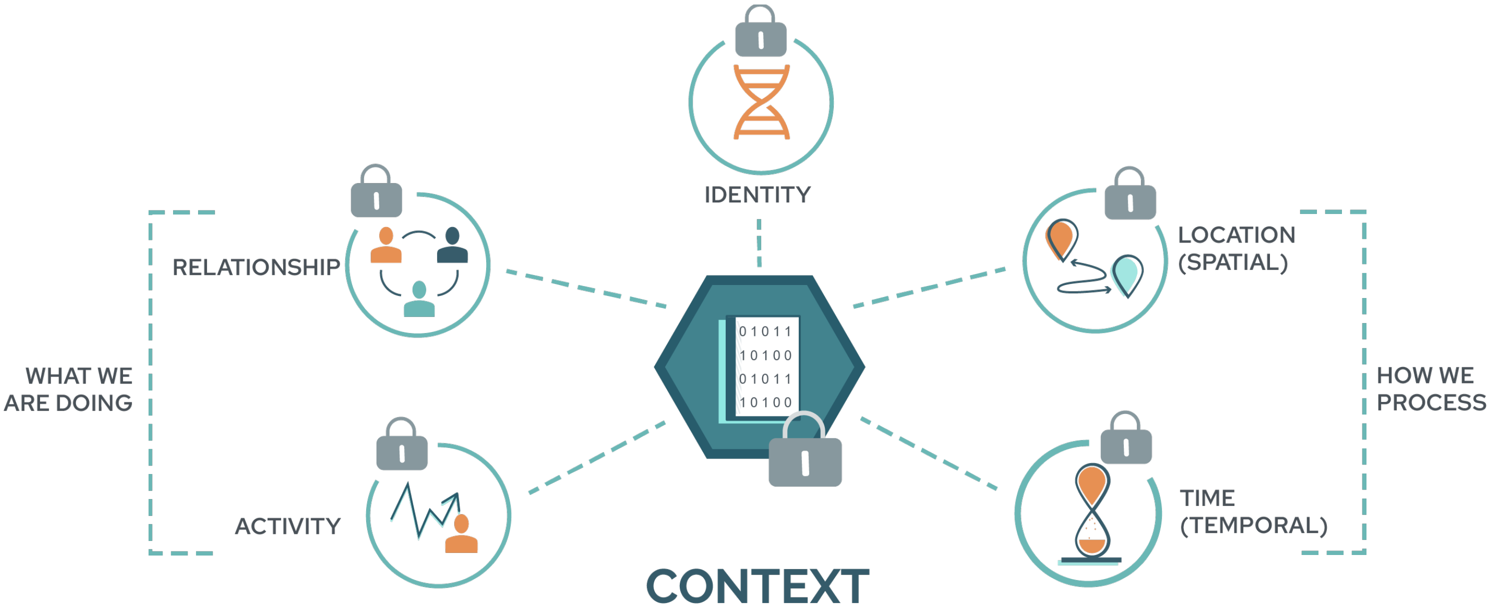
TECH INSIGHTS

Smart Data: Next-Gen Data Privacy and Intelligence

In a traditional Privacy-enhanced technology (PET) and Privacy-enhanced computing (PEC) environment, attributes like metadata, edge relationships, ownership, and use permissions are maintained separately from the data itself. Anyone who has tried to create and manage comprehensive data dictionaries and metadata dictionaries understands how difficult it can be to maintain the currency and accuracy of these directories.

Privacy-enhanced data (PED), or smart data, represents the next evolution in data privacy and intelligence. It is fundamentally a new data construct that fuses data attributes such as metadata, edge relationships, ownership, and use permissions into a new data object that is cryptographically signed and attested. In early publications, this was often referred to as self-aware data objects.

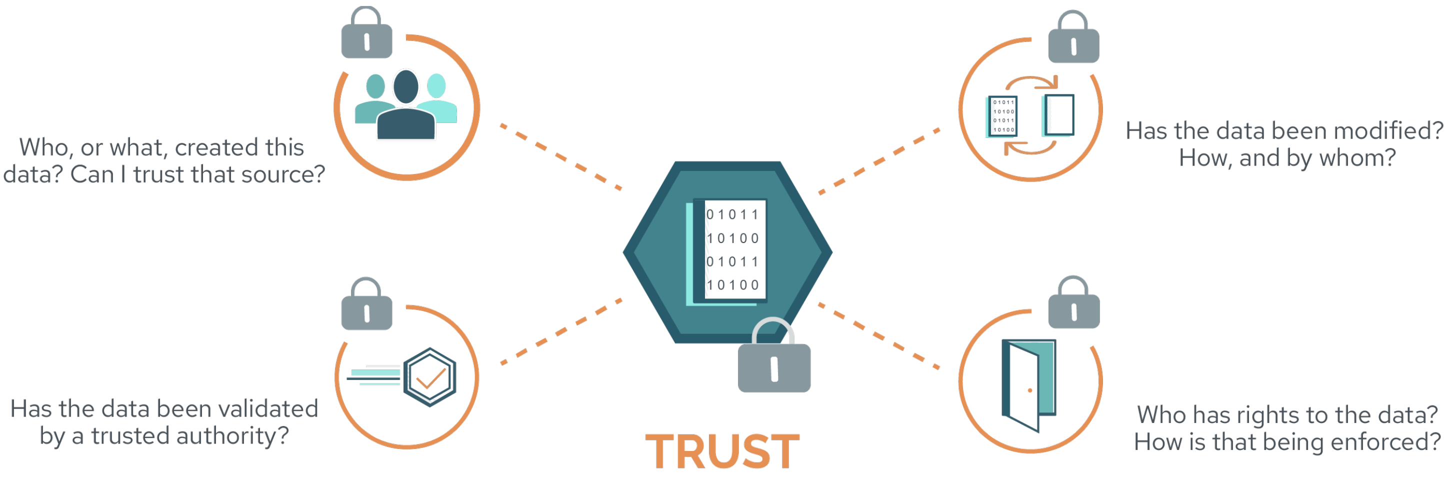
By fusing these attributes with the data itself, the smart data object is just that – smart. Certain embedded attributes, such as metadata and edge relationships, give smart data context. This context can be used in real-time to configure and drive the behavior of the processing systems. Instead of hard coding all the logic in the application or control systems, smart data applies real-time logic to each individual data object.



The analytical and intelligence power of this cannot be overstated. If each smart data object can independently operate in processing systems based on its unique attributes, the system as a whole is able to learn, adapt, and optimize far more quickly than in traditional models. With the explosive growth in data volumes, the deep intelligence that companies are trying to glean from that data, and the broader shift into Web3, smart data thrives where traditional data models have faltered.

In addition to providing context, a smart data object contains trust attributes. First and foremost, the smart data object embeds and enforces ownership and use permissions, so data security remains intact even as the data is moved and replicated. In addition, trust attributes provide a detailed audit of how the data has been changed or updated over time, how ownership and use permissions have changed, and whether the data has been authenticated or verified by a trusted entity.

By embedding trust attributes within the data, smart data solves another tough problem: data integrity and privacy. Because ownership and use permissions are part of the data itself, the ability to revoke permissions becomes a standard feature.


Who, or what, created this data? Can I trust that source?
Has the data been modified? How, and by whom?
01011
10100
01011
10100
TRUST
Has the data been validated by a trusted authority?
Who has rights to the data? How is that being enforced?

Why does all this matter? Smart data disconnects data from its central control systems, so data security and intelligence are as mobile as the data itself. This frees the data to be shared, replicated, and updated – all without compromising the data security, integrity, and intelligence that are required to run your Web3 business.

The Role of Blockchain

“You can’t store data on a blockchain.” It’s a statement we hear often. But having worked with highly sensitive data and cryptographic security methods for over 30 years, we can confidently say, “You’re wrong.”

Many of the “experts” who jumped on the blockchain bandwagon in 2017 and 2018 see blockchain as synonymous with distributed ledger technology (DLT). Those of us who have been working in this space for decades know that blockchain is actually comprised of multiple technologies that were combined to form what we now think of as blockchain.

By expanding our definition of blockchain beyond a limited DLT focus, we can see that same methods that are used to create DLTs and cryptographic data objects (aka, blocks) can be used to create privacy-enhanced data.

The core technologies inherent in blockchain allow us to assign ownership to a piece of data, manage permissions to that data, and establish data integrity and provenance. Once these core security layers are embedded into the data itself, the formerly “dumb” data object becomes a smart data object (i.e., a PED) which can be stored on chain, shared on chain, and even deleted (yes, deleted) on chain.

When coupled with PET and PEC techniques, PEDs provide a very robust layered privacy model. At BurstIQ, we bring together the fundamental methods of PET, PEC, and PED (in combination with advanced data modeling techniques) to create LifeGraph. LifeGraph uses PET, PEC, and PED constructs to create a highly secure and contextualized data picture of a person – their digital DNA. Smart data is embedded into a robust protocol stack that uses blockchain methods at multiple layers, enforcing data immutability, ownership, provenance, state, and, through specialized smart contracts, chain of custody, use, and access.

By combining PET, PEC, and PED technologies, it becomes possible to decentralize privacy and intelligence without one compromising the other. It becomes possible to maintain data trust, integrity, lineage, and security even as data moves around a decentralized ecosystem. And it becomes possible to run true distributed intelligence and gain deeper insights from it through the additional layers of context embedded in smart data.

In short, smart data makes it possible to deliver on the promise of Web3.

The Promise of Protected Data

The fundamental opportunity, and challenge, of Web3 is to create a future in which data is connected, individual privacy and ownership rights are respected, incentives are aligned, and trust is inherent.

Given that the whole purpose of PET/PEC is to protect data, protect privacy, and protect against misuse, coupling PET/PEC capabilities together with PED makes it possible to create a world in which the digital rights and dignity of every person are respected. A world in which corporate profits are determined by the degree to which a company can offer people value in exchange for the privilege of accessing their data, rather than the degree to which they can control and hoard that data.

Regulations and consumer demand are forcing companies to adapt to a Web3 world. Companies that adopt a Web3 data strategy are benefitting from greater consumer trust, higher value products, and increased market share. Most importantly, people are being empowered with the means to own, control, and derive value from their data in the way that works for them. And that is the true promise of Web3.

About BurstIQ

BurstIQ is redefining how businesses get maximum value from their data. LifeGraph is a Web3, privacy-enhancing data platform that infuses trust into digital solutions. The platform brings complex data together, manages ownership, and makes it smarter and more trustworthy for AI and machine learning. The LifeGraph data ecosystem gives organizations a continuously learning single source of truth. With it, they can get trusted answers from their data and turn insights into digital solutions that deliver more value to customers, patients, and employees – quickly and cost-effectively.

From operational data networks and workflow optimization to hyper-personalized digital engagements, LifeGraph brings privacy, security, ownership, and consent into a single, easy-to-adopt platform. The platform is used by large and small enterprises all over the world to create transformative digital solutions that address healthcare's biggest issues.

burst iQ