WHITE PAPER

How Smart Data Powers a Web3 World

burst iQ

Table Of Contents

Beyond Big Data

Data is the lifeblood of business. It is used to make decisions, inform processes, allocate resources, manage performance, and capture deep insights. In our personal lives, we rely on data to guide our health decisions and actions, from whether we should seek care and where to get the best treatment to how we protect ourselves and our families.

It's estimated that humans generate 2.5 quintillion bytes of data every day.[1] This data is created by billions of people, devices, applications, and organizations. People rely on mobile apps for health tracking, physicians enter medical information into electronic medical records, and fitness devices generate movement and location data – just about everything we interact with generates data. Additionally, COVID-19 has revolutionized how we "do" healthcare. Our society had to shift to virtual health and telemedicine quickly. Health workers found ways to do work remotely. Testing moved out of labs and into our homes. As a result, big data is even bigger than ever.

This influx of data holds tremendous potential but also a significant risk if the data isn't protected or used ethically. Your business needs a sound data strategy to ensure that they are using data effectively to build trust and deliver maximum value for customers and shareholders. That's where smart data comes in.

There is also a movement away from a centralized internet (Web 2.0) to a decentralized model (Web3). Your business can differentiate by adopting Web3 principles and demonstrating your commitment to individual data ownership. Smart data can play a significant role in helping your business meet these Web3 standards quickly and effectively.

In this article, we'll discuss how smart data helps build trust and value by transforming how data is managed, accessed, analyzed, and used to build trustworthy Web3 experiences. But first, let's examine how you currently manage data.

How Much Do You Trust Your Data?

According to a study by HFS Research, 75 percent of business executives do not have a high-level of trust in their data and 70 percent do not consider their data architecture to be "world class."[2]

Given how critical data is to business success, it's no wonder companies are worried. If you are relying on "bad" data to make the decisions that will make or break your business, you are flying blind. **Bad data has enormous downstream implications: bad intelligence, bad predictions, bad user experiences, and missed opportunities.**

How is Your Data Being Stored?

When data lives in silos, the level of trust your business can attribute to data is only as great as the level of trust you can attribute to the entity that controls the data. This may be manageable in a Web 2.0 world, where your business controls all the data you need. But in a Web3 world, you won't. In Web3, your business will need to break down data silos and create a single source of truth – and that single source of truth will need to include data you don't control.

Many organizations cite data security as a rationale for creating data silos. Data silos make it hard to analyze and share data, even internally. It's not uncommon to see data silos exist between departments or divisions, despite the value that could be gained from a more connected approach. Silos in healthcare reduce efficiency, impact the quality of care, and lead to wasteful and costly duplication of services.[3]

In recent years, data warehouses and data lakes have taken hold within large enterprises, somewhat alleviating the problem of internal data silos. But data warehouses still suffer from significant security vulnerabilities, cumbersome access management, and lack of flexibility. As Web3 takes hold and businesses are tasked with accessing, managing, and analyzing data they don't own or control, centralized warehouses are showing their limits.

"Think of how much data exists in healthcare alone – not just health records data, but also pharmacy data, genome data, and data from wearable devices. How can consumers trust that companies are using their data appropriately? How can businesses or researchers trust the authenticity of that data if they can't verify the source or can't verify that the data is unaltered? Unless data can be trusted, it just creates a lot of noise."

- Brian Jackson, President and COO of BurstIQ, A Web3 Data Security and Intelligence Company

According to a recent Gartner Chief Data Officer Survey, data and analytics leaders who share data externally generate three times more measurable economic benefit than those who do not.[4]

Are You Protecting Data Effectively?

According to a recent KPMG survey, "86% of the respondents feel a growing concern about data privacy, while 68% expressed fears about the amount of data collected. Some 40% of the consumers surveyed don't trust companies to use their data ethically, and 13% don't even trust their own employers."[5]

Health data, in particular, is highly sought after by hackers because it garners big money on the dark web. The healthcare sector suffered about 337 breaches in the first half of 2022 alone. More than 19 million records were implicated in healthcare data breaches in the first six months of the year.[6]

Ongoing healthcare data breaches have eroded patients' trust in the ability of providers and health plans to protect their data. A recent Harvard T.H. Chan School of Public Health and Politico survey showed that only 17% of patients have a "great deal" of faith that their health plan will protect their data, and only 24% trust their hospital to keep their data safe.[7]

For business owners, building (or rebuilding) trust doesn't equate to putting data back in silos. In order to succeed in a Web3 world, data needs to be both connected and secure. That requires a complete rethinking of how data is managed.

In the US, data breaches cost companies an average of $9.44M per breach.[8]

As your organization migrates data into connected networks, you must consider the benefits that connected networks offer, as well as how you will need to manage data differently in these systems.

- What impact will these moves have on how we manage data?
- How do we adapt to new regulations and consumer demands for data ownership?
- What do we need to do to protect our intellectual property?
- How can we reduce our data security risk and liability?
- How can we most effectively protect consumer data to maintain and restore consumer trust?

Leadership conversations around data security and trust must evolve in organizations across all industries, but especially in healthcare and life sciences. Turning data into smart data is a critical strategy to ensure data integrity, protect the data rights of patients and consumers, and improve the effectiveness of health-related products and services.

"I can't count the number of conversations we've had where an organization claims their customers' data is safe because they encrypt the data and keep it behind a firewall. That does not engender trust. As a consumer, I need to know that I have complete control over my data, not just cursory access through some privacy settings. As a business, I need to know that the data comes from a trustworthy source and hasn't been altered over time. That's what builds trust."

- Amber Hartley, Chief Strategy Officer, BurstIQ

How Smart is Your Data?

For data to be considered smart data, the data must possess the following characteristics:

Auditable

Can you prove that any changes made to the data were authorized and correct, or do you need to rely on the assurances of the entity controlling the data?

Authentic

Can you trace the data back to the original trusted source? Can that source be verified as trustworthy?

Complete

Is the data complete, or are there pieces missing (such as demographic information) that would add more context, understanding or trustworthiness?

Timely

Is the data current? Are there risks due to the age of the data? If so, what are those risks?

Compliant

Is the data secure? Does the data meet external and internal guidelines for regulatory compliance?

What is Smart Data?

OK, let's get technical for a minute. 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. Let's look at the main components of a smart data object: context, trust, and security.

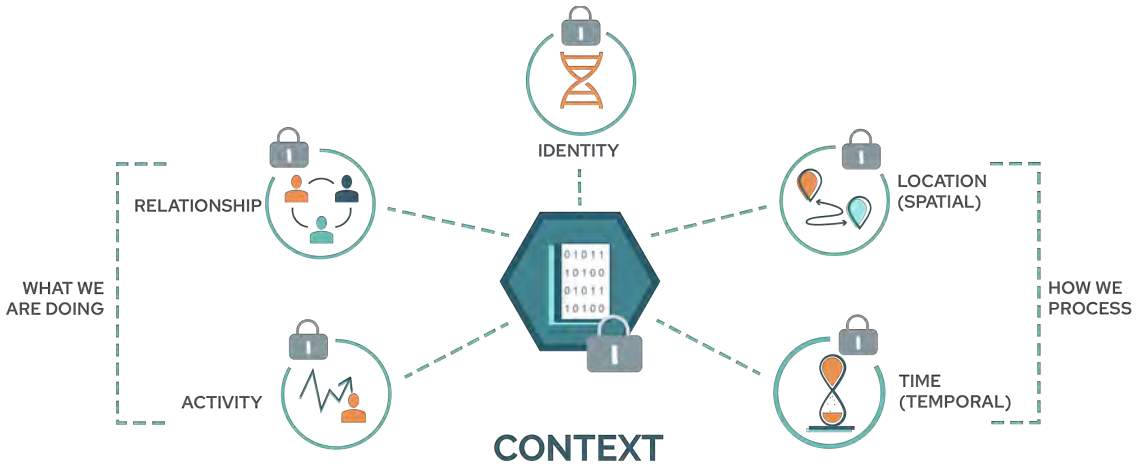
Context Leads to Better Understanding

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 is like having a real-time logic plug-in that drives the behavior of each data object independently.

Here's how this works in the real world: Let's say your business operates patient engagement solutions for people with Type II Diabetes. Your smart data object may be centered around a patient's recent medication prescription. In a smart data object, that prescription may have other attributes that help you understand this prescription better: who is the patient, and where do they live? Is this a new medication, or a renewal of an old med? What is their medication refill history? Are they sedentary, or active? Are they chatty on text, but never answer calls? Do they live alone, or with family?

When data is configured as smart data objects, all this other information is directly linked with the prescription data and can be used in real-time to inform the behavior of your processing system (in this case, an engagement algorithm). So, your engagement algorithm can immediately see that this is a new prescription. Based on past refill behavior and the current address of the person, it decides to recommend an online pharmacy and guide the person through the process. The same algorithm then automatically triggers a daily text reminder to take a 15-minute walk through the person's neighborhood. All because it understands more than the prescription itself; it understands the broader context of that prescription and serves up ways to make the patient healthier.

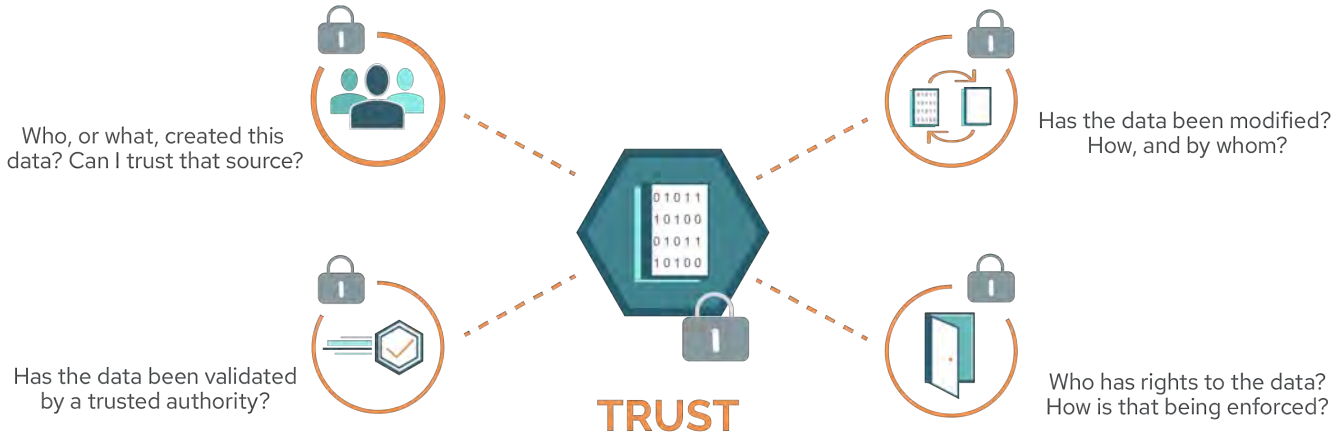


The analytical and intelligence power of this cannot be overstated. If each smart data object can independently operate in processing systems based on its unique attributes, the system as a whole is able to learn, adapt, and optimize far more quickly than in traditional models. With the explosive growth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

Trust Ensures Data Integrity

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 within the data itself, so data security remains intact even as the data moves and evolves. 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: ensuring the integrity and privacy of data you share with others and data shared with you. Because ownership and use permissions travel with the data, the ability to revoke permissions, and verify that revocation is being enforced, becomes a standard feature.



Security Wherever Data Moves

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.

In typical data management platforms, access management tools moderate data access using a role-based approach. In role-based access management, permissions are assigned to a role (administrator, case manager, etc.) rather than a specific individual, endpoint, or combination. Within that role, any user can access all the data assigned to that role. Role-based access management tends to be especially vulnerable to security breaches because a nefarious actor has many possible entry points to access a large amount of data. If they can spoof an authorized role or phish a known and authorized account, they can access all data authorized to that role.

To reduce this security vulnerability, smart data provides two additional data access layers, as shown in the figure below, that work together to limit both the possible breach points and the amount of data that can be accessed if a breach attempt is successful.

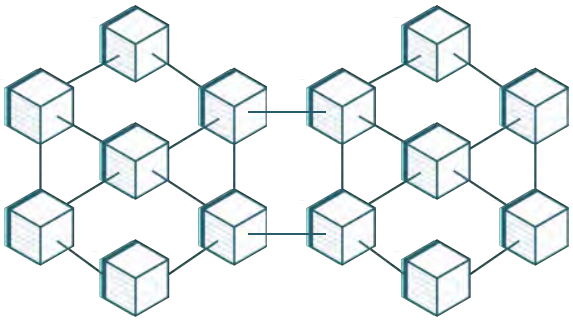
Cryptographic ownership is embedded and enforces within each individual data point.

Consent Contracts enforce both 1:1 consent-based data access and network-wide data governance.

These Layers are Unique to LifeGraph®

Role-based access controls enforce access to application services.

The Role of Blockchain



All of this is made possible through novel uses of blockchain technology. 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. Blockchain can be used to create connections, broker data-sharing transactions, verify value, and confer ownership.

Because smart data embeds data ownership within each piece of data, ownership can be decentralized – distributed among many collaborators or individuals – instead of being consolidated in the entity that administers the database. Accordingly, the value and bargaining power inherent in that data is also decentralized.

Smart Data Powers a Web3 World

Decentralization is one of the core tenets of Web3. But what exactly is this new iteration of the World Wide Web? Well, Web3 is defined by three fundamental principles.

Self-Sovereign Identity

Self-sovereign identity is the idea that individuals should own their digital identity and data, and control how their information is accessed, used, and monetized. Because smart data allows you to assign ownership to a piece of data, manage permissions to that data, and establish data integrity and provenance, it makes self-sovereign identity possible.

Power Shifts from Tech Giants to Individuals

Trust

Web3 is often described as "trustless," but this characterization is more than a bit misleading. The term "trustless" implies no trust. The term was first applied in the cryptocurrency space and was used to describe a process where one does not have to depend on a trusted entity (like a broker or bank) to conduct and verify transactions. In other words, you don't need to trust another person for something to be executed in a valid and verifiable way. However, because smart data (and the blockchain technology it uses) embeds validity and verifiability directly into the data, trust becomes an inherent part of the data itself. Web3 moves away from a "trust the broker" model into a "trust the data" model.

Decision-Making and Knowledge are Collective

Decentralization

Web3 supports multiple levels of decentralization: decentralization of data, ownership, control, decision-making, computing resources, value, and power. This represents a true paradigm shift that is made possible largely due to the capabilities of blockchain technology and smart data.

Internet and Data are Decentralized

Why Smart Data is Good Business

As the Internet Age evolves from a centralized Web 2.0 model into a decentralized Web3 model, businesses are being forced to rethink legacy data strategies and adapt to this new paradigm. Smart data is a fundamental building block that will help you quickly adapt to new business demands.

Data Ownership is Shifting

A Web3 movement is here. Consumers are demanding that businesses move away from data owned by a central authority (Facebook, Instagram, and Google, for example) to a decentralized framework where individuals directly own their data and control how it is shared and with whom. **Businesses that adapt to this movement early can successfully differentiate, build trustworthy reputations, and gain critical first-mover advantages in a Web3 world.**

Laws and Regulations are Changing

In response to consumer demand, regulations are being introduced that aim to tighten existing laws around data privacy and ownership. In addition, standards bodies such as W3C[9] and FIDO Alliance[10] are introducing technical standards that promote data portability and interoperability.[11] These standards create a bridge between traditional IT systems to new Web3-aligned smart data exchange networks. **Organizations that carefully contemplate their data strategy and how they will participate in smart data network models, where individuals have direct ownership of their data, will be better positioned for success in a Web3 era of increased privacy, consumerism, and connectivity.**

Cyber-Attacks are Increasing

While data networks share some of the characteristics of data lakes and data warehouses, they are designed to connect diverse and disparate datasets, including data an organization doesn't own. If not done well, this level of connectedness can expose organizations to increasing levels of risk.[12]

Organizations must think carefully about how to adopt smart data models, infrastructure, governance, and security protocols that help them stay ahead of cyber threats.

Ultimately, the growth in smart data networks will not only lead to advancements in data security and the proliferation of smart data but to advancements in data intelligence, personalization, digital twin technologies, and autonomous systems.

AI is Transforming Healthcare and Life Sciences

Healthcare and Life Sciences stand to benefit significantly from the advancements detailed above. Smarter data and smarter intelligence can help improve the effectiveness of both operational and clinical decision-making systems. **By understanding and being able to leverage the context and trust built into smart data, healthcare and life sciences companies can uncover deeper insights, automate complex processes, and provide more personalized experiences to their users. The consequences are far-ranging, affecting everything from organizational performance to public health.**

Hyper-Personalized Health Experiences are Essential

The emergence of smart data and Web3 holds great promise for improving the lives of entire populations. Providers can deploy smart data and Web3 technologies to accelerate digital transformation and operate more efficiently while continuing to deliver high-quality patient care. Smart data can even be used to create secure and private digital twins that can be used for precision testing of thousands of treatments, leading to better-informed decisions that improve patient outcomes and minimize potential harm. **This can take personalized medicine into a new era where patient care is informed not only by each person's medical history and health risks, but by their unique life context.**[13]

Ready to Transform Your Data into Smart Data?

At BurstIQ, we believe the health industry is at a tipping point. The technology exists to break down silos, make data smart, and connect data. BurstIQ is ready to help you adopt this technology so you can make data work harder for your organization.

Founded in 2015, we are on a mission to unleash the power of data to help each person live their healthiest, happiest life. We believe that smart data will democratize health on both a global and individual level. LifeGraph from BurstIQ revolutionizes how you manage data in a highly secure, private, and trustworthy way – all so you can deliver meaningful digital experiences that will make the world a healthier place.

For more information, visit: **www.burstiq.com**

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.

Sources:

[1] https://techjury.net/blog/how-much-data-is-created-every-day/#gref

[2] https://www.rtinsights.com/executives-dont-trust-data/#:~:text=Accordingly%2C%2025%20percent%20of%20organizations,to%2099%20percent%20high%20quality.

[3] https://www.weforum.org/agenda/2020/11/healthcare-silos-are-bad-for-us-heres-the-cure/

[4] https://www.gartner.com/smarterwithgartner/data-sharing-is-a-business-necessity-to-accelerate-digital-business

[5] https://info.kpmg.us/news-perspectives/industry-insights-research/data-privacy-survey-orson-lucas.html

[6] https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far

[7] https://www.fiercehealthcare.com/tech/more-than-70-hospital-data-breaches-expose-sensitive-information-putting-patients-at-risk

[8] https://www.ibm.com/reports/data-breach

[9] https://www.w3.org/

[10] https://www.csoonline.com/article/3604680/fido-explained-how-this-industry-initiative-aims-to-make-passwords-obsolete.html

[11] https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

[12] https://www.accenture.com/_acnmedia/PDF-137/Accenture-2020-Cyber-Threatscape-Executive-Summary.pdf

[13] https://www.forbes.com/sites/forbestechcouncil/2022/08/30/how-digital-twins-can-accelerate-healthcare-transformation/