Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on

Advancing Privacy Enhancing Technologies

Data Freedom Foundation

Alan Rodriguez – Founder Data Freedom Foundation

The Data Freedom Foundation is an open-source non-profit advocacy group and standards body creating and advocating for the adoption and advancement of Consent and Privacy Technologies.

Summary Video (2 mins)	Google Selfish Ledger Commentary (12 mins)	Creating Digital Rule of Law (39 mins - MIT CDOIQ Symposium)

Creating the Economy of Ideas

Who will Own the Third Generation of the Internet?

We are witnessing the emergence of an Economy of Ideas, or the third generation of the internet. Web3—a group of technologies that encompasses Privacy Enhanced Technologies (PETs), blockchain, cryptographic protocols, digital assets, decentralized finance, social platforms, NFTs, and DAOs, combined with smart glasses that merge physical and virtual reality into one inescapable Metaverse – is the third generation of the Internet. Together, these technologies will serve as the basis for new forms of economic and social interaction arising from self-governed communities of trust that allow people to collaborate, create, exchange, and take ownership of their digital identity and assets.

Volatile digital currencies and speculative, risky investments grab most media attention. That's simply the spectacle, the rockets' red glare and bombs bursting in air. It's a distraction from something much more important. What matters most are the flags and the communities and values those flags represent. What matters most are the self-governed and self-funded communities, currencies, marketplaces, ecosystems, standards, and protocols.

Groups of people worldwide are creating digital communities of trust imbued with specific values and goals. They're creating and self-funding their own decentralized financial system. Digital pioneers are creating a parallel digital economy that will co-exist and increasingly interoperate with the physical economy. A digital economy of ideas orchestrated by efficient, transparent, and accountable algorithms powering trustable intermediaries replacing our aging medieval institutions. A digital economy of ideas is coming to life and illuminating the way to an infinite digital frontier.

Few would debate that Web2, powered by massive global data monopolies, took a wrong turn along the way. Neither the public sector nor the private sector has figured out how to grapple with the Pandora's Box of privacy breaches, disinformation, monopolistic practices, and algorithmic biases that have come to define much of the Internet. Meanwhile, authoritarian governments have never had more data with which to surveil, censor, and manipulate their citizens and those of other nations.

We need to have a serious conversation about the role we want technology to play in open societies. In this sense, web3 isn't just a new wave of innovation. It's an opportunity for a reset that allows us to obtain profound new benefits while solving some of the thorniest problems arising out of the technologies of the past.

For the first time in human history, we look upon an infinite digital frontier combined with the technologies for communities of trust to organize, own, create, and self-govern a global Economy of Ideas. What it means to be human in a digital world will change based on what we chose to create. And Web3 technologies provide the foundation to organize, fund, and create anything we can imagine.

The Problem/Opportunity

The world faces a profound problem with data and trust. Data propagates online without essential metadata to document ownership, define terms of use, or record its history. This lack of trust (data quality) is the root cause of most data challenges facing organizations of all sizes.

Our cultural lack of trust in data is also fundamentally incompatible with an open, participatory, and free digital society. This lack of trust is the root cause of most data challenges facing organizations of all sizes.

Smart Data Protocol binds software to data as it moves to give our data self-awareness and intelligence to assert its ownership, to record its history, and to enforce the terms of any contained agreements. The Smart Data Protocol is the missing licensing solution to build practical applications with digital assets.

1. The Smart Data Protocol is the patent-holding missing licensing protocol for highly tailored and transient digital asset reuse equipped with secure access revocation by digital asset owners.
2. The Smart Data Protocol is the direct link between digital asset creators and their enforceable ownership enabling sophisticated licensing monetization.
3. The Smart Data is the Distributed Data Fabric and Digital Rights Management Protocol for interoperable Web3 applications and the future of the Internet.

Data Freedom Foundation has patented the first comprehensive solution to controlling how our data propagates online and is used by others, even after being shared.

Solution/Product

Data Freedom Foundation's patented Smart Data Protocol binds software to data as it moves to give our data self-awareness and intelligence, assert its ownership, record its history, and enforce the terms of any contained agreements. The Smart Data Protocol fundamentally changes the nature of data from the uncontrolled propagation of untrusted bytes to the precisely tailored propagation of high-quality and trusted information.

1. The Smart Data Protocol dramatically improves data quality, data security, data provenance, and data trust amplifying the value generation from all digital and data-driven initiatives.
2. The Smart Data Protocol automates most security, privacy, and regulatory compliance reducing the cost of data transactions by half.
3. The Smart Data Protocol improves data comprehension and democratization boosting digital transformation outcomes.

Smart Data Protocol - Target Industries: Smart Cities, Smart Homes, Smart Farms, Smart Transportation, Smart Manufacturing, Smart Energy, Smart Healthcare, Smart Wearables, Smart Retail, and Smart Supply Chains.

Partnerships:

1. **Global IDs: Our first paying customer/reseller.** Global IDs is the leading Data Governance PaaS used by Chief Data Officers and Data Governance teams in global Banking, Insurance, Pharma, Telco, and Retail industries.
2. **Sertainty:** Patented provider of Data Container Cryptographic Data Security that remotely controls data access.
3. **TodaQ:** Provider of Cryptographic Data Container Provenance that operates in a fully decentralized manner with zero transaction cost. TodaQ provides unforgeable credentials, immutable audit log, and verifiable proof of ID to any asset to assure ownership (tickets, records, agreements, tangible, and intangible assets).
4. **Reprivata:** Provides Universal Data Ownership via Patented Communities of Trust (CoTs) that enforces a legal basis for the ownership of our identities and data grounded in international patent and contract law.

Smart Data — Timeline of Intelligent Technology

The unstoppable progression to "Smart Everything" also known as "Software-Defined Everything".

'SMART' means "Self-Monitoring Analysis and Reporting Technology". Smart software-defined products are capable of environmental awareness, group intelligence, and can automatically respond to internal and external events. [1 Wikipedia]

A **smart object** enhances the interaction with not only people but also with other smart objects. Also known as **smart connected products** or **smart connected things** (**SCoT**), they are products, assets, and other things embedded with processors, sensors, software, and connectivity that allow data to be exchanged between the product and its environment, manufacturer, operator/user, and other products and systems. [2 Wikipedia]

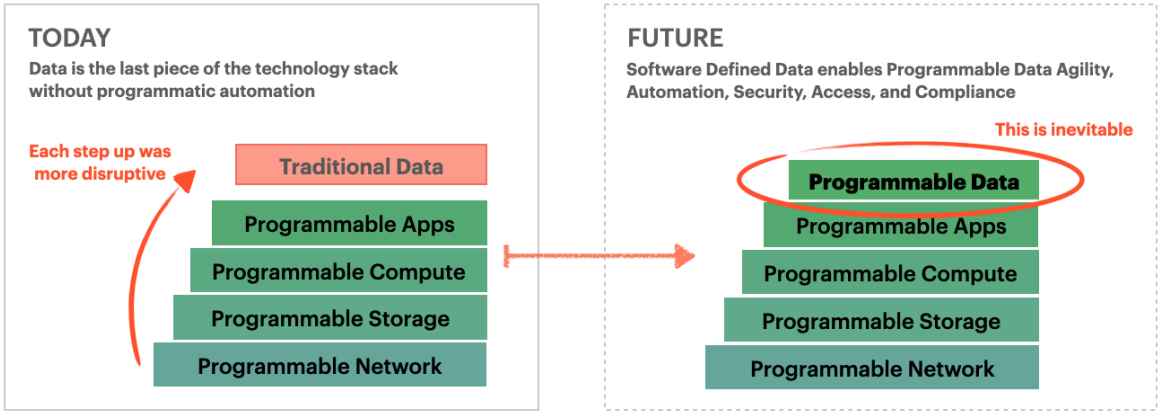
The smart object concept was introduced by Marcelo Kallman and Daniel Thalmann[4] as an object that can describe its own possible interactions. The focus here is to model interactions of smart virtual objects with virtual humans, agents, in virtual worlds.

Software-Defined "Smart" Everything

We've witnessed the slow and steady march of software control of complex hardware up the technology stack over the last twenty years from Software-Defined Networking and Network Virtualization to Software-Defined Storage and Storage Virtualization to Server Virtualization to Software-Defined Data Centers and Cloud Computing to Application Containerization and Application Virtualization.

Surprisingly, data remains the final tier of the technology stack that has not completed this software "smart" transformation. *Each step up the technology stack enabled automation which drove exponential cost efficiencies. Each step changed application architectures, allowing new business models, fundamentally altered technology roles, and the structure and operation of technology organizations.*

Arguably, each step up the technology stack was more disruptive than the previous steps. We believe Smart Data (software-defined data, programmable data, data virtualization with containerization, or data as code) will be the most disruptive step up the technology stack thus far.



Each step followed the Law of Diffusion of Innovation, with early adopters and innovators taking risks and benefiting immensely from first-mover advantages. We expect software-defined data to be more disruptive than previous steps.

As we look at each step up the technology stack over the last two decades, four repeating themes reveal what we can expect from The Smart Data Protocol:

1. Virtualization & Containerization as Software Abstractions
2. Application Programmable Interface (APIs) & Automation
3. Centralized Control & Distributed Enforcement from Policy Templates
4. Increasingly Self Aware, Adaptable & Environment Responsive

Virtualization & Containerization

Networking, Storage, and Server Virtualization all represent intelligent software and highly redundant hardware that was previously a single point of failure — a single hardware device. These are kinds of software-created network, or storage, or server abstraction.

Application Containers allow code to be packaged and distributed across different cloud platforms. These cloud platforms are software-defined data centers we can rent on demand that uses software-defined networking, storage, and compute as underlying technologies.

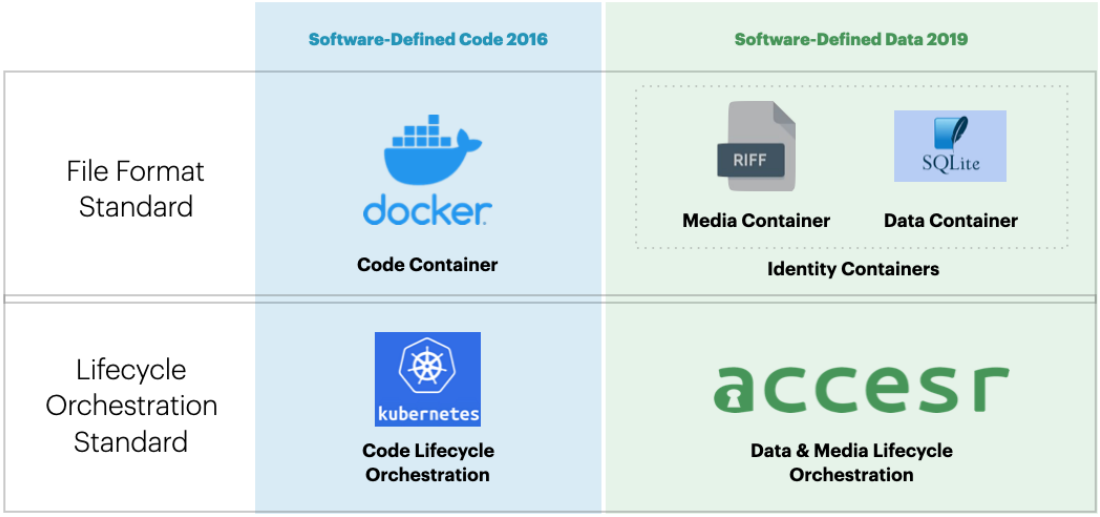
Data Virtualization is an existing enterprise technology that helps data management professionals understand and manage data flow within an enterprise. It enables internal applications to retrieve and manipulate data without requiring technical details about the data, such as how it's formatted at the source or physically located. It can provide a valuable master data source for a single customer view.

Data Virtualization does not currently extend beyond the organization boundary, limiting its ability to manage all organizational data. We propose adding Data Containerization that extends Data Virtualization to the network edge anywhere data moves inside and outside an organization.

SMART DATA = KUBERNETES FOR DATA

Our thinking builds upon Code Containers, called Docker files which ensure application code portability across all cloud platforms. Kubernetes provides Docker Code Container Lifecycle Orchestration across all compatible clouds coordinating creation, deployment pipeline automation, status monitoring, automated reconfigurations, versioning, and eventual deletion.

Data Containers enable secure and trustable distributed data automation across cloud platforms much the same way Application Containers enable safe and trustable distribution and orchestration of application code across cloud platforms.



On a more granular level, Accesr's Data Container Lifecycle Orchestration provides unprecedented data control for individual data owners, controlling creation, status monitoring, versioning, deactivation for non-compliance, reactivation for compliance, and finally deleted across all compatible applications and platforms.

Application Programmable Interface (APIs)

APIs are interfaces that allow different software programs to communicate and share data according to a set of clearly defined methods of communication. Developers can reuse and scale software architectures by making calls to available APIs of other programs. APIs are electrical sockets that connect programs and are the critical enabler of software automation.

APIs and their automation enabled the programmatic reconfiguration of networks and allowed traffic rules to adjust to changing networking needs. Or automate reconfiguration of server file systems to adapt their storage capacity based on dynamic and changing storage needs. APIs and automation enable entire data centers to be created within software, automated, and dynamically adjusted based on changing user and application needs.

All of this occurs with a fraction of the people it took to manage these systems without automation. Automation creates organizational agility and cost efficiencies while dramatically improving user experiences through enhanced consistency and quality. Data Container lifecycle APIs enable distributed Data Container orchestration and management for all targeted containers at each step in the data lifecycle.

Centralized Control & Distributed Enforcement

We repeatedly see centralized control paired with distributed policy enforcement across many technology layers. Organizations can set and automatically enforce policy constraints. They can change these constraints across potentially thousands of distributed systems by changing a single policy statement.

Increasingly Self Aware & Environment Responsive

Networks, servers, and applications became increasingly self-aware, adaptive, and responsive to their environment while operating within predefined administrator policies with instant recovery from every kind of hardware failure.

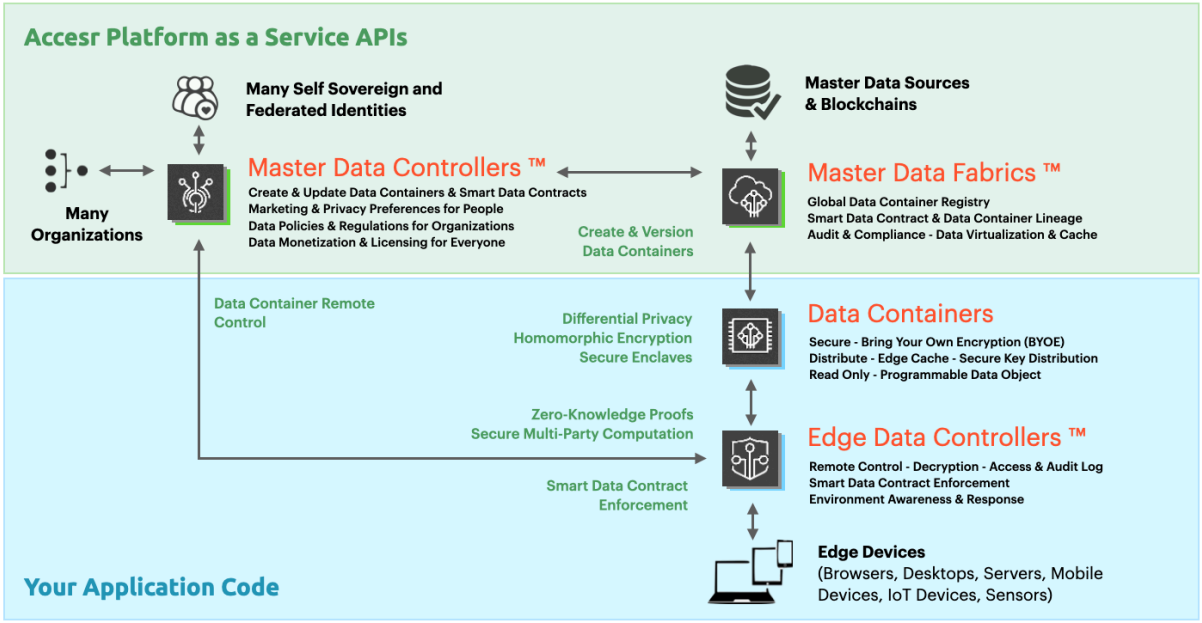
What if our data were self-aware and responsive to its environment? Imagine small open-source programmable data containers, holding only your data, encrypted with keys you control, moving around with Smart Data Contracts you create that constrain or guardrail the uses of your data — your personal data and your organizational data.

> *Applying these themes to data enables unprecedented data self-awareness; this allows a new era of data agility, regulatory and policy automation, distributed and dynamic data architectures, transparent and accountable data usage, with trustable data security, provenance, and quality*

Open Source Architecture for Data & Digital Rights - Converting centralized monopoly platforms into decentralized protocols and standards

We decided we needed two core distributed technologies, and we propose them as standards:

1. **Centralized Control:** Master Data Controller aggregates all our data and controls its current and future uses from one convenient location.
2. **Distributed Enforcement:** Programmatic Data Control & Automation secures our data with keys and access rules we control. We can alter all our data and approved uses, as it flows through and is acted upon by external technologies.



Central Control of Master Data

We consistently and repeatedly see the theme of centralized control paired with distributed enforcement across network devices, storage devices, servers, data centers, and application code. Organizations can set and automatically enforce storage, compute, server, and application code policy constraints. They can change these constraints across all distributed systems by changing a single policy statement from a central location.

We imagine an unlimited number of Master Data Controllers; each focused on the data transactions and data contracting needs of their respective communities, groups, or ecosystems. Master Data Controllers are where people, organizations, and groups establish a “home” for their individual or group data. They also control the uses of that data by others.

The Solid Protocol proposes a decentralized standard for establishing centralized control of our data within a distributed architecture. The Solid Protocol is the mid-course adjustment for the Web by its inventor, Sir Tim Berners-Lee. It realizes Tim’s original vision for the Web as a medium for the secure, decentralized exchange of public and private data.

A Solid Server hosts one or more Solid Pods. Pods are where you store your data:

1. Each Pod is fully controlled by the Pod owner (i.e., you).
2. Each Pod’s data and access rules are fully distinct from those of other Pods.
3. You can get a Pod from a Pod Provider, or you may choose to self-host your Pod.

You can have multiple Pods. They can be hosted by the same Pod Provider or by different Providers or be self-hosted or any combination thereof. The number of Pods you have and which Solid Server or Servers you use are effectively transparent to the applications and services you use. In the Solid ecosystem, data is linked through your Identity and not through the specifics of your Pod.

The Master Data Controller for Organizations provides one location to control all organizational Master Data, and by extension, all downstream data flows. It does this by managing all organizational data policies, external regulations that apply to internal data, licenses from external data providers, and user-provided personalization preferences. It encodes these data agreements into Smart Data Contracts and automates their enforcement inside and outside the organization.

The Master Data Controller for People provides one location to control the uses of all your personal data, and by extension, all downstream data flow. It does this by managing your application, site, and device personalization settings,

accessibility preferences, as well as marketing and privacy preferences. It encodes these data agreements into Smart Data Contracts and automates their enforcement everywhere your data flows and grows.

Data Containers

Data Containers are open-source transferable data files containing a single person's data and media like images, video, audio, key/pair value store, and relational value store. The Smart Data Protocol combines Sertainty.com Data Containers, with TodaQ.net cryptographic proof of provenance wrapped in an array of templated Privacy Enhanced Technologies.

The Sertainty data privacy protection technology encapsulates sensitive data inside self-protecting, self-authenticating, and self-governing computer files. This is accomplished by combining encryption keys, authentication credentials, and our intelligence engine with your data, creating impenetrable Sertainty files. Protection is adjacent to, not in conjunction with existing network security protocols. To add clarification to some phrases used above:

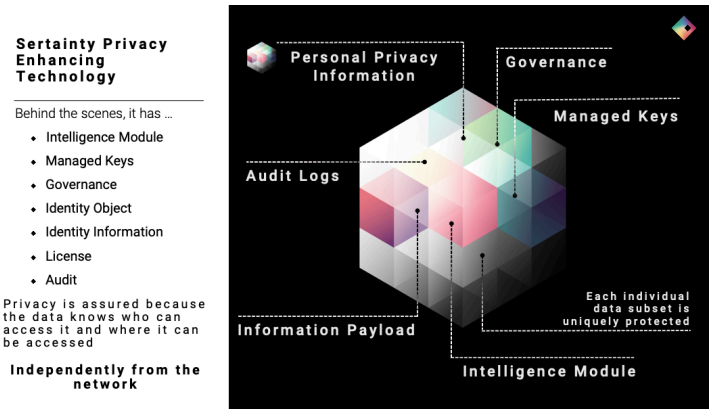
Intelligence Module – An embedded executable (think procedures inside a programming object) that is only accessible with an installed application having libraries and logic to access the files. Once the file is accessed, the executable controls data access, privacy and key management and auditing functions.

Self-Governing – The data owner determines the data's accessibility in terms of when, where, who, on what devices(s) and what network location(s). Those instructions are embedded in the file and enforced by the intelligence engine.

Self-Authenticating – Inside each file there is a Policy Implementer (PI) that contains information about each authorized user, enabling the intelligence engine to confidently authenticate users, processes, or devices, and thus ensure pricacy.

Self-Protecting – The intelligence engine acts as an internal key management system (KMS). The keys are both protected and transported within the file itself, but NEVER as clear text, this is NOT protection by obscurity. Because we embed our own KMS, we produce multiple keys that allow us to independently protect multiple internal structures.

Self-Reporting – Each time the Sertainty file interacts with an Operating or is modified, the event is permanently recorded in the file, and those interactions can then be securely sent to a SIEM Device.



The file components are broken into multiple parts, with each part separately secured, providing independent governance rules and encryption keys for each component. Sertainty uses AES-256 encryption plus other obfuscating techniques. The goal is to ensure the secured file is: used by the right person; at the right time; in the right location (physical or logical); on the right device. Encryption is a means to a goal, not the ultimate outcome.

Bring Your Own Encryption (BYOE)

As we contemplated the uses of Data Containers in real-world scenarios, intrinsic and undeniable privacy became the most interesting property. We quickly realized data owners could, would, and should encrypt their data with keys they control before placing their data inside their containers for distribution. We now consider this behavior of using one's encryption unavoidable. It's very difficult to stop. It's potentially impossible to stop. Even if we, or others controlling the technology, wanted to prevent this behavior. It's an unavoidable privacy-preserving property of Data Containers. The intrinsic and unavoidable privacy preservation of Data Containers continues to fascinate our team.

Smart Data Contracts

Smart contracts have evolved into sophisticated distributed policy engines often associated with blockchains. Smart Data Contracts build on Smart Contract technology and apply the same ideas to automate data transactions and data agreements. They document data policies, regulations, licenses, and user preferences in language software can execute and automate.

Smart Data Contracts define and enforce data licenses, regulations, policies, and preferences, allowing data owners to remotely control each Data Container by defining, revising and revoking:

1. Who can access our data
2. When can they access our data
3. Where can they access our data
4. What questions do they ask of our data - Zero-Knowledge Proofs
5. How they need to protect our data – Differential Privacy, Synthetic Data, Security Standard Complinace, etc
6. How they can share data with others – Secure Multiparty Computation.

Review, revise, or revoke your Smart Data Contracts at any time regardless of where your Data Containers are located.

Taken together, we start to see a standard for automating GDPR, CCPA, CPRA, and other regulations. Imagine fully automating the right to be forgotten or the right to data portability? Imagine automating internal data policies as data flows inside and outside an organization?

Key Point: While we can't automate all data usage terms that might exist in policies, regulations, licenses, and preferences, we now possess the technology to automate most of those terms. We believe that, with the proper foundation, future innovators will discover many new and interesting automation and encryption methods.

Edge Data Controllers

The Edge Data Controller gates and controls all access to Data Containers while automatically enforcing Smart Data Contract terms. Edge Data Controllers are like database executables interacting with Data Containers like database files. They are like data bodyguards or intelligent agents scanning and assessing their environment.

Data Containers are inaccessible without the cooperation of an Edge Data Controller providing secure key distribution and gating all data interactions per the terms of the attached Smart Data Contract defining the terms of the Zero-Knowledge Proofs and Secure Multi-party Computations.

Edge Data Controllers follow the familiar (CRUD) Create, Read, Update, Delete data lifecycle for all Data Containers. Edge Data Controller APIs in coordination with Master Data Controller APIs enable the Data Container lifecycle.

Intelligent Composable Applications

Programmers can think of Data Containers as Programmable Data Objects or modular software components that hold our data, our data usage rules, as well as presentation code. These rules allow and disallow data interactions. Presentation code can include dashboards for analytics data, a shopping cart within a social post, or a micro pay button to bypass a paywalled article.

Programmable Data Objects are a kind of Intelligent Composable Application with more agile, modular, and adaptable data architectures. They also enable automated preferences based on personalization at scale.

Edge Compute/Metaverse Integrations

Edge devices exist outside traditional IT boundaries without physical protection and workload integrity and without standards for data protection, detection, and remediation across potentially compromised networks and platforms.

Edge devices and data must interoperate across a growing number of organizations. The Internet of Things (IoT) includes a bewildering array of edge devices and use cases. The combined Global IDs/Accesr solution solves this missing standards problem and secures the remote data flowing across potentially insecure edge networks.

Non-Fungible Tokens/Blockchain Integrations

NFT Licensing doesn't work the way NFT advocates say. We cannot license, limit use, or revoke access to digital assets or data. NFT licensing is basically broken.

Our combined solution enables PETs, cryptographically secure data containers, and cryptographic data provenance to be used in combination with blockchains and NFTs solutions to finally solve digital asset and NFT licensing and monetization challenges.

Digital and data asset monetization require:

1. Transient or time-bound use with a commencement date, duration, renewals, and extension conditions.
2. Limitations on terms of use include responsibilities, geographic restrictions, rights of use, permissible channels of trade, sub-licensing, or assignability to another party.
3. Legal rights enforcement ensures the digital asset owner can take data assets back and revoke access per the terms of the license agreement.