INDEPENDENT THOUGHT

Blockchain in the Governent sector

Preparing the ground for a new breed of citizen services

In this paper we examine some of the big shifts happening across all industries in the current COVID climate, how these relate to organisational and user needs in the Government and public sector specifically, and how different players are adapting to these changes. We look at how blockchain can be a positive force for responding to public sector problems and opportunities; and in particular, what you can do next in *your* organisation in order to take advantage of this emergent technology.

This paper is sponsored by

IBM

Independent Thought provides independent technology industry insights to professionals working with emergent technologies. We work with tech suppliers to help them better anticipate and respond to their customers' needs, frame their marketing messages, and understand how their portfolios stack up against the competition; and with tech buyers and end-users in organisations large and small to help them to think themselves into new futures, become smarter customers, and get the best value from their tech investments.

www.IndependentThought.works
hello@IndependentThought.works

Top takeaways

1

Self-sovereign digital identity is blazing the trail for a wider portfolio of blockchain-based citizen services to follow.

Governments are beginning to capitalise on the apps and wallets that have started to find their way into individual citizens' comfort zones by building on trailblazing self-sovereign digital identity projects (like COVID-related health passports). These distributed, data-driven citizen services encompass a wider government purview – such as social security services, and the purchase / registration of large consumer assets (e.g. land and vehicles). For example, the EU is proposing that 80% of its citizens will be using a digital identity by 2030, as part of its *Digital Decade* initiative to transform public services more widely.

2

Pre-approved government blockchain network environments, running on government-sanctioned cloud services, are needed in order to make it easier for public sector projects that *want* to deploy blockchain tech to do so without each having to address the same issues from scratch.

An essentially "government-approved" blockchain service, running on a government-approved cloud, would make it much easier for public sector agencies to set up distributed applications. This is because many of the non-functional requirements around security, reliability, etc. will already have been addressed up front – and so the technology will much more readily be considered as part of the common enterprise architecture environment for such initiatives. But there's a "can't use this because it's not approved yet" loop which needs to be broken first. A high profile government project is needed to kick things off in the first place, to attract positive attention and serve as an exemplar upon which business case momentum for wider government blockchain initiatives can be built.

3

During the pandemic, many government projects have been effectively "running to stand still" in an effort to gather the data they need, and so have yet to turn their full attention to the benefits that emerging blockchain networks can bring.

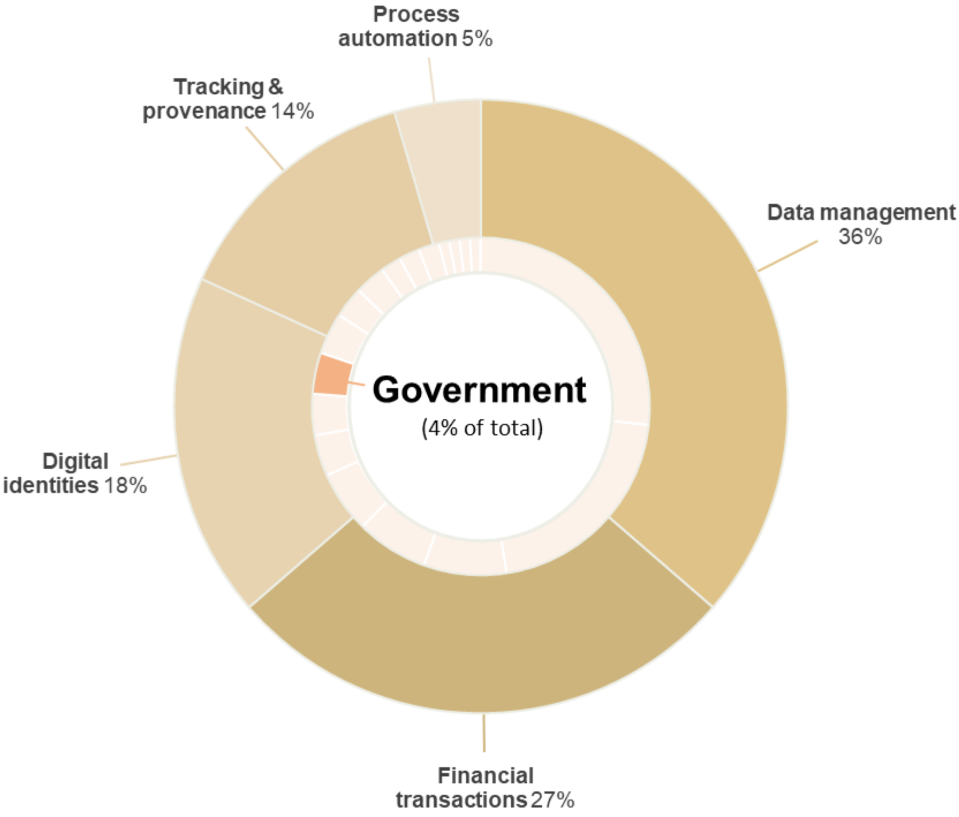
Governments have been keen to secure access to the data they need – both to drive more digital transformation in the citizen services arena, and also bring them the insights required to make more informed decisions about prioritising public spending. However, during COVID times, many have found it non-trivial enough to accomplish this *at all* because of fragmented supply chains, poorly integrated data ecosystems, etc. Let alone step up a gear to gather *further* data and gain service influence through membership of permissioned blockchain networks. As COVID's immediate crisis innovation priorities start to give way to longer-term horizon goals though, there's now a growing interest in how blockchain networks can drive the development of a new generation of citizen services. And also enhance opportunities to learn about what's needed and how they're used.

Setting the stage

Independent Thought's *Blockchain Index* research looks at the spread of blockchain use cases across industries, logging projects that have "changed state" over time – i.e. they've announced a major strategy initiative, initiated a proof-of-concept project or transitioned a pilot into production, or significantly scaled up an existing offering.

Despite there being numerous uses cases across the Government and public sectors which have historically shown affinity for blockchain-enhancement, a COVID focus on getting things done in the most "familiar" (vs new and novel) ways came to dominate many governments' outlook on blockchain tech during 2021. The more conservative sectors (Government amongst them) have tended to somewhat rein-in any pre-COVID enthusiasm for less well-established emerging tech (like blockchain)… even if they may ultimately provide for a more enhanced service and bring greater business benefits in the longer term.

Figure 1: Blockchain project activity in Government, 2021



Source: Independent Thought (Blockchain index)

Reticence and risk

IBM's research, born of recent blockchain engagements, bears this out. They've noticed that in the US, both Federal and State governments have tended to operate in a "we're going to do things the way we've done them before, just to get it done quickly" mode of late. And that's not necessarily included blockchain, regardless of whether it might be a great tool to have in the box this time around.

But as economies start to emerge from their (understandable) mid-pandemic aversions to all but the most tried-and-tested means, and begin again to look at what the best fit technologies *really* are… *then* blockchain affinity in particular use case areas becomes ever more strengthened. For example, immutability, consensus, and independent verification provides trust at a distance; and autonomous execution of smart contracts enables secure workflows to cross boundaries, etc. These characteristics can be applied “surgically” in variety of use cases areas – which, in the case of the Government sector, translates into an enhanced and more efficient portfolio of interconnected citizen services.

It’s a shift that’s happening right across industries as organisations (re-)engage with a longer tail of potential uses for blockchain – only this time with a mindset that’s less about what the technology can do in isolation. Instead, it’s more now about how aspects of blockchain’s capabilities can be “atomised” and applied *as and where required* in order to solve problems / exploit opportunities *without* having to replace everything that’s gone before. The *Blockchain Index* has logged notable examples across the globe where pockets of particular interest have grown up around use case patterns, often symptomatic of a *decentralised transformation* leapfrogging over more traditional digital transformation sequences when digitising previously manual processes.

Challenging reality

Blockchain tech possesses characteristics that chime well with governments’ “do more with less” agendas. Ditto with their desire to bring more citizen services online seamlessly, whilst simultaneously avoiding the data privacy pitfalls that have sometimes dogged earlier large-scale *centralised* data-based projects.

Governments have been able to get hold of *some* of the data they need in order to drive digital transformation in the citizen services arena… but currently this has tended to remain tied to data it *already* owns, or has access to through other related groups. Rarely has this involved interacting with permissioned blockchain networks in order to enrich sources.

However there *are* signs that blockchain involvement may now be on the horizon to help level-up government initiatives. Especially now that such networks are beginning to gain traction in other sectors – whose data may prove beneficial to government decision-making and service operation. Governments may still find the concept of convening their *own* network to be a step too far as yet, though. It’s often seen as “not their job” to expend the effort required to pull a network together. *Existing* blockchain networks, on the other hand – “where the conversation is already happening” – are another matter. So governments *are* beginning to apply blockchain… they’re just being selective about where (and how).

The turning point

Independent Thought’s *Blockchain Index* data suggests that current activity is chiefly spread across a number of use case themes (which feature also in other industry verticals), *viz:*

- **Data management** – covering applications that control or audit the access to, and distribution of, data; digital credentials; and rights management (mostly in the realms of blockchain-enhanced records management for property, patents, contracts, certifications, and the like). Over a third (36%) of Government sector projects logged by the *Index* during 2021 use the technology in this way;

- **Financial transactions** – including cross-border payments; digital currencies, asset tokenisation; fractional ownership, micro-payments and payment tracking. This accounted for over a quarter (27%) of Government blockchain activity in the *Index* during 2021;
- **Digital identities** of both people and devices – including personal identity, anonymity, and personalisation (some focusing on specific e-voting scenarios, others as the prelude to a roll-out of wider citizen services portfolios). This applied to nearly a fifth (18%) of the Government sector projects in 2021's *Index*;
- **Tracking & provenance** – including asset tracking, supply chain and logistics monitoring, proof of origin verification, etc.; and data provenance (14% of projects); and
- **Process automation** – primarily concerned with the application of smart contracts in intra- and extra-organisational workflows (5% of projects).

IBM's own research concurs. The company cites four main areas where interest is keenest across the sector – in all cases, as part of wider technology initiatives that deploy blockchain as "one of the tools in the box", *viz:*

- **Citizen services** – ranging from the current interest in vaccine passports, through further combinations of identity and data around wider social security services. These capitalise on self-sovereign identity's trailblazing moves, and the fact that apps, wallets, and behaviours are now already in place for many people. Such examples map to the *Index's* Data management and Digital identities use case taxonomies;
- **Treasury** – enabling the smart collection of taxes, for example deploying blockchain to digitise processes and assets as goods pass through ports; also facilitating the growth of new financial services that utilise tokens and CBDCs. These map to Data management, Digital identities, and Financial transactions;
- **Trade** – making it easier to do business… particularly where the government (acting through its agencies) owns the supply chain or tracks payments therein. These map onto pretty much all of the *Index's* use case taxonomies, because of the broad range of activities this covers; and
- **Governance** – where good governance leads to good government, such as in assuring the integrity of Environmental Social Responsibility (ESG) data. This was hitherto considered more of a "secondary" requirement, but has now been imbued with a new sense of purpose in the wake of Cop26. It's usefully also often able to be "bolted-on" to existing blockchain-solutions around trusted data sharing workflows. These map to Data management and Tracking & provenance in the *Index*.

The "transparency premium"

Increasingly, organisations across many different sectors are recognising the importance of not only *acting* in a proper manner when it comes to the treatment of personal data, the appropriation of funds, the origins of their raw materials and the conditions in which their products (and people) are treated across the supply chain… but also *being seen to be* doing so. And being able to *prove* that this is the case. The same can be said for governments and their agencies. Transparency is key in the public sector arena – from assuring safeguarding the collection of tax revenue and citizen data; through good governance around the use of that data; to the spending of public money and the award of external contracts, etc.

Blockchain technologies, when integrated into monitoring and management systems, provide excellent means by which good stewardship can be indelibly recorded and independently verified by third parties. This furnishes the organisations concerned with a "transparency premium" which they can apply to their overall market positioning, as well as providing individual assurances on a case-by-case basis.

And even as blockchain technology becomes part of more and varied service developments… it's not the *focus* of any initiative. They are considered by their stakeholders to be *projects*, not *blockchain projects.* Indeed, the growing imperative for tech-inspired innovation work to be able to demonstrate its worth quickly and provably in terms of business value means that we should increasingly be talking about *business* projects rather than rarefied "*technology* projects" anyway. After all, there's so much more that contributes to their success than the raw tech components alone – with blockchain being just one amongst them anyway. IBM's figures put blockchain contribution at around 15-25% of the total tech change in a backend project concerned with the trusted movement of data.

Waiting for a "G-Chain"

Cloud computing took off in many government circles when projects with a definition of data residency and privacy requirements began being able to take advantage of government-approved services. These moves effectively pronounced that cloud was indeed "good enough for government work" (for most workloads), allaying many of the collective concerns of public sector IT teams running historically on-premise systems. In a seemingly parallel journey, concerns expressed by some public sector bodies are highlighting the need to see blockchain networks running on these very same cloud services now too. This is in order for their underlying infrastructure choices to carry the same weight in terms of certification for security, reliability, etc.; hence overcoming concerns about managing blockchain nodes across potentially non-compliant environments.

It would also help dispel some of the persisting myths around blockchain risk where notions of private permissioned vs public permissionless networks are confused in mainstream media coverage. Often these are also conflated with dark web connotations because of the role that untraceable cryptocurrencies play in ransomware attacks on both public and corporate systems. Plus the anxieties of government regulators that are wary of open, permissionless networks in sensitive scenarios because of the KYC concerns that anonymity brings, and also the absence of any service "owner" to pursue if things go bad.

A suite of essentially "government-approved" permissioned blockchain services, running on government-approved clouds, would be much easier for public sector agencies to set up distributed applications on. Many of the niggling security, reliability, etc. questions will already have been addressed up front as part of the underlying infrastructure selection process that permitted the cloud set-up in the first place. But for this to come to pass, the right high profile, (positive) attention-attracting government projects need to be kicked-off in this way so as to get such an infrastructure off the ground in the first place.

Floating all boats, when "going it alone" isn't an option

Digital transformation agendas are often inwardly-focused – concentrating on change *within* the organisation; often modernising own structures and ways of working, etc. in response to perceived *outside* threats. But organisations don't work alone; they all operate as part of an ecosystem or supply chain. Government agencies included.

In order to make and strengthen a business case for blockchain, one question that needs to be asked is "what key business outcomes *can't* be achieved by the organisation acting alone?" From this there follows an appreciation of the concept that each participant needs to contribute to generating a return for the ecosystem as a whole, in order to get what it needs individually (in order to meet its own goals). And so the business case needs to be configured so as to show return both for the participant organisation's own objectives; and to sustain the overall network. It becomes "a rising tide which will float all boats".

In a commercial environment, this spirit of co-opetition that underpins the collaborations amongst partners in blockchain consortia can sometimes be a tough sell without quantifiable selfish gains also on the table. In a public sector context however, a desire to raise the tide and float the boats of all ecosystem players for the citizens' greater good is an outcome more readily accepted (and indeed sought out).

Customer examples

New York's *Excelsior Pass* – digital credentialing in the COVID age

New York State's *Excelsior Pass* (based on IBM Digital Health Pass) is a free, voluntary platform that provides secure, digital proof of initial COVID-19 vaccination or negative PCR / antigen test result. Some 5 million passes have been issued to date.

The principle *Excelsior Pass* applies is blockchain-anchored digital credentialing; something relevant in many scenarios beyond the Government sector. Anywhere, where a third party needs to verify the authenticity of an attestation made by an individual, and that individual would rather not share any more data than is strictly necessary in order to supply the proof.

It's a faster, cheaper, and privacy-safer way for individuals to expose select information about themselves – which may be as a "function" of the raw data (e.g. "I have been vaccinated [with an approved vaccine within an appropriate timeframe]", without sharing precisely when, where, or what the vaccine was). The verifier can then check the veracity of the attestation for as long as the issuer's chosen blockchain remains accessible.

But it's not just the health passport *app* which benefits from blockchain tech. With vaccine mandates in place or being discussed in numerous countries / states, there's also the question of how the governments in those regions are able to keep the required information pertaining to citizens' relevant health-related records secure, private, and immutable on the *backend* too. Blockchain has the characteristics to satisfy these requirements as well. With no need for trusted intermediaries to oversee any reconciliation process, it also reduces costs and enables such systems to be deployed at scale (and in more affordable ways).

Banque de France wholesale CDBC trial

In March 2020 the French national central bank (Banque de France) launched a programme of eight workstreams investigating the application of Central Bank Digital Currencies (CDBCs) for interbank settlement in wholesale money markets. The last of these completed mid-December 2021 and tested the end-to-end transactional lifecycle of digital assets. All transactions occurred across different, but interoperable, blockchain environments (Hyperledger Fabric and R3 Corda). Banque de France managed the instant securities settlement using CBDC, and HSBC managed the custody of the assets (with IBM as their technology partner, leveraging IBM's Weaver interoperability tool).

The trial marks a significant step forward in the use of blockchain in real world banking scenarios. In such environments, multiple parties mean there's often a need to interoperate securely across multiple blockchain platforms. And doing so in such a way as to preserve the atomic nature of data and asset exchanges. So this latest test of issuing, trading, and settling digital bonds isn't just important because of its use of CDBCs (with government policy implications). It's also important because it's a proof of value for blockchain interoperability in the wholesale money markets.

What's in it for you, and how to get started

Who goes first?

One of the recurring themes of blockchain in government ecosystems has recently been the question of *who goes first?* Whose responsibility is it to set up a blockchain network – a government and its agencies, tax authorities, auditors, logistics companies, manufacturers...

In many government use case situations, the argument's already been won that sharing data selectively and securely will facilitate the development necessary for whatever service is required. And the parties involved have agreed (at least in principle) to share that data and join multi-party, cross-boundary workflows (under certain conditions). But the initiative often needs a "grown-up in the room" to convene and supervise proceedings.

If you can't see an obvious candidate for convenor in your Government scenario – consider whether *your own* department / organisation can take on that role. Does it carry sufficient trust, detachment (from a conflict of interests), and credibility to act in this way and get proceedings underway? Can it generate momentum from which a consortium can evolve to take care of things once the ecosystem is in more of a steady stable state? It doesn't have to be a permanent position. A government blockchain project should aim to eventually make obsolete that part of its own role in the proceedings once a critical mass of membership has been reached and the distributed governance properly set up.

Pulling the right levers

Not every participant in a blockchain project will necessarily feel that the benefits have been evenly distributed too – or at least, not distributed *enough* in their favour. Blockchain-enabled ways of working put pressure on those parties which have previously held a natural role as intermediary – but that's not necessarily the only role they play. And indeed even if it *has* been up until now, that's not to say that there isn't an evolving element to their role which can enable them to still retain a sufficient enough stake in a new business ecosystem .

The key thing here is to understand the bigger picture and your organisation's role in it, going forward. And to be able to communicate this to key stakeholders who may appear to be intent on holding onto their stake as imagined in the former "as-is" state. Blockchain is a team sport, and blockchain services strengthen their rationale through growth by network effect: the more attractive the terms to everyone, the more parties join, the more the overall value increases accordingly, the more all boats are floated by the ensuing rising tide.

IBM is able to bring its position as a trusted technology partner to bear and help governments and their partners understand where the natural incentives are; which levers to pull in order to get citizen services blockchain projects off the ground. And, in doing so, helping to ensure that appropriately-placed blockchain-enhancements come *by design*, not by chance.