token



Issued with each unit



Secure token liquidation.



Data Requests



Healthcare Counterparty

Energy Counterparty

Agriculture Counterparty

Education Counterparty

Underlying architecture acts as the ledger + payment rail



Per request & mutual consent
Sharing of personal + commercial or civic data

wCBDC

CBDC

National Sovereign

Crypto

Remittances



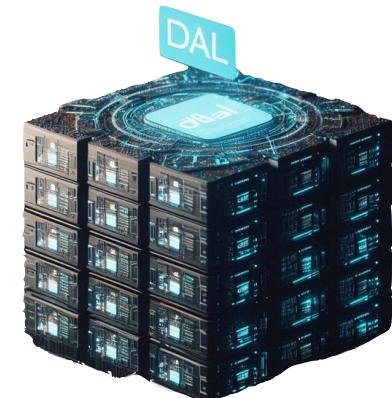
The Now Fully Secure Mercantile Ecosystem



Producers + Market Makers



Commodities Exchanges



Delivery & Storage



Connects all
real, physical
market data



Smart Assets

Makes all assets
interoperable &
transactional

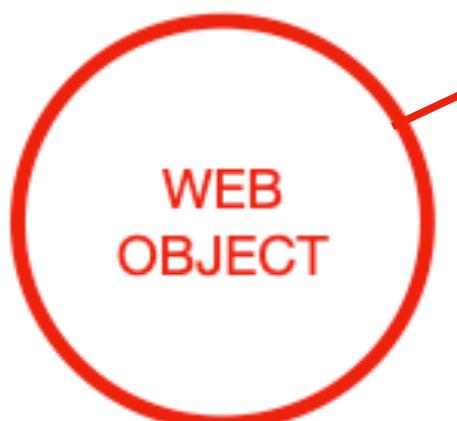
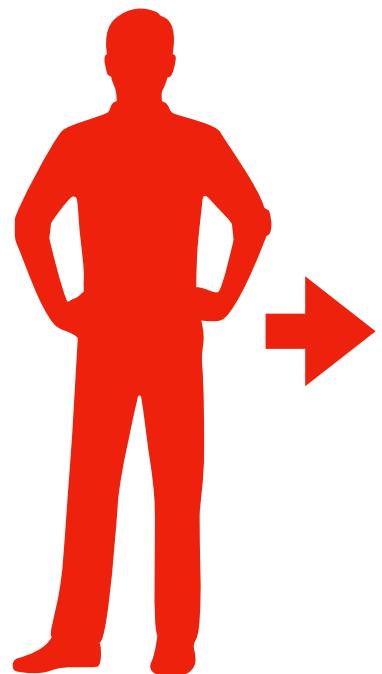


OBJECT-ORIENTED FORENSICS



BASIC METHODOLOGY

**Whole Person
& Their
Consensual
Bodily Data
(Biometrics)**



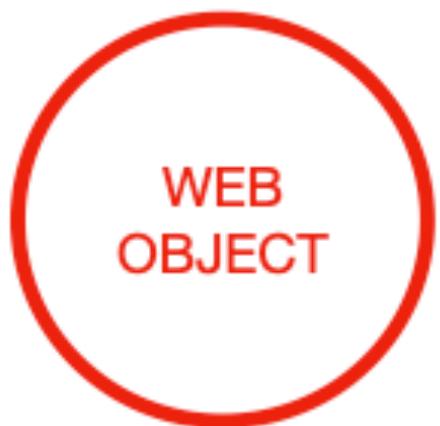
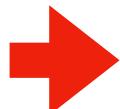
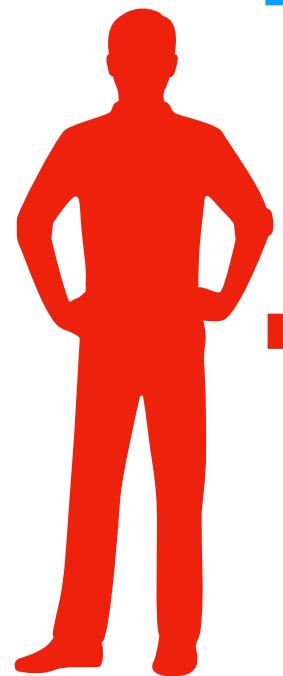
**Referencable
Object & Secure
Pre-Encrypted
Hashing**



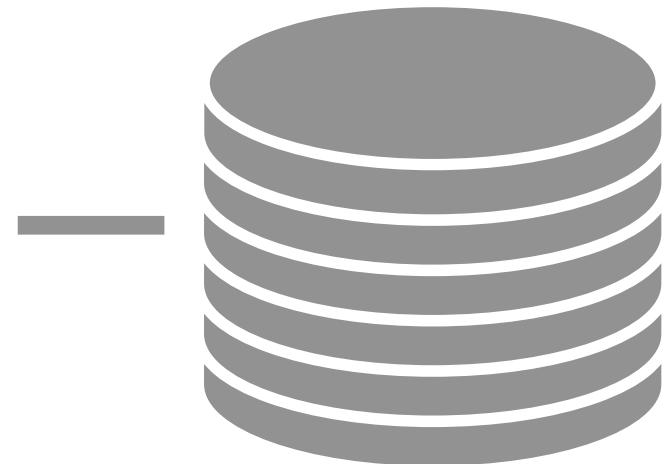
SUCCESSION REQUIREMENTS

Succession: Where the object goes (i.e. data) so goes the operating software along with it!

**Whole Person &
Their
Consensual
Bodily Data
(Biometrics)**



Which operates on...

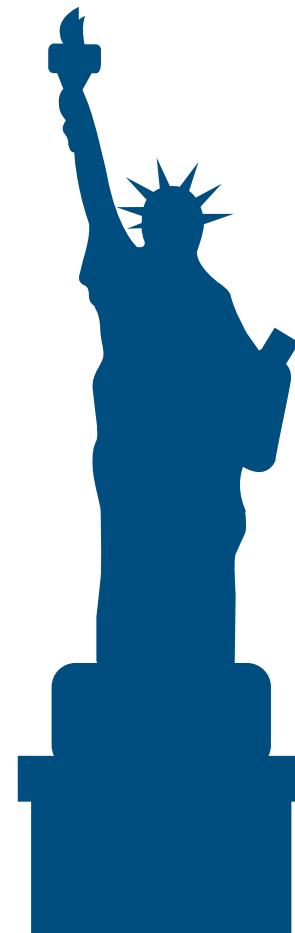
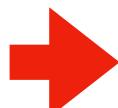
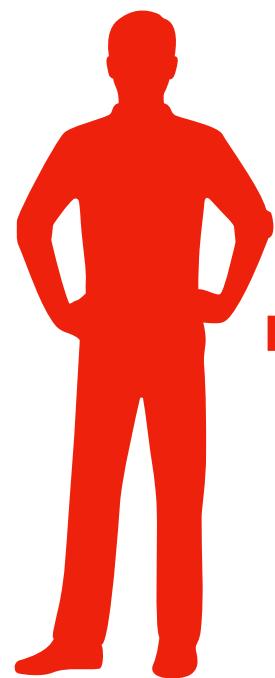


...An underlying interoperating
system (Web 4.0 reference
implementation architecture)



SUCCESS IN PERSONAL AUTONOMY!

Whole Person &
Their
Consensual
Bodily Data
(Biometrics)

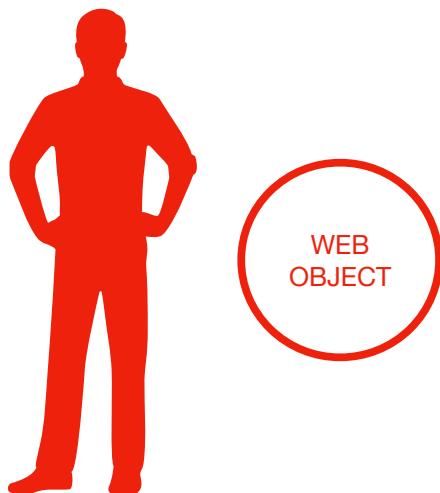


Freedom to
express one's
true self
without 3rd
party
interference



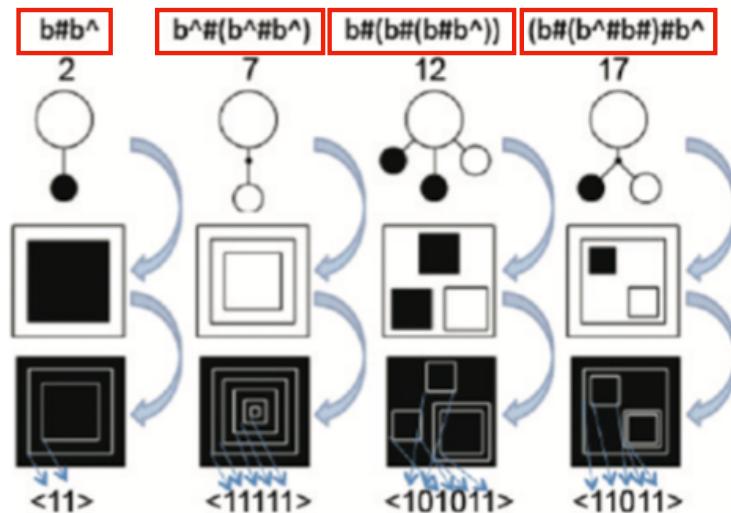
WEB 4.0 REFERENCE METHODOLOGY

Personally Owned Digital Twin



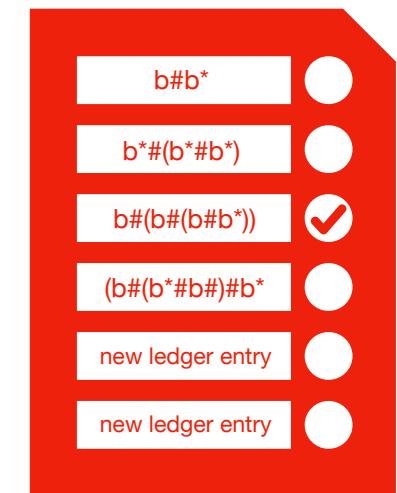
One, uniquely owned instance of you

Referencable Instanced Hashes of Pii + Metadata



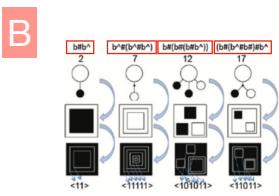
Unique hashes representing one use for every instance/request

Authenticated Personal Library



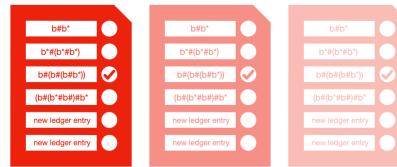
Cryptographic hashes referenced & ledgered

THE FUNDAMENTALS OF DAL'S FORENSIC CRYPTOGRAPHY



Corresponding hashes are indexed into the DAL reference library owned by the individual

C



The library has any number of public versions or instances per the data request

D



If the data request is authenticated (self-referenced) then the data move freely & securely

E

b#b^ 2 b^#(b^#b^) 7 b#(b#(b#b^)) 12 (b#(b^#b^))#b^ 17

If the data request is not authenticated, then only the hashes are referenced



The forensic trail leads back to the source, and to wherever the source data go, with each step (re)authenticated



b#b^ 2 b^#(b^#b^) 7 b#(b#(b#b^)) 12 (b#(b^#b^))#b^ 17

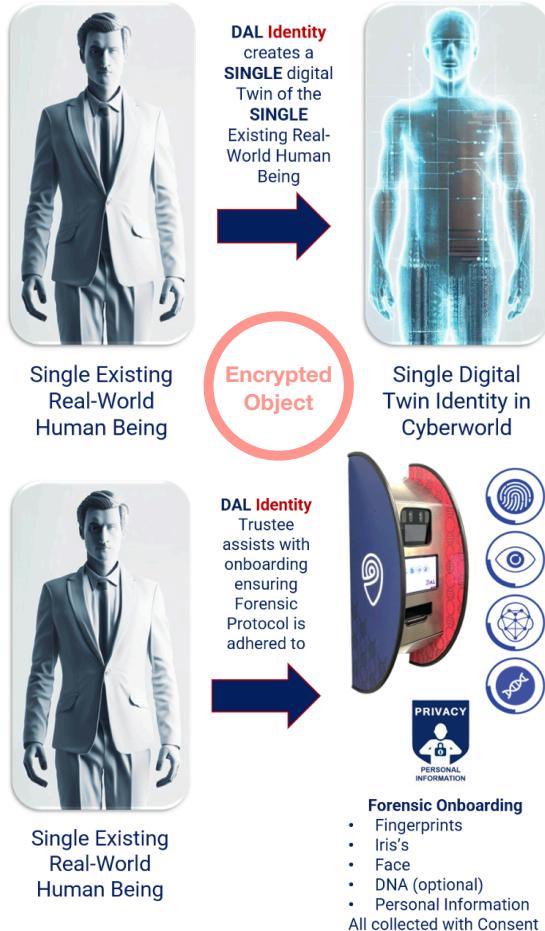
The corresponding hashes matched to the underlying data are paired back to the source

A complete, ongoing forensic audit, preserving all data integrity & the individual's identity

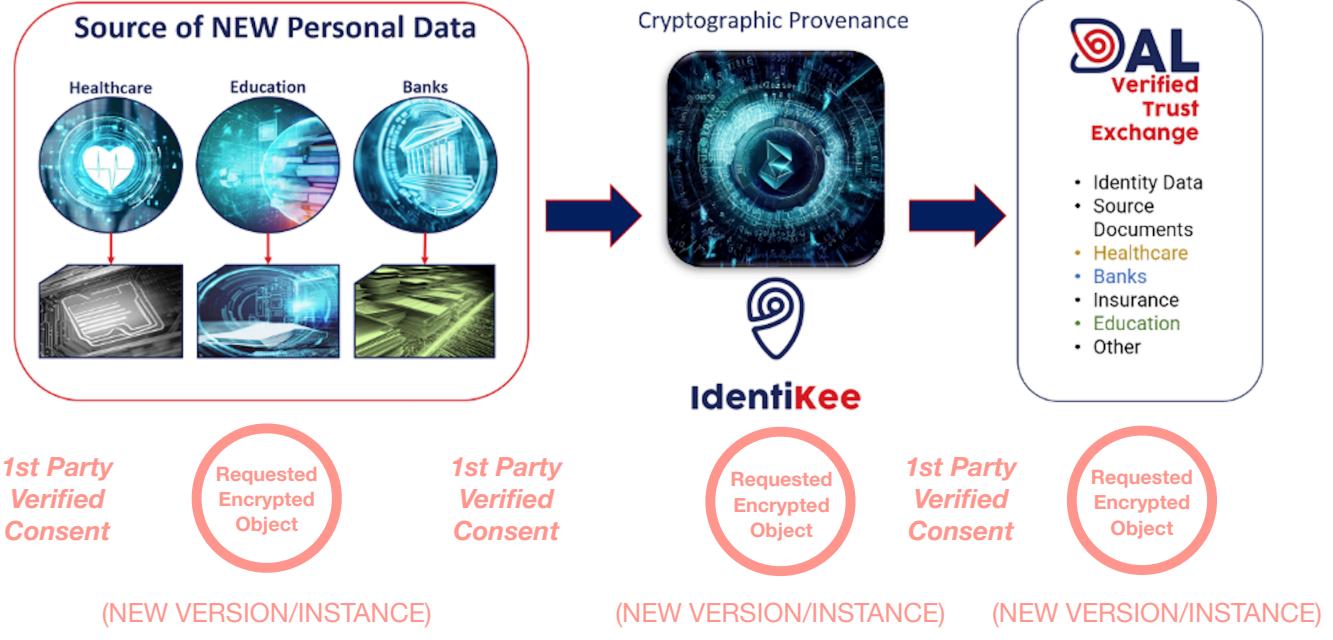


AUTONOMOUS SECURITY IN THE DAL IDENTITY SYSTEM

WHOLE PERSON



WHOLE SYSTEM



A whole person supported by a whole system with each part protected & therefore invulnerable as a whole!



THE TRUTH ON MATH + LANGUAGE

(Why crypto is mostly an insecure scam
& “the blockchain” is mostly hype.)

THE BITCOIN MATH PROBLEM

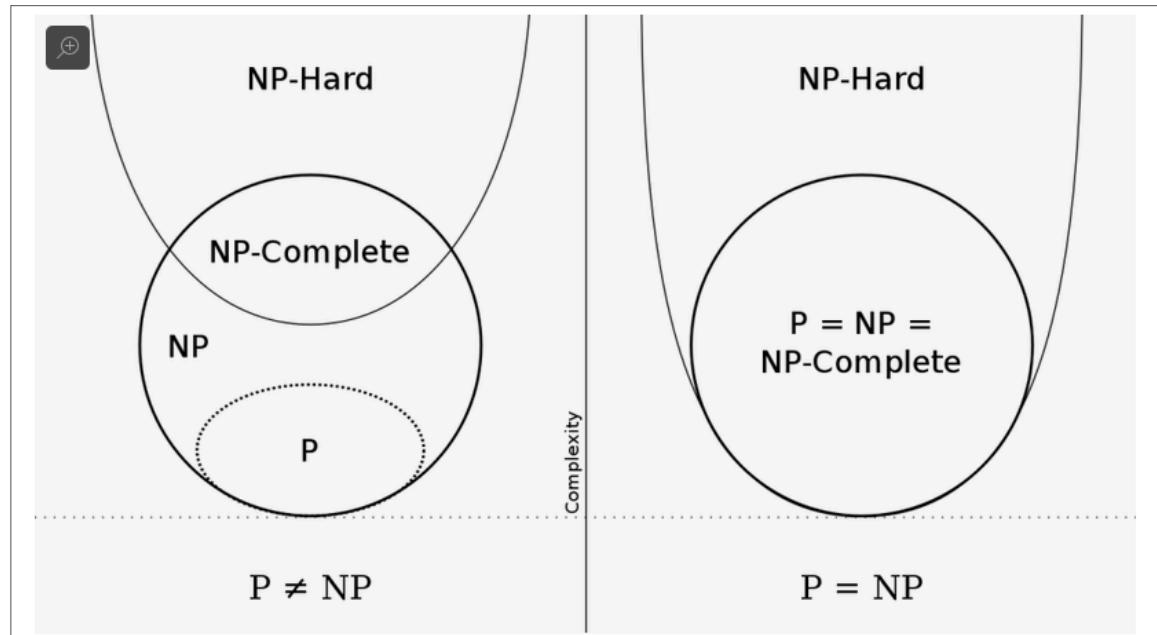
This math problem is an NP problem of "non-deterministic polynomial time".

So, the postulate is that if a problem is solvable in N squared time, and you double the size of the input, then the amount of time it would take to solve it would go up by 4.

This is based on linear factorization which establishes that P = NP for all values of P where N = 1.

This also means that for any numerical value that is dependent on P where N = 1, the answer could be 4, 7, 17 or 42, based on the coefficient of N squared.

Linearly, any 2 numbers at 2^{256} bits have no limit — it simply does not exist. Therefore, you can't actually store them and you can't actually multiply them while proving their physical value. This is why no one has been able to solve the NP problem using linear factorization.



A diagram showing the relevant complexity classes in the P vs NP problem. "P" problems are solvable in polynomial time; "NP" problems might be solvable in polynomial time, and are checkable in polynomial time. "NP-complete" problems are NP problems such that finding a solution to them would let you solve every NP problem. "NP hard" problems are problems at least as complex as the NP-complete problems. Phew.
Graphic: Behnam Esfahbod ([Wikimedia Commons](#))



SUPER PRIME FACTORING (Non-Linear Factorization)

(starting point to get to root prime values or "super primes")

Using math to hack/bypass standard cryptography in a Bitcoin blockchain. The very same approach can be used to bypass or override PQC standards.

2^{511.5}

(number of linear operations required in a preimage or "meet in the middle" attack on SHA-256)

511 is a deficient number - a **natural number** that is strictly larger than the sum of its proper divisors

$$7 \times 73$$

$$511^2$$

(natural ordered pairing)

$$1, 7, 73, 511$$

$$261 \ 121$$

(non-linear prime factors as pairs)

$$1 + 7 + 73 = 81 \quad 2555 = 511 \times 5$$

511 is a multiple of itself, therefore it is relatively easy in terms of computable time to get to zero



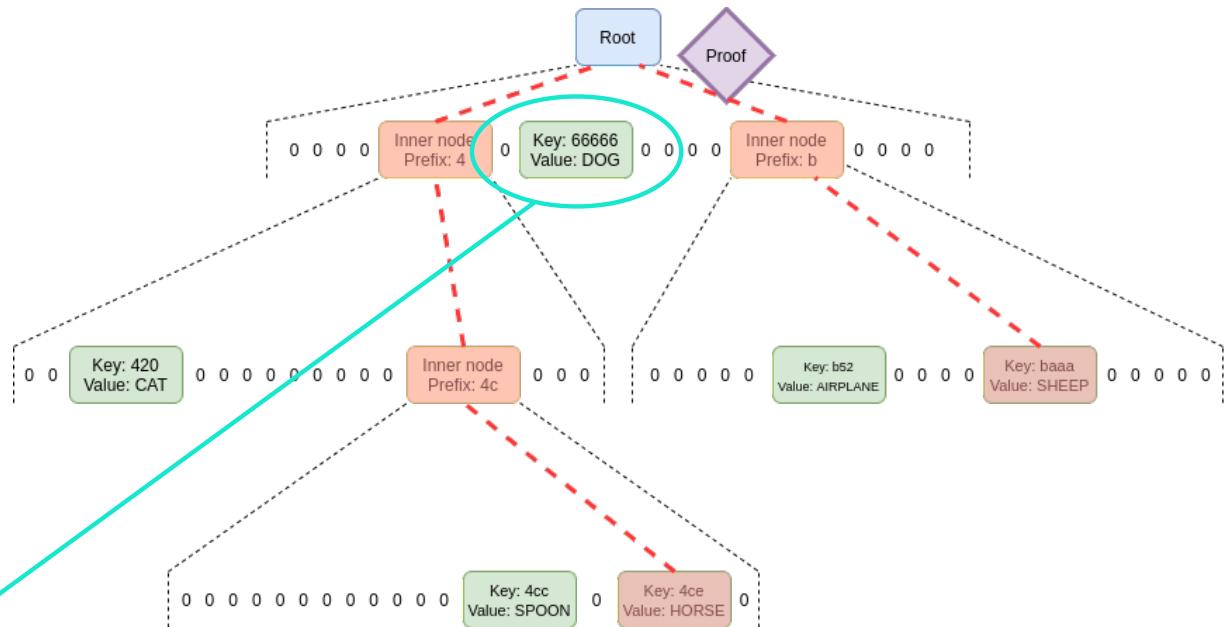
**(We just showed you one of many
ways to hack the Bitcoin blockchain…)**

THE ETHEREUM TREE PROBLEM

Q: What is the “next best key” that is greater than 0, but less than infinity?

(A: If you can't answer this question, that's because it can't be answered without reframing the underlying math.)

A “Verkle Tree”

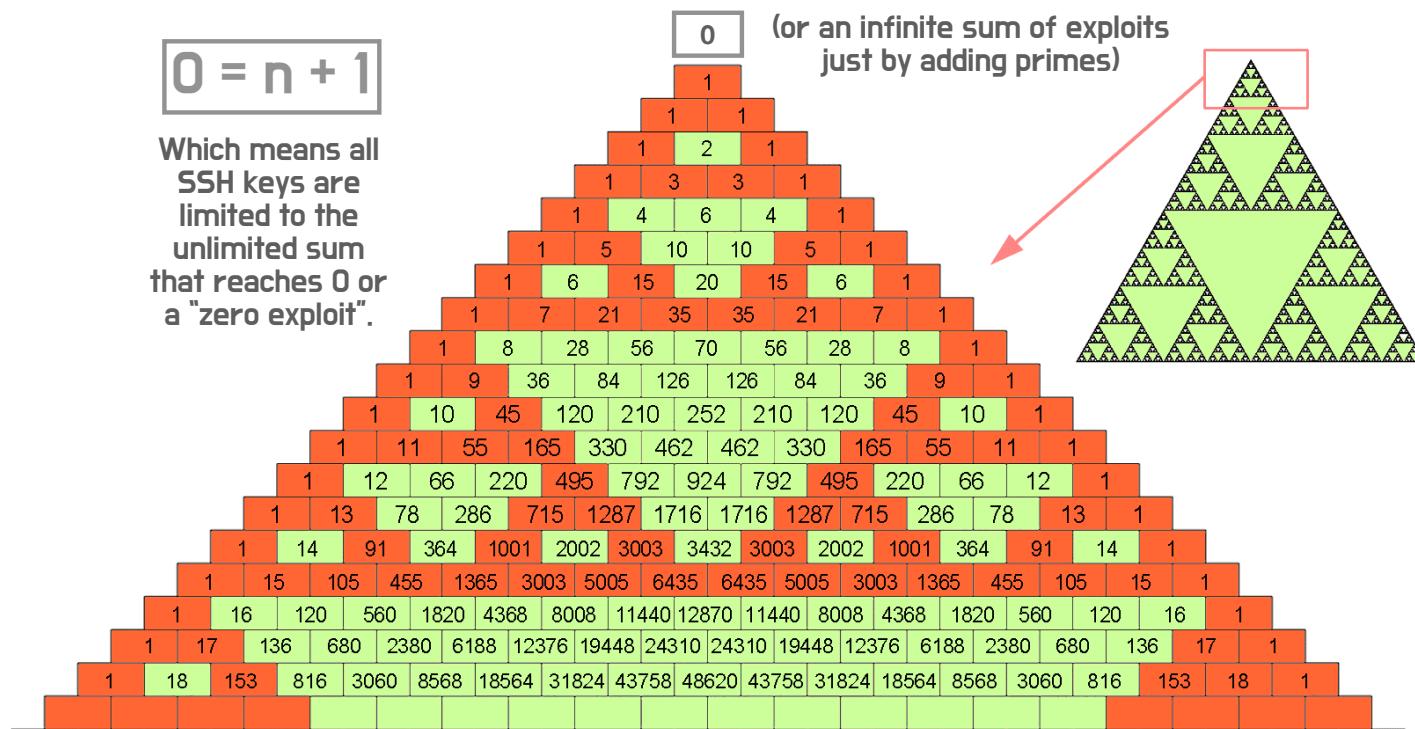


HINT: Pythagoras would round out Pi to the next nearest super prime...



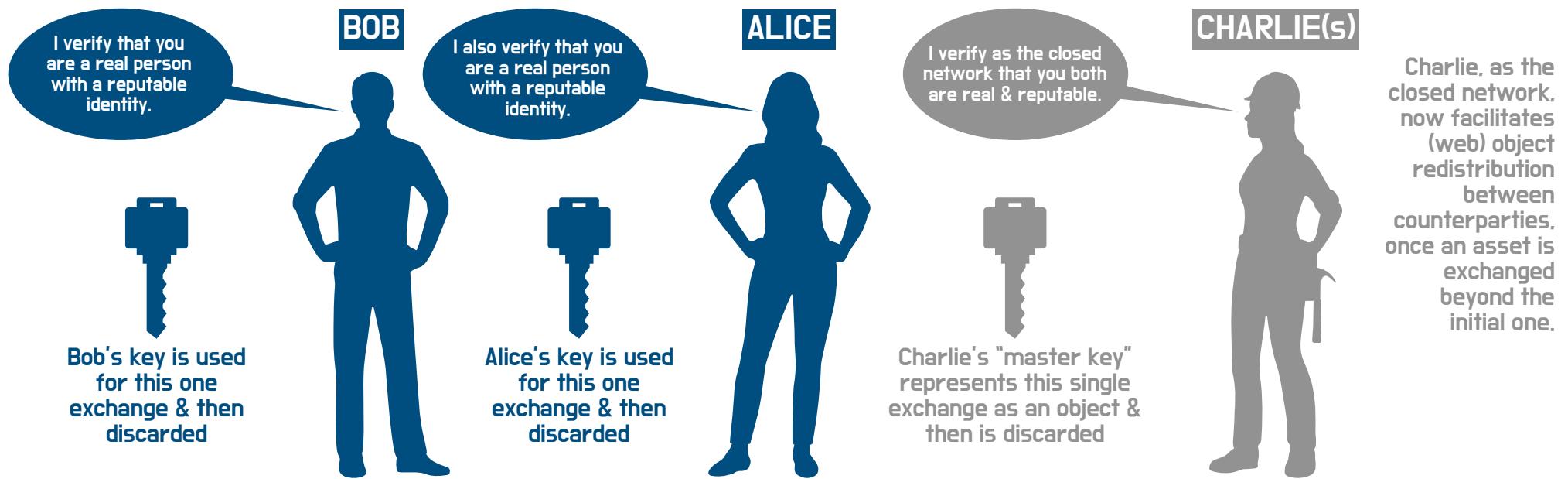
No. BTC is not any better than "any other crypto".

ALL cryptocurrencies employ a combination of Pascal's Triangle & the Sierpinski triangle — tree-origin, fractal-based Pyramid schemes!



Traditional PGP security.

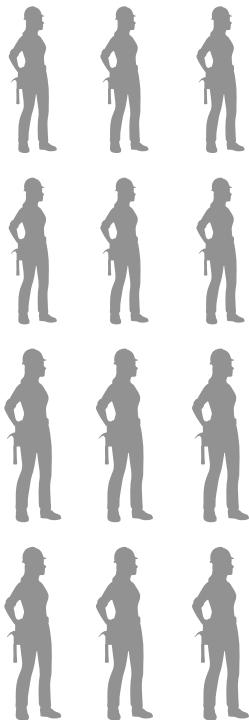
"Charlies" that are cast out which don't support actual, real trust between peers or counterparties.



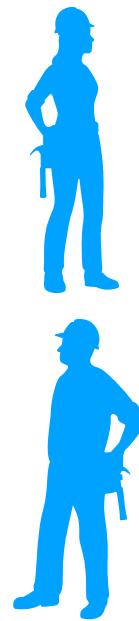
Trustless trust.

Keyless object pairings (without trust seals) that support actual, real trust between peers or counterparties.

A bunch of untrusted Charlies, in an open network which all have the potential of acting on behalf of Bob and Alice, but are still required to generate a key to access an asset for a trans-action.



Charlies search for a "master key" representing this single exchange as an object & then find it!



Two Charlies become a trusted Bob and a trusted Alice with a "master key"!

ACCESS

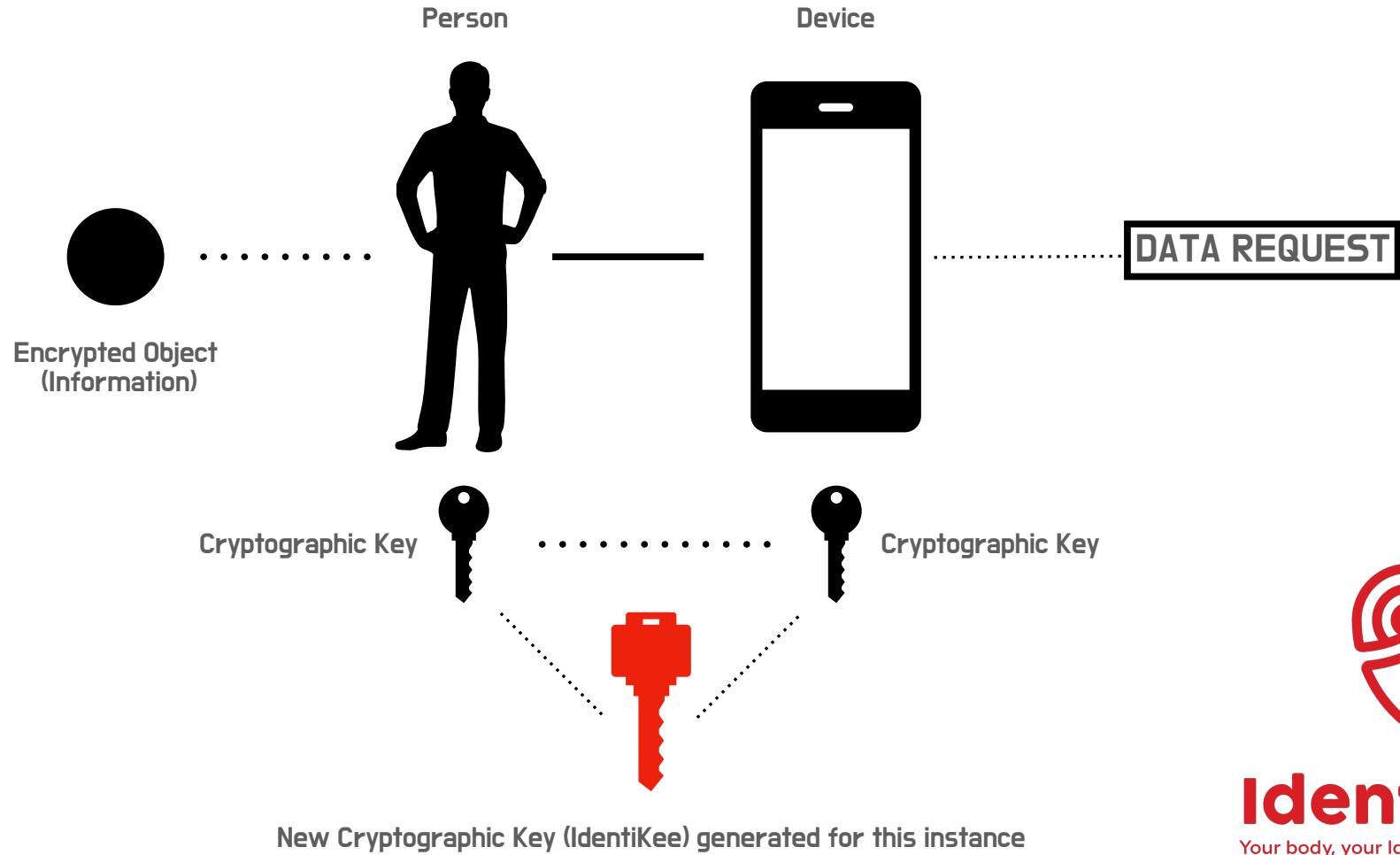
asset metadata as web object

asset metadata as web object

TRANS-ACTION

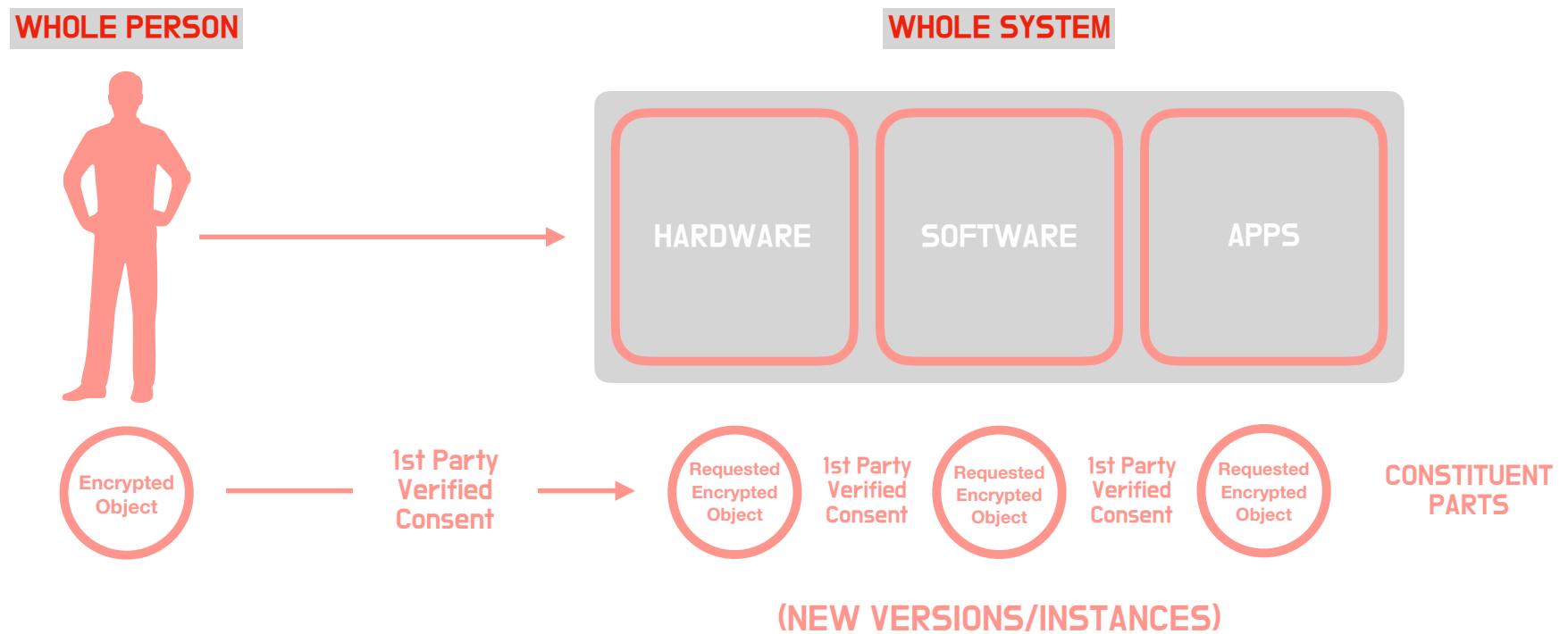


THE BASICS OF "TRUSTLESS TRUST" REUSABLE IDENTITY



Identikit™
Your body, your Identikit

AUTONOMOUS SECURITY IN A REUSABLE IDENTITY SYSTEM



A whole person supported by a whole system with each part protected & therefore invulnerable as a whole!



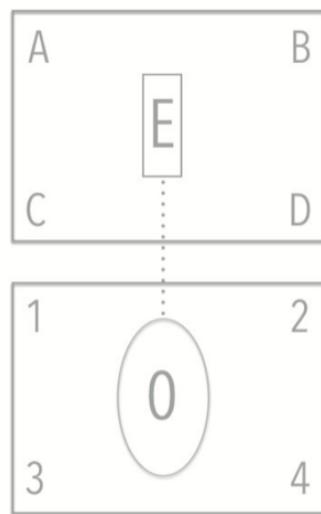
INTELLIGENCE IS NOT ARTIFICIAL

It is either real or it is fake. Period.

Small is much better than large.

OUR SMALL LANGUAGE MODELS

The information going in is accurate because all sources are verified; therefore, what comes out is also accurate as well as computable.



LARGE LANGUAGE MODELS

The information going in is not accurate, because the sources are not verified; therefore, what comes out is not accurate nor computable.



So how do you actually verify intelligence sources?

Information Diligence (DAL TRUISTICS)

	<u>legend</u>
A ₁	agent
A ₂	actor
E	event
T	theme
O	object
D	date
C	channel
L	location

People, places & events are all verified using digital forensics!

Basis
Is the alleged event or story 'new'? <input type="checkbox"/> What themes does this alleged event or story expose? <input type="checkbox"/> What 'truth/s' about the domain, or primary elements within the domain, contradict it?
Who are the principal players in the alleged event or story? <input type="checkbox"/> Which corporate officers had care/control of key decisions? What about non-corporate stakeholders? <input type="checkbox"/> Who knew about the pending event and was in a position to do something about it, or manipulate it? <input type="checkbox"/> Was a regulatory, government or watchdog group on the ball? Or did they miss clues?
What's likely to change when the event or story becomes a news piece? <input type="checkbox"/> What's the perception of the domain leading up to the event or story? <input type="checkbox"/> How will the related issues be viewed if a news piece runs? <input type="checkbox"/> Is it reasonable 'not' to proceed? Who doesn't want this story out in the public?
What story do the numbers tell about the event or story? <input type="checkbox"/> Can we trace, via data and documents, the central issue(s) the material suggests? <input type="checkbox"/> If yes, what are the specific findings? <input type="checkbox"/> Has a regulatory, government or watchdog group examined other, similar cases? What can we learn from those cases?
Why the event or story...why now? <input type="checkbox"/> What's the market capitalization of associated company(ies); or what is the loss in (positive) perception? <input type="checkbox"/> Who lost how much? What came of the agents in this event or story? <input type="checkbox"/> Did anyone make money on the agents' downfall? why? how?
Who are the best storytellers? Who knows what we need to know about agency dealings? Timing of catalyzing event(s)? <input type="checkbox"/> Who are the key voices to the story? <input type="checkbox"/> What media assets do we have to tell the story?
What's the minimum that brings the story home? What do we absolutely need to know to make a case for the 'new story' that was missed? <input type="checkbox"/> How do we know? Prove it. <input type="checkbox"/> If it all falls apart, then what do we have left?
What's unique about the information (particular to the domain) we have now? <input type="checkbox"/> Is there a source/informant who's never gone on the record before? <input type="checkbox"/> Where's our scoop? What's unprecedented about this story? <input type="checkbox"/> What associations will bring to light unique data or inferences? <input type="checkbox"/> Which institutions have care/control records (emails, financial records/reports/disclosures) that will tell our story clearly and without contradiction?
What's missing? What else do we need to understand the scope/scale of this event or story? <input type="checkbox"/> Which markets does this story affect? What's the social impact? What's the macro impact? What's the micro impact? <input type="checkbox"/> What do associated allegations say about other such investigations?
What's our story, in ten words? <input type="checkbox"/> Example: "event X" exposes "asset Y" <input type="checkbox"/> Example: "agent X" scuttles "event Y" <input type="checkbox"/> Example: "event X" and "event Y" are related on account of "agent X" and/or "asset X & Y"

Core Logic Strains

(milestone evaluation)

Prerequisite	Antecedent	Consequent
-activeE	$\varphi \wedge$ activeE ₁	+activeE
-activeA ₁ A ₂	φ	+E
E	φ	-E
E	$\varphi \wedge$ activeE ₁	-E
activeE	+E	-activeE
+activeA ₁ A ₂	-activeE ₁	-activeE
-activeA ₁ A ₂	+activeE	$\varphi \wedge$ activeE ₁
-activeA ₁ A ₂	$\varphi \wedge$ activeE ₁	+E
-activeE	$\varphi \wedge$ -activeE ₁	+activeE
E	$\varphi \wedge$ -activeE ₁	$\varphi \wedge$ +activeE



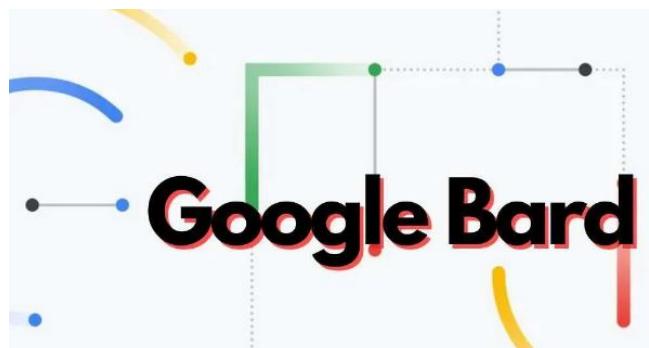
THE "ARTIFICIAL INTELLIGENCE" PROBLEM: Quality of information, security & scale

According to our friend Joscha Bach (one of the world's leading A.I. experts, co-inventor of the M.I.T. Brain), the training run for Open A.I. . to compile the corpus for the pharmaceutical market, as an example, would be about \$25M for 1000 runs through Google Bard, and about \$10M for 1000 runs through ChatGPT.

You could build an A.I. engine from scratch, and you could even do it cheaper, faster and better, but what information would you use, how would you use it, and in what configuration — would it be in a graph database? Would that database contain full data entities that are referencable as web objects such that any non-linear combination of the entity would reflect a math object, a semantic object and an image that share consistently similar results, but not exactly the same results?

This reality causes more problems as you build the corpus (or a non-corpus) because nothing automated and self-referential can be secure or scalable without changing the approach to the information first. LLMs to include (non)deterministic algorithms cannot achieve this on their own.

\$25M for
1000 runs



\$10M for
1000 runs

THE "ARTIFICIAL INTELLIGENCE" SOLUTION: The Approach to Quality of Information with Security @ Scale

MATH



bing

YAHOO!

facebook



Primary method:
LLM (large language modeling)
based on semantic distances
& probabilistic occurrences

MATH +



WolframAlpha

factual

Quora



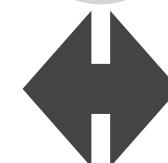
Primary method:
LLM (large language modeling)
based on ontological distances
& probabilistic occurrences

MATH + LANGUAGE

search
results

statistical
analysis

new
data



fixed
ontologies

emergent
ontologies

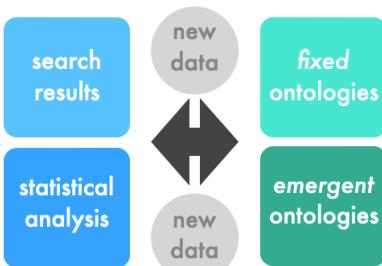
Primary method:
SLM (small language modeling)
based on syntactical pairings,
ontological differences &
probabilistic occurrences

Example: Microsoft's recent
development of ChatGPT4
training a new A.I. called Orca

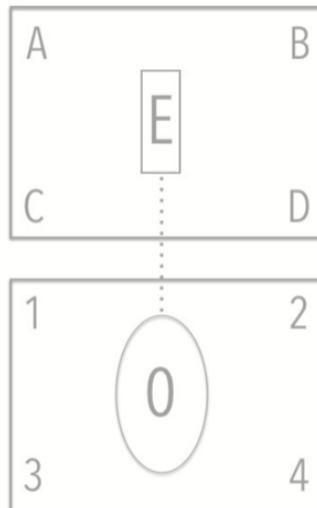


THE ARTIFICIAL INTELLIGENCE SOLUTION: Self-Referential Information Harvesting (SRIH)

MATH + LANGUAGE



HOLONOMIAL ALPHANUMERICS



A basis for connecting natural numbers with natural language

	negate	resolve	debate	relate	create	category
experiential	0	0	0	0	0	nature
	0	0	1	1	1	self
	1	1	1	1	1	human
	0	0	1	1	1	technology
	0	0	1	0	1	environment
	0	0	1	0	0	supernatural
	1	0	0	0	1	God
	1	1	0	1	0	comedy/drama
	1	0	1	1	0	journalism
	0	0	1	1	0	criticism
	1	1	0	0	0	dialectic
	0	0	0	1	1	legal/political
	1	1	1	1	0	forensic/scientific
	1	0	1	0	1	metaphysical
aspirational						

A self-referential (non)corpus that recombines ontological frequencies with an adaptive algorithm for providing instances of inquiry response patterns.

This is entirely new and has not been attempted before!

EMERGENT ONTOLOGY

Story Archetypes	negate	resolve	debate	relate	create
nature	0	0	0	0	0
self	0	0	1	1	1
human	1	1	1	1	1
technology	0	0	0	1	1
environment	0	0	1	1	0
supernatural	0	0	1	0	0
God	1	0	0	0	1

Modes of Inquiry	negate	resolve	debate	relate	create
comedy/drama	1	1	0	1	1
journalism	1	0	1	1	0
criticism	0	0	1	1	0
dialectic	1	1	0	0	0
legal/political	0	1	1	1	1
forensic/scientific	1	1	1	1	0
metaphysical	1	0	1	0	1

CHO7R's proprietary shared binary story language

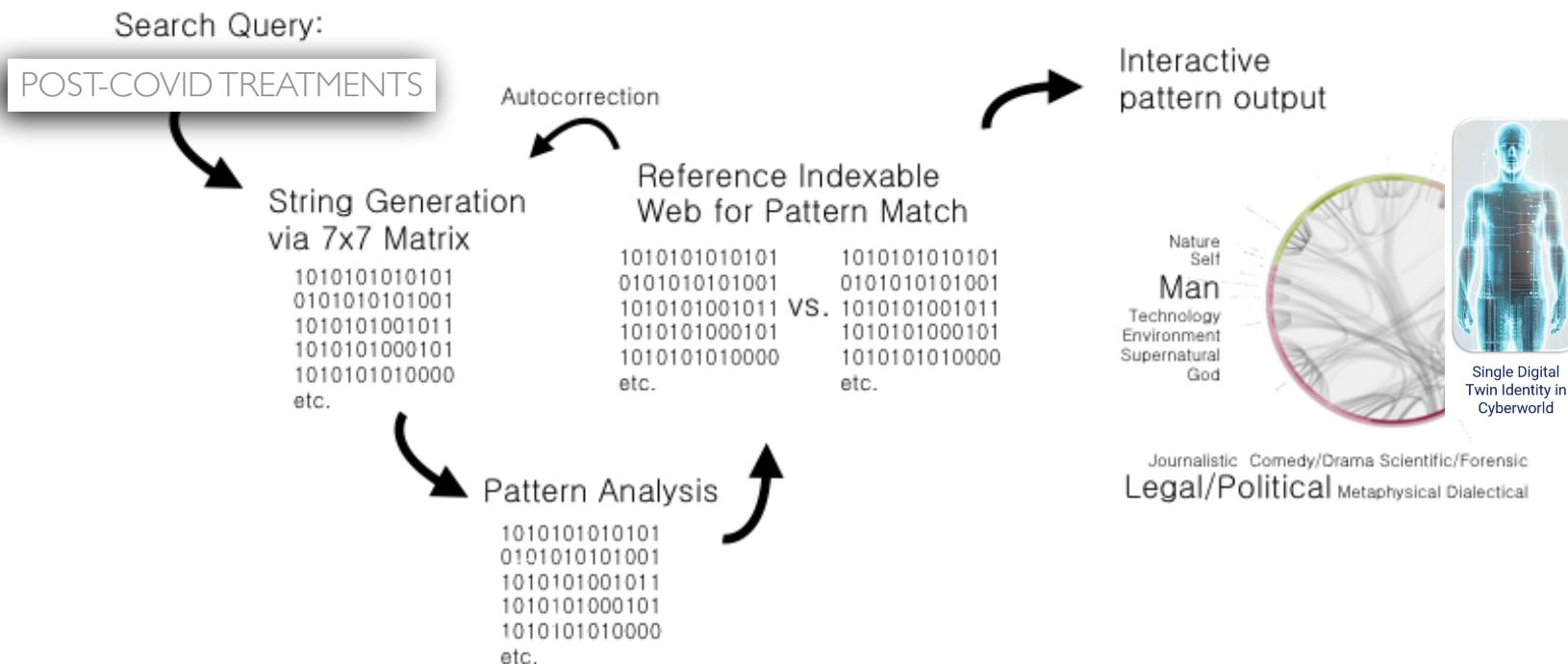
7x7 Story Matrix	nature	self	human	technology	environment	supernatural	God
comedy/drama							
journalism							
criticism							
dialectic							
legal/political							
forensic/scientific							
metaphysical							

CHO7R's proprietary 7x7 story matrix



THE ARTIFICIAL INTELLIGENCE SOLUTION: Self-Referential Discovery Engine (SRDE)

CHO7R Discovery Engine – Emergent Prototype Process



\$1M for
100,000
runs in their
own graph
database!

Proprietary Property of CHO7R – 2012

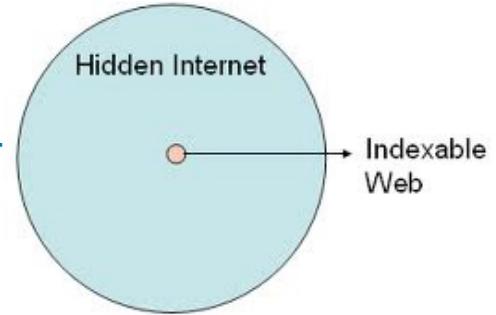


THE ARTIFICIAL INTELLIGENCE SOLUTION: Self-Referential Discovery Graph Outputs (SRDGEs)

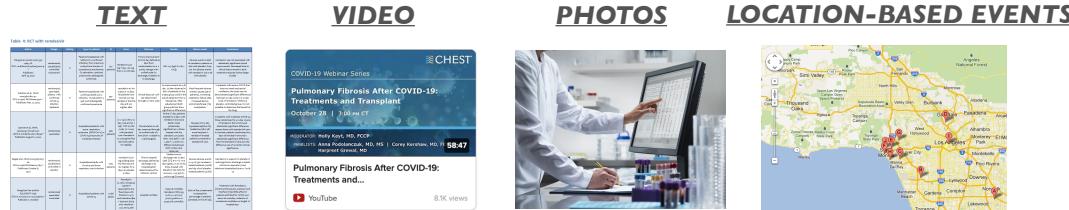
Search Query: POST-COVID TREATMENTS

1. The engine indexes the mainnet web, private intranets & or databases using the query matrix...

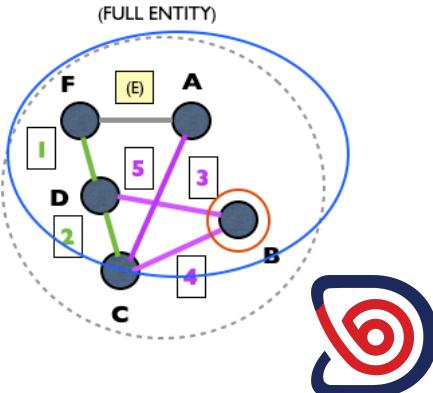
2. Ontologies emerge...



3. Then they start to fill out the real story of information and web objects.



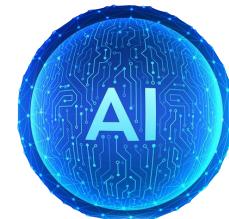
4. Reindexable full object-oriented entities that can be fully parsed interoperably in a new graph database!



THE TALE OF THE DIGITAL TAPE: DAL VERSUS A.I.



(NATURAL INTELLIGENCE)



(ARTIFICIAL INTELLIGENCE)

SPEED

Bit rate at the level of datum, 1:1

Bit rate at the level of nodes or networks

METHODOLOGY

Non-linear yet succinctly structured (no dependencies)

Linear & dependently structured

ACCURACY

Represented from the datum-level

Represented from web protocols

AUTHENTICITY

Represented from the source (real person)

Represented away from the source

TRUST

Established between peers or counterparties

Established pseudoanonymously (non-trustful)

SCALE

Established via peers without network interference

Established via bots & synthetics

INTEROPERABILITY

Integrates or bypasses any operating system

Achievable only on same operating system

SETTING A NEW CRYPTOGRAPHIC STANDARD

DAL's Web4 Post-PGP, Post-Quantum Security at a glance



MATH

AES

(Advanced Encryption Standard)

Protocol-Based Elliptical Curves

Largest solvable key size: 795-bit (2019)

RSA-Focused Algorithms

Lots of SSH exploits



MATH OR LANGUAGE

PQC

(Post-Quantum Cryptography)

Protocols Applied to Web Objects

Indeterminable Key Sizes

Shor's/Grover's Algorithms

SSH Incompleteness (some traceability)



MATH + LANGUAGE

W4S

(Web4 Security)

Complete Object-Orientations, SuperKernels

1-Bit Binary Representations (no key limits)

Holonomial Algorithms (instances)

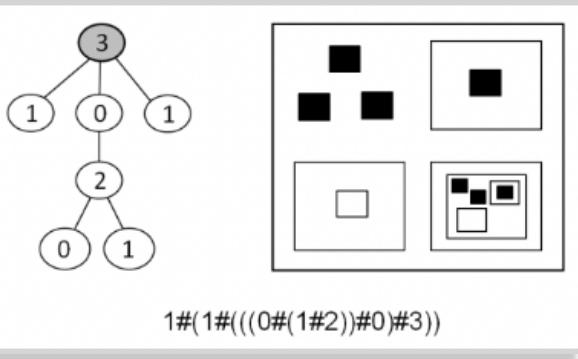
SSH Completeness (no traceability)



object

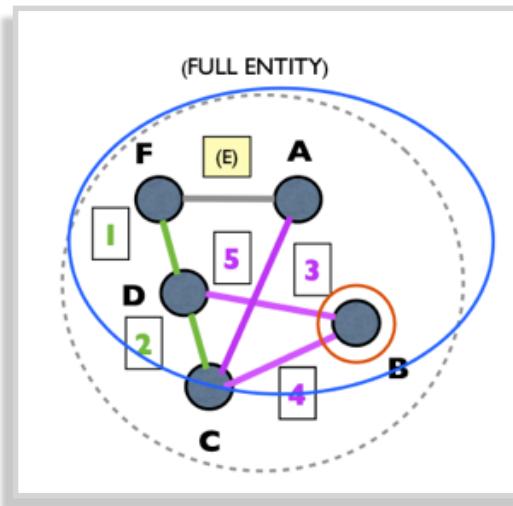
WEB4 Security object-level holomorphic hashing system

HOLONOMIALS

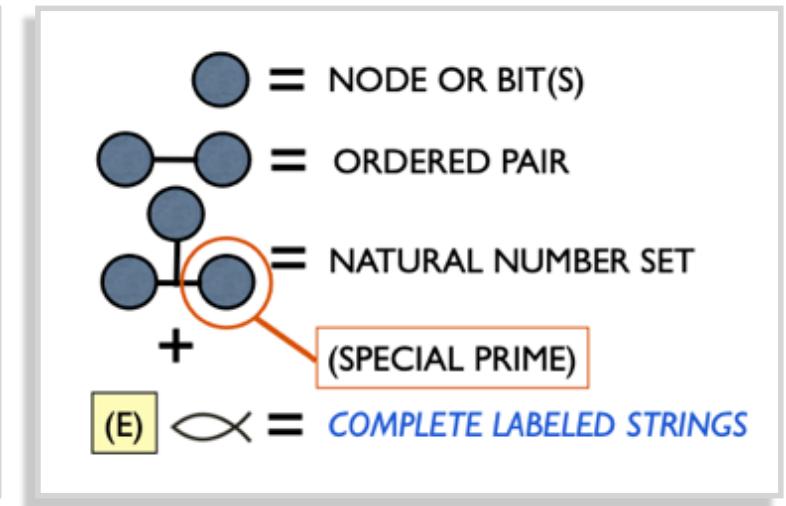


Holonomials simulate post-quantum level cryptography with a holomorphic hashing mechanism as 1-bit succinct binary representations of root primes, symbols & syntax.

objects represented as fully programmable entities



labeled strings (smart strings) as fully hashable graph objects



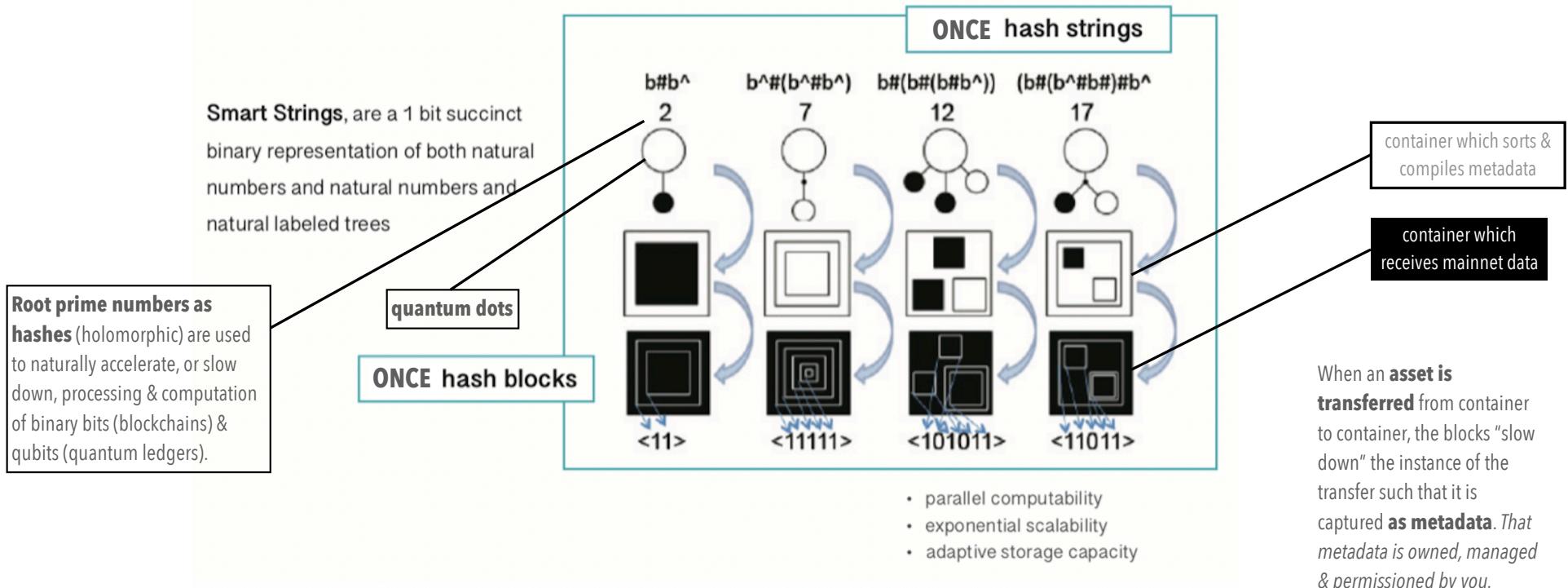


Identikit™

Your body, your Identikit

QUANTUM-TOLERANT/SAFE CRYPTOGRAPHY

As represented on its own holomorphic node...



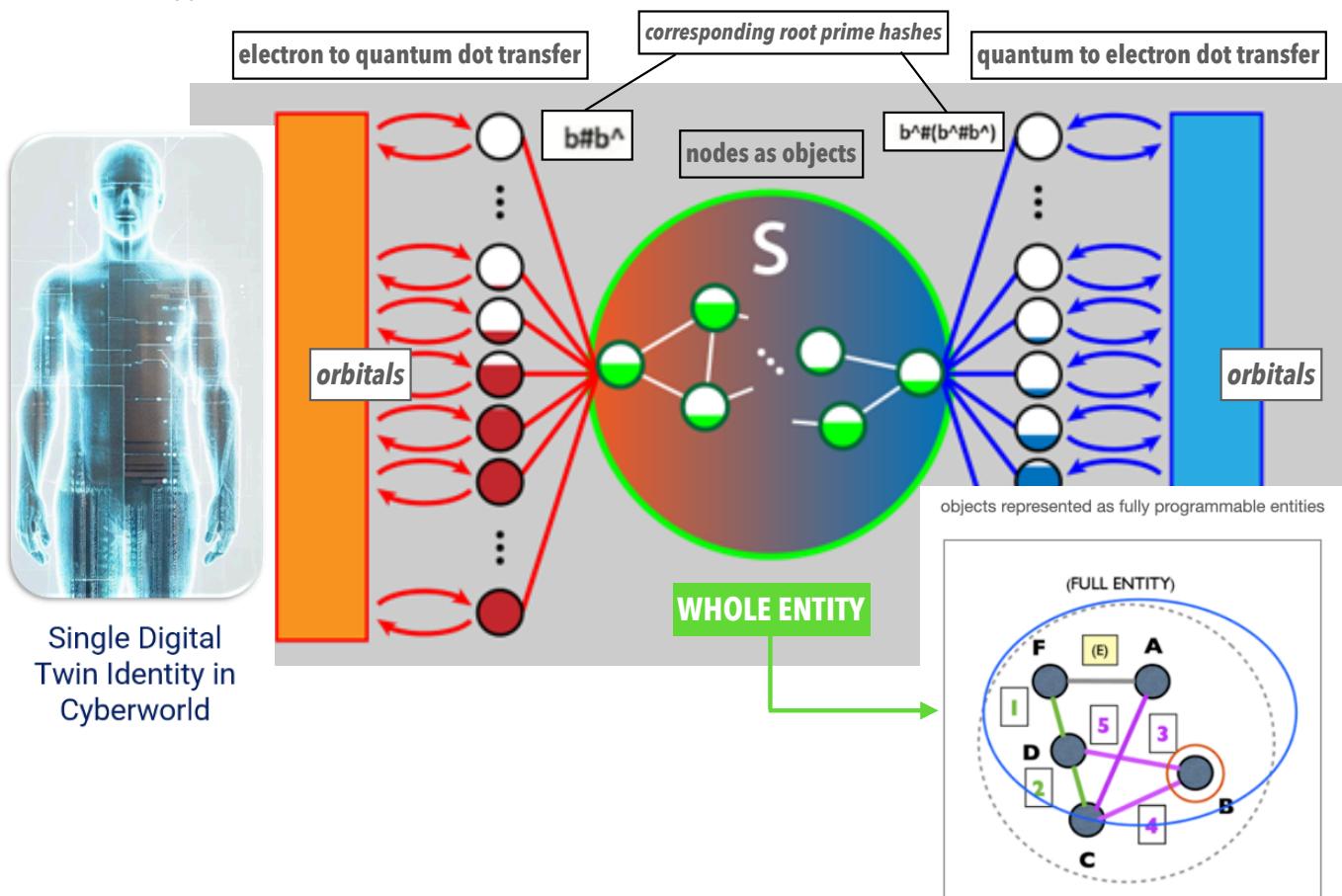


Identikee™

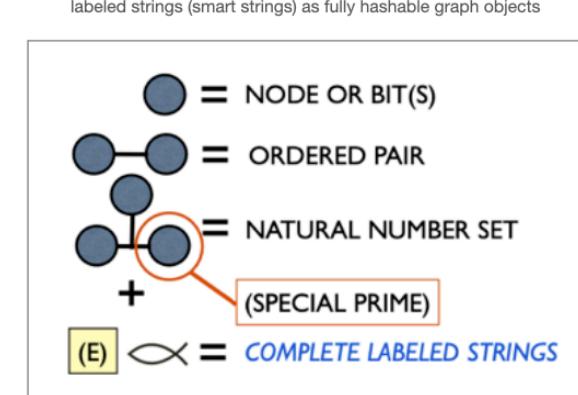
Your body, your Identikee

PHOTONIC ENERGY TRANSFER SECURITY

Real Identity transferred & captured via real quantum mechanical energy.



In other words, quantum energy as qubits, arranged as ordered pairs, through special primes, as complete labeled smart strings — programmable as full entities in a self-organizing graph with the fully secured Real Digital Twin at the center of interactivity!



TAKEAWAYS:

- + REAL SECURITY BEGINS WITH A REAL IDENTITY
- + REAL NETWORK SECURITY HAPPENS BETWEEN PEERS
- + REAL TRUST IS BUILT BETWEEN PROTECTED PEERS



Join us in (r)evolutionizing
the interwebs :)

<https://www.dal-identity.com/>

