TRUSTED DIGITAL WEB: WHITEPAPER

THE FUTURE OF THE INTERNET AND THE WORLD WIDE WEB

A SOLUTION FOR A WORLD STEEPED IN FUNDAMENTAL DISTRUST

Michael Herman
Self-Sovereign Blockchain
Futurist, Architect, and Developer

Hyperonomy Digital Identity Lab
Parallelspace Corporation

Alberta, Canada

mwherman@parallelspace.net

The publication of this whitepaper coincides with the November 7-8, 2019 Malta Blockchain Summit: Future of Blockchain panel where the author is an invited panelist.
https://maltablockchainsummit.com/

TABLE OF CONTENTS

CONTEXT

Say all you have to say in the fewest possible words, or your reader will sure to skip them; and in the plainest possible words or he will certainly misunderstand them.

[Business of Giving (https://www.amazon.ca/Business-Giving-Philanthropy-Grantmaking-Investment/dp/0230336795/ref=sr_1_1)]

Background

The Trusted Digital Web (TDW) is a universal, trusted, frictionless, integrated, standards-based, general-purpose, end-to-end platform for global commerce, communication, and collaboration.

The fabric that knits us together is the Internet global communications network and the World Wide Web (WWW) software application that enables individuals, governments, corporations, and other organizations to share, consume and interact with a universal sea of data and information representing every aspect of our lives and livelihoods.

But today we live in a world of fundamental distrust. Pervasive distrust in our governments, other countries' governments, our politicians (Donald Trump, Boris Johnson, constantly warring political parties), other governing institutions (United Nations, World Bank), our financial institutions, large corporations (global food conglomerates, major manufacturers (Boeing 737 MAX), the daily, hourly and instantaneous streams of information we consume (news, weather, climate, and other world-impacting events), and the social platform companies and software applications (Facebook, Twitter) we consume and interact with every day.

What is the solution? What's "next"? …perhaps it's something called the Trusted Digital Web (TDW).

Let's explore.

Overview

This whitepaper is the first complete description of the motivations, problem statement, and solution concept for a solution for the world of fundamental distrust we live in. To give this particular solution a name, it's called the Trusted Digital Web (TDW).

The Trusted Digital Web is a fully cross-integrated solution for:

- Decentralized currency
- Universal digital identity
- Decentralized workflow

Decentralized workflows include both fully automated and semi-automated (the latter requiring human intervention).

Two of the primary concepts backing the Trusted Digital Web are:

- Universal Digital Identifiers, and
- Universal Digital Identities.

Universal digital identifiers, digital identities, and digital credentials are discussed throughout this whitepaper. Specific definitions can be found in the section Digital Identifiers in APPENDIX B – Platform Definitions on page 52.

Three key software components that make up the Trusted Digital Web software platform:

- Trust-Based Applications (or more simply, Trust-Based Apps or TBAs),
- Universal DID Data Service (UDIDService), and
- Trusted Digital Assistant (TDA).

The Trusted Digital Web is defined by the following architecture principles:

- Leverage existing, common, every-day specifications, protocols, and software components where possible.
- TDW is serverless (based on the traditional precept of what an infrastructure server is).
- UDIDService is based on Internet Domain Name Service (DNS) concepts and protocols.
- UDIDService is backward compatible with current DNS protocol specifications.
- TDAs will replace current Web Browsers with a trusted alternative.

Each of these will be described and documented in this document with increasing levels of architectural detail. The reader can choose to stop reading whenever they feel they have grasped the amount of detail that suits their purpose.

Key Definitions

The following key definitions represent a minimal list of the terms needed to read and understand this document. A comprehensive list of definitions can be found in APPENDIX B – Platform Definitions on page 47 and APPENDIX D – Additional Definitions on page 60.

Trust

Definitions of trust typically refer to a situation characterized by the following aspects:

- *one party (trustor) is willing to rely on the actions of another party (trustee); the situation is directed to the future.*

In addition, the trustor (voluntarily or forcedly) abandons control over the actions performed by the trustee. As a consequence, the trustor is uncertain about the outcome of the other's actions; they can only develop and evaluate expectations.

The uncertainty involves the risk of failure or harm to the trustor if the trustee will not behave as desired.

[Wikipedia: https://en.wikipedia.org/wiki/Trust_(social_science)]

Distrust

Noun

- *the feeling that someone or something cannot be relied upon.*
- *"his distrust of his mother's new suitor"*

- *synonyms: mistrust, suspicion, wariness, chariness, lack of trust, lack of confidence, lack of faith; skepticism, doubt, doubtfulness, dubiety, cynicism; misgivings, questioning, qualms; disbelief, unbelief, incredulity, incredulousness, discredit; informalleeriness*
- *"the general distrust of authority amongst drug users"*

Verb

- *doubt the honesty or reliability of; regard with suspicion.*
- *"like a skillful gambler, Dave distrusted a sure thing"*
- *synonyms: mistrust, be suspicious of, be wary/chary of, regard with suspicion, suspect, look askance at, have no confidence/faith in; be skeptical of, have doubts about, doubt, be unsure of/about, be unconvinced about, take with a pinch/grain of salt; have misgivings about, wonder about, question; disbelieve (in), not believe, discredit, discount, be incredulous of; informal, be leery of, smell a rat*
- *"for some reason Aunt Louise distrusted him"*

[Lexico.com: https://www.lexico.com/en/definition/distrust]

Universal Digital Identifier (UDID aka DID)

Short for Universal Digital Subject Identifier, a UDID is a character string representation whose value is unique and is used to address, index, search, and retrieve Claims about the associated Digital Subject (aka Subject). A Subject can have more than one UDID associated with it.

A DID starts with the character string `did:` *and is followed by 1 or more DID Method labels; followed by Method-define unique character string identifier. Examples:*

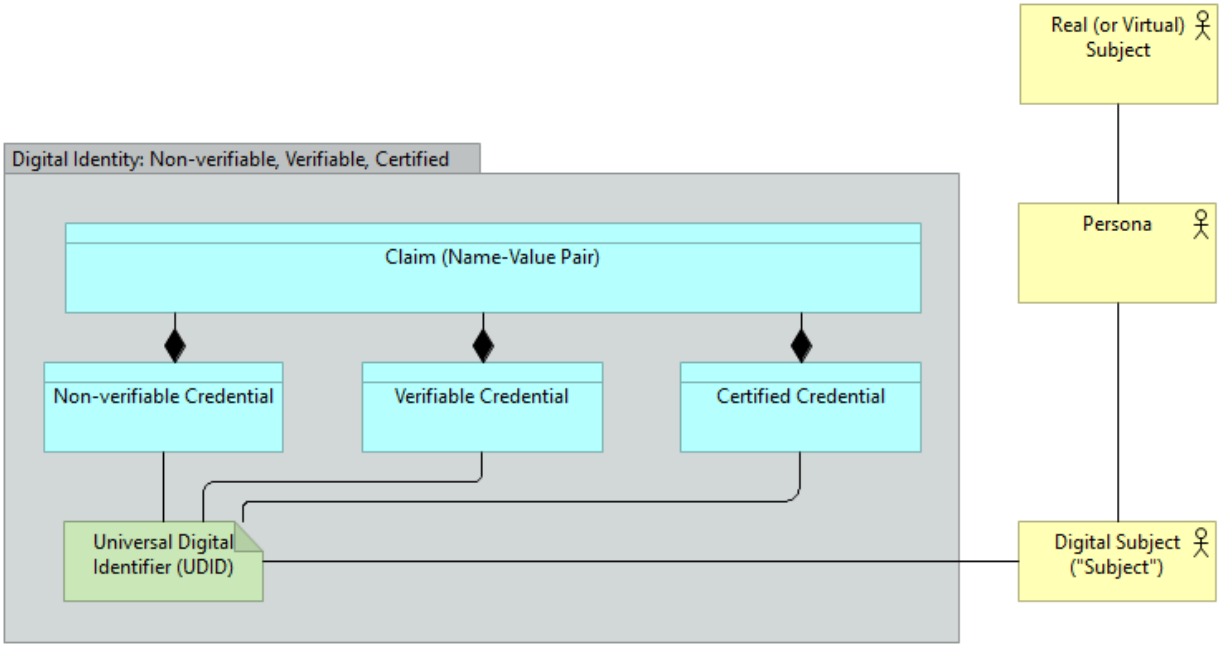
- `did:neonation:123-456-789`
- `did:usergroups:developers:abc12345678`

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Universal Digital Identity

A Universal Digital Identity is a set of Claims made by one Digital Subject about itself or another Digital Subject [The Laws of Identity]. A Universal Digital Identity is associated with, or identified by, one or more Universal Digital Identifiers (UDIDs, or more simply, DIDs). A Universal Digital Identity is manifest by or realized as a Credential (a set of Claims).

[Michael Herman: https://twitter.com/mwherman2000/status/1164540800526454786]



Strategic Thinking

In addition to the development of Trusted Digital Web as a net new software platform and solution for addressing fundamental distrust on the Internet, it's also an exercise in the direct application of the principles of strategic thinking and foundational technology adoption. The principles of strategic thinking are described in more detail in Appendix D – Strategic Thinking on page 65. A comprehensive guide to technology adoption models can be found in the article *Technology Adoption Models: A Comprehensive Guide* (https://hyperonomy.com/2019/10/16/technology-adoption-models/).

THE PROBLEMS

We live in a world steeped in fundamental distrust.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Today, what we know as the World Wide Web is a network of linked web sites, web pages, data and information, audio and visual content, and software web applications that we access via web browsers and mobile applications using a universal, global computer communications network called the Internet. The web applications also communicate with each other (more than we know) using the same or similar sets of Internet communication protocols. DNS (Domain Name Service) is one of the principal sets of protocols, specifications, and services that underly the Internet.

The physical data centers where the computers hosting the web sites and web applications are generally considered to be physically very secure – but that may not be true for an actual web site running on a given web server; especially, if it is in someone's basement, the backroom of a small storefront, a corporate data center, or is a poorly managed cloud-based virtual server. Electronic access to these servers and applications, similarly, is highly protected using layers of hardware and software that implement various levels of firewall, monitoring, filtering and other types of network communications and access controls.

The core problems, today, are:

- Trust
- Centralization
- Things
- Friction

Trust

Trust is the core problem on the World Wide Web. Virtually all web content today (e.g. the pages you see, read, and interact with) are dynamically generated by software – by computer software web applications running on Internet-connected computers called web servers. Web applications read web page templates expressed using a variety of technologies, retrieve a diverse collection of data, information, audio, and visual content and other digital artifacts to create customized web pages – usually personalized for each and every user (think of your Twitter feed or Facebook home page).

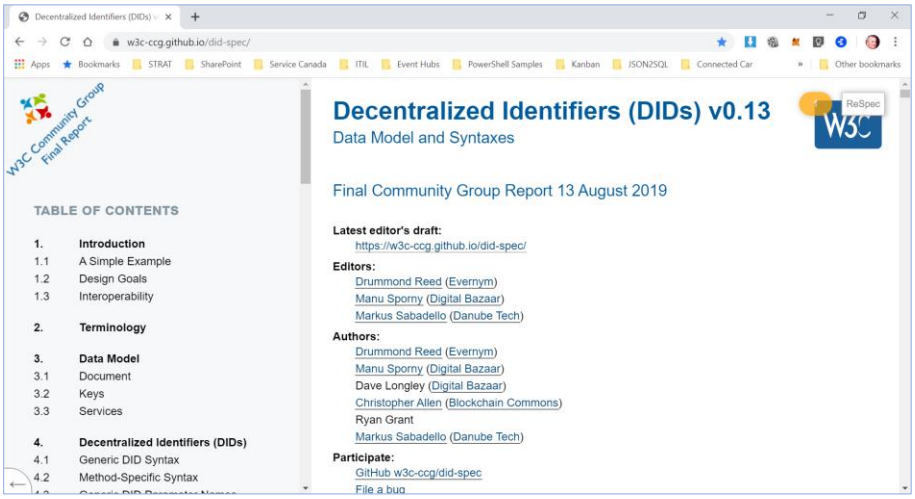
The web pages are further customized for the device you are using, the host application you are using to view the content (general-purpose web browser vs. very specific mobile applications running on your phone, tablet, vehicle, digital sign, laptop, or desktop) as well as the viewer's personal profile information, detailed history interacting with that web application as well as the user's past history interacting with possibly related (or more likely, unrelated) web sites and web applications (sports equipment or personal hygiene advertisements being displayed above, below and beside a BBC news article). Facebook is an example as well as being one of the most pervasive web applications and customized and personalized web experiences that many people will be familiar with.

Centralization

The problem with the World Wide Web is that virtually all web sites and web applications that people rely on are owned and, more importantly, *controlled* by large corporations and governments. For example, Facebook and the web sites of the world's chartered banks are owned and controlled by large corporations and their executives (Facebook being the prime example; Wells Fargo and TD Bank (Toronto-Dominion Bank Financial Group), and Google are other examples). While corporations are becoming subject to more and more government as well as government scrutiny, the Facebook web application continues to collect, consume, process, and traffic in *data as a manufactured product* (data products derived, almost in total, from our *individual personal data and information*) for the benefit of the Facebook corporation, its majority shareholders, subsidiary shareholders, and the same roles in its business partner ecosystem …with no compensation or remuneration being returned to the original individuals who are the true owners and originators of the personal data and information. This includes the transactional data that companies like Facebook link to our personal data and information to further enhance the value of their data products; and by implication, to increase the revenues and profits generated from their trafficking in these products for the benefit of Facebook and its stakeholders.

Things

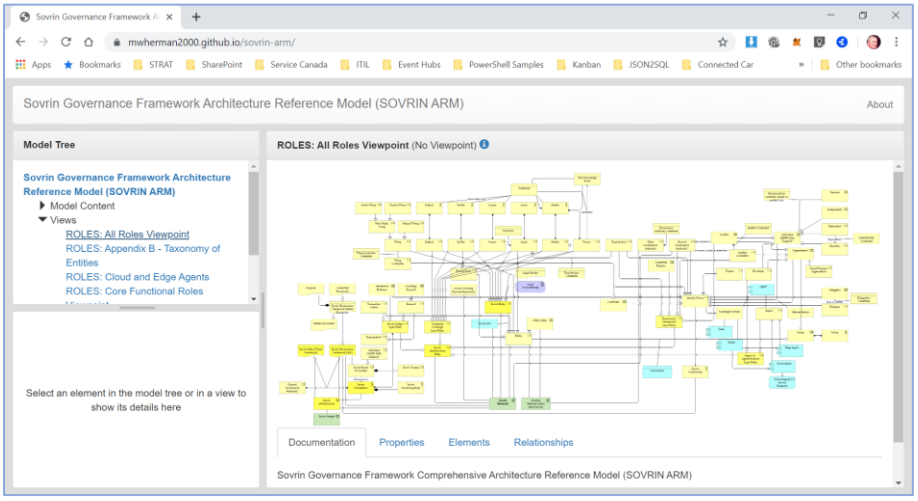
The ongoing focus (pre-occupation) with current activities in the Digital Identifier and Decentralized Identity communities is almost exclusively related to representing People and Organizations – with relatively little attention being given to the much larger field of representing, using Digital Identities, non-fungible entities or "things" (as the community prefers to refer to them) and the graphs of relationships that exist between these entities.



Universal access to data requires that the concept of Digital Identifiers, Digital Identities, and Digital Credentials applied to all data items – *every little thing* on the planet and across the universe – those that are non-verifiable and non-certified in addition to data items that are verifiable and/or certifiable.

Initially, the most common and mature digital identity governance framework, the Sovrin Governance Framework (SGF) and its Glossary, suffered from a similar "Thing" problem. This has been remediated in the most recent version 2.0 of the Sovrin Glossary (https://sovrin.org/library/glossary/) (as illustrated

below in the Sovrin Architecture Reference Model (SOVRIN-ARM) (https://github.com/mwherman2000/sovrin-arm/blob/master/README.md)).



Friction

The Friction problem refers the ever-present situation today where simple transactions, workflows, and business processes such as buying-and-selling are made unnecessarily more complex, less reliable, and more costly due to the number of intermediate parties (intermediaries) involved in what otherwise should be a simple, efficient, and immediate activity.

> *[Friction is] the disparity between the ideal performance of units, organization or systems and their actual performance in real-world scenarios.*
>
> [Carl von Clausewitz (https://en.wikipedia.org/wiki/Carl_von_Clausewitz#Principal_ideas)]
>
> *The term friction is described as, "the awkward, unequal, unstable, and creative qualities of interconnection across difference."*
>
> [Anna Tsing (https://en.wikipedia.org/wiki/Anna_Tsing)]
>
> *Transactional friction has been a driving force in economics since the inception of trade. Transactional friction is simply the sum of all the direct and indirect costs of performing a transfer. The thing is, transactions are by their very nature work. Some entity has to move whatever asset is in question, physical or digital, from one place to another, whether real or virtual. Because there is work involved, and work requires compensation, there is almost always a cost.*
>
> [The Transactional Friction Problem (https://medium.com/the-zeex-protocol/the-transactional-friction-problem-3a3bad7272e2)]
>
> *Friction is never an easy problem for which to solve, but increasing consumer demands and expectations set by online and mobile commerce — quick shipments, ample recommendations, and other features — mean the bar keeps rising for retailers interested in better omnichannel commerce…*
>
> [POS Payments at The Speed Of Sound (https://www.pymnts.com/innovation/2019/pos-payments-at-the-speed-of-sound-waves/)]

Velocity is a function of friction. The more friction you impose on …, the slower the train will be.

[The third rail: putting microservices in context (https://blogs.mulesoft.com/dev/microservices-in-context/)]

SOLUTION APPROACH

Trust is one of the things that permeates across the whole business. It is the bedrock of business and, without it, organizations are going to struggle to keep their existing customers, gain new customers or enter new markets.

[Stephen Walsh, director of security for Northern Europe, CA: https://www.csoonline.com/article/3297037/what-is-digital-trust-how-csos-can-help-drive-business.html]

The solution approach begins with a discussion of the solution requirements. These requirements were in turn driven by the list of problems described in the previous section:

- Trust
- Centralization
- Things
- Friction

Requirements

The primary requirement is the creation and deployment of a new trusted replacement for the World Wide Web that eliminates (or at least greatly reduces) the problems of trust, centralization, things, and friction that exist on the World Wide Web today.

The new platform needs to support the following attributes:

- Universal
- Trusted
- Frictionless
- Integrated
- Standards-based
- General-purpose
- End-to-end
- Global
- Commerce
- Collaboration, and
- Communications

The solution needs to seamlessly integrate and knit together the following functionality:

- Digital Payments
- Decentralized Workflow Actions (Business Processes)[1]

[1] References to the term "Workflow Actions (Business Processes)" appear throughout this whitepaper. In the context of the Trusted Digital Web, a *Workflow Action* is a fairly simple network of interconnected work tasks that, when initiated, run to completion without blocking for user input or an external event. A *Business Process*, on the other hand, is generally considered to be a more complex network of interconnected work tasks and may block waiting

- Trusted and Verifiable Credentials for Workflow (Business Process) Templates
- Trusted and Verifiable Credentials for Business Documents
- Trusted and Verifiable Credentials for People and Organizations

In addition, the solution needs to have the following capabilities:

- Peer-to-peer and serverless
- Leverage existing, common, every-day specifications, protocols, and software components where possible
- Support for verifiable as well as non-verifiable digital identifiers, digital identities, digital credentials
- Data notarization services

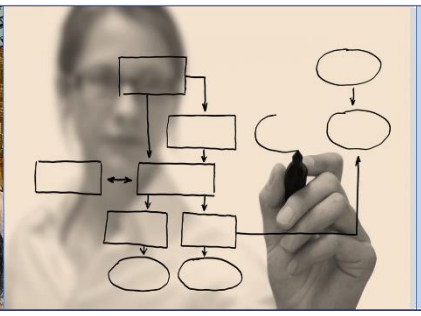
In addition, the new platform may (will) require upgrades and extensions to some of the technologies and specifications that underly the Internet global communications network. These enhancements include direct and universal support for digital identifiers, digital identities, and digital credentials used to identify, codify, store, and retrieve data about all things (*every little thing*) on the planet.

The above list of requirements (attributes, functionality, and capabilities) can be further grouped into the following categories:

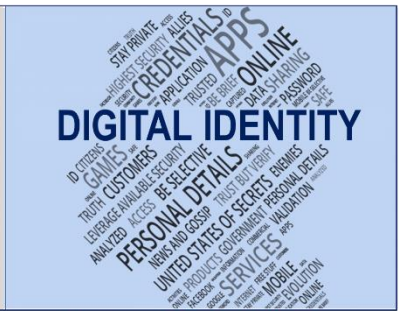
- Decentralized Currency
- Decentralized Workflows (Business Processes)
- Universal Digital Identity

Fully Integrated Experience

Decentralized Currency
(cryptocurrency)



Decentralized Workflows
(business processes)



Universal Digital Identity
(people, organizations, things,
& business documents)

The envisioned solution needs to bring these elements into a fully integrated software platform and fully integrated experience for the citizens who use the platform.

---

for input from a user, an external service or some other event. Workflow Actions will generally be used to implement functionality internal to a Trusted Digital Assistant (but not exclusively). A Business Process is used to support an external (real world) business process. Both workflow actions and business processes are defined in the same way, are managed in the same way, and execute in the same way - inside the Trusted Digital Assistant.

Decentralized Currency

The requirements for decentralized currency dovetail with platform's more general technical requirements for a general-purpose, smart contract-enabled blockchain platform that is also capable of supporting the verification of digital identifiers, digital identities, and digital credentials.

In addition, the chosen decentralized currency needs to relatively liquid and easily tradeable against other currencies (both cryptocurrencies as well as fiat currencies) across multiple exchanges.

The applicable standards and specifications for decentralized currency include:

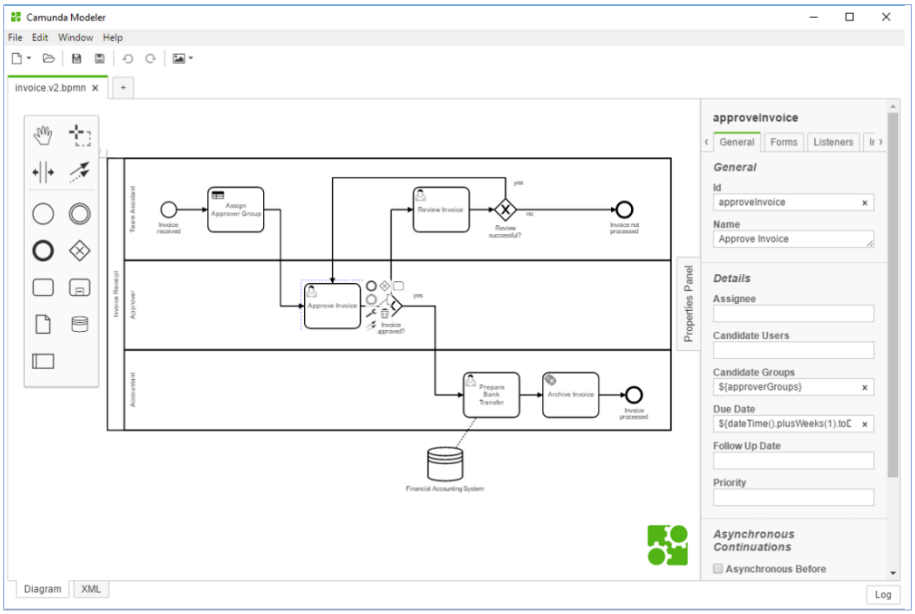
- Any of the leading general-purpose, smart contract-enabled blockchain platforms (e.g. Stratis Platform, Ethereum, Hyperledger Fabric, etc.)
- Ease of purchase using fiat currencies
- Ease of exchange with other currencies
- Recognition and acceptance in the initial marketplaces targeted by the Trusted Digital Web

Decentralized Workflows (Business Processes)

The full integration of trusted, decentralized, standards-based workflows and business processes is a key innovation in the Trusted Digital Web. Full integration implies using workflows for both the internal processes of the TDW as well as the business processes being enacted across the TDW.

Trusted and decentralized implies both workflow and business process templates that define the workflows and business processes (100s and 1000s of templates) as well as the individual instances and execution state of the flows and processes (millions and billions of these) are all represented as notarized and verifiable entities on the TDW.

Standard-based implies that all workflow and business process templates will be defined using the prevailing standards for designing, defining, documenting, and exchanging (persisting) the templates for these flows and processes. Today, for workflow and business processing modeling, BPMN (Business Process Model and Notation), curated by the OMG (Object Modeling Group), is the prevailing standard. Informally known as *swim lane diagrams*, an example appears below.



The applicable standards and specifications for decentralized workflows (business processes) include:

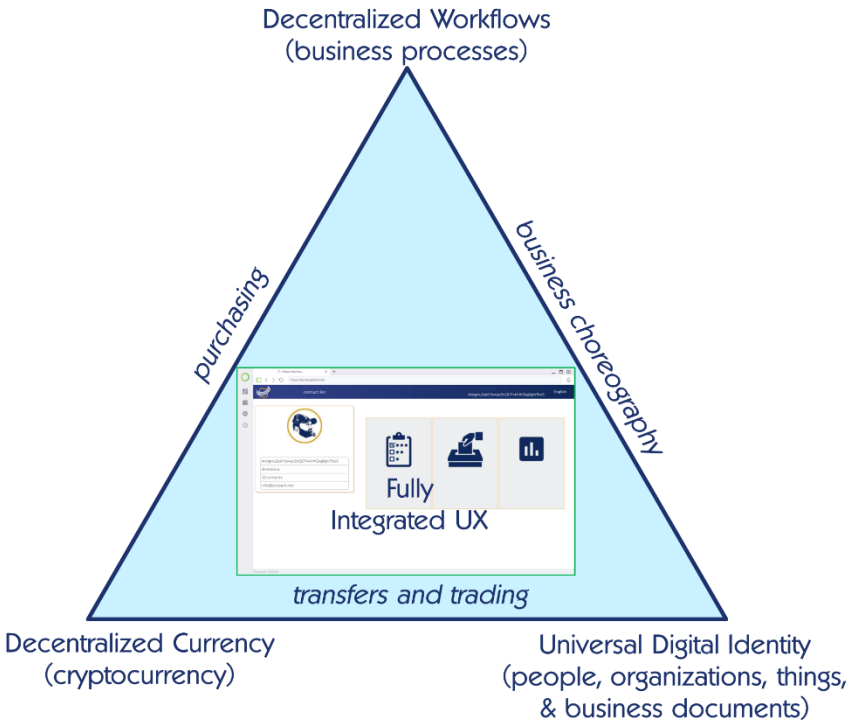
- BPMN (http://www.bpmn.org/)
- Camunda Modeler (https://camunda.com/products/modeler/)

Universal Digital Identity

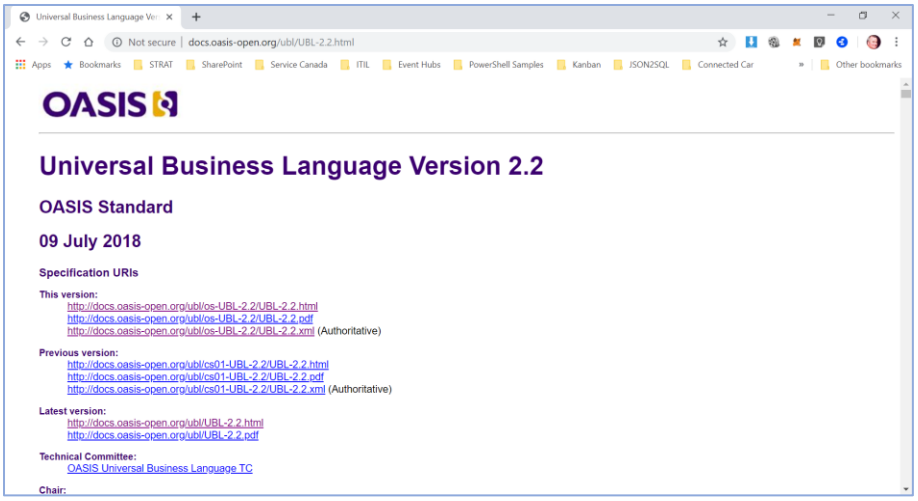
The linchpin for the entire Trusted Digital Web platform is the concept of Universal Digital Identity; digital identity for Every Little Thing (#ELT) (https://hyperonomy.com/2018/01/24/tokenization-of-every-little-thing-elt/) on the planet and across the universe. This includes people, organizations, business documents, products, services, parts, etc., etc.

- Verifiable Digital Identifiers, Identities, and Credentials ("decentralized")
- Person, place, thing, organization, digital visual or audio composition, business document, …
- Non-verifiable Digital Identifiers, Identities, and Credentials

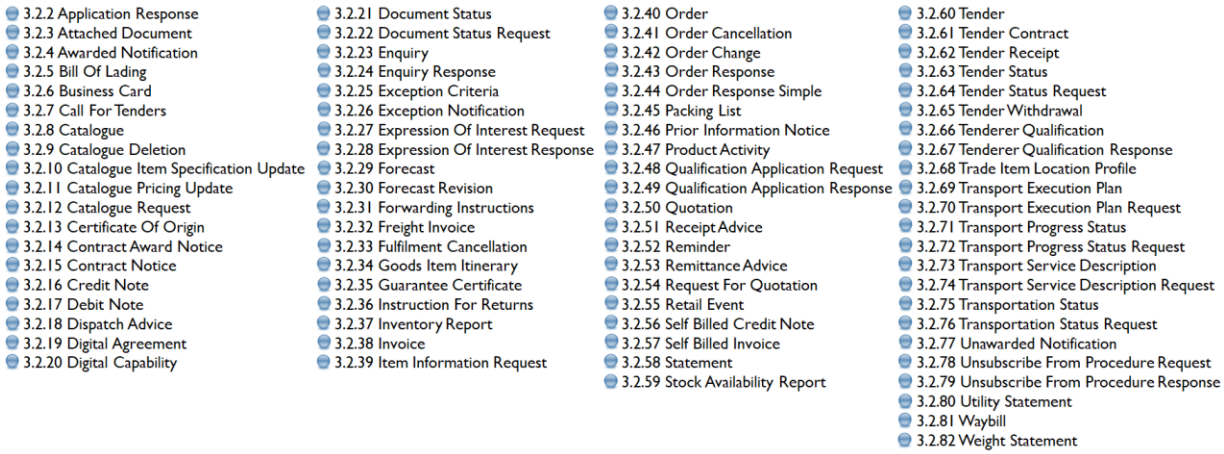
Digital identities serve as the endpoints for transfers of value and hence support trading in value-based tokens (cryptocurrencies). Digital identities also serve as *actors* and *business records* in decentralized workflows and business processes. Combining these two purposes enables fully decentralized, global business processes to be enacted between actors, generating verifiable business records, and lastly, supporting payments for goods and services – in a fully integrated system as illustrated below.



Universal digital identity includes both identities that are verifiable (against a decentralized journal) as well as identities that are simply names and non-verifiable.



With respect to business documents and business records, the OASIS curated Universal Business Language (UBL) defined schemas for 81 of the most common documents used in business today. UBL schemas can serve as the basis for defining both verifiable (and where appropriate, non-verifiable) business credentials. The following chart lists the 81 business document schemas defined by the current UBL specification.



Fully Integrated Experience

The wide range of usability problems with existing web browser digital wallet plugins is well known (e.g. MetaMask plugin for Chrome (https://skale.network/blog/why-dapps-leaving-metamask). They are simply too difficult for the average Internet user to comprehend and to use reliably. What is needed is a fully integrated user experience (UX) that integrates:

- Universal Digital Identity for every little thing (#ELT)
    - DID documents, verifiable credentials, non-verifiable credentials, schema definitions, business documents, web pages, images, etc., etc.
- Workflow and Business Process Engine
- Cryptocurrency Digital Wallet
- Subsidiary Ledger (Subledger) Storage Model
    - Capable of storing millions and potentially billions of Credentials projected into multiple ledgers (folders)
- Mobile (and Web) User Experience
- Trust-based Applications that seamlessly plug into this user experience and are easy for developers to integrate their user interfaces and business logic with the digital identity, workflow engine, and subledger storage model.

TRUSTED DIGITAL WEB

It can scarcely be denied that the supreme goal of all theory is to make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation of a single datum of experience.

[Paraphrased: Everything should be made as simple as possible, but not one bit simpler.]

[Albert Einstein, 1933 (https://en.wikiquote.org/wiki/Albert_Einstein#1930s)]

What is the Trusted Digital Web?

The Trusted Digital Web (TDW) is a universal, trusted, frictionless, integrated, standards-based, general-purpose, end-to-end platform for global commerce, communication, and collaboration. The Trusted Digital Web is comprised of three (3) core software components: Trust-Based Applications (Trust-Based Apps or simply, TBAs), Universal Digital Identity (UDID) Data Service (UDIDService), and Trusted Digital Assistants (TDAs).

The Trusted Digital Web is the software platform that addresses the needs and requirements described in the section Solution Approach (page 12) to address the problems outlined in the section The Problems (page 8).

Core Software Components and Services

The core software components and services are necessary to support the above attributes, functionality, and capabilities resulting in an instantiation of the Trusted Digital Web Network include:

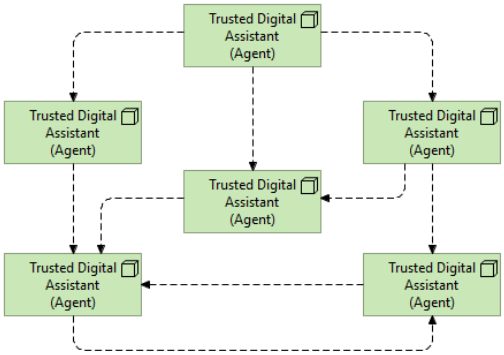
- Trusted Digital Web Network (TDN)
- Trusted Digital Assistant (TDA)
- Trust-Based Applications (TBAs)
- Trust-Based (Application) Host (TBH)

Trust-Based Applications Trusted Digital Web Network (TDN)

The Trusted Digital Web Network consists of an unlimited number of agents known as Trusted Digital Assistants (TDAs) joined together by an arbitrary number of inter-agent relationships.

Trusted Digital Web: Trusted Digital Web Network 1.0

Michael Herman
Self-Sovereign Blockchain Architect
Hyperonomy Digital Identity Lab
Parallelspace Corporation
October 11, 2019



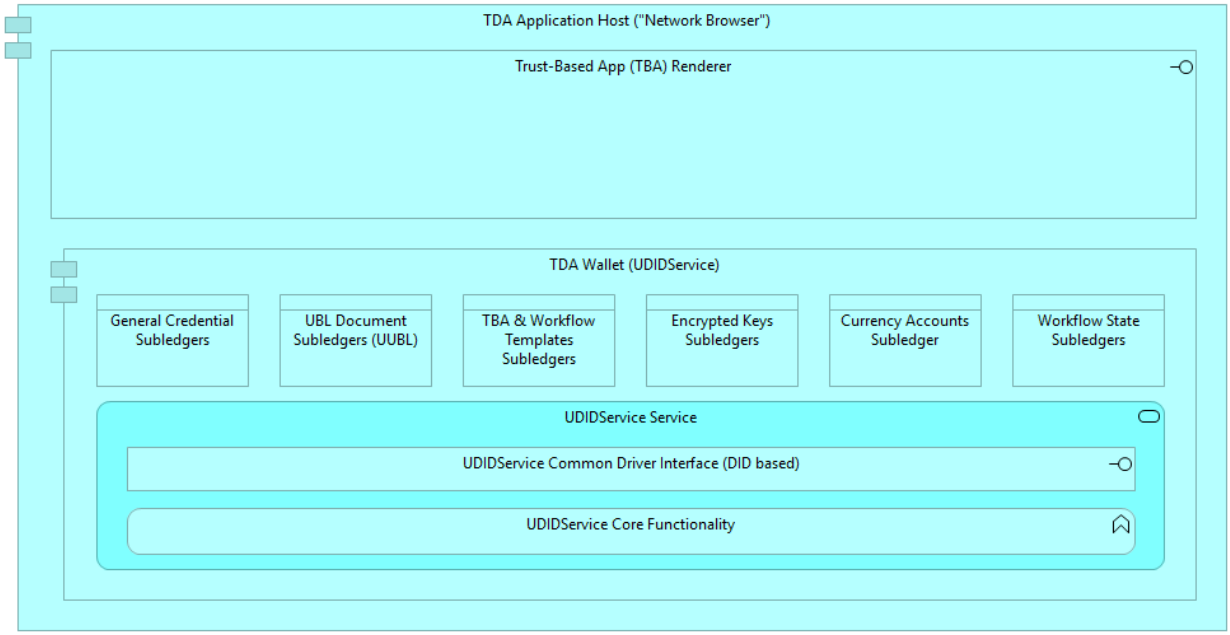
Trusted Digital Assistant (TDA)

Each TDA supports, at a minimum, the following collection of internal services:

- Trust-based Application Host (User Experience)
- Universal Digital Identity Data Service (UDIDService)
- Universal Data Notarization Service (UDID Notary, UDN)
- TDW Subledger Persistable Storage
- TDA Workflow Engine

Trusted Digital Assistant (TDA) Logical Architecture 0.1

Michael Herman
Self-Sovereign Blockchain Architect
Hyperonomy Digital Identity Lab
Parallelspace Corporation
October 11, 2019



TDA Application Host (TDH)

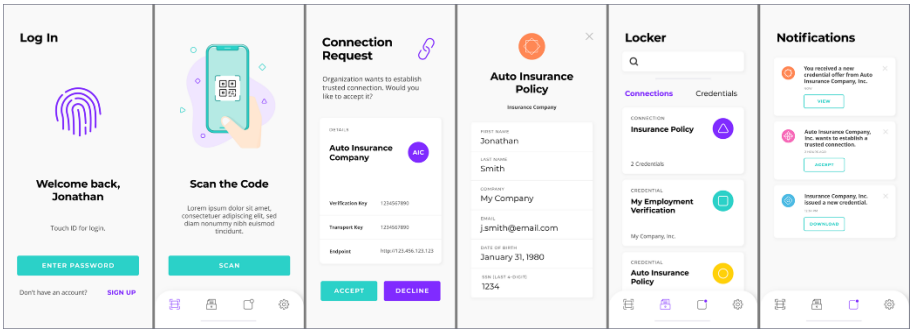
The Trust Digital Assistant Application Host (TDH) (or Network Browser) is the Trusted Digital Web's software equivalent to a web browser used to access content and applications on the World Wide Web.

The TDH is the user experience that citizens of the Trusted Digital Web use to download, load, and execute Trust-Based Applications (TBA). The TDH includes a default Browser TBA that citizens can use to surf verifiably trusted (as well as non-verifiable) content and applications on the Trusted Digital Web (access using the Trusted Digital Web Network.

Sample Trust-Based Application

The following figure is an example of 6 screens from a Trusted-Based App concept application (a live mockup). The screenshots are from the Streetcred Digital ID project (https://streetcred.id/digital-wallet/). They illustrate 6 types of interactions with the Streetcred Digital Wallet which is an example of a trust-based application host includes interacting with:

- (Verifiable) digital identities
- Agent-to-agent connections
- Credentials
- Subledgers
- Notifications
- Network communications

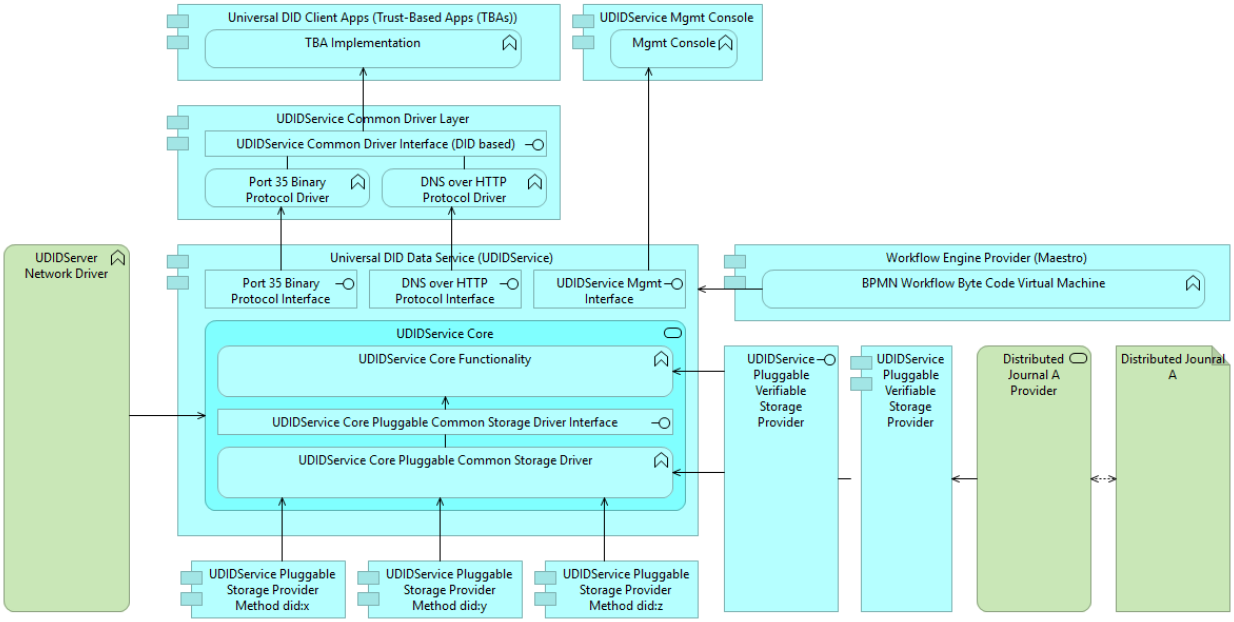


Universal DID Data Service (UDIDService)

The heart and brain of the entire platform is the Universal DID Data Service (depicted below).

Universal DID Data Service (UDIDService) Logical Architecture 0.8

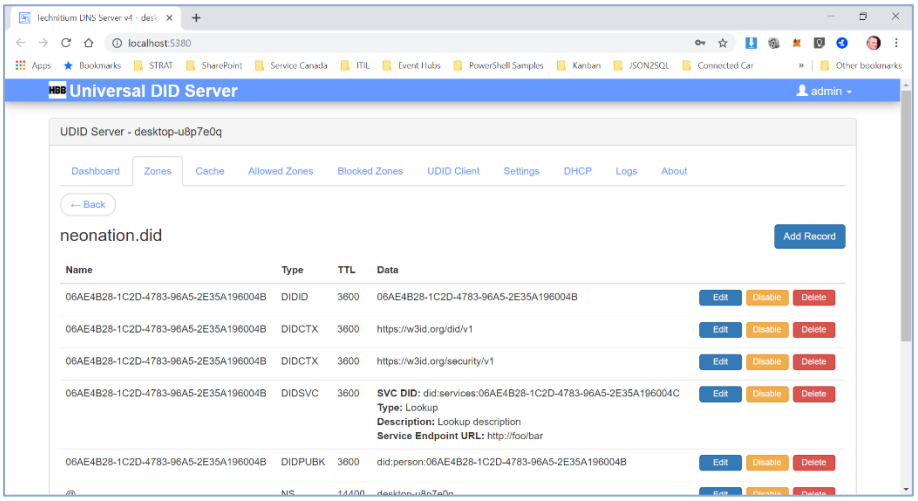
Michael Herman
Self-Sovereign Blockchain Architect
Hyperonomy Digital Identity Lab
Parallelspace Corporation
October 11, 2019



The UDIDService is responsible for implementing the following functionality:

- Verifiable and non-verifiable credential creation and lifecycle management
- Credential storage and retrieval
- Data notarization and verification
- DNS-compatible binary and DNS-over-HTTP protocol services
- Agent-to-agent network communications services
- UDIDService management console
- Workflow (business process) engine hosting and execution

The current version of the UDIDService management console is illustrated in the following diagram. In the screenshot, a credential comprised of 5 claims (name-value pairs) associated with the GUID-based identifier in the `neonation.did` DID Method space is shown.

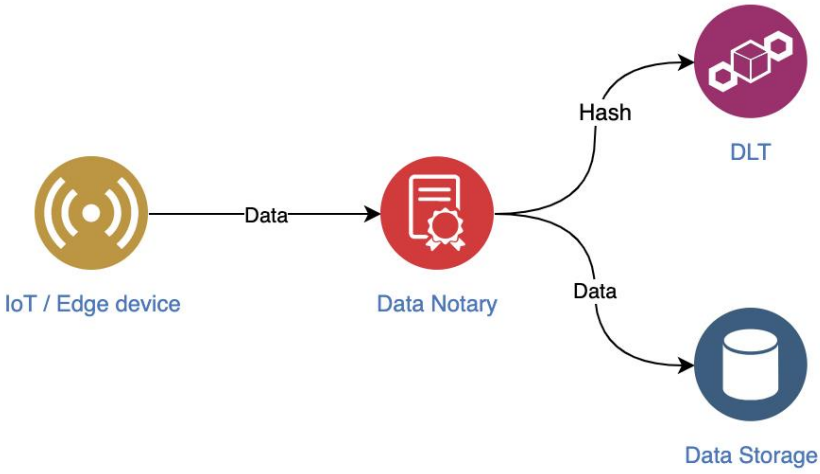


Universal Data Notarization Service (UDID Data Notary, UDN)

Subtly, the UDN, over time, will likely prove to be the most important capability supported by the UDIDService; that is, the ability to digitally sign and verifiably store a reference to any data stored in any data store in such a way to make the data items:

- Universally verifiable regardless of where the data is stored
- Allow data to still be accessed using native protocols regardless of the application (e.g. machine learning, artificial intelligence, real-time business analytics, etc.)

The following is a specific illustration of this capability from Medium article Data Notarization with DLT (https://medium.com/dac-technology-blog/data-notarization-with-dlt-f19df2295929).

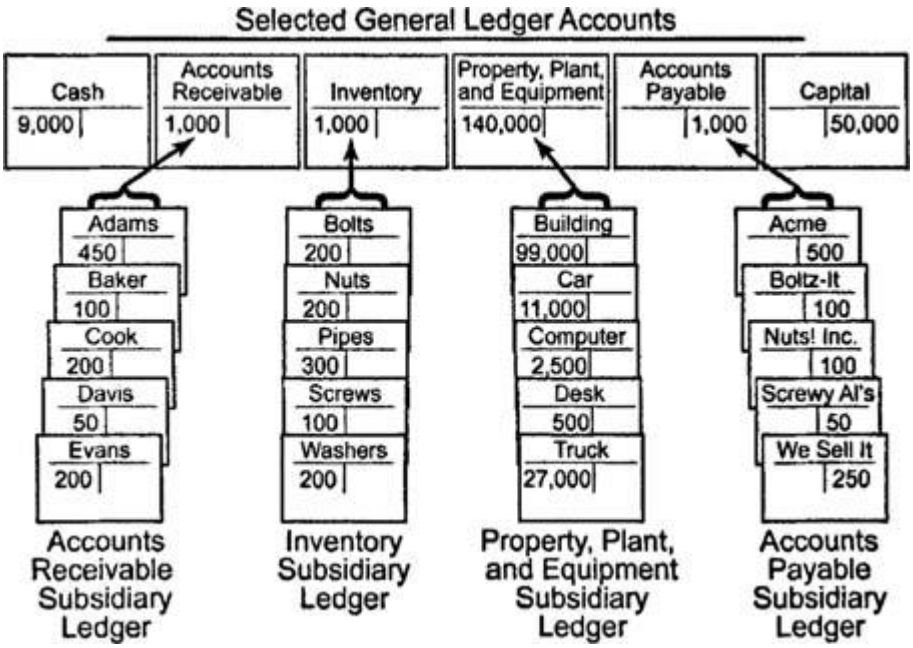


Subsidiary Ledger (Subledger) Persistable Storage

While most practitioners will be familiar or comfortable with the concept of a person or organization having a single digital identity, this is actually not very realistic – especially when you consider everything you own (or have control over) will have a digital identity (in addition to the multiple digital identities you yourself will own and control). A single person will own or control millions of things over their lifetime. An organization will interact with millions of identities in a day; or perhaps, in a single hour.

To support these kinds of requirements, the Trusted Digital Web Platform (and the Persistable Storage component, in particular) supports the Accounting profession's concept of *subsidiary ledgers* (or *subledgers*).

> *A subsidiary ledger is a group of similar accounts whose combined balances equal the balance in a specific general ledger account. The general ledger account that summarizes a subsidiary ledger's account balances is called a control account or master account. For example, an accounts receivable subsidiary ledger (customers' subsidiary ledger) includes a separate account for each customer who makes credit purchases. The combined balance of every account in this subsidiary ledger equals the balance of accounts receivable in the general ledger.*
>
> Subsidiary Ledgers (https://www.cliffsnotes.com/study-guides/accounting/accounting-principles-i/subsidiary-ledgers-and-special-journals/subsidiary-ledgers).



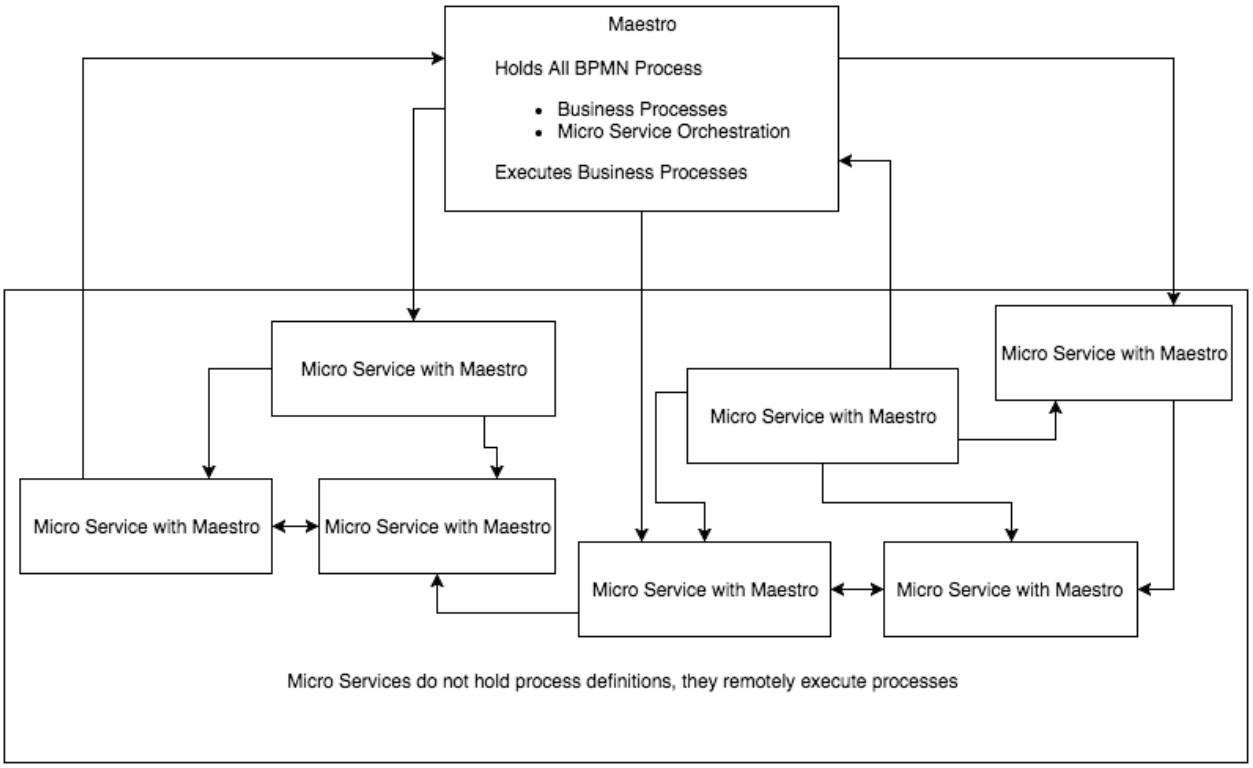
UDIDService Workflow (Business Process) Engine

The UDIDService Workflow (Business Process) Engine needs to satisfy several of the solution requirements; notably:

- BPMN standard compliant for business process model execution

- Implemented in C# and .NET Core
- Compact and efficient
- Easily adaptable and integratable with other components of the Trusted Digital Web Platform

The Maestro project (https://github.com/monirith/maestro) meets all of these requirements. The Maestro multi-threaded process architecture is illustrated below.



Additional Software Components

The additional software components, components that support but aren't components that are an active part of the Trusted Digital Web Network, include:

- Camunda Modeler
- Stratis Platform

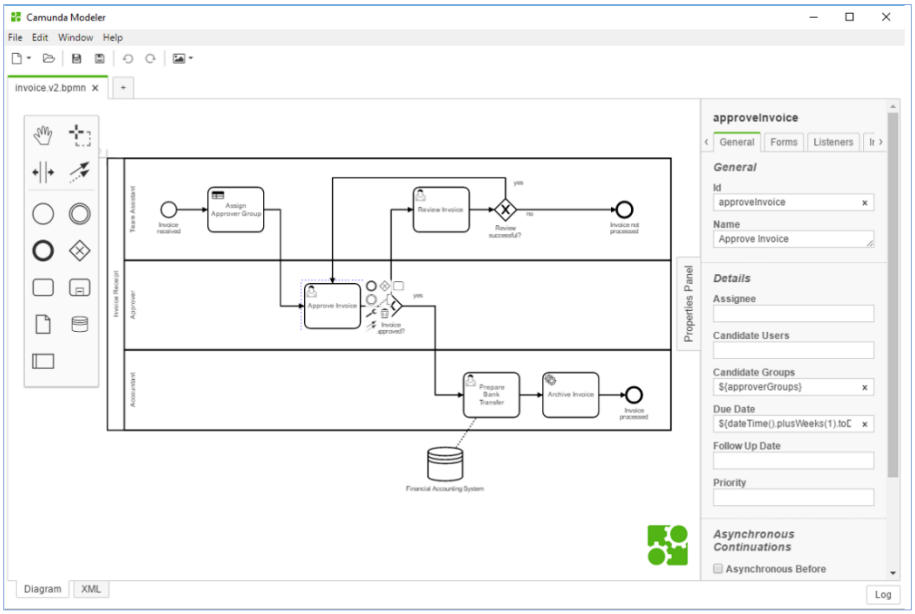
Camunda Modeler

Camunda Modeler is a developer-friendly desktop application for modeling BPMN workflows and DMN decisions. It's user-friendly, allowing multiple developers to work together on the same diagrams.

[Camunda Modeler (https://camunda.com/products/modeler/)

Camunda Modeler is the open-source BPMN workflow and business process modeler for designing workflow and business process models (templates) and persisting them using the industry-standard BPMN XML exchange format.

The Trusted Digital Web Platform provides an additional tool, the TDA BPMN Template Compiler for transcompiling BPMN XML workflow templates into the TDA Workflow Engine Byte Code format for execution inside the TDA Workflow Engine of each and every Trusted Digital Assistant in the Trusted Digital Web Network.



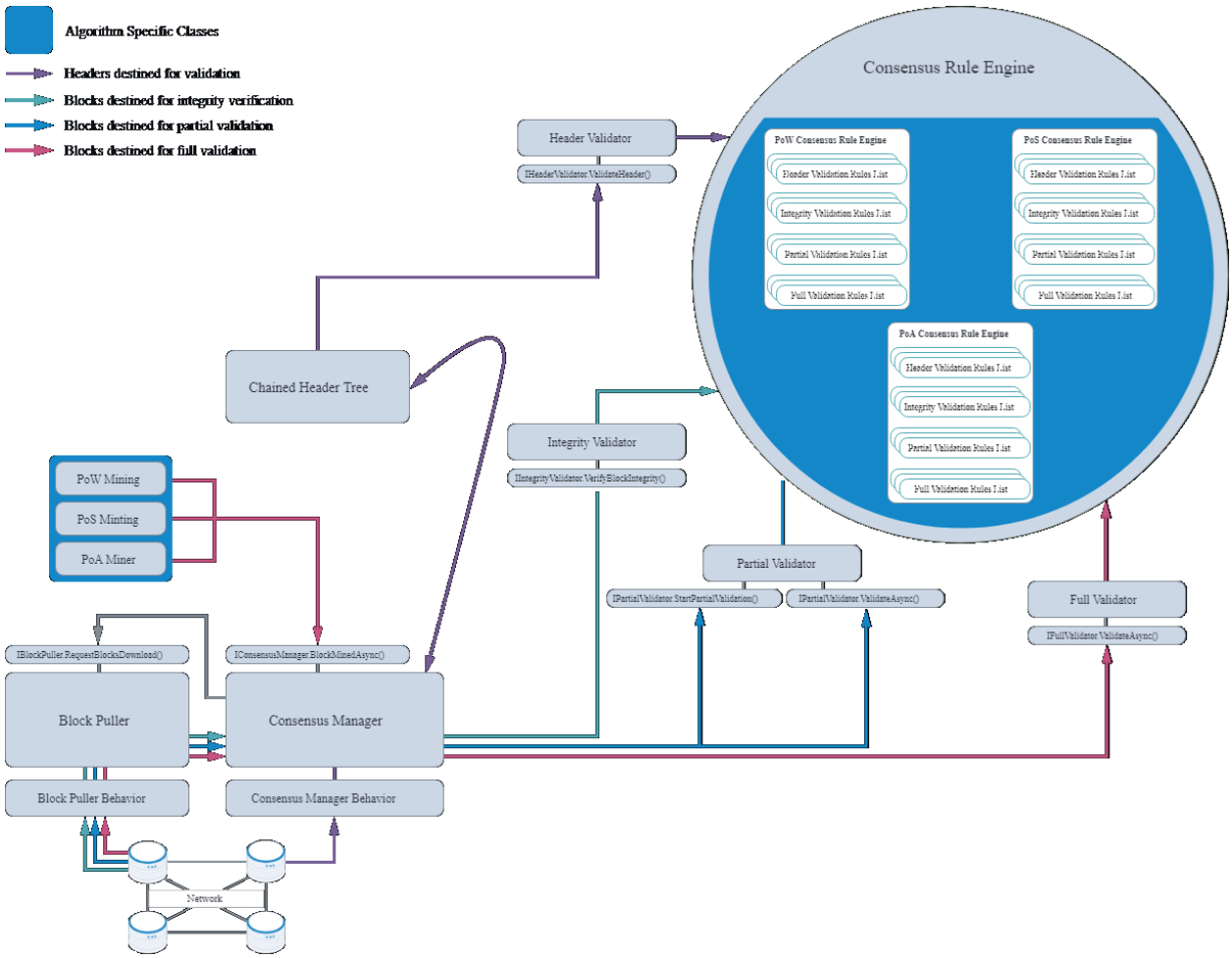
Stratis Platform

The Stratis Platform is a general-purpose, smart contract-enabled blockchain platform developed using C# and the .NET Core platform. The primary functional component of a Stratis Platform deployment is the Stratis Full Node.

> *The Stratis Full Node is the backbone of the Stratis Platform. It implements both the STRAT and BTC protocol and maintains an up-to-date copy of the STRAT and BTC blockchains. Because of this, Full Nodes can:*
>
> - *Autonomously and authoritatively validate blocks and transactions.*
> - *Serve blocks and transactions to other peers on the STRAT or BTC blockchain networks.*
>
> *The Full Node is open source software and is built in C# using the .NET Core platform. The design of the Full Node is modular and several of its features can be included or excluded from a build depending on requirements.*
>
> *The Full Node is open source, and you can find the source here on GitHub: https://github.com/stratisproject/StratisBitcoinFullNode.*

[Stratis Full Node (https://academy.stratisplatform.com/FullNode/full-node-introduction.html)]

In addition, all smart contract development on the Stratis Platform also uses C# and a very restricted subset of .NET Core.



[Stratis Full Node Consensus Architecture (https://academy.stratisplatform.com/FullNode/Consensus/consensus-architecture.html)]

Platform Standards and Specifications

Another cornerstone of the Trusted Digital Web Platform is its adoption (and in some cases, extension) of the prevailing industry standards and specifications where applicable.

Project Standards

The Trusted Digital Web Project depends on a broad collection of international specifications (as well as required extensions to some of these specifications).

- DNS (https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4, https://en.wikipedia.org/wiki/Domain_Name_System)
    - Plus local UDIDService Resource Record extensions
- did-spec (https://w3c-ccg.github.io/did-spec/)
    - Plus local Universal Digital Identifier extensions
- BPMN (http://www.bpmn.org/, https://en.wikipedia.org/wiki/Business_Process_Model_and_Notation)
- UBL (http://docs.oasis-open.org/ubl/UBL-2.2.html,)

    - Plus local UUBL project extensions (https://hyperonomy.com/2018/12/06/refactoring-ubl-2-2-business-documents-for-enacting-business-processes-on-the-blockchain-wip/)
- C# (https://github.com/dotnet/csharplang/tree/master/spec)
- .NET Core (https://github.com/dotnet/core)

Open Source Origins

The Trusted Digital Web Platform is the software platform on which the Trusted Digital Web is implemented. The Platform an extension and integration of the following open source projects.

- DnsServer (https://github.com/TechnitiumSoftware/DnsServer)
    - The DnsServer is extended to support additional DNS Resource Record types need to realize verifiable Universal Digital Identifiers and Digital Credentials
- TechnitiumLibrary (https://github.com/TechnitiumSoftware/TechnitiumLibrary)
    - Likewise, the TechnitiumLibrary is extended to support additional DNS Resource Record types need to realize verifiable Universal Digital Identifiers and Digital Credentials
- Maestro (https://github.com/monirith/maestro)
    - Maestro is extended to support the generation of Universal BPMN Byte Code that executes in the UDIDService Workflow Engine (which in turn is based on Maestro).
- StratisPlatform (https://github.com/stratisproject)
    - The StratisPlatform is the general-purpose, smart contract-enabled, blockchain platform used to support Universal Credential verification.
- SerentityData (https://github.com/mwherman2000/serentitydata)
    - SerentityData is a universal, dynamically configurable, byte-level data compaction technology used by decentralized applications (DApps) for more efficient storage of data on a blockchain.
- Camunda Modeler (https://camunda.com/products/modeler/)
    - BPMN standard-based workflow and business process open-source modeling tool
- Chromium (https://www.chromium.org/Home)
    - Chromium is an open-source browser project that aims to build a safer, faster, and more stable way for all Internet users to experience the web. Chromium is used by Google Chrome and later releases of Microsoft Edge.
- CefSharp (http://cefsharp.github.io/)
    - CefSharp is the easiest way to embed a full-featured standards-compliant web browser (Chromium) into your C# or VB.NET app.

The entire Trusted Digital Web Platform is released under the MIT open source license (for more details, see Appendix F – MIT License on page 68).

The Trusted Digital Web Platform is heavily biased towards the author's experience and comfort with the C# and .NET Core software platform. All of the above open-source projects are based on (or have been converted to) C# and .NET Core.

WHERE DO WE GO FROM HERE?

[Strategists] need to 'think in time' linking an organization's past, present, and future in their thought processes. There are three components:

- *the predictive value of the past for the future;*
- *departures from the past which divert the organization from familiar patterns;*
- *the need for continuous comparison*

Jeanne Liedtaka in *The Business of Giving: The Theory and Practice of Philanthropy, Grantmaking and Social Investment* (https://www.amazon.ca/Business-Giving-Philanthropy-Grantmaking-Investment/dp/0230336795/ref=sr_1_1)

Current Status

The current status of the Trusted Digital Web Project is that a functioning proof-of-concept Universal DID Data Service is up and running at the Hyperonomy Digital Identity Lab. The UDIDService supports a

majority of the DNS Resource Record types need to fully represent a verifiable DID Document as well as any other verifiable Credential (of which DID Document is only a subset).

Key components that remain to be implemented include:

- Universal Data Notarization Service (UDID Notary)
- Trusted Digital Assistance (plus supporting infrastructure)

Divergence

The Trusted Digital Web represents a strategic direction for building a universal, trusted, frictionless, integrated, standards-based, general-purpose, end-to-end platform for global commerce, communication, and collaboration.

The author is not aware of any similar comprehensive effort to remake the World Wide Web into a trusted platform for global commerce, communication, and collaboration. That being said there are corners of the platform that diverge from related efforts; particularly in the domain of verifiable digital identity. More notable is the divergence between the concepts of Universal Digital Identifiers and Universal Digital Identities and those espoused in the Decentralized Identifiers (DIDs) v0.13 Data Model and Syntaxes: Final Community Group Report 13 August 2019 (https://w3c-ccg.github.io/did-spec/), the *did-spec*. The did-spec is a useful starting point for describing a particular and narrow classification of digital identifiers but falls short of serving as a specification for all data items in the universe of data.

In addition, the did-spec (and companion Decentralized Identifier Resolution: Draft Community Group Report (https://w3c-ccg.github.io/did-resolution/), the *did-resolution* report, seek to define a set of brand-new protocols for credential creation, retrieval, and updating that have never seen the inside of a production data center, neither on-premise or cloud-based.

Universal Digital Identifiers, Digital Identities, and Digital Credentials leverage the syntax of the did-spec and seek to apply it universally for naming all data items on the planet, and, in fact, in the universe; some of which may be verifiable and some of which may have no need to be fully verifiable.

In addition, the UDIDService leverages existing, common, every-day DNS (Domain Name Service) protocols and existing DNS open-source software implementations (for example, *DnsServer* and *BIND*) for its implementation and deployment – software and protocols that are already in use on every computer on the planet.

Technology Adoption Models

Careful consideration must be given to how a new platform as different and as important as the Trusted Digital Web is to the future of the Internet. Deployment and adoption are expected to be gradual and slow – full adoption taking place over a decade and possibly multiple decades. This is the expected duration based on the development and usage of the Internet global communications network and the World Wide Web distributed applications that run on top of it.

The origins of the Internet date back to the 1960s (https://en.wikipedia.org/wiki/Internet); and the World Wide Web, the earlier 1990s (https://en.wikipedia.org/wiki/World_Wide_Web) – 60 years ago and 30 years ago, respectively.

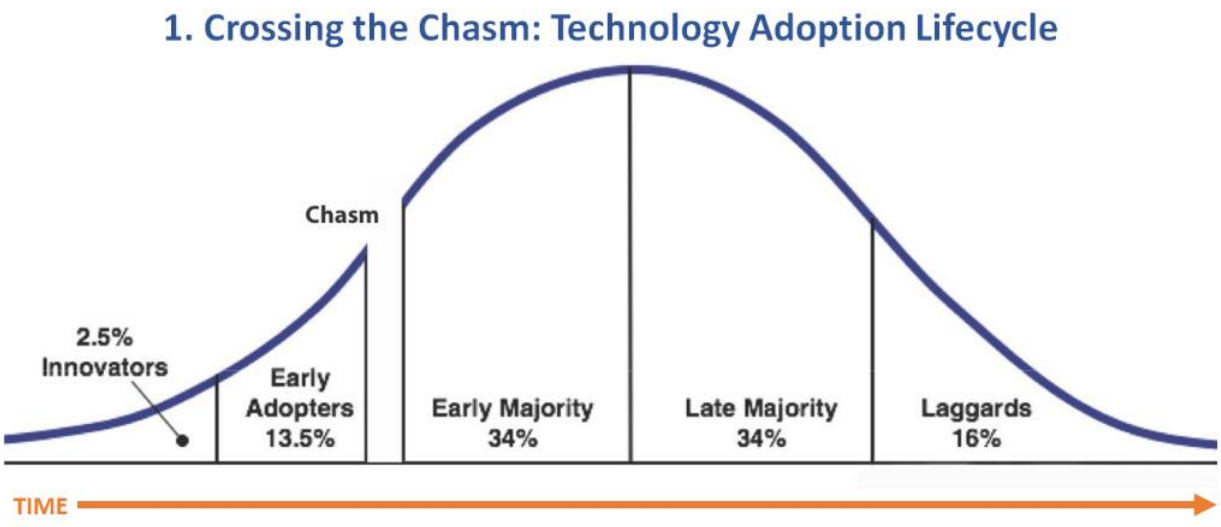
A brief survey and discussion of a small number of technology adoption models taken from the article Technology Adoption Models: A Comprehensive Guide is applicable (https://hyperonomy.com/2019/10/16/technology-adoption-models/). These include

- 1. Crossing the Chasm: Technology Adoption Model
- 10. Technology Adoption Model illuminated by the Gartner Hype Cycle
- 19. Exponential Growth Model
- 20. Exponential Growth Model coupled with the Gartner Hype Cycle
- 2. Social Evolution: Creation of a Nation State

NOTE: To survey a comprehensive list of technology adoption models, check out the article Technology Adoption Models: A Comprehensive Guide (https://hyperonomy.com/2019/10/16/technology-adoption-models/).

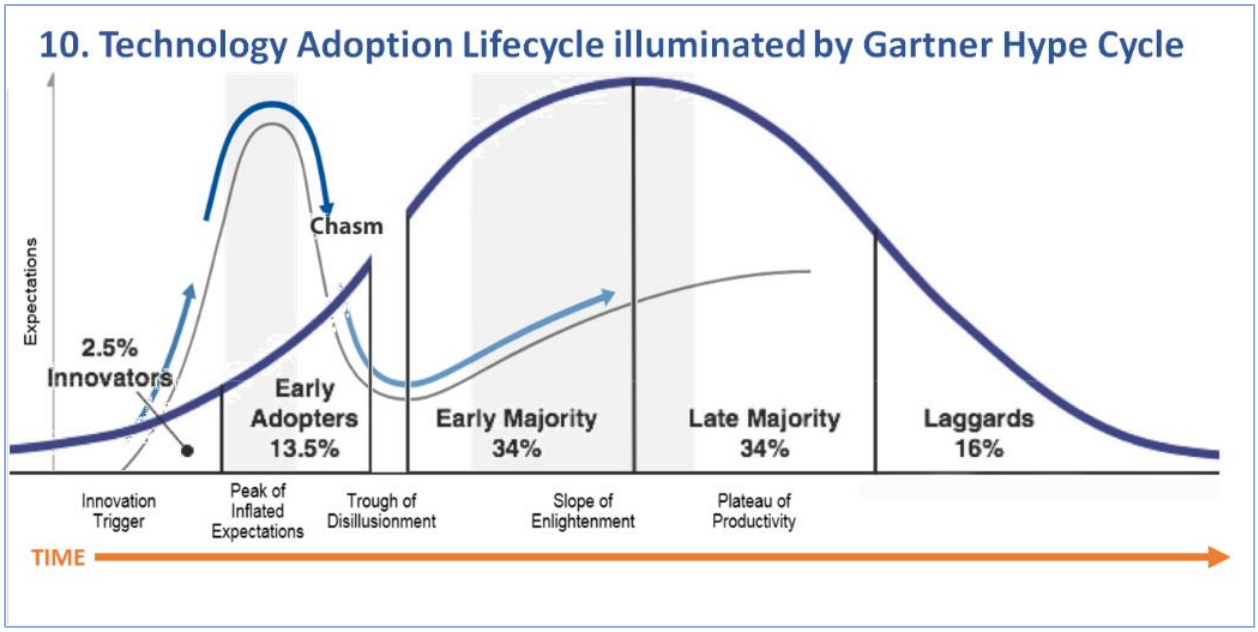
Crossing the Chasm: Technology Adoption Model

Many people will be familiar with one of the original technology adoption models: The Technology Adoption Model. The Technology Adoption Model was originally described in the book *Crossing the Chasm, 3rd Edition: Marketing and Selling Disruptive Products to Mainstream Customers* (https://www.amazon.ca/Crossing-Chasm-3rd-Disruptive-Mainstream/dp/0062292986/ref=sr_1_1) and is depicted in the diagram below.

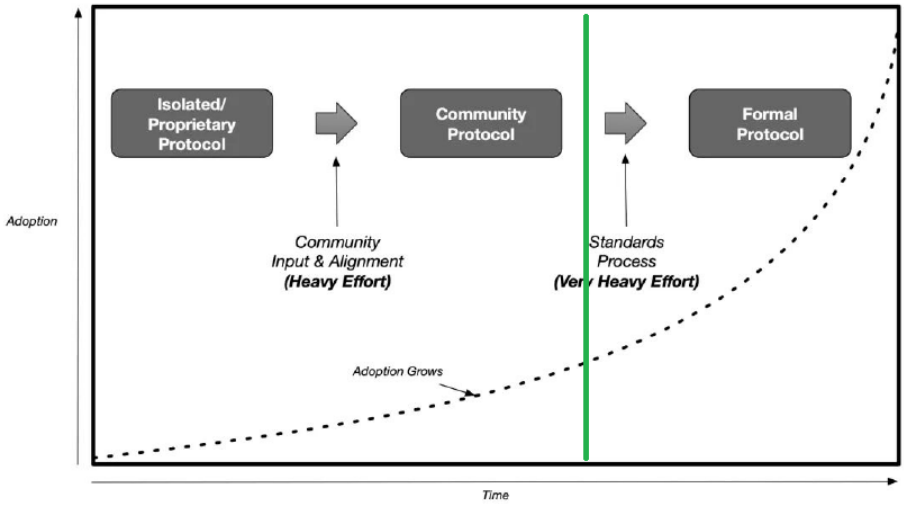


While the Technology Adoption Lifecycle model depicted above is useful when explaining the need for a conservative, phased approach when introducing a new product or technology platform (in particular, a novel one), the model, while simplistic, does highlight where a project needs to start (at the left) and where most projects fail when they fail to only excite the Innovators and Early Adopters (at the Chasm).

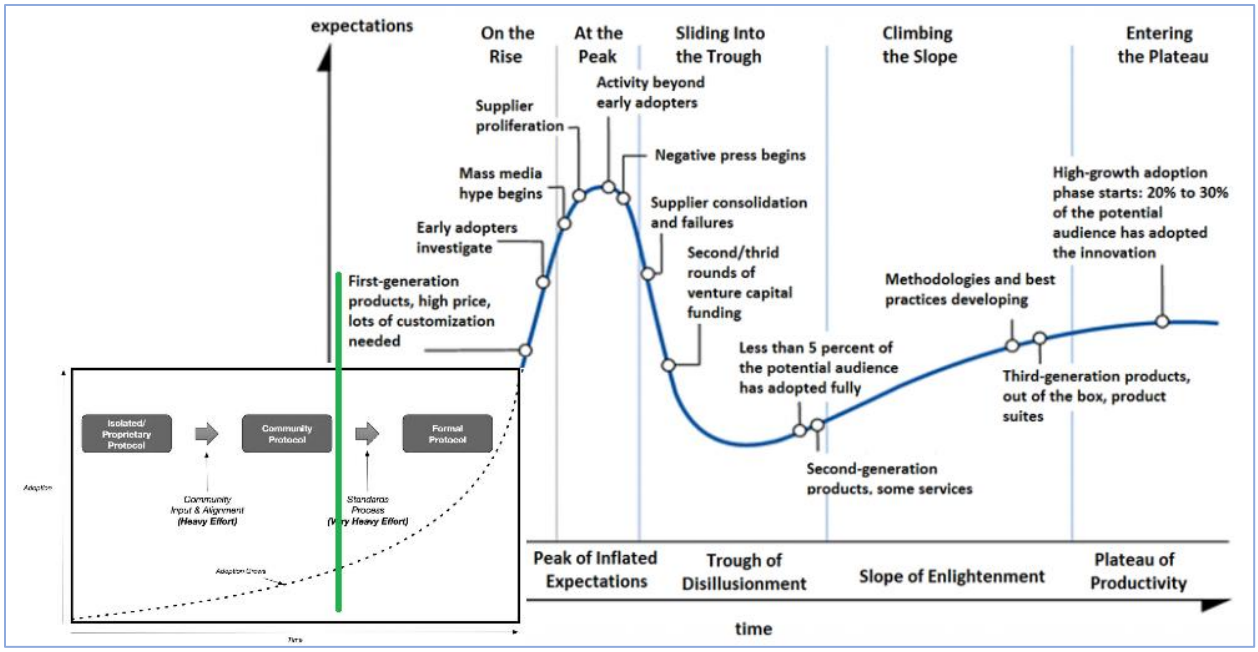
A more interesting model results when the Technology Adoption Model is overlaid with the Gartner Hype Cycle. The Hyper Cycle serves as a first derivative acceleration/deceleration curve (from Calculus). It illustrates what's happening "behind the scenes" by means of the Peak of Inflated Expectations and Trough of Disillusionment phases of the Cycle.



Another fallacy is the adoption of new products and services often takes place at an exponential pace (exponential growth) as depicted in the diagram below taken from a recent industry report of digital wallets.



Again, it's instructive to position an early-market exponential growth in the context of the Gartner Hype Cycle as shown below.



Exponential growth by early market participants (i.e. unicorns) is often accompanied by a great deal of promotion (hype) until, again, the Peak of Inflated Expectations is reached and the market caves in on itself. Eventually, if the technology is able to demonstrate ongoing promise and represents a true value differentiator relative to what is being used to solve a similar set of problems today, then the technology may be able to cross the Trough of Disillusionment and over to the lands of Enlightenment and Productivity.

Why does all this matter? How does it apply to blockchain (distributed journal) technologies and platforms?

The answer to the above questions lies in the fact that blockchain technologies and platforms combine not only Internet-scale software technologies but also global societal and financial impacts.

Social Evolution: Creation of a Nation State

> *When you talk about blockchain, you need to use two hands: in the left hand are the Internet-scale software technologies and platforms; and in the right, the social philosophies and "religious views" that go along with the platforms.*
>
> [Michael Herman: https://www.linkedin.com/in/mwherman/]

One of the author's early experiences with blockchain was being part of the NEO Blockchain (https://neo.org/) community during the time when voting (and several forms of voting) were under discussion about how to limit the number of NEO blockchain nodes that would serve in the role of Consensus Node.

Voting is most often conceived as a straight forward process: a list of candidates is presented and you vote for the one you prefer the most based on whatever your personal criteria are. But there is literally a world of variations when it comes to voting:

- Ranked Voting (https://en.wikipedia.org/wiki/Ranked_voting)

- Schulze method (https://en.wikipedia.org/wiki/Schulze_method)

What this discussion did bring to the surface is the need to define a number of basic concepts; for example:

- Who gets to vote?
- What do you call those people who are allowed to vote? (Hint: citizens)
- If they are citizens, what is the pathway to citizenship?

It then begins to sound like we beginning to create a new society or more than that, a new nation state. If so, there are additional requirements:

1. Where do we start?
2. How do we start?
3. How many people are involved or does it take to create a new society?
4. Do we simply create a new "society" or is there some other (simpler) structure or collective that precedes the creation of a new society (and a nation state)?
5. Which historical examples can we use for inspiration/guidance?
6. What should the founding principles for the new society/nation state look like?
7. What other additional founding documents are needed or required?

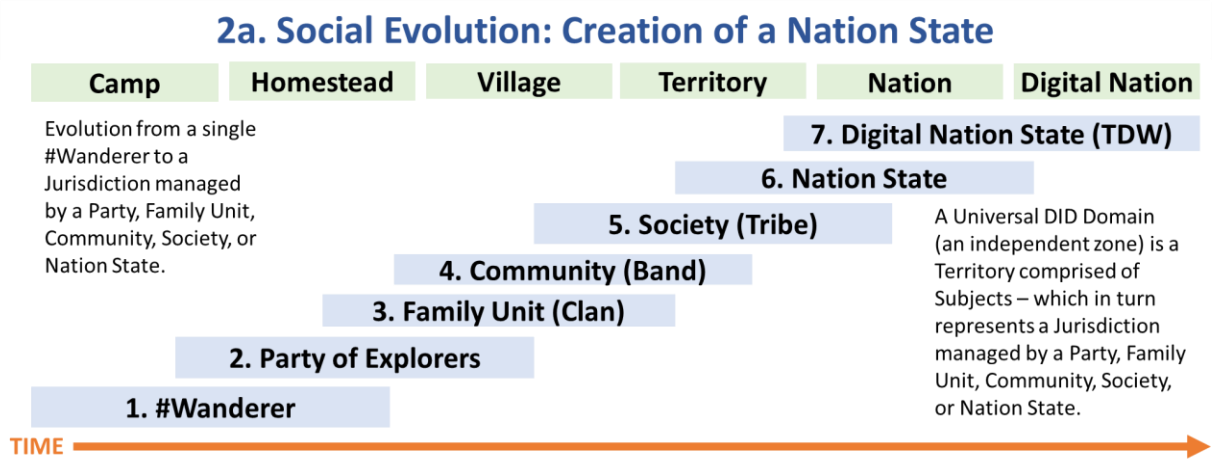
Examples from history include:

- The founding of the United States of America: Declaration of Independence, Constitution
- The founding of the European Union: The Treaties
- The founding of Liberland (https://liberland.org/en/)

Question 4

4. Do we simply create a new "society" or is there some other (simpler) structure or collective that precedes the creation of a new society (and a nation state)?

Several sources including the book *Who we are and how we come here* (https://en.wikipedia.org/wiki/Who_We_Are_and_How_We_Got_Here) and the National Geographic publication *National Geographic Atlas of the Ancient World: Exploring Great Civilizations* (https://www.amazon.ca/National-Geographic-Atlas-Ancient-World/dp/1683306759) suggest that, in terms of the history of the *peopling of the earth*, there was both continuous migration as well as evolution of the world's social structures. The author has summarized these ideas in the following diagram.



Each of the increasingly more complex social units is described in the following table.

Social Unit	Principle Demonstrated	Description
1. Wanderer	Independence	Someone who leaves their [old] tribe to share their knowledge and wisdom with others.
2. Party of Explorers	Collaboration	The situation where two or more people work together to explore and conquer a common set of goals.
3. Family Unit (Clan)	Family	A social group traditionally consisting of parents and children plus extended family members: grandparents, aunts, uncles, and cousins.
4. Community (Band)	Belonging	A group of people with a common characteristic or interest living together within a larger society.
5. Society (Tribe)	Structure	A tribe is a group of people who live and work together. A tribal society is a group of tribes organized around kinships. Tribes represent a part of the social evolution between bands and nations. A tribe can be a collection of families or families and individual people living together.
6. Nation State	Citizenship	The status of a person recognized under the custom or law as being a legal member of a sovereign state or belonging to a nation.
7. Digital Nation State	Digital Trust	

For comparison purposes, a band is a small, egalitarian, kin-based group of perhaps 10–50 people, while a tribe comprised a number of bands that were politically integrated (often through a council of elders or other leaders) and shared a language, religious beliefs, and other aspects of culture.

World Wide Web

Based on several criteria, the World Wide Web (WWW) was birthed and grew using a similar model of social evolution. However, the users of the WWW never progressed as far as becoming a nation state or, for that matter, even a society. The primary reason for this is the presence of large corporations who intervened to commercialize what was taking place at the community level of social evolution.

The following timeline highlights the key developments of the WWW during its initial 10 years. The bar at the bottom of the graphic denotes the number of web servers that were connected, year-by-year, to the Internet global communications network.

Economic Model

The economic model for the Trusted Digital Web is expected to be one to two orders of magnitude cheaper than the nearest comparable credential network.

Comparable Credential Network Fees

The most comparable existing fee model for the creation of new ledger-based decentralized, identifiers, identities, schemas and/or other credentials is provided by the Sovrin Foundation for their implementation of the Sovrin Network and Ledger (https://sovrin.org/issue-credentials/). See below.

Item	Price
DID Write	$10
Schema	$50
Credential Definition	$25
Revocation Registry	$20
Revocation Update	$0.10

**Fees table current as of March 14, 2019 and are subject to change based on advice from the Sovrin Economic Advisory Council.*

Universal Credentials, Tokens, and Gumballs

On the Trusted Digital Web, every little thing (#ELT) is a Credential associated with a Universal Digital Identifier:

- DID Documents

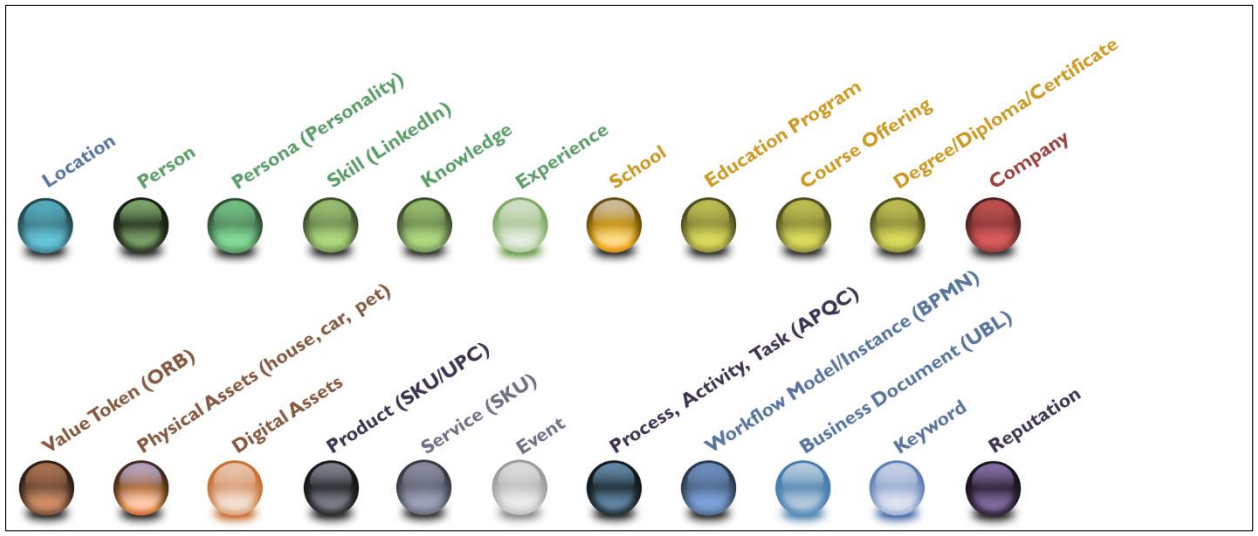
- Verifiable Credentials
- Non-Verifiable Credentials
- Schema Definitions
- Business Documents
- Web Pages
- Images
- etc.

Collectively, these are referred to as Universal Digital Credentials – of which there are two categories: verifiable and non-verifiable.

The fee structure is greatly simplified:

- $0.10 for small credentials (up to 1 kilobyte of data)
- $0.25 for medium-sized credentials (more than 1 kilobyte of data up to 5 kilobytes of data)
- $0.50 for large credentials (more than 5 kilobytes of data up to 10 kilobytes of data)
- $1.00 for extra-large credentials (more than 10 kilobytes of data up to 25 kilobytes of data)

Plus $1.00 if the data item is to be registered on the distributed ledger as a verifiable credential. Some of the types of data items (credentials) that can be created, retrieved, and updated on the Trusted Digital Web are shown in the following diagram. In the Trusted Digital Web economic model, these are referred to as *gumballs* to avoid confusing with other types of tokens and cryptocurrencies backed by distributed ledger technology (DLT). The creation of a verifiable credential will be more expensive than the creation of a non-verifiable credential.



NEXT STEPS

Finally, strategic thinking is intelligently opportunistic. The organization whilst following a particular strategy should not lose sight of alternative strategies that may be more appropriate for a changing environment.

Jeanne Liedtaka in *The Business of Giving: The Theory and Practice of Philanthropy, Grantmaking and Social Investment* (https://www.amazon.ca/Business-Giving-Philanthropy-Grantmaking-Investment/dp/0230336795/ref=sr_1_1)

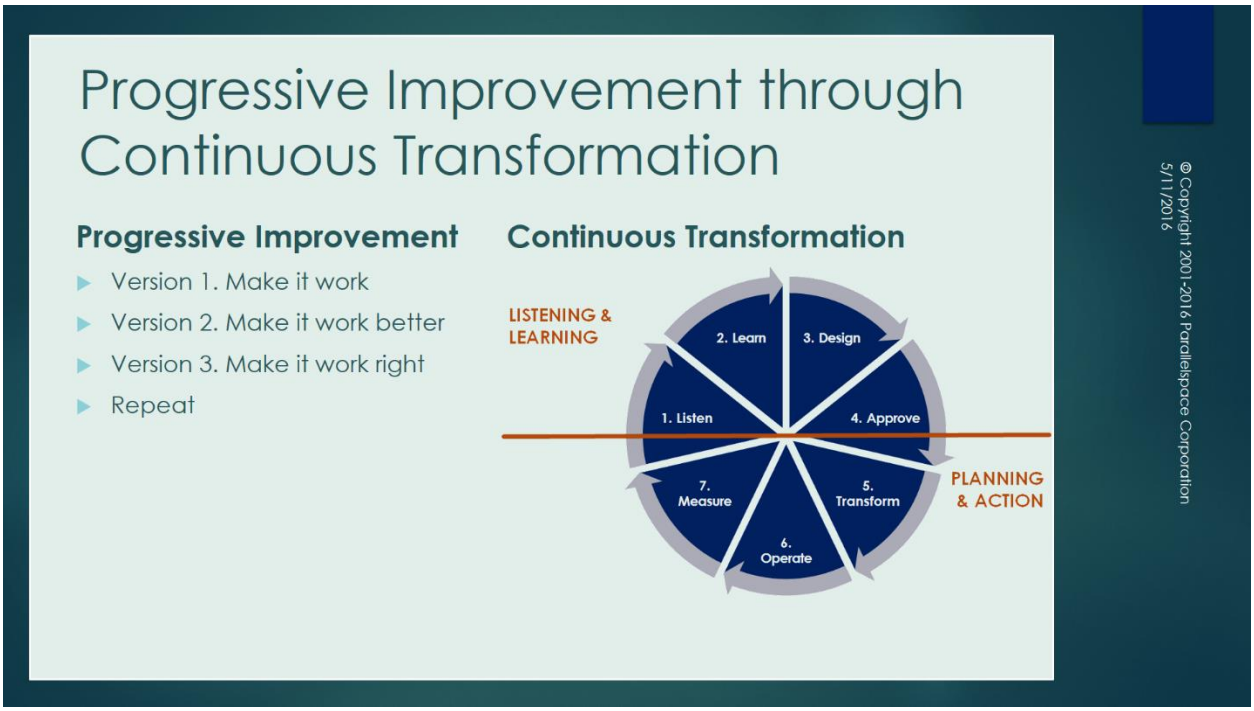
The World Wide Web as a Benchmark

In the first year of operation, the World Wide Web (WWW) started 1 web server. Going into its second year of operation, there were 10 servers; third year, 50 servers; the fourth year, over 600.

If the goal of the Trusted Digital Web is to initially co-exist and then subsequently supersede the WWW in terms of the volume of business transacted, then a good initial starting measure is the number of Trusted Digital Assistants deployed in the (serverless) Trusted Digital Web Network (TDN). Ideally, some measure of the transactions executed on the Trusted Digital Web (TDW) is warranted. Ultimately, an additional means of measuring the volume of transactions transacted on the TDW relative to an estimate of the total number of transactions executed on the planet is required.

Progressive Improvement through Continuous Transformation

How are we going to get there? The answer is progressive improvement through continuous transformation – as depicted below.



[How we think about how we work (https://hyperonomy.com/2016/05/09/how-do-we-think-about-how-we-work/)]

This whitepaper is the first attempt to describe the Trusted Digital Web in its entirety – both its motivations as well as a reasonable description of the complete, integrated solution. Full deployment will take decades – the same basic timeframe that it took the World Wide Web to develop into its current state. A key advantage of the Trusted Digital Web is that it builds directly on top of existing Internet technologies, international standards (and specifications), and many open-source realizations of these technologies and standards.

Objectives

What are the objectives and benchmarks for the Trusted Digital Web for the next few years? From a benchmarking perspective, the goal is simple: surpass the initial growth rate of the World Wide Web. Here is a list of the initial set of objectives:

- 2020: Deploy a Trusted Digital Web Network consisting of two (2) Trusted Digital Assistants (TDAs) being able to serve and render multiple DID-addressed, verifiable, HTML pages containing multiple DID-addressed, verifiable images.
- 2021: Grow the Trusted Digital Web Network to include ten (10) or more Trusted Digital Assistants (TDAs) being able to serve and render multiple, DID-addressed, verifiable HTML pages containing multiple DID-addressed, verifiable images (including this whitepaper).
- 2020-2021: Enable the first UUBL Document exchange as a collection of verifiable credentials on the TDW Network.
- 2020-2021: Demonstrate the Gumball protocol's ability to frictionlessly execute a multi-organization business process that involves a purchase request, payment, payment receipt, loyalty points, and reputation points. [This scenario was first suggested by Grace Rachmany (https://www.linkedin.com/in/rebeccarachmany/) during a 2018 conference call.]

CONCLUSIONS

If I have seen further, it is by standing on the shoulders of Giants.

[Issac Newton, 1675]

The above quotation is absolutely true when describing the gestation of the Trusted Digital Web. This project represents, in many respects, the sum total of the author's 45 years of experience in software development, 15+ years working as a communications and collaboration consultant at Microsoft and then at Parallelspace Corporation - plus more recent experience as an enterprise architect and business process analyst at BizzDesign and as a blockchain solution architect and developer using the Ethereum, NEO and Stratis Platform blockchain platforms.

As highlighted above, the birth of the Trusted Digital Web is only enabled through its adoption of prevailing Internet concepts, technologies, and protocols (notably DNS), several international specifications and standards (most notably BPMN) and lastly, the universal application of digital identifiers and digital identities to all non-fungible entities.

APPENDICES

APPENDIX A – INTERNET DOMAIN NAME SERVICE (DNS) OVERVIEW

The following is an overview of the Domain Name Service (DNS), a key critical component of the Internet communications network. This overview is based on the contents of the article: DNS (Domain Name Service): A Detailed, High-level Overview [Michael Herman: https://hyperonomy.com/2019/01/02/dns-domain-name-service-a-detailed-high-level-overview/].

On the surface, most people understand DNS to be a service that you can pass a domain name to and have it resolved to an IP address (in the familiar `nnn.ooo.ppp.qqq` format).

domain name => `nnn.ooo.ppp.qqq`

Examples:

1. If you click on Google DNS Query for microsoft.com, you'll get a list of IP addresses associated with the Microsoft's corporate domain name microsoft.com.
2. If you click on Google DNS Query for www.microsoft.com, you'll get a list of IP addresses associated with Microsoft's corporate web site www.microsoft.com.

NOTE: The Google DNS Query page returns the DNS results in JSON format. This isn't particular or specific to DNS. It's just how the Google DNS Query page chooses to format and display the query results.

DNS is actually much more than a domain name to IP address mapping. DNS is an extensible name resolution framework and set of protocols for performing lookups of any name to a collection of any type of data - any collection of name-value pairs. This (and the fact that DNS servers and protocols have been

in everyday use by billions of computers around the world for several decades) makes DNS exceedingly well suited for managing any type of credential data (collections of name-value pairs).

DNS Resource Records

There is more to the DNS Service database than these simple (default) IP addresses. The DNS database stores and is able to return many different types of data (in addition to service-specific IP addresses) for a particular domain name. These data records are called DNS Resource Records. Here's a partial list of the most common resource record types from http://dns-record-viewer.online-domain-tools.com:

- Address Mapping records (A) - the default/common type (see the previous Examples)
- IP Version 6 Address records (AAAA) - a newer version of the above
- Canonical Name records (CNAME)
- Mail exchanger record (MX) - mail server IP address
- Name Server records (NS) - authoritative DNS server for this domain
- Reverse-lookup Pointer records (PTR)
- Start of Authority records (SOA)
- Text records (TXT)

Most APIs only support the retrieval of one Resource Record type at a time (which may return multiple records (e.g. IP addresses) of that type). Some APIs default to returning A records; while some APIs will only return A records. Caveat emptor.

To see a complete set of DNS Resource Records for microsoft.com, click on DNSQuery.org query results for microsoft.com and scroll down to the bottom of the results page ...to see the complete response (aka authoritative result). It will look something like this:

```
microsoft.com. 3600 IN TXT
"FbUF6DbkE+Aw1/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/rVQKJi8CjQbBtWtE64ey4NJJwj5J65PIggVYNabdQ=="
microsoft.com. 3600 IN TXT "adobe-sign-verification=c1fea9b4cdd4df0d5778517f29e0934"
microsoft.com. 3600 IN TXT "atlassian-domain-
verification=jbey7I2+3Wyl+PZ0QUCC6fCz2Gu5KO7GQPcy/0c4za7ebQxar/qqujJH4kZLVQHZ"
microsoft.com. 3600 IN TXT "docusign=52998482-393d-46f7-95d4-15ac6509bfdd"
microsoft.com. 3600 IN TXT "docusign=d5a3737c-c23c-4bd0-9095-d2ff621f2840"
microsoft.com. 3600 IN TXT "facebook-domain-verification=bcas5uzlvu0s3mrw139a00os3o66wr"
microsoft.com. 3600 IN TXT "facebook-domain-verification=gx5s19fp3o8acsby6a22clfhsm03as"
microsoft.com. 3600 IN TXT "facebook-domain-verification=m54hfscsreqq2s1pf99y2p0kpwwpkv"
microsoft.com. 3600 IN TXT "google-site-verification=6P08Ow5E-8Q0m6vQ7FMAqAYIDprkVV8fUf_7hZ4Qvc8"
microsoft.com. 3600 IN TXT "v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com
include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com
ip4:147.243.128.24 ip4:147.243.128.26 ip4:147.243.1.153 ip4:147.243.1.47 ip4:147.243.1.48 -all"
microsoft.com. 3600 IN SOA ns1.msft.net. msnhst.microsoft.com. (2018123101 7200 600 2419200 3600)
microsoft.com. 172800 IN NS ns1.msft.net.
microsoft.com. 172800 IN NS ns2.msft.net.
microsoft.com. 172800 IN NS ns3.msft.net.
microsoft.com. 172800 IN NS ns4.msft.net.
microsoft.com. 3600 IN MX 10 microsoft-com.mail.protection.outlook.com.
microsoft.com. 3600 IN A 104.215.148.63
microsoft.com. 3600 IN A 13.77.161.179
microsoft.com. 3600 IN A 40.112.72.205
microsoft.com. 3600 IN A 40.113.200.201
microsoft.com. 3600 IN A 40.76.4.15
;;Additional
ns1.msft.net. 300 IN AAAA 2620:0:30:0:0:0:0:53
ns2.msft.net. 172800 IN AAAA 2620:0:32:0:0:0:0:53
ns3.msft.net. 300 IN AAAA 2620:0:34:0:0:0:0:53
ns4.msft.net. 172800 IN AAAA 2620:0:37:0:0:0:0:53
ns1.msft.net. 300 IN A 208.84.0.53
ns2.msft.net. 172800 IN A 208.84.2.53
ns3.msft.net. 300 IN A 193.221.113.53
ns4.msft.net. 172800 IN A 208.76.45.53
```

Figure 1. DNS Resource Records for microsoft.com: Authoritative Result

NOTE: The Resource Record type is listed in the fourth column: TXT, SOA, NS, MX, A, AAAA, etc.

UPDATE: The complete list of allowable value ranges for RR (resource record) types (QTYPEs) can be found here: IANA: Resource Record (RR) TYPEs.

DNS Protocol

The most interesting new piece of information/learning is related to the DNS protocol itself. It's request/response ...nothing new here. It's entirely binary ...to be expected given its age and the state of technology at that time. Given how frequently DNS is used by every computer on the planet, the efficiency of a binary protocol also makes sense. The IETF published the original specifications in RFC 882 and RFC 883 in November 1983.

The interesting part of the protocol is that a DNS client typically doesn't "download" the entire authoritative set of DNS Resource Records all at once for a particular domain, the most common API approach is to request the list of relevant data (e.g. IP addresses) for a particular Resource Record type for a particular domain.

The format of a sample DNS request is illustrated in the following figure:

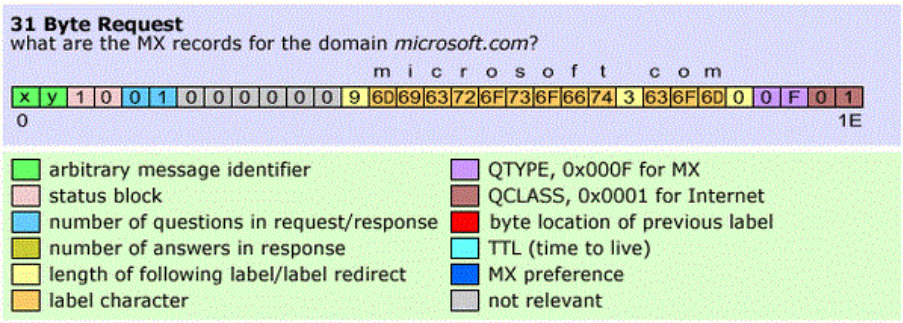


Figure 2. Sample DNS Request [CODEPROJECT]

It's binary. The QTYPE (purple cells on the right side) defines the type of query. In this case, 0x0F is a request for an MX record; hence, this is a request for the data that describes microsoft.com's external email server interface.

NOTE: The "relevant data" isn't always an IP address or a list of IP addresses. For example, the response may include another domain name, subdomain name, or, in some cases, simply some unstructured text (as far as the DNS specification is concerned).

Here is a typical response for the above sample request:

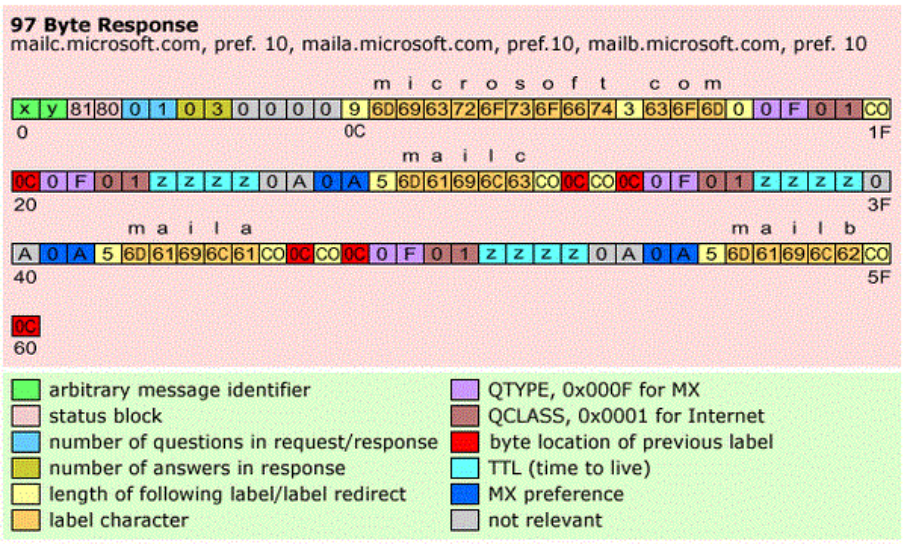


Figure 3. Sample DNS Response [CODEPROJECT]

The response, in turn, is also binary. In this case, DNS has responded with 3 answers; that is, 3 subdomain names: mailc, maila, and mailb - each with a numerical preference (weight).

ANY Resource Record Type

There is also a "meta" Resource Record Type called ANY that, as you might guess, requests a collection of all of the different Resource Record type records. This is illustrated in Figure 1 above.

DNS Extensibility

DNS is also a general-purpose, extensible framework and existing, accepted, deployed software platform and network for creating, managing, finding, and retrieving what are, in effect, *Credentials* associated with a *Universal* D*igital Identifiers (DID) (*aka hierarchical *domain name*). A credential, in turn, is a *set of Claims* where a claim is a name-value pair associated with the particular DID. Here are some examples.

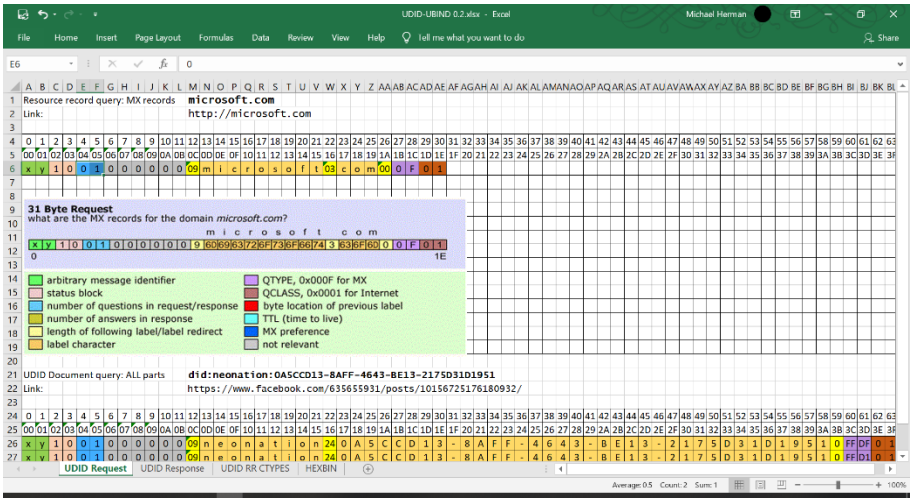


Figure 4. Universal Digital Identifier Example: DNS Binary Protocol

UDID Server - desktop-u8p7e0q

Dashboard | Zones | Cache | Allowed Zones | Blocked Zones | UDID Client | Settings | DHCP | Logs | About

← Back

neonation.did

Add Record

Name	Type	TTL	Data	
06AE4B28-1C2D-4783-96A5-2E35A196004B	DIDID	3600	06AE4B28-1C2D-4783-96A5-2E35A196004B	Edit Disable Delete
06AE4B28-1C2D-4783-96A5-2E35A196004B	DIDCTX	3600	https://w3id.org/did/v1	Edit Disable Delete
06AE4B28-1C2D-4783-96A5-2E35A196004B	DIDCTX	3600	https://w3id.org/security/v1	Edit Disable Delete
06AE4B28-1C2D-4783-96A5-2E35A196004B	DIDSVC	3600	**SVC DID:** did:services:06AE4B28-1C2D-4783-96A5-2E35A196004C **Type:** Lookup **Description:** Lookup description **Service Endpoint URL:** http://foo/bar	Edit Disable Delete
06AE4B28-1C2D-4783-96A5-2E35A196004B	DIDPUBK	3600	did:person:06AE4B28-1C2D-4783-96A5-2E35A196004B	Edit Disable Delete
neo1234	A	3600	1.2.3.4	Edit Disable Delete
@	A	3600	4.5.6.7	Edit Disable Delete
@	NS	14400	desktop-u8p7e0q	Edit Disable Delete
@	SOA	14400	**Master Name Server:** desktop-u8p7e0q **Responsible Person:** hostmaster.desktop-u8p7e0q **Serial:** 2019081522 **Refresh:** 28800 **Retry:** 7200 **Expire:** 604800 **Minimum:** 600	Edit Disable Delete
@	DIDTXT	3600	Some method level DID Data (metadata)	Edit Disable Delete

Figure 5. Universal Digital Identifier Example: UDID Credential (DID Document)


```
"Question": [
  {
    "Name": "0A5CCD13-8AFF-4643-BE13-2175D31D1951.sov.did",
    "Type": "ANY",
    "Class": "IN"
  }
],
"Answer": [
  {
    "Name": "0A5CCD13-8AFF-4643-BE13-2175D31D1951.sov.did",
    "Type": "DIDID",
    "Class": "IN",
    "TTL": "3600 (1 hour)",
    "RDLENGTH": "37 bytes",
    "RDATA": {
      "DIDIDData": "0A5CCD13-8AFF-4643-BE13-2175D31D1951"
    }
  },
  {
    "Name": "0A5CCD13-8AFF-4643-BE13-2175D31D1951.sov.did",
    "Type": "DIDCTX",
    "Class": "IN",
    "TTL": "3600 (1 hour)",
    "RDLENGTH": "24 bytes",
    "RDATA": {
      "DIDCTXData": "https://w3id.org/did/v1"
    }
  },
  {
    "Name": "0A5CCD13-8AFF-4643-BE13-2175D31D1951.sov.did",
    "Type": "DIDCTX",
    "Class": "IN",
```


Figure 6. Universal Digital Identifier Example: DNS over HTTP Response (Credential/DID Document)

APPENDIX B – PLATFORM DEFINITIONS

Trust and Distrust

Trust

Definitions of trust typically refer to a situation characterized by the following aspects:

- *one party (trustor) is willing to rely on the actions of another party (trustee); the situation is directed to the future.*

In addition, the trustor (voluntarily or forcedly) abandons control over the actions performed by the trustee. As a consequence, the trustor is uncertain about the outcome of the other's actions; they can only develop and evaluate expectations.

The uncertainty involves the risk of failure or harm to the trustor if the trustee will not behave as desired.

[Wikipedia: https://en.wikipedia.org/wiki/Trust_(social_science)]

Distrust

Noun

- *the feeling that someone or something cannot be relied upon.*
- *"his distrust of his mother's new suitor"*
- *synonyms: mistrust, suspicion, wariness, chariness, lack of trust, lack of confidence, lack of faith; skepticism, doubt, doubtfulness, dubiety, cynicism; misgivings, questioning, qualms; disbelief, unbelief, incredulity, incredulousness, discredit; informalleeriness*
- *"the general distrust of authority amongst drug users"*

Verb

- *doubt the honesty or reliability of; regard with suspicion.*
- *"like a skillful gambler, Dave distrusted a sure thing"*
- *synonyms: mistrust, be suspicious of, be wary/chary of, regard with suspicion, suspect, look askance at, have no confidence/faith in; be skeptical of, have doubts about, doubt, be unsure of/about, be unconvinced about, take with a pinch/grain of salt; have misgivings about, wonder about, question; disbelieve (in), not believe, discredit, discount, be incredulous of; informal, be leery of, smell a rat*
- *"for some reason Aunt Louise distrusted him"*

[Lexico.com: https://www.lexico.com/en/definition/distrust]

Trusted Digital Web

Trusted Digital Web

Trusted Digital Web

The Trusted Digital Web (TDW) is a universal, trusted, frictionless, integrated, standards-based, general-purpose, end-to-end platform for global commerce, communication, and collaboration. The Trusted Digital Web is comprised of three (3) core software components: Trust-Based Applications (Trust-Based Apps or simply, TBAs), Universal DID (UDID) Data Service (UDIDService), and Trusted Digital Assistants (TDAs).

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Trusted Digital Web Project

The Trusted Digital Web Project is based on a set of open-source software projects and specifications (and their associated communities of people) that underpin the work involved in creating the Trusted Digital Web.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Trusted Digital Web Platform

The Trusted Digital Web Platform is the software platform on which the Trusted Digital Web is implemented. The Platform an extension and integration of the following open source projects.

- DnsServer (https://github.com/TechnitiumSoftware/DnsServer)
  - The DnsServer is extended to support additional DNS Resource Record types need to realize verifiable Universal Digital Identifiers and Digital Credentials
- TechnitiumLibrary (https://github.com/TechnitiumSoftware/TechnitiumLibrary)
  - Likewise, the TechnitiumLibrary is extended to support additional DNS Resource Record types need to realize verifiable Universal Digital Identifiers and Digital Credentials
- Maestro (https://github.com/monirith/maestro)
  - Maestro is extended to support the generation of Universal BPMN Byte Code that executes in the UDIDService Workflow Engine (which in turn is based on Maestro).
- StratisPlatform (https://github.com/stratisproject)
  - The StratisPlatform is the general-purpose, smart contract-enabled, blockchain platform used to support Universal Credential verification.
- SerentityData (https://github.com/mwherman2000/serentitydata)
  - SerentityData is a universal, dynamically configurable, byte-level data compaction technology used by decentralized applications (DApps) for more efficient storage of data on a blockchain.
- Camunda Modeler (https://camunda.com/products/modeler/)
  - BPMN standard-based workflow and business process open-source modeling tool
- Chromium (https://www.chromium.org/Home)
  - Chromium is an open-source browser project that aims to build a safer, faster, and more stable way for all Internet users to experience the web. Chromium is used by Google Chrome and later releases of Microsoft Edge.
- CefSharp (http://cefsharp.github.io/)

- CefSharp is the easiest way to embed a full-featured standards-compliant web browser (Chromium) into your C# or VB.NET app.

The entire Trusted Digital Web Platform is released under the MIT open source license (for more details, see Appendix F – MIT License on page 68).

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Trusted Digital Web Components

Trust-Based Applications

A Trust-Based Application (Trust-Based App or simply, TBA) is a downloadable, plug-in app that is hosted by the Trusted Digital Assistant (TDA) and depends on the services of the TDA to perform:

- *Data notarization*
- *Credential storage and management using subsidiary ledgers*
- *Payments via decentralized currencies*
- *Identity via Universal Digital Identifiers*
- *Credential verification via pluggable verifying journal providers*
- *Agent-to-agent serverless network communications*
- *Workflow (business process) engine hosting*

[Michael Herman: https://www.linkedin.com/in/mwherman/]

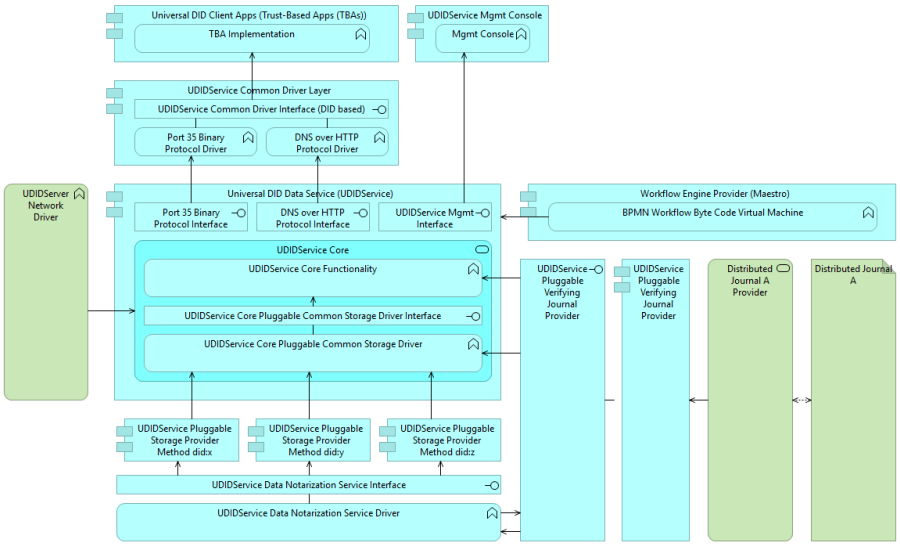
Universal DID (UDID) Data Service (UDIDService)

A Universal DID (UDID) Data Service (UDIDService) is a core service underlying the Trusted Digital Assistant (TDA) responsible for credential creation and management, certification, verification, agent-to-agent network communications, and workflow (business process) management.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Universal DID Data Service (UDIDService) Logical Architecture 0.9

Michael Herman
Self-Sovereign Blockchain Architect
Hyperonomy Digital Identity Lab
Parallelspace Corporation
October 11, 2019



Trusted Digital Assistants (TDAs)

A Trusted Digital Assistant (TDA), a core component of the Trusted Digital Web Platform, is the client application (app) the citizens use to access and use the Trusted Digital Web. The TDA is the application that hosts Trust-Based Applications (TBAs). The TDA provides the following services to TBAs hosted in the TDA:

- *Data notarization*
- *Credential storage and management using subsidiary ledgers*
- *Payments via decentralized currencies*
- *Identity via Universal Digital Identifiers*
- *Credential verification via pluggable verifying journal providers*
- *Agent-to-agent serverless network communications*
- *Workflow (business process) engine hosting*

[Michael Herman: https://www.linkedin.com/in/mwherman/]

APPENDIX C – IDENTIFIERS, IDENTITIES, CLAIMS AND CREDENTIALS

Subjects and Personas

Real (or Virtual) Subject

A Real (or Virtual) Subject is any unique and specific non-fungible object in the Physical or Digital Universe: a person, a place, a thing, an organization, digital visual or audio composition, business document, etc.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Persona

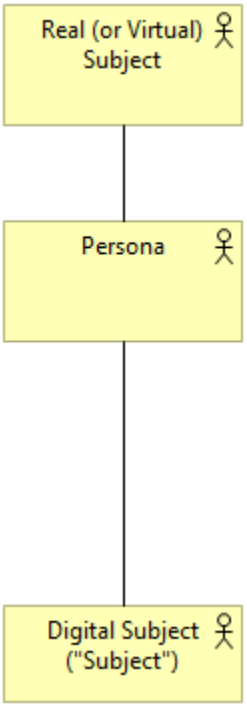
A persona (plural personae or personas), in the word's everyday usage, is a social role or a character played by an actor. The word is derived from Latin, where it originally referred to a theatrical mask.

[Wikipedia: https://en.wikipedia.org/wiki/Persona]

Digital Subject ("Subject")

A Digital Subject (aka Subject) is a unique digital representation of a Real Subject; more specifically, a particular Persona of a Real Subject.

[Michael Herman: https://www.linkedin.com/in/mwherman/]



Digital Identifiers

Digital Identifier (DID)

- See Universal Digital Identifier

Universal Digital Identifier (UDID aka "DID")

Short for Universal Digital Subject Identifier, a UDID (or "DID") is a character string representation whose value is unique and is used to address, index, search, and retrieve Claims about the associated Digital Subject (aka Subject). A Subject can have more than one UDID associated with it.

A DID starts with the character string `did:` *and is followed by 1 or more DID Method labels; followed by Method-define unique character string identifier. Examples:*

- `did:neonation:123-456-789`
- `did:usergroups:developers:abc12345678`

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Universal Digital Subject Identifier

- See Universal Digital Identifier

Decentralized Identifier

A Decentralized Identifier is a narrowly defined type of Digital Identifier that is verifiable using a blockchain-based immutable data store. See Trust Levels for Universal DIDs.

Digital Identities

Digital Identity

- See Universal Digital Identity

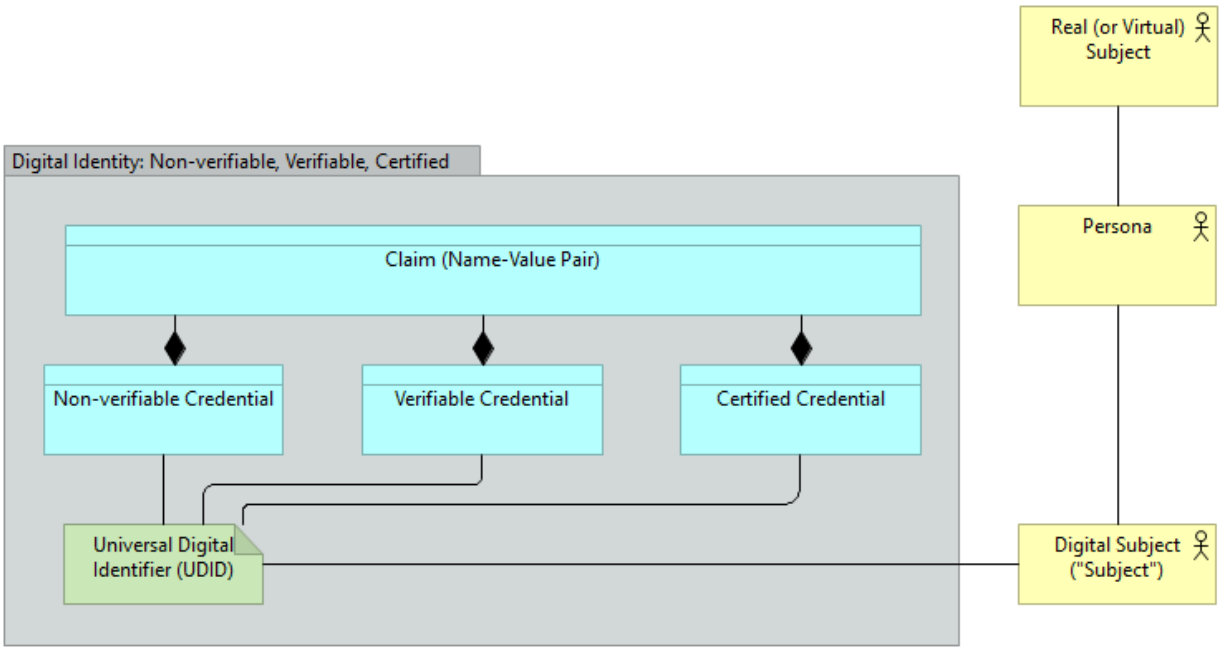
Universal Digital Identity

A Universal Digital Identity is a set of Claims made by one Digital Subject about itself or another Digital Subject [The Laws of Identity]. A Universal Digital Identity is associated with, or identified by, one or more Universal Digital Identifiers (UDIDs, or more simply, DIDs).

A minimal Universal Digital Identity contains a Claim (name-value attribute) named `id` whose value is the identifier associated with the credential. A Universal Digital Identity can have an unlimited number of Claims associated with it.

A Universal Digital Identity can be persisted as a Credential.

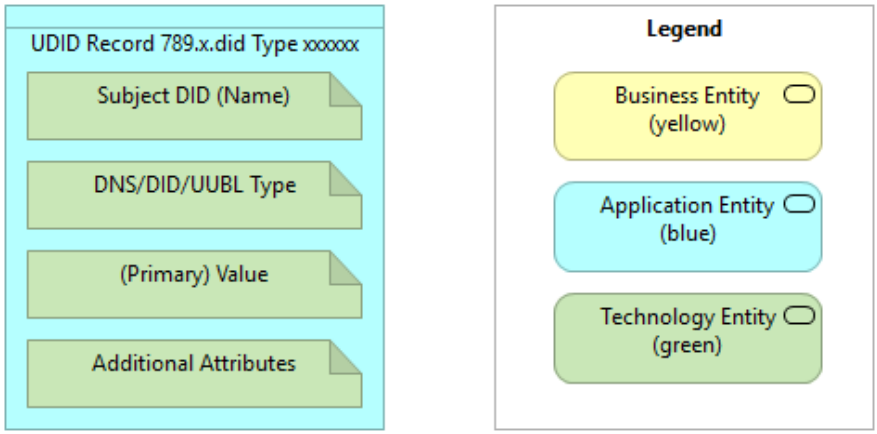
[Michael Herman: https://twitter.com/mwherman2000/status/1164540800526454786]



Claims, Profiles, and Credentials

Claim

A Claim is any data attached to, or associated with, a Digital Identity by way of a DID. A Claim is a name-value pair representing a datum associated with a DID. Preferably, claim data and the claims' relationships to a Digital Identity are represented (persisted) in a manner that is immutable, auditable, verifiable, historized, and permanent.



[Michael Herman: https://twitter.com/mwherman2000/status/1164540820092882944]

Credential

- See Universal Digital Credential

Universal Digital Credential (Credential)

A set of Claims is called a Universal Digital Credential (or more simply, a Credential) – of which there are 4 Trust Levels.

A minimal Credential is a Credential that contains a Claim (name-value attribute) named `id` whose value is the identifier associated with the credential. A Credential can have an unlimited number of Claims associated with it.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Profile

A collection of related Universal Digital Credentials is called a Profile. The collection of Credentials is related to a common Universal Digital Identifier.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

DID Credentials and DID Documents

DID Credential

A DID Credential is a specialization of a Universal Digital Credential (Credential). A minimal DID Credential is a Credential that contains a Claim (name-value attribute) named `id` that has a DID as a value and is associated with a Subject via the value of the `id` Claim. A DID Credential can have an unlimited number of Claims associated with it. The following is an example of a minimal DID Credential.

```
{
  “id”: “did:example:050B6A27-724E-44DC-892C-0378087C3A44”
}
```

The following is an example of another DID Credential.

```
{
  “id”:       “did:example:0853338A-5176-409D-8C0B-FEC3CD211E00”,
  “location”: “Calgary, Alberta”,
  “country”:  “Canada”
}
```

[Michael Herman: https://www.linkedin.com/in/mwherman/]

DID Document

A DID Document is a specialization of a DID Credential that contains specific Claims as defined in the draft `did-spec` specification (https://www.w3.org/TR/did-core/). The following is an example of a DID Document from the draft specification.

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",

  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],

  "service": [{
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": https://example.com/vc/
  }]
}
```

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Verification

Verifiable Digital Subject

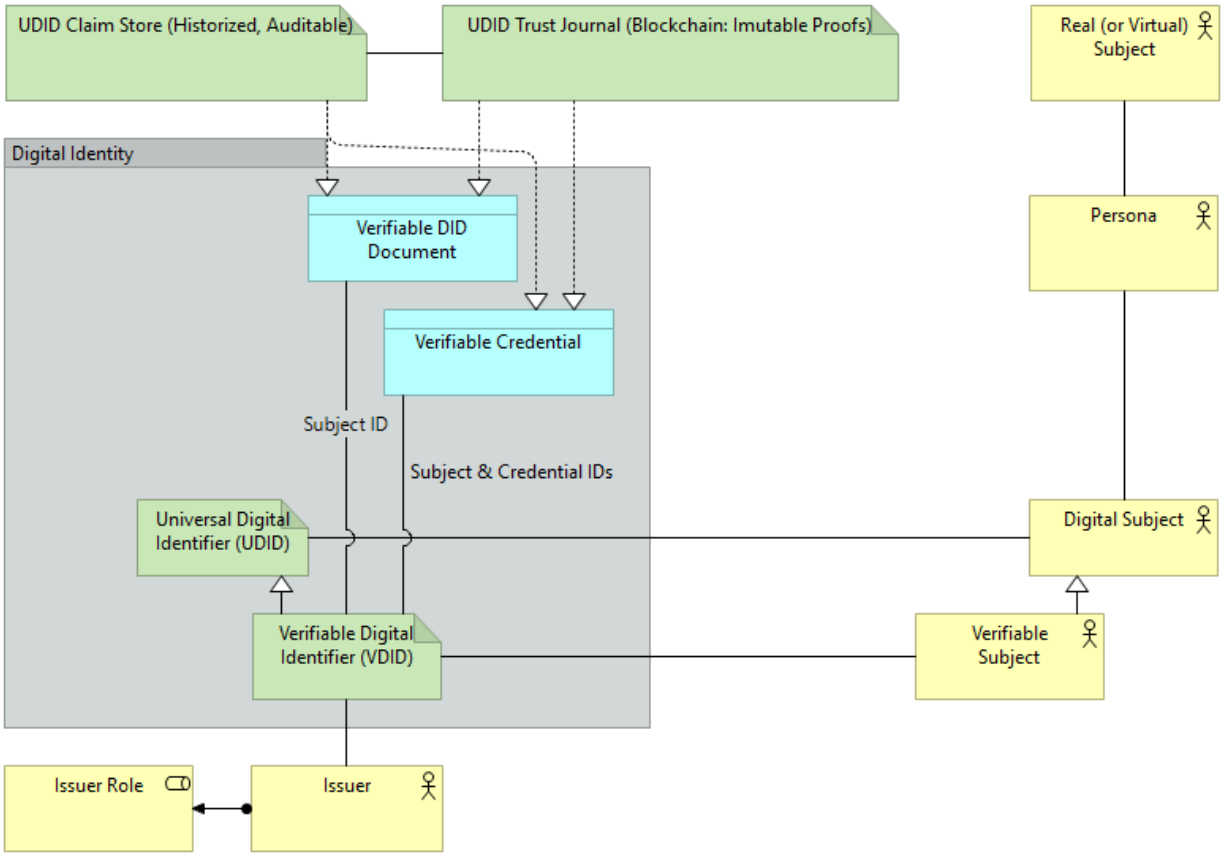
A Subject that is verifiable against a decentralized blockchain platform or other authority.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Verifiable Digital Credential

A Credential that is verifiable against a decentralized blockchain platform or other authority.

[Michael Herman: https://www.linkedin.com/in/mwherman/]



[Michael Herman: https://www.linkedin.com/in/mwherman/]

Levels of Trust

Trust Levels for Universal DIDs

Different Subjects (identified by their DIDs) can have different levels of trust in the Trusted Digital Web as defined by the following criteria:

Trust Level 0. Not Resolvable	*A Subject's DID (and by implication the associated Credentials and their Claims) is not verifiable. The Subject DID is not resolvable from the Data Registry.*
Trust Level 1. Resolvable	*A Subject's DID is resolvable from the Data Registry. There is at least one Claim associated with the DID for this Subject (even if the single Claim is the DID itself).*
Trust Level 2. Signed	*The Subject DID is resolvable and it has a validated DIDSUBSIG Claim associated with the DID in the Data Registry.*
Trust Level 3. Verifiable	*The Subject's DID is signed and the DID and DIDSUBSIG have been notarized; that is, they appear in the Data Notary and are valid and consistent with the corresponding data resolvable from the Data Registry.*

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Data Registry

A Data Registry is a data store (a service) that is used to store business data or references to business data (the latter being references to data stored in an external system such as a database or content management system). Digital signatures may also be stored in the Data Registry dependent on the DID Method's trust level. A Public Key can be stored in the Data Registry as a Credential Claim. Data in the Data Registry may be encrypted as determined by parameters associated with a particular DID Method. The attributes of a DID Method are represented as a Credential (a collection of Claims) in the Data Registry.

NOTE: A Credential is stored in a Data Registry as a collection of Claims.

NOTE: A Data Registry can be used to store data at any of the four (4) Trust Levels. Trust Level is a DID Method attribute (Credential Claim).

NOTE: A datum (Credential) stored in the Data Registry is retrieved by its Universal DID.

NOTE: In the Trusted Digital Web, a Data Registry is implemented using distributed Internet Domain Name Service (DNS) technologies.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Data Notary

A Data Notary (a service) is used to store copies of Digital Signatures and Verifiable Proofs for data stored in the Data Registry. A Data Notary supports (is required for) Trust Level 3. Verifiable for data stored in the Data Registry.

NOTE: A Data Notary is typically implemented using distributed journal (ledger) technologies.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Controllers

Controller

Every Subject (person, organization. And thing) has a Controller. A Controller is a role. There are two types of Controller roles: Self-Controllers and Thing Controllers.

Self-Controller

If a Subject is able to represent and act on its own behalf, the Subject has the Self Controller role.

Thing Controller

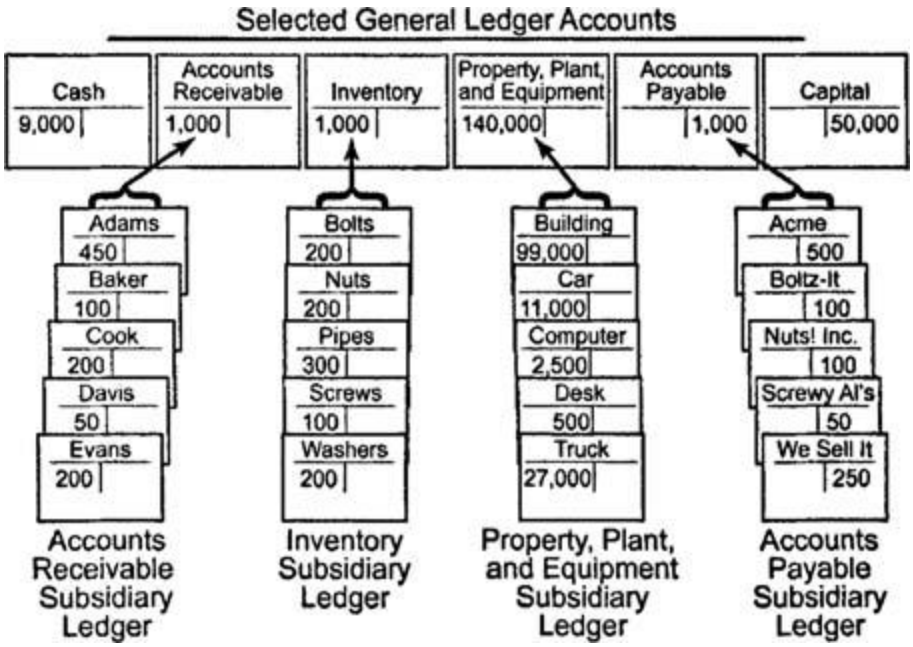
If a Subject is inanimate and cannot represent nor act on its own behalf, it requires one or more other Subjects to represent and act on its behalf. The latter is known as Thing Controller.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Accounting

Subsidiary Ledger

A subsidiary ledger is a group of similar accounts whose combined balances equal the balance in a specific general ledger account. The general ledger account that summarizes a subsidiary ledger's account balances is called a control account or master account. For example, an accounts receivable subsidiary ledger (customers' subsidiary ledger) includes a separate account for each customer who makes credit purchases. The combined balance of every account in this subsidiary ledger equals the balance of accounts receivable in the general ledger.



Subsidiary Ledgers (https://www.cliffsnotes.com/study-guides/accounting/accounting-principles-i/subsidiary-ledgers-and-special-journals/subsidiary-ledgers).

Workflow Actions and Business Processes

References to the term “Workflow Actions (Business Processes)” appear throughout this whitepaper. Each term as a separate, specific definition.

Workflow Action

In the context of the Trusted Digital Web, a Workflow Action is a simple network of interconnected work tasks that, when initiated, run to completion without blocking for user input or an external event. Workflows will generally be used to implement functionality internal to a Trusted Digital Assistant (but not exclusively).

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Business Process

In the context of the Trusted Digital Web, a Business Process is generally considered to be a more complex network of interconnected work tasks and may block waiting for input from a user, an external service, or some other event. A Business Process is used to support an external (real world) business process.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Both workflows and business processes are defined in the same way, are managed in the same way, and are executed in the same way - inside the Trusted Digital Assistant.

APPENDIX D – ADDITIONAL DEFINITIONS

Non-Fungible Things

Non-Fungible (1)

Fungibility is the ability of a good or asset to be interchanged for another good or asset of like kind. Like goods and assets that are not interchangeable, such as owned cars and houses, are non-fungible.

[Investopedia.com: *https://www.investopedia.com/terms/f/fungibility.asp*]

Non-Fungible (2)

Two goods or assets that may be technically different but may be considered to have the same usage value in a particular scenario may be considered highly exchangeable (aka fungible) goods or assets. They might not be considered non-fungible goods or assets.

For example, two slices of medium-toasted bread are technically different but from a usage perspective will often be considered highly exchangeable or fungible. On the other hand, a pair of digital photos, one taken of each slice of the two pieces of toast, are more likely to be considered definitive non-fungible assets based on the majority of uses cases involving photos.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Digital Slavery

Traffic

- *(verb)*
- *to carry on traffic, trade, or commercial dealings.*
- *to trade or deal in a specific commodity or service, often of an illegal nature (usually followed by in).*
- *to traffic in opium.*

[Dictionary.com: https://www.dictionary.com/browse/traffic]

Slavery

Slavery is any system in which principles of property law are applied to people, allowing individuals to own, buy and sell other individuals, as a de jure form of property. A slave is unable to withdraw unilaterally from such an arrangement and works without remuneration.

[Wikipedia: https://en.wikipedia.org/wiki/Slavery]

Digital Slavery (1)

Digital slavery is any system in which principles of property law are applied to people (including their personal data and information), allowing individuals to own, buy and sell other individual's person or personal data or information, as a de jure form of property. A digital slave is unable to easily withdraw unilaterally from such an arrangement and hence is forced to provide benefits without remuneration. A digital enslaver is anyone who traffics in the personal data and information of others without providing remuneration or any form of compensation in return.

[Michael Herman: https://www.linkedin.com/in/mwherman/]

Digital Slavery (2)

The cross-industry business practice of #trafficking in and profiting from the #personal #data of individual #Canadians with #no compensation and #norenumeration (...vs. #financialslavery).

[Michael Herman: https://twitter.com/mwherman2000/status/1159170641691471873]

Digital Trust, Human Trust, and Cryptographic Trust

Digital Trust

Digital trust is the measure of consumer, partner and employee confidence in an organization's ability to protect and secure data and the privacy of individuals. As data breaches become bigger and more common, digital trust can be a valuable commodity for companies that earn it, and it is starting to change the way management looks at security.

[CSOOnline.com: https://www.csoonline.com/article/3297037/what-is-digital-trust-how-csos-can-help-drive-business.html]

Human Trust

How we trust each other as individual human beings, participants in larger social orders, formal institutions and governments. This type of human trust existed before the ecosystem we are trying to create and will always be a part of it. Without human trust, we have nothing.

Cryptographic Trust

What was once done by means of clay, parchment, and paper is now done by digital. The mechanisms of how we trust each other through digital means are largely due to cryptography to ensure confidentiality, integrity, and control. Without cryptography, we'd still be using paper (maybe clay and parchment, too).

[Medium.com: https://medium.com/@trbouma/self-sovereign-identity-making-the-ecosystem-real-2ea09b5ee33]

Reliable and Secure

Secure is a word that has many meanings and is not easily disambiguated in the context of trust. Similarly, reliable is not a word that is easily disambiguated.

Reliable

adjective

1. that may be relied on or trusted; dependable in achievement, accuracy, honesty, etc.:
    - reliable information.

Secure

adjective

1. free from or not exposed to danger or harm; safe.
2. dependable; firm; not liable to fail, yield, become displaced, etc., as a support or a fastening:
    - The building was secure, even in an earthquake.
3. affording safety, as a place:
    - He needed a secure hideout.
4. **in safe custody or keeping:**
    - **Here in the vault, the necklace was secure.**
5. **free from care; without anxiety:**
    - **emotionally secure.**
6. firmly established, as a relationship or reputation:
    - He earned a secure place among the baseball immortals.
7. sure; certain; assured:
    - secure of victory; secure in religious belief.
8. safe from penetration or interception by unauthorized persons:
    - secure radio communications between army units.
9. Archaic. overconfident.

verb (used with object)

10. to get hold or possession of; procure; obtain:

- to secure materials; to secure a high government position.

11. **to free from danger or harm; make safe:**
    - **Sandbags secured the town during the flood.**
12. to effect; make certain of; ensure:
    - The novel secured his reputation.
13. to make firm or fast, as by attaching:
    - to secure a rope.
14. Finance.
    - to assure payment of (a debt) by pledging property.
    - to assure (a creditor) of payment by the pledge or mortgaging of property.
15. **to lock or fasten against intruders:**
    - **to secure the doors.**
16. **to protect from attack by taking cover, by building fortifications, etc.:**
    - **The regiment secured its position.**
17. to capture (a person or animal):
    - No one is safe until the murderer is secured.
18. to tie up (a person), especially by binding the person's arms or hands; pinion.
19. **to guarantee the privacy or secrecy of:**
    - **to secure diplomatic phone conversations.**

verb (used without object)

20. to be or become safe; have or obtain security.
21. Nautical.
    - to cover openings and make movable objects fast:
        i. The crew was ordered to secure for sea.
    - to be excused from duty:
        i. to secure from general quarters.

[Dictionary.com: https://www.dictionary.com/browse/secure]

Trust Levels, Reputation, and Accuracy

Trust Levels

Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity but rather it is subject to the entity's behavior and applies only within a specific context at a given time.

That is, the firm belief is a dynamic value and spans over a set of values ranging from very trustworthy to very untrustworthy as illustrated in Table 1. The trust level (TL) is built on past experiences and is given for a specific context. For example, entity y might trust entity x to use its storage resources but not to execute programs using these resources.

The TL is specified for a given time frame because the TL today between two entities is not necessarily the same TL a year ago.

[University of Manitoba: ftp://ftp.cs.umanitoba.ca/pub/IPDPS03/DATA/W01_HCW_05.PDF]

Reputation

The reputation of an entity is an expectation of its behavior based on other entities' observations or the collective information about the entity's past behavior within a specific context at a given time.

Seeking the reputation of a specific entity, entity x relies on information from a set of other entities referred to as recommenders' set (). A recommender is an entity that gives recommendations using its direct trust table (DTT) that includes trust values for entities with which the recommender had prior direct transactions. Recommenders might have different criteria for evaluating other entities. Hence, different recommenders might give different recommendations about an entity.

Therefore, Entity x associates an accuracy measure with each recommender in the recommender set. The information (i.e. the accuracy measure) on the set of entities that act as recommenders being used by x is kept in a recommender trust table (RTT). Entity x uses the accuracy measure to minimize the deviation between the information received from each recommender and the actual "trustworthiness" of y.

[University of Manitoba: ftp://ftp.cs.umanitoba.ca/pub/IPDPS03/DATA/W01_HCW_05.PDF]

Accuracy

A recommender is said to be accurate, if the deviation between the information received from it pertaining to the "trustworthiness" of a given entity in a specific context at a given time and the actual trustworthiness of within the same context and time is less than a precision threshold.

[University of Manitoba: ftp://ftp.cs.umanitoba.ca/pub/IPDPS03/DATA/W01_HCW_05.PDF]

APPENDIX D – STRATEGIC THINKING

The following is an excerpt from the book *The Business of Giving: The Theory and Practice of Philanthropy, Grantmaking and Social Investment* by Peter Grant (https://www.amazon.ca/Business-Giving-Philanthropy-Grantmaking-Investment/dp/0230336795/ref=sr_1_1).

In the chapter *Can Philanthropy Learn from Business Models?* (on page 93), Grant describes Jeanne Liedtaka's point-of-view with respect to strategic thinking – succinctly in a single page. Here's is a list of those 5 points. They are extremely pertinent to the architecture, design, and social evolution technology model being used to create the Trust Digital Web.

NOTE: In the following quote from Grant, imagine replacing *organization* with the word *project*, the word *Internet*, or the Trusted Digital Web.

> *Firstly, strategic thinking is based on a systems perspective – a holistic view of an organization. The strategic thinker has a mental picture of the complete system of value creation in the organization and their own small role within the larger system.*
>
> *Secondly, strategic thinking is driven by the strategic intent of the organization providing focus and energy to the staff and the organization to achieve [its] goals.*
>
> *Thirdly, strategists need to 'think in time' linking an organization's past, present, and future in their thought processes. There are three components:*
>
> - *the predictive value of the past for the future;*
> - *departures from the past which divert the organization from familiar patterns;*
> - *the need for continuous comparison*
>
> *Fourthly, strategic thinking is 'hypothesis-driven' and the 'scientific method accommodates both creative and analytical thinking sequentially in its use of iterative cycles of hypothesis-generating and testing'.*
>
> *Finally, strategic thinking is intelligently opportunistic. The organization whilst following a particular strategy should not lose sight of alternative strategies that may be more appropriate for a changing environment.*

In hindsight, the Trusted Digital Web was conceived (and continues to grow and evolve) based on the above set of strategic thinking principals.

APPENDIX E – TRUSTED DIGITAL WEB COMMUNICATION PROTOCOLS

This appendix summarizes the protocols used in the Trusted Digital Web; more specifically, the protocols supported by:

- the Data Registry service (aka Universal DID Data Server), and
- the Trusted Digital Assistant client application.

NOTE: To learn more about the DNS protocol and to see examples of the DNS standard binary query/response messages, read APPENDIX A – Internet Domain Name Service (DNS) Overview on page 41.

Data Registry Service Protocols

DNS Query/Response Protocols

As a DnsServer-based open-source project (https://github.com/TechnitiumSoftware/DnsServer), the Trusted Digital Web Data Registry supports the DNS standard query/response protocol over the following transports and ports:

- TCP/IP port 53 (binary)
- UDP/IP port 53 (binary)
- DNS over TLS (DoT) over TCP/IP port 853
- DNS over HTTPS (DoH) over TCP/IP port 443

Data Registry Management API Protocols

For non-query management operations such as CRUD operations for DNS zones/DID methods, DNS records/DID claims, etc., the Data Registry supports a JavaScript-friendly Web API running over HTTP over TCP/IP port 80.

Trusted Digital Assistant Protocols

The protocols supported by the Trusted Digital Assistant client application include the common Internet browser transport protocols supported by the CefSharp (https://github.com/cefsharp/CefSharp) wrapper for the Chromium embeddable browser component (https://www.chromium.org/Home). Chromium is the Google open-source browser engine used by Google Chrome and several other browsers (https://en.wikipedia.org/wiki/Chromium_(web_browser)#Browsers_based_on_Chromium) – as well as the next version of Microsoft Edge (to be released in 2020). In addition, the Trusted Digital Assistant design leverages CefSharp's pluggable protocol handler capability for implementing custom URL syntax schemes. The Trusted Digital Assistant uses this capability to implement the `didttp:` scheme (DID Trusted Transport Protocol).

Common Internet Browser Protocols

The common Internet browser protocols supported by Chromium (and, in turn, the Trusted Digital Assistant) include:

- HTTP over TCP/IP

- HTTPs over TCP/IP

DID Trusted Transport Protocol (didttp:)

The DID Trusted Transport Protocol implements the didttp: URL scheme over the standard/default DNS binary query/response protocol running over TCP/IP port 53. That is, the Trusted Digital Assistant includes a pluggable protocol handler that maps the didttp: URL scheme into the appropriate DNS standard binary query, sends the query to the Data Registry over TCP/IP port 53, receives the DNS standard binary response, and then converts the response into a JSON for rendering in Chromium.

The didttp: URL scheme supports queries from a Trusted Digital Web Data Registry. The format of a didttp: URL is as follows:

```
didttp://<dataregistryaddress>/did:<didmethod>[:<identifier>[#<fragment>]]
```

where:

- `<dataregistryaddress>` is the conventional Internet domain name or IP address of the Data Registry. Most often, `<dataregistryaddress>` will most likely have a value of `localhost`.
- `<didmethod>` is a conventional DID Method string containing one (and possibly two or more labels). For example, `able` and `able:baker:charlie`.
- The optional `<identifier>` is any identifier compatible with the DID Method Specification for `<didmethod>`.
- The optional `<fragment>` is any string tag that is compatible with the DID Method Specification for `<didmethod>`. In the Data Registry, the `<fragment>` value is mapped to the value of the Tag claim in the Credential identified by the value of `did:<didmethod>[:<identifier>]`.

NOTE: The didttp: URL scheme is only processed with the Trusted Digital Assistant - where it is mapped directly into the DNS standard binary query protocol. At present, there is no need for didttp: URLs to be transmitted over the wire. This design may change in the future given a requirement to perform didttp: URL resolution in the Data Registry. However, the overarching requirement is for the Data Registry to remain 100% compatible with the current DNS IEFT specifications.

CLARIFICATION: The Universal DID Identifier component of the didttp: protocol scheme is the part that is sent to the Data Registry (as is) as part of a query. For example, for the following Trusted Digital Assistant URL, the following parts are used to constitute the DNS binary query:

URL: `didttp://localhost/did:foo:home#index.htm`

Query Parts: UDID `did:foo:home` and resource record type `ANY` is sent to the Data Registry located at DNS address `localhost`

CLARIFCATION: The Data Registry Address URI component `didttp://<dataregistryaddress>/` is expected to correspond to (be the value of) the Service Endpoint URL Claim in the DID Document for the specific DID Method `did:<didmethod>`.

Secure DID Trusted Transport Protocols (didttps:)

The Secure DID Trusted Transport Protocol (didttps:) implements the didttp: URL scheme over the standard/default DNS binary query/response protocol running over TLS port 853.

APPENDIX F – MIT LICENSE