# Section Three.
# Internet, New Technologies and Sustainable Development

# Digitally Transforming the Web into an EcoSphere of EcoSystems

*Charlie Northrup <Charlie.Northrup@neursciences.com>*
*BEDFORD, HN, United States of America*

*Abstract*
This paper explores the possibilities of membership in a hyperconnected framework where every individual, household, and organization is represented by a digital twin – an intelligent software agent responsible for managing their digital ecosystem. The framework provides for the identification, authentication, authorization, and auditing of the people, places, and things involved in the exchange of value within and across these ecosystems.

## *1. Beyond the Web*

In 1990 the World Wide Web emerged as a disruptive technology opening a new digital frontier. Thirty years later, consumers would spend over $25.6 trillion online.[1] Like every disruptive technology before it, the Web would forever change society. With 30 years of historical data to look upon, we can now consider what we got right and what can be improved. This analysis will help us evolve the digital world for the next generation.

The World Wide Web started at the National Center for Supercomputing Applications (NCSA) at the University of Illinois. In 1990 Tim Berners Lee proposed a document information sharing system as a way for members of academia to share research papers.[2] The system would become the Web. Back then, you simply entered a URL, and it displayed a web page. There were no logins or passwords, and you did not have to prove you are not a robot.

1 United Nations Conference on Trade Development, "UNCTAD Estimates of Global e-commerce 2018" (2020) <https://unctad.org/system/files/official-document/tn_unctad_ict4d15_en.pdf> accessed 7 July 2021.
2 Tim Berners Lee, 'Information Management: A Proposal' (w3.org, 1989-1990) <https://www.w3.org/History/1989/proposal.html> accessed 7 July 2021.

From the beginning, the Web has evolved despite its largest weakness and most pervasive problem, the lack of a membership model. The Web's own architecture provided the features that enable bad actors and also causes its inability to universally prevent nefarious and fraudulent presentations and conveyances.

The original architect of the Web consisted of a collection of stateless document-sharing Web servers. The Web browser connected to the server identified by a Domain Name System lookup of the host name to request a document. The clients were identifiable and addressable only within the scope of the server to which they were connected. The stateless architecture of the Web meant each time the browser connected to a server; it was as if the two had never interacted before.

Four years later, a startup company which became Netscape licensed the web technology from the university's licensing company. Headed by CTO Marc Andreesen, who developed the popular NCSA Mosaic web browser, Netscape offered the first consumer-ready version of the web browser for the Microsoft Windows operating system. By 1994 Netscape began exploring a way to change the stateless document sharing system into an e-commerce platform through the use of "cookies".

Cookies enabled the server to store state information with the client browser. For example, cookies enabled the server to know if the client had previously visited the website and what items were in its shopping cart. The public became more aware of the privacy concerns when the Financial Times published a store in February 1996.[3] After much discussion and public hearings held by the Federal Trade Commission, cookies became standardized in 1997.[4][5]

There are valuable lessons to be learned here. Firstly, 1997 marked the "end of free." The use of cookies enabled websites to erect paywalls. As a result, it was now possible to provide subscription-based services. Secondly, 1997 marked the moment every server could collect, own and

3 Tim Jackson, 'This Bug in Your PC is a Smart Cookie' (Financial Times, 02 December 1996).

4 Federal Trade Commission, 'Consumer Privacy on the World Wide Web' (FTC,1998) <https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-consumer-privacy-worldwide-web/privac98.pdf> accessed 7 July 2021.

5 David Kristol and Lou Montulli, 'HTTP State Management Mechanism' (1997) IETF RFC 2109 <https://datatracker.ietf.org/doc/html/rfc2109> accessed 7 July 2021.

store information about the client. Monetization of that data began slowly and quickly accelerated as businesses realized the value.

Initially, the general public tolerated the use of cookies between the browser and a given server. However, people soon discovered they were being tracking across different websites through third-party cookies creating a significant privacy risk. For example, why would a social network need to know what medications a person ordered from an online pharmacy? Would a employer learn that an employee was purchasing a pregnancy test?

Over 130 jurisdictions across the world have since added some form of data privacy laws to address digital data privacy concerns.[6] The United States currently has a patchwork of laws at the federal level, such as FISMA and HIPAA, to address sensitive verticals, but no overall national privacy law, leaving each state to define its own.[7] [8] As more jurisdictions add their own specific laws, compliance could pose significant risk and cost to small and medium-sized businesses.

*2. Lack of a universal self-validating/authenticating membership model*

Perhaps the single most significant limitation of the client-server architecture of the Web is the lack of a universal membership model. In general, the lack of a membership model exacerbated the Web's profound identity and trust crisis. This forced service providers to rely on 3rd party unauthenticated email addresses as a imperfect indicator of identity and the basis of trust. In the current situation, when users cannot remember a password, they select a reset password button which sends a hyperlink to your email account. The disadvantage is that over 3B fake emails go out every day, including numerous phishing attacks trying to trick people into clicking a link to a bogus website.

A recent Coveware report indicated nearly 80 % of the ransomware events in the first quarter of 2021 were started with email phishing at-

6 Morrison Forester, 'Catch Up on Privacy Around the World on Data Privacy Day 2021' (Morrison Foerster, 2021) <https://www.mofo.com/resources/insights/210127-data-privacy-day.html> accessed 7 July 2021.

7 Federal Information Security Management Act of 2014, (2014) <https://www.congress.gov/113/plaws/ publ283/PLAW-113publ283.pdf> accessed 7 July 2021.

8 Health Insurance Portability and Accountability Act of 1996, (1996) <https://www.congress.gov/104/plaws/ publ191/PLAW-104publ191.pdf> accessed 7 July 2021.

tacks.[9] Verizon noted 94% of malware was delivered through an email phishing attack vector.[10] Checkpoint describes the email phishing attack vector as the biggest threat in the online world today.

In summary, Web users are not, nor ever have been members, or citizens of the Web or the larger digital world. Users are limited in scope and sense of agency. They persist only within the closed digital ecosystem of the domain they are connected to. Users do not own their addressable identities, nor do they have a discoverable personal point of presence outside of the closed ecosystem. They lack the set of keys that comes with membership.

Membership, in the NeurSciences' context, gives users an identifiable and addressable point of presence, a set of personal keys to lock and unlock their resources, and a personal assistant application to manage those keys. The personal assistant is an intelligent software agent that uses the member's keys for identity, authentication, authorization, and audit. This eliminates the need for the end user to remember complex passwords. Instead, the agent manages the digital complexity for the member. The agent and the member's keys provides the mechanism for the user to protect or manage the privacy of their data and the means to automate the exchange of value within and across all digital ecosystems.

### *3. Disintermediating the Intermediaries*

The emergence of the P2P Bitcoin Blockchain in 2009 is notable for several reasons.[11] Firstly, it introduced a digital commodity that could be bought and sold. Secondly, it disintermediated the intermediaries. Thirdly, it allowed anybody and everybody to participate as a peer.

A Bitcoin is a digital commodity. It is not a currency in the true sense of the word. Instead, it is a commodity valued at precisely what somebody is willing to pay for it at a given moment in time. In many jurisdictions, individuals need to keep track of the value when they purchased the

9 Coveware, 'Ransonware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate' (Coveware.com, 2020) <https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate> accessed 7 July 2021.

10 Verizon, '2021 Data Breach Investigation' (Verizon.com, 2021) <https://www.verizon.com/business/resources/reports/dbir/> accessed 7 July 2021.

11 Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (Bitcoin.org, 2008) <https://bitcoin.org/bitcoin.pdf> accessed 7 July 2021.

Bitcoin and the value when they sold the Bitcoin. They are then taxed on the gain or loss accordingly.

The Bitcoin platform eliminated the need for intermediaries such as central banks. Instead of having a central bank to clear transactions, anybody could participate and get paid in Bitcoins for clearing the transaction. Eliminating the intermediaries removes the central authority's monopoly on controlling the money supply. Central banks typically increase the money supply to grow an economy and decrease the money supply when the economy grows too fast.

Bitcoin is based on a public ledger. The benefit of a completely open ledger is that anybody can inspect and prove its correctness. In addition, the open ledger enables everybody to see the current balance of each account.

A series of public and private key pairs are used in each transaction to ensure security. In simple terms, if Alice wants to send Bob a Bitcoin, then Alice would use her private key to sign off that she is sending the Bitcoin to Bob's public key. Anybody can use Alice's public key to authenticate the transaction. Bob would then use his private key to gain access to the Bitcoin.

To satisfy government regulations on Know Your Customer, Alice should know who Bob is. However, with the Bitcoin blockchain, there is no individual identity. Therefore, Alice would not know with any certainty who Bob is. The only thing that Alice would know is his address which Bob could change as frequently as he wants.

Some jurisdictions may require anybody involved in the exchange of Bitcoins and fiat currencies to be registered and licensed. In the United States, the laws can sometimes conflict between member states and even between the states and federal government. For example, the state of New Hampshire (NH) required Bitcoin exchanges operating in their state to acquire a Money Service Business license. A subsequent NH law changed that by exempting Persons conducting business using transactions conducted in whole or in part in virtual currency. At the Federal level, however, the Internal Revenue Service classifies and taxes Bitcoins as a commodity.

To prevent money laundering and other nefarious acts, the Governments typically monitor the traffic and impose specific rules. For example, to purchase a Bitcoin, you may be required to go through a licensed exchange that imposes strict Know Your Customer rules. The rules may require you to provide a photo ID, a driver's license, a utility bill, and so on. In addition, the central exchange may record and report your transactions to ensure compliance with tax laws in your jurisdiction.

The general perception is that fiat currency and central banks will retain their power for the foreseeable future. This is because the banks play an integral role in government and are not going away anytime soon. Yet, in the digital world, the word "soon" is somewhat relative to perspective. From the viewpoint of the central banks, they want to retain control on the money supply. Yet from the perspective of the cryptocurrency advocates, the role of the central bank will diminish.

### *4. Disintermediating the Web Browser*

The inventors of disruptive technology enjoy the power shifts it enables, while those that follow the status quo find their markets collapsing around them. The smartphone was one such disruptive technology. It helped service providers to disintermediate the need for the web browser.

The Apple app store, released in 2008, along with voice-activated assistants such as Siri in 2011, played critical roles in disintermediating the need for the browser.[12] Firstly, the apps provided a direct connection between the end-user (client) and the app provider. Notifications enabled the app providers to alert the user of pending actions and events. Secondly, the convenience of voice-activated requests and audible responses eliminated the need to use the browser for simple tasks such as requesting today's weather forecast. The disruption occurs by eliminating online advertisement monetization events that would have otherwise occurred through the client-server web browser.

Amazon released their voice-activated Echo product in 2016, followed by Google Home later that year. Both products allowed the consumer to use voice recognition to interact with the devices. As more smart devices come online, it further reduces the reliance on a web browser for interacting in the digital world.

### *5. The Benefits of Membership*

Membership provides you a set of keys and a software agent to manage those keys for you. The agent uses the keys to unlock your point of presence and manage your digital ecosystem. Each member has its own digital

12 Apple, 'The App Store Turns 10' (Apple.com, 2018) <https://www.apple.com/newsroom/2018/07/app-store-turns-10/> accessed 7 July 2021.

ecosystem which collectively are referred to as a Digital EcoSphere. Identity within the Digital EcoSphere is enabled by the MultiKey infrastructure (MKI) which is a key based version of the public key infrastructure.

Your agent uses your keys to secure your content and secure your communications. Each member uses multi factor authentication to pair with their agent. Your agent guards your digital ecosystem and manages all the digital complexities so you do not have to.

### *6. We are at the beginning of the beginning*

Neal Stephenson's 1992 science fiction novel "Snow Crash" introduced the metaverse as a threedimensional space where people, as digital avatars, interact with each other and other software agents.[13] Although it was limited to the digital world, it did set the stage for thinking differently about augmented reality. It also raised questions about integrating the digital world with the physical world at the same time.

In 2014 Kevin Kelly of Wired Magazine stated: "We are at the beginning of the beginning." It was the first time Kelly described a meta organism he referred to as Holos, which forms from the combination of Gaia (the aggregate of Earth's like), Humanity, and Technium.[14] The meta organism Kelly was referring to is different from the metaverse introduced in Neil Stephenson's "Snow Crash". Stephenson's metaverse was focused on virtual reality while Kelly's meta organism encompassed everything.

In 2016 Klaus Schwab, founder of the World Economic Forum, suggested we are entering a 4th Industrial Revolution that will blur the distinction between the physical, biological, and digital spheres.[15] In Schwab's view it is more about the fact that everything will be interconnected than how the interconnection works at the technical level. Although he did not elaborate on "how," he did note that when it occurs, it will change everything about the way we live, work, and play.

The common theme is that of a hyperconnected world extending well beyond the Web as we know it today. However, the idea of a hyperconnec-

---

13 Neal Stephenson, *Snow Crash* (Bantam Books (US) 1992)

14 Danielle Engelman, 'Kevin Kelly Holos Rising' (2014) <https://blog.longnow.org/02014/12/01/kevin-kellyseminar-media/> accessed 7 July 2021.

15 Klaus Schwab, 'The Fourth Industrial Revolution: What it means and how to response' (weforum.org, 2014) <https:// www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> accessed 7 July 2021.

ted world is not without its concerns. Some people fear it will lead to intelligent machines overtaking the world. Ray Kurzwell, a futurist and Chief Technical Officer at Google, refers to it as the technological singularity – the moment in time in which technological growth has unforeseen changes to human society.

While some futurists believe the singularity will always be near, others believe it is already happening. With 30 years of history, we can now look back to consider some of the unforeseen changes in human society brought about by the Web. For example, cyberbullying, malware, ransomware, social isolation, and others. Yet, we also achieved enormous benefits, such as government accountability, immediate access to information, e-commerce, telehealth visits, and the ability to work from home.

### *7. Fiefdoms to Hyperconnectivity*

When history looks back at this stage of the Web, it might describe it as similar to the fiefdoms of feudal lords. Each website is owned and operated in isolation. The domain owner dictates who can participate in the ecosystem and what role(s) they can perform, such as buyer, seller, distributor, broker, or consumer of content. The owner carefully controls what their subjects (subscribers) can and cannot do within their walled domain and decides the monetization events. The client-server model enables the owner to maintain a monopoly and assert total control over their domain.

Looking beyond the Web, we see companies such as Pizza Hut planning pizza deliveries by drone and Amazon envisioning large-scale drone delivery systems. Flying drones is one thing, but getting the drones to independently and autonomously interact with a physical environment is more complex. Not only would the drone need to interact with the physical environment, but the drone will also encounter other entities independently and autonomously operating in the environment.

Tesla and Google expanded the concept to unmanned autonomous vehicles driving on our streets. The challenge is the potential harm such vehicles could cause to life and property. Given that a human-operated vehicle could accidentally take the life of a driver, passenger, or pedestrian, so too could an independent, autonomous vehicle. The implication is simple. It is no longer sufficient to think of independent, autonomous cars and trucks without considering how these machines can interact with each other.

The idea of autonomous, independent entities is a very different model from the Web as we know it today. In the real world, a visitor can enter a city, shop at any number of stores, dine at various restaurants, and ultimately return to their home town. In today's client-server Web, the client must provide a secret password to gain entry. Upon exit, the client immediately returns to their home. They must repeat this process over and over again. You can see how the digital world and the natural world models do not align.

### *8. The Need for a New Framework*

The Web's client-server framework precludes the client from participating as an independent addressable collaborative member of a global ecosystem. The client is neither identifiable nor addressable outside of the scope of its current domain. In a peer-to-peer framework, however, the client could easily be represented and participate as a member.

In the P2P blockchain model, each peer has a digital wallet. The wallet itself is a collection of private and public key pairs. Each private and public key pair plays an essential role. The private key, as the name implies, is meant to be kept a secret. A Bitcoin address is derived from the public key. When somebody sends a Bitcoin to your Bitcoin address, you will be the only person in the world with the corresponding private key to unlock it. The best common practice is to use a different Bitcoin address (hence a different public-private key pair) for each transaction. It is essential to understand that each transaction on the P2P Bitcoin blockchain is publicly available. That is, anybody and everybody can view the ledger and see the balance of each address. What they cannot tell is who owns the address as that information is kept private.

Any new framework must ensure the privacy of its participants while operating with the laws of the participant's host country. Certain government's such as Canada, India, Ireland, Norway, and the UK, along with those of the EU are at the forefront of data privacy. At the same time, taxing authorities require access to certain information. Similarly, justice departments want to ensure there is no illegal activity occurring. It is a delicate balance between the needs of privacy, finance, and the rule of law.

The design of a new framework must also consider the speed of adoption. After 30 years, the Web's client-server architecture will not simply be replaced. On the other hand, the adoption of digital currency is on the horizon, with its decentralized peer-to-peer model gaining attention.

This implies both the client-server model and the peer-to-peer model must persist in a single unified framework – a framework of everything.

Furthermore, the new framework has to provide and manage the keys that allow it to extend beyond the Web and the Internet as we know it today. It must be able to incorporate everything: independent, autonomous vehicles, machines, and even robotic devices with and without mobility. In certain cases, these machines may have no network connectivity at all. In other cases, the machines will untether from the network and reconnect at a later time. Depending on their form factor, communication may be limited to a speaker, a microphone, and optical devices such as a camera and/or an infrared transceiver. Most importantly, the framework must support the ad-hoc dynamic connections and communications to support even one-off transactions.

The new framework provides each user with sets of keys to associated keyed resources. This enables each participant to independently manage their own private digital ecosystem while being interconnectable with all other ecosystems under agreed rules. The individual decides who can participate in their ecosystem, similar to managing a contact list. Unlike a simple contact list, the participants have active direct connections with that individual's ecosystem. In this regard, the new framework enables collaborative ecosystems that are collections of independently owned and operated ecosystems. This collection of uniquely addressable ecosystems is a digital ecosphere.

A smart city is a type of digital ecosphere. It includes one or more digital ecosystems independently operating within the smart city. For example, the departments within the city government are independent of each other but collectively must adhere to and operate within the rules of the city charter.

The extents of the smart city are defined by the property boundaries. Each property can be independently owned and operated. The digital twins of these properties can be managed by software agents. Some of these agents work for the city, while others work for individuals, households, and organizations. Unlike the Web, these agents are peers that persist across digital ecosystems. At times the smart city will also have guests and anonymous visitors, each represented by digital twins that are peers.

The smart city must provide a dynamic mesh infrastructure enabling the peers to traverse and interact with the various shared services provided by the city workers as well as those services offered by the city's participants. It must do this while ensuring the peers persist across the digital ecosystems within the smart city. Just as there are peers representing people, there will also be peers representing places and things.

A smart vehicle will have a peer. When the vehicle enters the smart city, its peer can register its point of presence. In this manner, the city's Intelligent Transportation System can communicate with the smart vehicle agent independently of identifying the vehicle occupants. Meanwhile, the vehicle occupants can interact with the smart city grid to locate nearby points of interest such as restaurants, stores, doctors, parking, or other services. The smart city can help provide a direct connection between the occupant and the service provider.

In this hyperconnected view of the world, a truck entering the smart city can communicate with the city, notify its destination, and properly time its arrival. The destination can communicate with the truck to determine the bill of lading detail, the type, and size of the truck, and notify the truck which loading dock it should arrive at. The destination building can adjust its energy utilization within the loading dock area by calculating how long it will take to unload the content, which exposes the building to outside temperatures and humidity during that process.

## *9. The Transformation*

On the one hand, we can build a new independent decentralized framework as a standalone platform and integrate a web front end. That, however, does not solve the problem of the closed central authority model of the Web. Alternatively, we can build a parallel decentralized framework where the entire Web is represented as a resource available to the agents working for individuals, households, and organizations. We refer to this as the Universal Framework of Things (UFT).

The UFT views everything as a "Thing." This is distinct from the view of objects in the object oriented world, where an object is an instance of a superclass. Instead, a "Thing" is simply something a machine can do, act upon, or otherwise use. The simplicity of the model is that it allows us to represent people, places, and things of the real world as Things in a digital world. For example, you are represented by an intelligent software agent (a Thing).

The framework enables us to abstract away issues of languages and grammar, protocols, and syntax as Things. For example, some machines use the Internet and others communicate using sound and optics. Yet, both machines have a known identity and can collaborate as machines in a smart city.

In the UFT, identity is modeled as a Thing. This allows various identity models to be incorporated for different purposes. For example, a machine

can be identified by a serial number independently of identifying its owner and/or operator. The operator may simply be identified as the operator of the machine with this serial number. On the other hand, when completing a financial transaction, the operator may be identified by name, driver's license, and, when required, even their taxpayer identification number. Other identity models include biometrics.

Today the majority of identities represented on the Web are based on third-party unauthenticated email services which are prone to abuse and attack. Industry titans such as Google are working hard to require multi-factor-authentication (MFA) as a default option. The FIDO-2 standard is being promoted as a solution to proving a human is on the other end of the connection. Yet, in the new digital world, we will have more agent-to-agent communications.

In a hypothetical exchange, an offering agent will disclose a set of acceptable identity models to the potential accepting agent. The agent accepting the offer will use an acceptable identity model with the least identifiable information required. The sending of any identifying information must be authorized by the individual, household, or organization the agent is working for.

### *10. MultiKey Infrastructure (MKI)*

The agents can participate in a MultiKey Infrastructure to augment the use of the Public Key Infrastructure. Each MultiKey Key provides an agent with over $2^{512}$ cryptographically derived keys, any one of which can be used as another MultiKey Key. This creates a hierarchical arrangement of derived keys, all of which are cryptographically linked to the starting MultiKey Key.

In a simple view, the agent acts upon components of data, such as the components of a URL, to derive the hierarchical cryptographic keys from the starting MultiKey Key. For example, "https:" would generate one cryptographic key. Similarly, www.neursciences.com would generate another cryptographic key within the https MultiKey Key, and so on. By providing each agent a unique MultiKey Key to start, the agent can immediately generate unique keys for each and every URL of the Web.

MultiKey Keys can be distributed in digital form or in a physical form factor such as an ablated Holographic Memory ID (HMID) tag. The HMID tags are impervious to EMP attack and inert to radio frequency interrogation. Instead, the HMID tag requires line of sight optical interrogation,

such as with an LED light of a smartphone camera. With 3.4 billion smartphones in use today, anybody can participate.

## *11. Summary*

A new digital world is emerging where people, places, and things, need to be irrefutably identified, verified, and authorized in order to interconnect safely. The current Web framework of isolated domains is unable to easily support the required interoperability as only the servers are identifiable and addressable. In this paper, we describe transforming the Web into a Digital Ecosphere of independently owned and operated interconnected digital ecosystems. It is transformational in that it enables every individual, household, and organization to be represented as first class members of the digital world.