IDC Customer Spotlight

Sponsored by: **Gospel Technology**

Author: Dominic Trott

August 2017

Gospel: The First Practical Enterprise Application of Blockchain

Executive Summary

Digital transformation (DX) is crashing on the shores of the enterprise like a tsunami, driving demand for cloud computing, Big Data analytics, mobility, and social business. These trends have a profound impact, enabling new ways of working, fostering customer intimacy, and enhancing end-user experience. But it also means existing approaches to enterprise data are now broken.

DX results from the business imperative to speed up decision making. Data must be more accessible to enable this. The flow of data needs to improve not just within the enterprise, but also with third parties such as contractors and partners across the value chain. Collaboration across end-to-end value chains is imperative to react to and even predict shifting customer needs.

As well as being accessible, data must also be trusted. While DX initiatives bring business benefits, the flipside is the deperimeterization of data security. DX drives users to store data on third-party (cloud) platforms and access or share it across mobile devices and social platforms. These exist beyond boundary controls such as web or messaging gateways, firewalls, or endpoint protection.

This deperimeterization is driving access paranoia. Rather than enterprise data being freed from traditional, siloed environments, the typical response is for artificial segregation to be further entrenched. Any approach to enterprise data cannot focus purely on corporate data, which is sensitive in its own right. Personal data must also be considered, whether it relates to customers, employees, or any other stakeholders (e.g., investors). Growing realization of the impact that increased legislation such as the EU's General Data Protection Regulation (GDPR) will have on the privacy, governance, and security of both corporate and personal data is adding to this instinctive reaction to lock down data. However, there are significant knock-on effects.

Persistence with siloed data environments flies in the face of the very reasons why enterprises are compelled to pursue DX. This not only slows down data collaboration, and therefore the achievement of business goals, but also drives users to find "workaround" solutions that will allow them to achieve their goals outside the corporate IT environment — so-called shadow IT. But this only serves to further erode security and privacy, undermining an organization's overall compliance and risk management posture.

Trying to resolve the access/trust imbalance with the same approaches will simply result in the same problems. Instead, enterprises ought to rethink their approaches

to data handling. Private blockchain is emerging as a catalyst to resolve this dilemma.

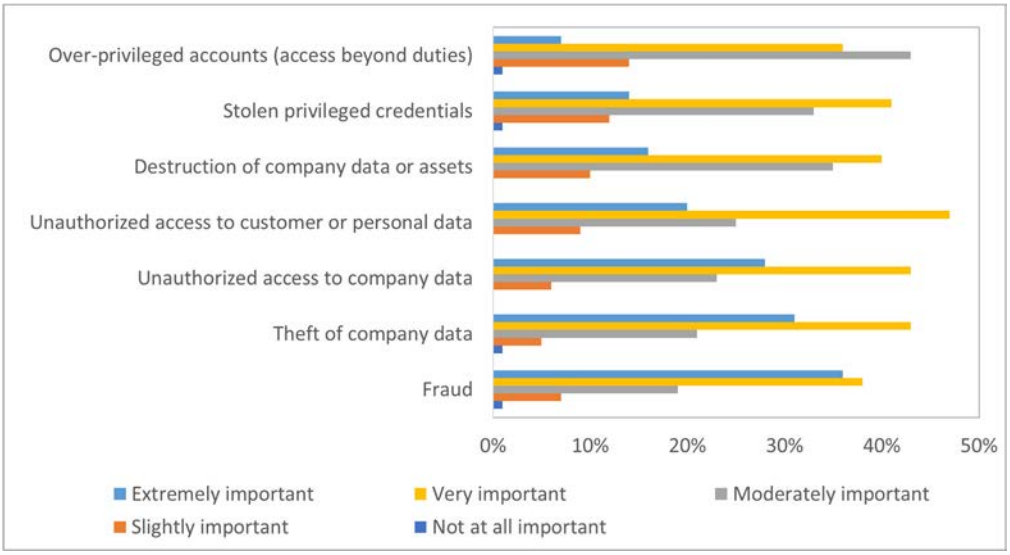
It is fair to say that many of the developments around blockchain are hype topics that will not resolve enterprise issues around the access/trust imbalance. Examples include cryptocurrencies and public blockchain environments. But the evolution of the foundational technology, particularly around private blockchain environments based on platforms such as Hyperledger, means it is now ready to provide enterprises with sufficient scale and resilience to answer the challenge. In IDC's view, it is these characteristics of private blockchain that are designed to meet enterprise-grade requirements that underpin the first practical applications of the technology to address the very real issues enterprises now face.

DX and the Deperimeterization of Data

A key limitation on the ability to realize the business goals linked to DX initiatives is that the deperimeterization of infrastructure and access via cloud computing, mobility, and social business typically has not been matched by the deperimiterization of data itself. In many cases enterprise data remains within siloed enterprise application environments.

In large part, this detachment between the transformation of enterprise architecture and enterprise data is the result of paranoia surrounding insider threats. As shown in Figure 1, unauthorized access is viewed as a primary threat that is important to manage.

Figure 1: How Important is the Management of the Following Threats?



Source: IDC, 2016

Whether it is malicious insiders, such as the infamous case of Edward Snowden, or simply an "unwitting" vulnerability caused by insufficient security hygiene behavior, enterprises are terrified of unwanted third-party access to sensitive enterprise data. In either case, the concern is significant because, even if security controls are 100% effective, when credentials are compromised then even the best protection becomes redundant.

So, while there is good reason for caution around deperimeterized data access, there are significant ramifications of being over-cautious. The first of these is the restriction placed on DX-related business considerations such as cooperation and collaboration around enterprise data. This inhibits the flow of data within the enterprise, let alone between third parties across the value chain.

The second implication springs from the first. If end users find themselves unable to achieve their targets through the corporate environment, they will be driven to find alternative solutions. This is where shadow IT arises, taking enterprise data outside the visibility and control of security and IT teams. There are countless examples across all sectors of confidential customer information, financial performance figures, intellectual property, and many other types of sensitive data being compromised due to the use of less secure transfer methods (such as email) that punch holes in the protections put in place. So, while security and IT professionals may view that the enforcement of siloed data environments reduces exposure to risk, the result is an even greater exposure.

This situation highlights the need for a cultural change as much as a technical one to both maximize the benefits and minimize the risks of DX. IDC's research indicates that DX is a board-level priority, with almost 90% of enterprises stating that DX is a key part of their corporate strategy. The combination of these two implications means that, despite access paranoia, enterprises still end up with a crisis of trust. With complexity rising around the types and volumes of enterprise data held, with the constantly evolving threat landscape, and with data handling approaches remaining rooted in convention, IDC only expects this challenge to become worse.

Regulatory Reform Calls for a Rethink on Data Collaboration

Multiple regulatory reforms around data privacy and security are emerging from the U.S., the EU, and beyond. These are driving a change of mindset in the way that enterprise data is handled, stored, and shared. Key examples are highlighted in Figure 2.

Figure 2: Sample International Data Privacy and Security Regulations

Source: IDC, 2017

For the purposes of this report, the focus for regulatory reform will fall on the EU's GDPR. This is due to its timeliness, enforceable from May 2018, as well as the scale, impact, and reach of the regulation. However, it is important to note that GDPR is only one example that forms part of a broader trend that will continue to have a global impact on enterprise.

The Significance of GDPR

For starters, it is IDC's view that the regulation represents a significant step up in the level of risk related to enterprise data handling for any business worldwide with connections to data subjects (i.e., individuals) that are either citizens or even just residents of the EU. This means that GDPR is not just an EU regulation, but a regulation for doing business with the EU.

When it comes to the enterprise risk of GDPR, much attention has fallen on the punishments that can be doled out. Most well-known are the fines of up to 4% of worldwide group (not just subsidiary) revenue (or €20 million, whichever is higher) that can be levied for non-compliance. Also significant are provisions for class-action lawsuits, the requirement for mandatory breach notifications (raising the issue of brand reputation), and even the risk in the most egregious cases of non-compliance of a ban on processing EU personal data altogether.

These punishments are significant, and that is intentional — GDPR is designed to be "effective, proportionate, and dissuasive." However, even more important is the impact on data handling processes and culture. To be GDPR compliant, organizations must prove how, for example, personal data remains private and secure by design and by default. They must have a view on who has access to what data, why, and what they have done with it. They need to give regard to the state-of-the-art technology in addressing GDPR compliance. They also need to ensure that they have an audit trail to demonstrate each of these points.

These considerations call for a shift in data privacy and security mindset and culture. Traditionally this tends to be an afterthought, implemented later as an additional "layer" after the delivery of any project. While this may be sufficient for "tick box" compliance exercises, the layer approach has two downsides.

First, usability will suffer, with post-implementation security controls likely to inhibit achievement of the project's goals. Second, there are likely to be gaps in coverage if the level of security is insufficient for the degree of protection required. But GDPR means that, for any change in the handling of personal data, the impact on that data must be considered from the very beginning.

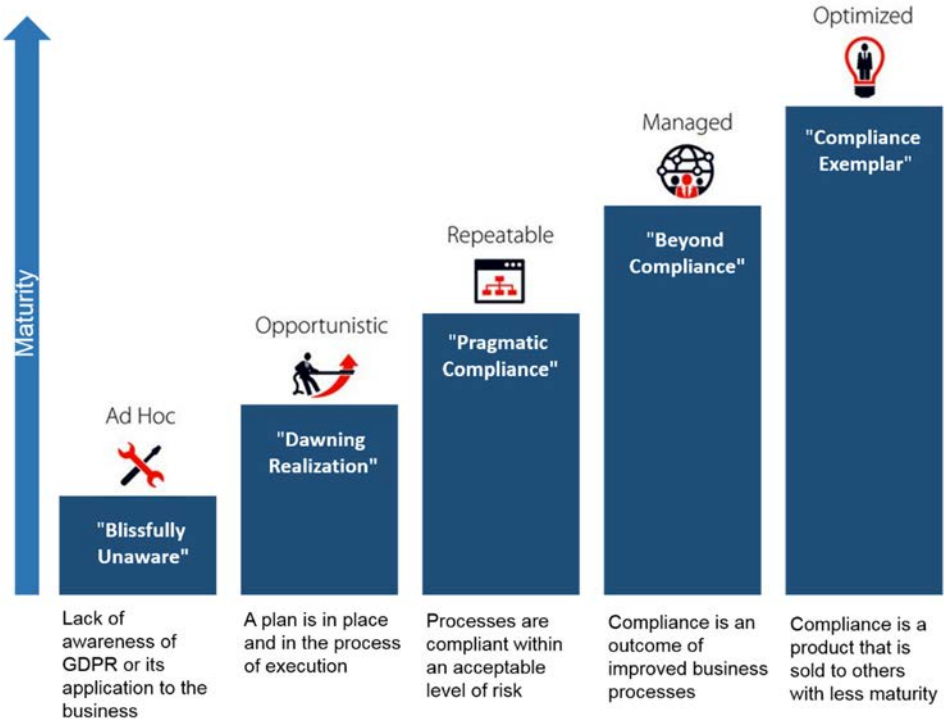
While GDPR is designed to drive improvement in the handling of personal data by enterprises, it is expected that this will cause enterprises to reconsider their approach to data handling in its entirety. Enterprises are revisiting their data handling approaches all the way from the cultural approach at one level, to enterprisewide processes, and through to the technology that enables them.

Therefore, while personal data is the regulatory catalyst driving these changes in behavior, corporate data handling will have to be addressed as part of end-to-end approaches required to address concerns such as privacy and security by design and default that are called for in GDPR.

GDPR Readiness

While GDPR is imminent, and the impact significant, enterprise readiness varies hugely, with significant room for improvement. IDC's research into GDPR readiness has identified five key stages of maturity, as shown in Figure 3.

Figure 3: GDPR Maturity Model



Source: IDC, 2017

As of July 2017, according to IDC's research, the largest category is "dawning realization," representing 40% of enterprises, which is in fact short of compliance. Meanwhile, 17% are still "blissfully unaware." So, while the remaining 43% of enterprises (25% "pragmatic compliance," 18% "beyond compliance," 1% in "compliance exemplar") are ready for GDPR in one shape or form, well over half of enterprises (57%) are not ready, despite enforcement being mere months away.

For many organizations, the time for gradual change has long passed. Radical overhaul is required around the technology, processes, and culture in their approach to data privacy and security. IDC believes that private blockchain can be a catalyst for enterprises to quickly and effectively climb the maturity scale.

Blockchain: A Call to Action for Managing Enterprise Data

DX means that enterprises must find ways to redefine their approach to data handling. This is not just within their own organization, but also with third parties across the extended data value chain. What is more, concerns around access and trust mean this must include heightened privacy and security. It is IDC's view that private blockchain must be part of this refinement process.

What is Blockchain?

Before coming onto the enterprise implications of blockchain, one must first understand what blockchain is. Blockchain is built on the distributed ledger principle where data is replicated and shared across multiple systems.

In a distributed ledger system, users can access and verify the integrity of the ledger data. They can also add transactions under a specific set of rules. This occurs without the need for a central authority to manage and reconcile transaction data. This allows efficient, real-time, secure data sharing. It is not important how or where data is stored, but how consensus is achieved. Hence distributed ledgers are defined by a consensus mechanism between the nodes. The product is an immutable and distributed database of digital assets.

Blockchain itself is a consensus algorithm and a type of distributed ledger that contains unchangeable digital data in packages called blocks. Blocks are formatted in a chain of ongoing blocks detailing a series of transactions. Data in each block is hashed and linked to the previous block. This process ensures the integrity of all data in the overall blockchain. In many enterprise cases, the hash is then encrypted to offer even greater assurance as to the integrity of data within the blockchain.

Blockchain enables a distributed network of nodes to continuously reach consensus on the content of blocks of data. When this algorithm is deployed, the blocks are ordered to form a constantly growing linear chain, where each block is linked to a previous block and can only be appended to the end of the chain. This provides an immutable log of operations during deployment.

Public vs Private Blockchain

There are two types of blockchain environment: public or "permissionless" deployments, and private or "permissioned" deployments.

Public blockchain environments are open to all, accessible by anyone with a connection to the internet. This is to say they are "disintermediated." Users can connect to the environment anonymously, meaning that public blockchain deployments cannot be used to attest to the validity of identity. Yet transactions are visible to everyone on the blockchain, which could potentially be anyone.

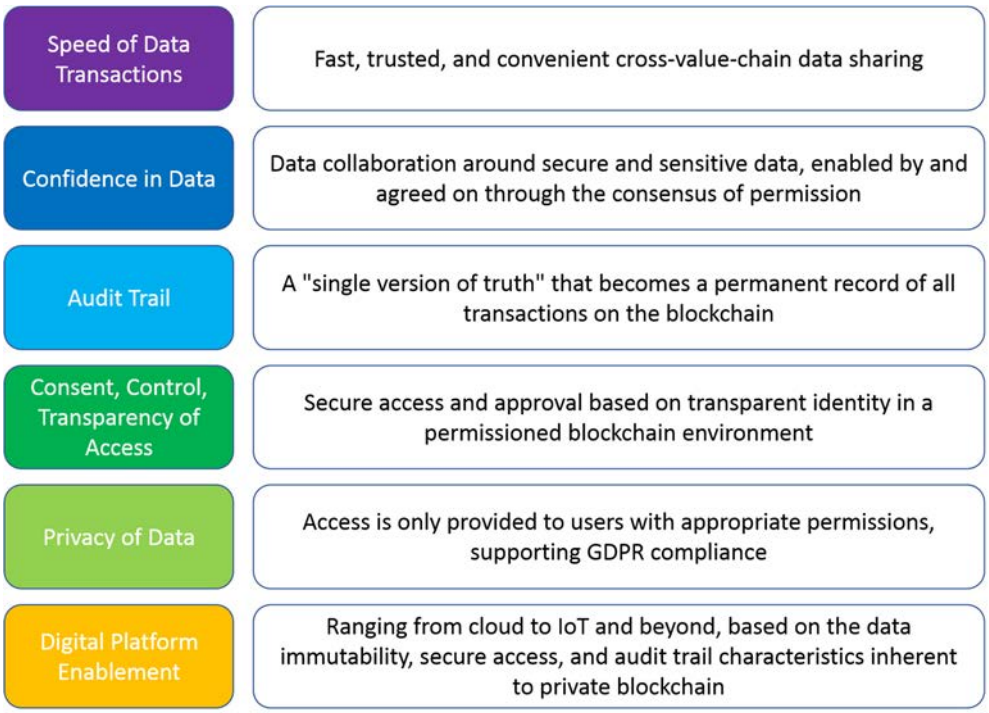
Because the identity of public blockchain users is often unknown, they operate on a proof-of-work basis. In the case of Bitcoin, a prominent public blockchain, this is achieved through the completion of algorithms to "mine" bitcoins and add new blocks. Bitcoin demonstrates how public blockchain is open yet anonymous. This explains why among other things it is popular for malicious activities such as ransomware payments.

Private blockchain environments are open only to those who are invited to join them and possess approved credentials. This may be controlled by a single "leader" or a group of participants. Because the identity of users is known and trusted, proof-of-work is not required to allow transactions. Instead, they rely on the establishment of consensus through cryptographic signatures, rather than relying on centralized approval or mediation.

The Enterprise Implications of Private Blockchain

It is IDC's view that there are several characteristics inherent to blockchain that position it as a technology that can help reconcile the enterprise imbalance between access and trust that arises from DX. These can be broken down into six high-level themes, as demonstrated in Figure 4.

Figure 4: Enterprise-Ready Attributes of Blockchain



Source: IDC, 2017

A key implication of these characteristics is the impact that this has on compliance with data privacy and security regulations. For example, trust in data, record of transactions, transparency of identity, and permission/consent of access are all features called for by GDPR. Blockchain provides a means of achieving each of them by design and by default.

In fact, IDC breaks down the role of technology in GDPR compliance into three components, for each of which private blockchain has implications, as follows:

1. Information governance (i.e., managing the data life cycle)
2. Meeting specific requirements (i.e., right to be forgotten, consent, encryption, data portability, record keeping, etc.)
3. Reviewing "state-of-the-art" (establish "appropriate technical and organizational measures" relevant for your organization and context)

The third implication is the ability of private, permissioned blockchain to act as a bridge that integrates the enablement of DX business imperatives with a solution to trust concerns and regulatory reforms through a single platform. It is through this integration that blockchain enables the business to resolve the imbalance between data access and trust that has emerged from traditional, siloed data handling environments.

There are four key characteristics here that allow private blockchain to perform this transformational role:

1. The permissioned participation and consensus-based operating models ensure trust in the identities of users and consent for users' access to data. This contributes to the security and privacy of enterprise data.
2. These same characteristics mean that private blockchain models are not inhibited by the time and resource requirements of public blockchains, allowing data transactions to be conducted instantaneously, or at least close to real time. This supports the need for timely access to relevant enterprise data as required by DX strategies.
3. The "audit trail" characteristics inherent to blockchain, with each block being added onto the chain of all previous transactions, provides a single source of truth in both the nature of transactions and the identities of who carried out transactions. This is key for the security of data, but also for regulatory compliance.
4. The distributed nature of blockchain means multiple users have instant and secure access to all the data they are entitled to. This is in contrast with siloed models, whose inherent inflexibility are driving shadow IT and therefore compromises security, privacy, and regulatory compliance.

It is clear that, in order to meet the business imperatives of DX, security, privacy, and regulatory compliance, there is a need for enterprises to adopt new cultures, processes, and technologies. Persisting with the same old models and expecting different outcomes is clearly an untenable approach. IDC believes that, implemented correctly, private blockchain can be the catalyst for change that enables this imbalance to be resolved.

Demonstrating this point, Vivek Kundra, investor in Gospel Technology, former CIO U.S. Federal Government, and current COO of Outcome Health, describes the impact of private blockchain on enterprise data handling as follows:

> *"The use of private permissioned blockchain within the enterprise environment is a huge leap forward for the future of data integrity, as companies move to make information more accessible across decentralized infrastructure and business partner relationships. The growth in customer and personal data being generated and processed, coupled with legislative pressure to maintain control of its usage, requires an immutable and trusted data solution."*

Market Moves Enabling Enterprise Scalability

There are already indications that enterprises are investigating the potential that blockchain represents for securing their digital strategies. This is indicated by the emergence of a range of pilot projects incorporating blockchain technology for purposes beyond just cryptocurrency implications. However, the technology is still emerging, meaning that there remains plenty of room for expansion.

Mounting Enterprise Attention on Blockchain

There are encouraging early signs of enterprise interest in and adoption of blockchain. However, it is also fair to say that the market has been distracted from the opportunity to solve the trust/imbalance issue surrounding enterprise data handling due to the large degree of hype that surrounds the topic.

For example, there has been significant media focus on public blockchain-enabled cryptocurrencies, such as Bitcoin. This has been so extensive that many in the industry have taken to focusing nomenclature for blockchain propositions and implementations around the term distributed ledger technology to avoid confusion with cryptocurrencies.

Meanwhile, many applications of blockchain are simply irrelevant to addressing enterprise issues. For example, the impact of blockchain is often publicized in relation to opportunities such as enabling the sharing economy and providing identities for refugees. While these applications of blockchain can be transformative in their own way, they do not address enterprise data handling.

Blockchain Communities and Hyperledger

Nonetheless, enterprise interest in blockchain to enable deperimeterized data models continues to mount. A major driver of this is the formation and expansion of collaborative forums, projects, and platforms for blockchain development. These are aimed not only at driving awareness of the applicability of blockchain to solve enterprise challenges, and exploring its potential, but also to overcome the scalability obstacles blockchain poses.

Hyperledger is a key example of these nascent blockchain communities. This is the Linux Foundation's blockchain community initiative, aiming to harness the power of open source to advance blockchain as an enabler for DX. Hyperledger was officially launched in February 2016, and currently includes more than 120 member companies. Demonstrating the serious enterprise credentials of both the community and blockchain as a technology, its membership includes global firms such as Accenture, Airbus, American Express, Fujitsu, IBM, Nokia, and SAP.

The enterprise implications of blockchain, as outlined in the "Blockchain: A Call to Action" section of this report, explain the strong and growing enterprise interest in Hyperledger. However, another important driver is the fact that Hyperledger is actively working to overcome some of the challenges inherent to blockchain that have inhibited broader uptake to date. A key example here is around the issue of removing some of the blockchain scalability concerns by reducing the latency of transaction processing caused by consensus operations.

Conclusion

For enterprises operating in today's post-perimeter reality, "business as usual" is no longer realistic when it comes to data handling. The ongoing occurrence of security breaches alone is enough evidence to render the arguments of security, visibility, and control linked to traditional, "siloed," data environments redundant.

Security breaches are not the only driver. Also significant are the business imperatives of widespread, faster access to data as a means of speeding up and improving decision making. These two sides of the same coin add up to a "perfect storm" that requires change in order to reconcile these imbalances.

Distributed ledger technology, and blockchain environments that are built on top of it, are emerging as a solution to this imbalance. The mounting enterprise interest in the topic, backed up by a growing number of reference cases, is testament to the technology's enterprise readiness. Importantly, this goes way beyond the power of public blockchain models and cryptocurrencies, and is relevant not just to the financial services industry but on a truly horizontal basis.

IDC envisages that the blockchain-enabled transition to deperimeterized data handling models will be driven by "natural selection." Those adopting this approach will be better placed to innovate at pace, correlating data across both internal and external connections. This in turn will make them more attractive partner organizations that will value the speed and trustworthiness of transactions on offer.

These organizations will also be armed for compliance with data protection regulations calling for concepts such as privacy and security by design and default, state-of-the-art technology, and the demonstration of compliance. As seen in the Enterprise Implications section of this report, blockchain plays a role in each area.

Blockchain will also help to make enterprises more attractive to their customers, for two key reasons. First, blockchain provides an opportunity for enterprises to position themselves as trusted partners, able to hone competitive advantage through the security, privacy, and widespread access of their data handling, all without compromising on speed of access. Second, it also presents the opportunity for customers to benefit directly from the benefits of blockchain, becoming members of the permissioned distributed ledger network.

Importantly, enterprises do not view these business benefits as a pipedream. The growing levels of interest, participation, and deployment indicate that enterprises are already testing the waters in the search for new approaches that feature blockchain as a means of building trust, security, privacy, and access into data flows.

This mounting interest is also indicative of the fact that blockchain is increasingly recognized as a technology that can handle the scale and complexity required to support data handling transformation on an enterprisewide basis, and beyond. In fact, it has the potential to become the catalyst that enables end-to-end digital deperimeterization. For example, enterprises could use private blockchain models to match digital infrastructure and assets, spanning cloud, mobile, and IoT, with a distributed and decentralized environment to handle the secure and rapid flow of data across all touchpoints. This simply could not happen using traditional models.

Gospel Technology Company Profile

Gospel Technology is a leading software company in the enterprise blockchain space, fixing data sharing challenges for businesses needing to distribute critical information internally and externally with total security, trust, and control.

This approach allows organizations to remove manual workarounds, eliminate data breaches, remove human errors, and stop accidental data loss. Organizations are also realizing that traditional IT infrastructures have degrading security profiles, lowering overall data security while the cost of maintaining these environments continues to increase. Financial information, confidential customer records, intellectual property, meta data, and other unstructured files are all at risk from this access/trust imbalance.

Gospel's solution builds a fabric of trust to distribute data which is enterprise grade scalable, highly resilient, and secure.

The platform's "privacy by design" data logic built on top of the distributed ledger technology is also what sets it apart, facilitating the more complex aspects of legislation such as GDPR and the use of personally identifiable information (PII), including the right to be forgotten and consent-based control over how an individual's data is utilized by third parties.

Gospel's clients come from a range of sectors (retail, finance, automotive, government, healthcare, media, telco, and manufacturing) where the need for control over access and an immutable record of any sharing history is key, providing trust in an untrusted environment.

Gospel Technology is headquartered in London, with a worldwide partner network that gives it a truly global reach.

https://gospel.tech/

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.