Digital asset custody

What do asset managers and asset owners need to know about digital asset custody and custodians?

Future of Finance

Coming Soon

Future of Finance

Digital Money

June 16th 2025

Is It Game Over for Fiat Currency Finance?

The Aon Centre, The Leadenhall Building, 122 Leadenhall Street, London EC3V 4AN

This Future of Finance one day Digital Money Event will explore issues of pressing concern to Central Banks, Bank, Payment Infrastructure Organisations, Stablecoin Issuers. Attendees will include those working in the securities, money, payments or foreign exchange (FX) markets, and any users of securities, money market, payments and FX

Find out more on our website

www.futureoffinance.biz

On 4 December 2024 Future of Finance hosted a one-day event at the offices of AON in London. Entitled *Digital asset custody: What do asset managers and asset owners need to know about digital asset custody and custodians?*, the event attracted 160 registrants from asset managers, banks, custodian banks, digital asset custodians, exchanges, financial market infrastructures, insurers, investment consultants, law firms, regulators and technology vendors. This is an account of what they and the panellists contributed to the seven sessions that day, both live and in the multiple-choice questionnaire they completed in advance, the results of which are also published here.

Sponsors

Host

Supporters

Keynote Address

Digital assets must be part of a technological transformation led by humans

Keynote Speaker: Lord Chris Holmes of Richmond MBE, a member of the United Kingdom House of Lords

I should say to everybody here that when it comes to any finances, financial services or financial products, you should take not one word of what I say at all. For this single reason. I did win a number of gold medals. It was only when I retired that I discovered that the silver medals are worth more than the gold medals.

So it can be with investments. They can go down and they can go down and sometimes they can go up. But luckily, I am not registered or authorised by any of our financial services regulators, so I have no chat on that front for you. But, on the upside, I have brought a Labrador with me and so, at any point, if you get tired of what I am saying, or you find yourself drifting off, just look at the Labrador.

Thank you for laying on such a lovely event in such a glorious building, a lovely setting on a beautiful December day. What I would like to do is talk a little bit about what I am trying to achieve in Parliament, focusing specifically on the digital asset opportunity and just talk a little bit about some of the bills that are currently in play.

I am sticking around, so please do grab me if you want a word, or indeed afterwards do connect with me on LinkedIn @ Lord Chris Holmes. There is plenty more chat about all of this stuff on the LinkedIn platform.

A focus in parliament on human-led technology

It was a complete surprise for me to end up in Parliament. I was just finishing off working on the London Olympic Games of 2012. It was 2013, so obviously were just dissolving the company then. All the magic was gone. We had done it. The legacy was set in place. It was June 2013. I got a call on my mobile phone and the lady on the end said, "Hello, is that Mr. Holmes?" I said, "Yes." And she said, "This is Downing Street. I have got the Prime Minister on the line. Are you able to take the call?" "I mean, I guess so." And then more randomly she goes, "Okay, caller, putting you through, go ahead." With what exactly?

But it is fabulous to have been given the opportunity, largely as a result of working very closely with the Prime Minister and Cabinet on putting on the Olympic and Paralympic Games in 2012. I got the opportunity to be in Parliament and really I have tried to focus all of my efforts around technologies: human-led technologies for public good, for private good, for common good, for all our good, for economic, social, for psychological, growth, if we get it right. All of this potential, none of it inevitable.

You have heard of the Select Committee reports that I have authored (see the Sidebar on page 6) and indeed the Distributed Ledger Technology (DLT) report, more of which in a bit. But ultimately it seems to me that we can give ourselves the greatest opportunity to succeed in this digitally enabled, technology-transforming world if we human lead, if we human determine, if we deploy all of what we know about human values, ethics, philosophy, psychology, social theory and more. If we deploy all of that and if we pull on those two most golden of threads - inclusion and innovation, both in their broadest terms - we have the greatest chance of success.

Lord Chris Holmes is the most successful Paralympian in the history of British participation in the Paralympics. He won nine gold medals in all, including six at a single Paralympics, gained a string of World and European titles and broke 35 world records. He was also a driving force behind the immensely successful London Olympics of 2012. Lord Holmes is now bringing the same energy and determination to bear on digitisation and digitalisation. He has long implored the United Kingdom Government to act, invest and innovate to make the most of the opportunities created by the latest iterations of digital technology: blockchain, cryptocurrencies, smart contracts, Artificial Intelligence (AI) and the Internet of Things. He co-authored the House of Lords Select Committee Reports on Digital Skills in 2015, Artificial Intelligence in 2018 and Democracy and Digital Technologies in 2020. Under his own auspices, Lord Holmes published the influential *DLT for Public Good: leadership, collaboration and innovation* report of 2017. He was integral to the passage of the Electronic Trade Documents Act of 2023, which enabled the digitisation (or dematerialisation) of trade documents such as bills of lading and bills of exchange. Lord Holmes is also adviser to several tech and fintech companies.

And we need this because, let us be honest, it is pretty tough out there right now. Geopolitically, we live in an unstable, uncertain, tricky world and this impacts on all parts of our life, not least what we are trying to do with digital assets. The macroeconomics are tricky, different tricky in different jurisdictions, in different economies, but tricky across the piece.

We have such extraordinary paradoxes at the heart of our humanity right now. We have never been more connected and yet we have such a rise in populism, nationalism, retreatism. We have never been more connected and yet we have never seen such high levels of mental un-wellbeing. But we can address all of this through human-led technologies in our human hands, through inclusion and innovation. So, to those technologies.

The need to thread digital technologies together

You would imagine right now, if you read the papers online or in paper format - both are available - or watch the TV news, you would imagine that the only technology in town is generative artificial intelligence (gen AI). Not even understanding AI as a constellation of various technologies, you would imagine it is just "gen AI." And, in many ways, ChatGPT, the biggest thing it has done is chat about itself and done a lot of self-promotion. And it is an incredibly powerful technology. And AI beyond that has an incredibly powerful potential. It is a rich constellation of technologies. But alongside that, I have always believed it is important, and tried, to thread together all of these, if you will, new technologies.

New technologies in our human hands. Not least blockchain, distributed ledgers. And it is why I wrote my report in 2017 on distributed ledger technologies, because, as you will be well aware, and it is still largely the case now, blockchain and Bitcoin, for many people, are the same thing in their mind. In fact, I was at a conference maybe only three years ago, where somebody who should have known better stood up and he said, "I was at an event a couple of weeks ago and they were giving away £20 of blockchain." I mean, was it heavy? What format did it come in? But that underpins the point. It is problematic in terms of understanding, but it is problematic then in terms of what we are all trying to achieve with distributed ledger technologies.

Grasping the difference between cryptocurrencies and blockchain technology

It has to move beyond that, otherwise it will be so tied into that narrative around Bitcoin, which so often for so many people is utterly binary. You are either in it and you love it or you hate it and just describe it variously as a Ponzi Scheme or the like. But as we know in this room, distributed ledgers are so much more powerful. And in terms of the potential for not just the exchange, but the creation, the enablement, of value. Extraordinary possibilities, of themselves. But then, when put in combination, when put in concert with other technologies such as various AIs, things become very interesting indeed.

And the one example I often pull out of my report on DLT is that of the current system of medics needing to prove their credentials before being able to work in the National Health Service (NHS). This is obviously incredibly important. You want to know that the person operating on you, the person you are consulting, you want to know that they have the qualifications, they have the experience, they have the credentials that they are asserting. But to achieve that, currently, costs - and it is a cost to the NHS – 25,000 doctor days. Improving credentials. It is important to prove credentials. But imagine, with a pretty straightforward DLT solution, you could collapse those 25,000 days and convert them into 25,000 days of care. That is transformational for the NHS, with no additional penny of resource being put into the service.

The scale of the opportunity in digital assets

So the technology is proven. The technology has extraordinary potential. And that is why it is so interesting to see how we are now developing and seeing the global development of this technology underpinning digital assets. And bear in mind, this is still relatively new for so many people and for so many institutions right around the world. And yet by 2030 I think it is fair to say that the majority of value will be exchanged via digital assets. Just one example - tokenisation of real-world assets is estimated to be around US$10 trillion by 2030. Which is pretty extraordinary when, relatively, they have only just arrived in the last few years. And reached that point of people understanding the underpinning value proposition and value creation, not just value exchange.

And what opportunities for those involved in custody. It is incredibly important to the success of digital assets. Looking to how one wants to deploy optionality around wallets. In short, hot, warm, cold? And the implications therein. Do we go self-custody or managed custody? Do we look at the advantages that then come from that custodial relationship? How can one look into driving increased value through trades as a result of holding those digital assets?

So many opportunities, so much potential, but all needing to start from that self-same truth: human led. We determine, we decide, we choose how to develop, how to deploy and how to hold digital assets for the benefit of individuals, for the benefit of business.

And why we know how to do this is because, specifically, we understand risk. We know how to assess it. Yes, this is a new environment, but we know how to look into it and how, again, in combination, we can use other technologies to assist in real-time with that risk analysis.

We understand security. We understand privacy. We understand all of the elements to construct and make the right custodian solutions for digital assets. So we have the technology. We understand the potential of digital assets. We understand what we need to make a success of it.

The example of the Electronic Trade Documents Act

Some use cases.

Last year's Electronic Trade Documents Act is a really good example of what these new technologies enable. Now, you would imagine trade, surely, it is already digitised, it is already happening. Well, think again. Because the problem comes from the fact that trade documents are possessory in nature. What that means is you hold the paper, you hold the goods. So think bearer bonds in another world as well. Same thing.

Now it was impossible to put those on a digital platform until you had the technology which would enable you to hold in law that document and prove that no one else held it and that you had perfected the holding of that document. DLTs enable that. And the great thing about the piece of legislation we put together, even though currently it is DLTs – blockchain - that enable that, we in the legislation do not mention any technologies at all. Which, with any luck, will make the bill both technology-neutral and technology-futureproof. Because we focus on criteria, and we focus on principles. A good way to legislate.

The politico-socio-economic impact of blockchain technology

Let us look at fractionalisation. Because, again, back to what I said at the outset, we are in geopolitically, macro-economically and nationally difficult times. What can digital assets and this approach deliver to those issues? Be it the energy crisis, levelling up, the cost-of-living crisis.

Well, imagine fractionalisation in the housing market. The ability to do nothing short of enabling young people to get a stake in a market that they are so shockingly and unfairly excluded from right now in so many circumstances, not least in this city of London. Fractionalisation enables a stake to be had.

What about the fabulous international nature of this country? Well, again, digital assets offering potentially seamless, effective, secure means of international workers being able to make payments back to their families and friends and connections back home.

Two live issues, two economic issues, two political issues, two social issues where digital assets can help.

The advantage of English Common Law

To legislation we currently have in play.

You will be aware that the Law Commission produced a large report, as they do, 380 pages. I have read them so you do not have to. They informed the Property (Digital Assets etc) Bill. And it is a really good draft piece of legislation they brought forward. Because we have an extraordinary opportunity in this country. Not just because of the fabulous financial services ecosystem that we have in this city and across the country, not just because of our higher education system, not just because of the time zone and our geography, but most of all because we have the great good fortune of English Common Law, the ability to draft and to legislate in a way that fits within that dynamic, that agile legal system.

So later today you will be discussing, rightly, the different regulatory frameworks in key jurisdictions- the United States, Europe, the German-specific example, and looking across to Asia-Pacific (APAC), not least the extraordinary things that are happening in Singapore and Hong Kong, to name but two.

You will be well aware of the Markets in Crypto Assets Regulation (MiCAR). A good effort from the European Union (EU), similar to the Artificial Intelligence Act (AI Act) that they passed earlier this year. But inevitably in that legal code, it is highly prescriptive, trying to nail down everything - as is the way that one legislates in that code. It is good, but to bring in new concepts that will then need to develop over time, they use a prescriptive rather than principles-based approach.

The opportunity that we have in this country is to just give a slight touch, just a slight touch on the tiller to Common Law when it comes to digital assets. Without going into legal detail around property rights, there are essentially two classes of property rights in this country. The bill asks, "Do they currently enable digital assets or should there be the consideration of a third class, if it is considered digital assets do not currently fit into either a thing-in-itself, so a good, or a thing-in-action, such as a debt?" So essentially tangible and intangible are the two classes of property rights that we currently have under English law.

How digital assets can drive economic growth

So that will be the path of progress of the bill. And ultimately, whichever way the bill comes out, it is a thoroughly good thing that attention is being put onto this area because, again, in this country, and across economies around the world, we need to look for areas of growth.

You heard the Prime Minister, you heard the Chancellor of the Exchequer, in various situations, not least the Mansion House speech of 14 November 2024, talking about growth, growth, growth.

Now, of course we all need growth, we all want growth. But if you look to the areas where we are likely to be able to develop and bring on growth, you really have to conclude that it is these technologies, not least digital assets in all their potential form, which can be such a deliverer of growth and from that all the social and economic potential that can flow from it.

So a Digital Assets Bill is in play at the moment. I would welcome your views, your thoughts on it. We will have that done, probably by just before Easter, I would imagine. And again, it is good that it is happening, good that we are having this flow of legislation, having an Electronic Trade Documents Act. Now we are doing digital assets. Then we will be looking at Decentralised Autonomous Organisations (DAOs) and other elements. Hopefully in the new year we will see more AI legislation as well to go alongside this.

But my aim also is to try and thread these things into other elements of legislation, to keep pushing the point and keep seeing how we can improve all statutes.

So we have got the Product Regulation and Metrology Bill. There are opportunities there. We have got the Data Bill. And the interesting thing about the Data Bill, and you may well be aware of it, particularly Part Three, with the smart data provisions which enable so much of this next stage of what we can do with Open Finance.

This is the third iteration of the Bill and each time it has come to us, it has had a different name. I have no idea why, but hopefully we will get this one through. And so you will only have to remember the one name, which is Data Use and Access Bill. But there are lots of things in there, lots of things that are germane to digital assets and the discussions that you will all be involved in today. It is a great programme. I am looking forward to hearing some of the presentations. Lots to think about.

But be in no doubt, digital assets have the potential to transform, to create, to generate opportunities. The potential, at an individual, at an institutional, at a national, at an international level, is enormous. If we get it right, if we think through how we want these assets to be, if we look at the most obvious candidates to look to convert into digital form in the first instance, if we look at how we can bring that value into being, that will be truly transformational. And again, human-led, human in-the-loop, human-enabling, human-empowering technologies. Digital assets driving growth, driving potential for all of us.

Enjoy today, make new contacts, make new connections, make new friends. Enjoy all the presentations. As I say, chat to me, connect with me here or on LinkedIn. Ultimately, let us look to the opportunities, let us look to the possibilities. Together, let us drive forward with digital assets.

Panel 1

What happens when your asset managers start to invest in assets your custodian knows nothing about?

Panellists: Angie Walker, Global Head of Banking and Capital Markets at Chainlink; Anoosh Arevshatian, Group Chief Risk Officer at Zodia Custody; Keith O'Callaghan, Managing Partner at Archax Capital Limited; Qian Jian, Director, Digital Assets Strategy, SWIFT; and Dr Robert Barnes, co-CEO at BPX Digital Securities Exchange.

Why do digital asset custodians exist at all when blockchain was invented to eliminate the need for trusted intermediaries?

Issuers and investors, and intermediaries such as asset managers and brokers, are agreed that custodians are essential to secure mainstream adoption of digital assets. Such universal agreement reflects the fact that custodians reassure investors, asset managers and brokers that their assets are safe, and their privacy and confidentiality will be respected. Custodians also provide a crucial link with traditional asset markets, bringing digital assets within the scope of the regulations and the data standards that have enabled traditional markets to scale. Financial market infrastructures such as central securities depositories (CSDs) are also seen as providing convenient bridges between new and established asset types. Views differ on whether the need is best met by specialist digital asset custodians or by traditional custodian banks, which now have an opportunity to expand their product coverage.

How well are traditional custodians adapting to the digital asset opportunity?

Some traditional custodians are building digital asset custody services. The banks that are entering the market – and it is still a minority of the global custodian banks – are responding to rising institutional flows. They find the learning curve is steep, since they must integrate technological, operational and legal components. The custodians must understand and connect to multiple blockchain protocols, integrate off-chain assets while servicing on-chain representations of the same assets and adapt the fiduciary structure of traditional custody agreements to digital asset custodianship. They also find the settlement and safekeeping requirements of security and fund tokens are different from the settlement and safekeeping requirements of cryptocurrencies, so custodians are grappling with varying service requirements. In addition, they face the twin challenges of continuous changes in digital asset custody technology and digital asset custody technology vendors, whose ownership is subject to change through merger and acquisition. The cost and difficulty of integrating digital asset systems with traditional post-trade systems erects a further barrier to adaptation. But where custodians are really struggling is the settlement process for digital assets. They cannot interact with any counterpart without issuing a due diligence questionnaire and, even after the counterpart is approved, rely on bi-lateral test transfers, whitelists of counterparties and manual checks. A settlement system of this kind is impossible to scale, but custodian banks have no alternative vision of the type of settlement infrastructure that scale requires, and certainly no strategy to achieve it.

Why are so few established custodian banks taking an interest in digital assets?

The limited engagement by custodian banks is not for want of interest in blockchain technology. Virtually every custodian has experimented with the technology. The obstacle is the inability of the tokenisation enthusiasts at the banks to persuade risk committees to sanction investment. The principal explanation of this reluctance is the lack of legal certainty. After all, if a

risk committee feels a legal contract will not be enforceable in the courts, they will lack the trust and confidence to authorise bankers to enter such contracts. Without the confidence that the law will support the ownership and transfer of digital assets, investment is bound to be limited. Conversely, once that confidence is in place, growth will accelerate because custodians can reassure their buy-side clients that a smart contract, for example, will be upheld by the courts. Once risk committees understand legal certainty is achievable, more custodians will enter the market. Which is why token enthusiasts at custodian banks should ensure their risk committees understand the legislative progress that is being made in the United Kingdom and the European Union (EU).

Custodians have always struggled to safekeep "out of network" assets that are not issued into a central securities depository (CSD). How are they reacting to the tokenisation of real-world assets (RWAs) outside CSDs?

Custodians asked to safekeep the RWAs currently being tokenised certainly do not enjoy the benefits of working with an established clearing and settlement infrastructure akin to that of the traditional securities markets. Issuers and exchanges have focused on the data "oracles" that govern the valuation of the tokens and have relied on digital asset custody technology vendors to provide custodians and their buy-side clients with the reassurance they need. In the absence of a CSD, custodians struggle to keep track of ownership and the transactions that govern ownership. But a CSD for digital assets is now being built. Montis, a subsidiary of the Archax digital asset exchange, has applied for a CSD licence in Luxembourg. Once it is secured, tokens can be issued into and settled in a digital CSD as well as traded on Archax. Montis has also applied for entry to the Digital Securities Sandbox (DSS) set up by the Bank of England and the Financial Conduct Authority (FCA) so it can provide issuance and settlement services for digital assets in the United Kingdom. It can be argued that what is missing from digital asset custody is not traditional custodian banks but the equivalent of traditional financial market infrastructures. Building these might require a greater degree of cooperation between market participants.

Why do digital assets, which can be issued, traded, settled and safekept on a public blockchain, even need a CSD?

Primarily to make transactions in digital assets legally enforceable under the Settlement Finality Directive of the European Union (EU). Settlement in a CSD also simplifies the aggregation of transactions in digital assets with transactions in traditional assets, which are settled under the same laws. Luxembourg law has gone further and permitted the issuance and registration of both conventional and digital assets on any digital technology, including blockchain. By making assets technology-agnostic – in other words, operationally identical - in this way Luxembourg law makes it easy to aggregate assets and transactions in those assets across traditional and tokenised markets. The real value of a CSD in the future will be its ability to transfer and register ownership of both digital and conventional assets in the same way, with legal certainty. Business will gravitate to the jurisdictions that grasp the connection between legal certainty and increased scale in digital asset markets.

What do end-investors think about custody?

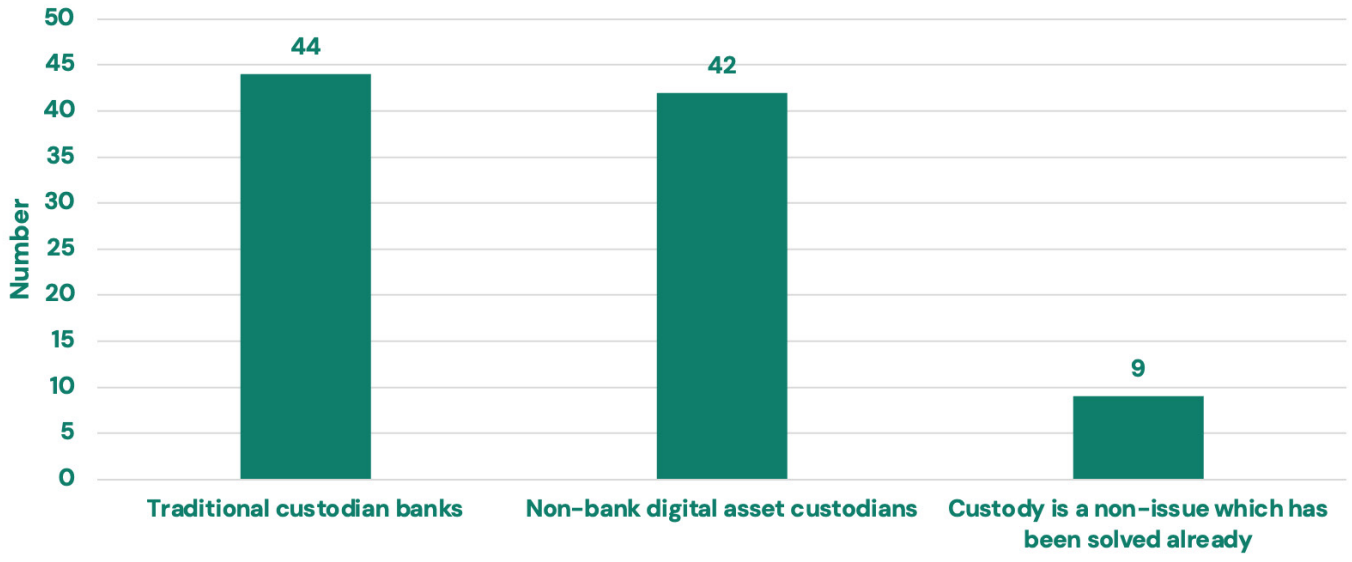
Investors are not yet convinced that digital assets offer superior returns to traditional assets and know that they are bound to be less liquid. What is visible to investors - albeit mostly through their asset managers and custodians - is the increased cost and complexity of investing in digital assets in terms of connectivity, on-boarding and account-opening, because of the lack of market infrastructure and data standards. Naturally, investors are concerned that rogue actors will steal their digital assets. They expect custodians to make them whole in the event of losses for which the custodian is responsible. They also expect custodians to operate on a regulated, fiduciary basis that ensures their assets are safe even if the custodian fails. But investors are not willing to engage independently with the technicalities of digital asset custody. They expect their traditional custodians to solve the problem of digital asset custody for them. An implication of this is that institutional investors are unlikely to appoint a non-bank digital asset custodian as a service provider. This argues for closer co-operation and even mergers between traditional custodian banks and non-bank digital asset custodians.

Does the custody industry have a responsibility to build the infrastructure to facilitate investment in digital assets?

They have an opportunity, not a responsibility. Market developments indicate the buy-side demand for digital asset custody services in the near-term will come not from the tokenisation of the public equity and debt markets but from tokenised and tradeable private credit, carbon credits and money market funds. In the longer term, custodians enjoy further opportunities in the transfer of wealth from Baby Boomers to Millennials and Generation Z. As the cryptocurrency market has proved, younger consumers want to trade, invest and safekeep their savings in digital form via apps. They also expect investment portfolios to be personalised to their wants, needs and values. In principle, tokenisation makes it easier to achieve these goals. Custodians will have to provide services that enable asset and wealth managers to deliver what younger consumers want, or they will not survive, so there is risk if custodians fail to rise to the opportunity. That said, the principal driver of growth in token investment will remain what has always driven investment: namely, the tax treatment of investments. Wealth will gravitate to the stable, legally reliable jurisdictions that offer the most generous tax treatment of investments, and custodians will have to be prepared to follow it. Ultimately, tax is more important than technology, or tokenisation.

What the Audience Said

Which Type of Custodian is Best Placed to Safekeep Security and Fund Tokens?



Panel 2

What do regulators have to say about your custody arrangements?

Panellists: John Siena, Associate General Counsel and Co-Head of Regulatory Strategy at Brown Brothers Harriman (BBH); Monica Gogna, Partner and Head of the Financial Institutions Law Group at EY; Romin Dabir, partner at Reed Smith; and Yvonne Deane Harte, Director for Secondary Markets and Post Trade policy at UK Finance.

Custodians have been obliged since 2019 to check that holders of cryptocurrencies and Stablecoins are not money launderers, terrorists or sanctions evaders.[1] What impact have those obligations had on the day-to-day practice of digital asset custodians?

Both traditional custodian banks and specialist digital asset custodians have recognised the need to comply with the Financial Action Task Force (FATF) obligations to run Anti Money Laundering (AML), Countering the Financing of Terrorism (CFT) and sanctions screening checks on cryptocurrency and Stablecoin transactions. Indeed, FinTechs are hiring individual experts from custodian banks to show them how to do customer and counterpart due diligence checks. After all, compliance with the FATF recommendations presents several challenges. One is that implementation varies between jurisdictions. Another is that jurisdictions update their guidelines continuously. And although the checking procedures are fundamentally the same across digital and traditional asset transactions, blockchain technology does pose novel challenges such as self-hosted digital wallets and anonymous wallet addresses. The irony of the need to check whether cryptocurrencies are being used by criminals – given that the initial promise of blockchain was a "trustless" alternative – is not lost on custodians of either kind.

What is the approach of regulators in the United Kingdom to digital asset custody?

The approach by the Financial Conduct Authority (FCA) is consistent but not yet complete. It is based on the existing requirements in the Client Asset Sourcebook (CASS) which sets the rules – record-keeping, segregation of assets, internal controls and so on - that regulated firms must follow when holding customer cash or assets. But the work of revision to accommodate digital assets in promised legislation will not be finalised for 18 to 24 months.[2] Importantly, English law is less onerous than European Union (EU) law in terms of custodial liability if digital assets go missing, with a promise of a proportionate rather than total responsibility. Questions about liability for assets delegated to third party custodians remain open. There are also proposed requirements to maintain operational resilience, meet audit rules, and place the custody function in a separate entity. Two years is probably a realistic, if disappointingly lengthy, timetable to put an end to the current regulatory uncertainty surrounding digital asset custody in the United Kingdom.

1. In 2019 the Financial Action Task Force (FATF) "Travel Rule" required custodians to disclose customers' personally identifiable information in cryptocurrency and Stablecoin transactions. Not every jurisdiction has implemented the obligations or implemented them in the same way. A 2024 report by FATF (*Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs*, June 2024) found 75 per cent of 130 countries were either partially or not compliant at all with the crucial Anti Money Laundering (AML), Countering the Financing of Terrorism (CFT) and sanctions screening Recommendation 15. At the national level, advice evolves continuously. The European Banking Authority (EBA), for example, has published updated versions of its original AML and CFT guidelines of 2017 in 2021, 2023 and 2024.

2. For more on the proposed legislation, see page 24.

Why do United Kingdom regulators move so slowly?

The speed at which regulators can move is constrained by laws which stipulate, for example, that consultations and pilot tests must be conducted (this is part of the logic that lies behind the regulatory sandboxes introduced in the United Kingdom in 2015 and 2024). In addition, the art of successful regulation is to preserve the safety and stability of financial markets without stifling innovation. Today, the United Kingdom government is asking regulators to encourage innovation, competition and growth but without a compensating assurance that, if something goes wrong, they will not be publicly named and shamed for failing to foresee and avert the problem that arose. That said, regulators in the United Kingdom are not adept at marketing, in terms of signalling to the world that London is open for digital asset business. Yet officials at the Bank of England are admired by other regulators around the world for their attention to detail, rigorous analysis and thoughtful approach to innovation. The United Kingdom is also leading Europe on the journey to a shorter settlement timetable and, by fostering collaboration between all parts of the securities industry, helping to ensure the transition to settling on trade date plus one day (T+1) is a comfortable one. Innovative legislation such as the Electronic Trade Documents Act and the Property (Digital Assets etc.) Bill also proves that the United Kingdom is building a corpus of law to underpin regulation of digital assets. Unfortunately, this innovative work is not being translated into a means of selling London as an international digital asset issuance, trading and custody centre. That failure to translate domestic thought leadership on reform of law and regulation to accommodate digital assets into a marketing campaign is a missed opportunity for the United Kingdom. The world is willing to follow a British lead in this area, but it is not being given.

Are regulators in the United Kingdom constraining innovation by the private sector?

Unlike the public sector, where personal compensation is not tied to the pace of new product development and distribution, banks are under pressure to innovate in pursuit of profit. However, the pace of innovation even by the private sector has slowed down. In the 1980s an innovation such as the first multicurrency Medium Term Note (MTN) took six months from conception to launch. Hybrid capital instruments for banks to comply with the capital adequacy rules of the Basel Committee on Banking Supervision (BCBS) were also agreed and launched within the same timetable. However, since the great financial crisis of 2007-08 - one of the causes of which was judged to be over-enthusiastic financial innovation - banks have introduced risk management and product development processes that prevent the rapid introduction into the market of new ideas.

Is the slow pace of regulatory change damaging the position of London as a digital assets centre?

The marketing of London as a clear, safe and stable jurisdiction for digital asset issuance and investing matters, especially now. In the light of the more positive approach that is likely to be taken towards the industry by the Trump administration in the United States, and the efforts made by several European jurisdictions to attract tokenised business, the United Kingdom needs to improve its competitive position in digital assets. On the face of it, taking two years to launch the digital gilt-edged issue (the Digital Gilt Instrument, or DIGIT) announced in November 2024 is reasonable. It will take time to research viable maturities – which investor wants to take a ten- or 20-year view of a novel instrument such as a digital gilt right from the outset? - and choose the blockchain protocol and build the issuance, distribution, secondary market trading, custody and asset servicing infrastructure and systems. In addition, His Majesty's Treasury and the Debt Management Office (DMO) have short-run financing needs, and they are being asked to make an investment in the short term that will yield rich dividends in the long run only. So, a degree of caution is understandable. Indeed, the DIGIT will be issued not by the DMO but as a pilot scheme within the Digital Securities Sandbox (DSS) launched in September 2024 by the Bank of England and the FCA. But caution should not freeze all initiative. It should not prevent the United Kingdom government from issuing a large, say, £2 billion, sovereign debt issue in fully digital form in the meantime. Or digitising the much simpler Treasury bill market, whose short-dated securities are generally held to term by investors so there is no need to develop a secondary market. Treasury bills could be digitised in just six months.

Flagship issues of this kind would be bold statements of intent by the United Kingdom authorities. They are also an invaluable opportunity for the industry (Gilt-edged market makers (GEMMs), inter-dealer brokers, exchanges, custodian banks, paying agents, central securities depositories, trading platforms and investors) to work with government (His Majesty's Treasury, the Debt Management Office, the Bank of England and the FCA) in a collaborative task force to identify and solve technical issues ahead of the launch of a fully digitised gilt issuance, trading and custody programme.

Are the gilt-edged market makers (GEMMs) keen to participate or fearful of being disintermediated?

The GEMMs have an interesting perspective on digital gilts. Unlike the FinTech innovators, which are excited about promoting what their commercial offerings can bring to the markets, the GEMMs are asking themselves practical questions about how much of a digital gilt issue they can buy and how confident they are about selling it on to investors. The reason UK Finance has advocated a cross-industry task force to work on digital gilts is a belief that the more participants that have a material interest in developing digital gilt issuance, the better. A private placement with a handful of enthusiastic investors is easier to organise, but an issue which engages the GEMMs as well as investors would be more useful in terms of market development. As it happens, it was the GEMMs and the investors which first proposed to the government (via UK Finance) that the digital gilt programme begin with Treasury bills.

Is regulation of custody retarding the progress of token markets in the United Kingdom?

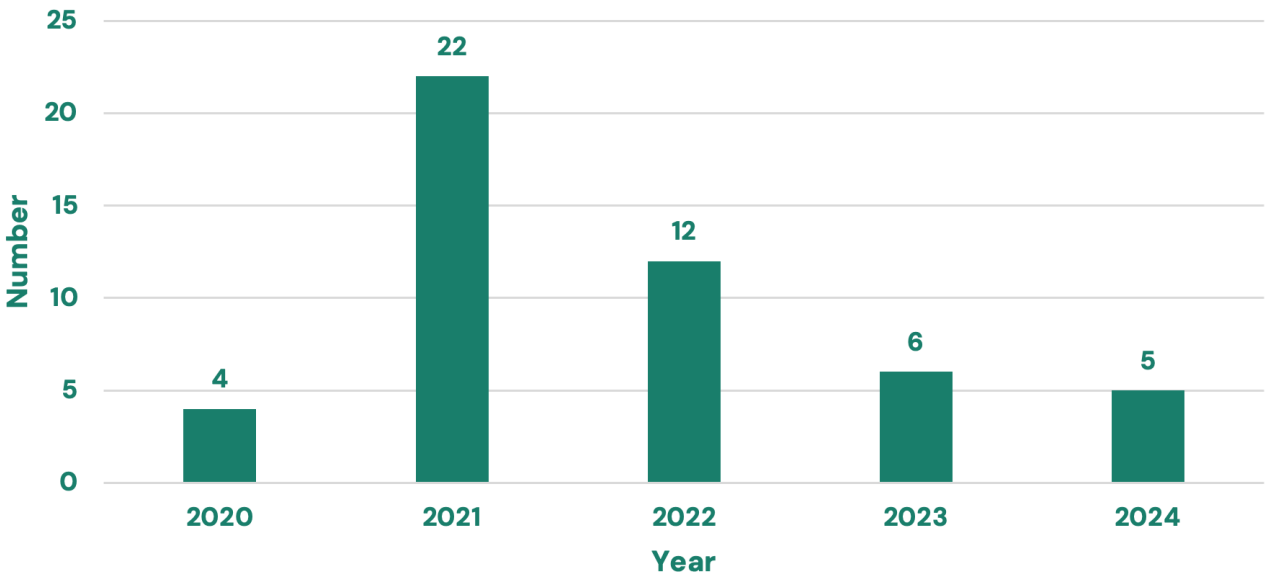
Yes. Asset managers willing to invest in tokenised securities on behalf of institutional clients must check that the global custodian services purchased by the client are adequate to the risk and capable of interacting with the blockchain on to which the tokenised securities are issued. This complicates the allocation of tokenised investments, which in turn inhibits the growth of a secondary market by narrowing distribution. Global custodian banks could alleviate this problem by developing or adopting solutions to the lack of interoperability between blockchains, and they do not need regulatory permission to do that. Another problem which could be relieved by regulators is their hostility to delegation of custody of digital assets, or sub-custody arrangements. Sub-custody is a standard feature of trading and investment in traditional asset markets but has yet to be accepted by regulators in the digital asset markets. The United Kingdom has an advantage in this area. Its traditional custody regulations accept that different rules will apply in different jurisdictions. So, they permit different approaches to be adopted when sub-custodians are appointed in jurisdictions where the local regulations do not accord neatly with United Kingdom requirements.

Have regulators in the United Kingdom failed to develop a sufficiently diverse eco-system for digital assets to thrive?

"Crypto asset" firms that have applied to the FCA for registration under the Anti Money Laundering (AML), Countering the Financing of Terrorism (CFT) and sanctions screening regulations in the United Kingdom number just 46 registered entities and three formerly registered entities. The ranks of applicants have fallen sharply since the peak year of 2021 (see the Chart below)[3]. However, the low number of registered entities reflects the fact that the FCA initially rejected many applicants, which deterred future applicants. Nevertheless, this difficulty has encouraged entities to register in less meticulous markets such as Italy or Poland, where the numbers of registered entities are much higher. The United Kingdom would benefit from a more stable and predictable path to regulatory approvals in digital asset markets.

3. https://register.fca.org.uk/s/search?predefined=CA

Number of Cryptoasset Registration Applications Approved by the FCA



Are digital asset custodians being asked to assume too much risk?

In April 2009, global custodian banks were shocked when a French court ruled that both Société Générale and RBC Dexia were liable for losses incurred by asset management clients because of the collapse of Lehman Brothers, even though the banks did not have the assets in custody at the time because they were controlled by Lehman Brothers as prime broker. However, European Union (EU) regulators later wrote such liabilities into hedge fund (the first iteration of the Alternative Investment Fund Managers Directive, or AIFMD, of 2011) and mutual fund (the fifth iteration of the Undertakings for Collective Investment in Transferable Securities Directive, or UCITS V, of 2014) regulations. Similar provision is made in the Markets in Crypto-Assets Regulation (MiCAR) regulation, where cryptocurrency custodians are liable to their clients for any loss of crypto-assets or access to those assets up to their market value. This liability is disagreeable to digital asset custodians, but it has the merit of providing the unambiguous regulatory clarity that digital asset market participants say they want. That said, custodial liability for customer losses does represent an obstacle to scaling digital asset markets.

What is the United States government approach to regulation of digital asset custody?

In 2022-23 the Securities and Exchange Commission (SEC) introduced changes that increased costs and risks for specialist digital asset custodians and deterred global custodian banks from offering digital asset custody services at all. In March 2022, SEC Staff Accounting Bulletin No. 121 (SAB 121) prescribed that digital assets held in custody on behalf of customers should be shown on the balance sheet - an unprecedented requirement for a previously off-balance sheet business. In February 2023 the SEC proposed revisions to the "custody rule" embedded in the Investment Advisers Act of 1940. The revisions insisted asset managers work with "qualified" custodians that can pass a suitability test only. They would also oblige custodians to segregate customer and proprietary assets, including the client cash banks use to fund their business and earn net interest margin. The revisions further proposed to widen custodial liability for losses of customer assets to include discretionary investment management decisions, such as credit, short positions, collateral and derivative contracts; previously out-of-scope assets such as real estate, commodities, syndicated loans and privately managed funds; and assets in custody with third parties such as sub-custodians and central securities depositories (CSDs). At the same time, the Office of the Comptroller of the Currency (OCC) reversed its previous policy of issuing banking licences to specialist digital asset custodians, retarding their evolution. These various measures have had a chilling effect on digital asset custody in the United States. SAB 121 prompted one global custodian bank to abandon its plans to launch digital asset custody services altogether. However, another, BNY, argued successfully for an exemption from SAB 121. Peers are likely to follow the BNY example, and industry expectations are rising that SAB 121 will be withdrawn in its entirety[4]. The fate of the proposed changes to the "custody rule" is yet to be decided. The SEC remains formally committed to making changes. The industry is hopeful an SEC answerable to a Trump administration and a Republican Congress will adopt a less forceful stance.

Is regulatory competition between jurisdictions helpful for digital asset custodians?

No. With major financial jurisdictions such as the United States, United Kingdom, Germany, France, Luxembourg and Singapore adopting different approaches to the regulation of digital assets, global custodian banks face a legal and regulatory environment that was already fragmented and is now fragmenting even further. Every custodian remains answerable to their primary regulator in their country of origin, which creates a further risk that primary regulatory obligations fall out of joint with local regulatory opportunities. Fragmentation also creates a potential loss of clarity about which law will apply if assets go missing or there is some other breach of a custody contract. Custodian banks are operating on a global scale, but law and regulation are

4. On 23 January 2025, subsequent to the Future of Finance event, the SEC confirmed in Staff Accounting Bulletin 122 (SAB 122) that it was rescinding the guidance in SAB 121

not. In essence, the lack of technological and operational interoperability in the digital assets industry is matched by an equal lack of legal interoperability. As a result, outcomes to the same issues are bound to vary between jurisdictions. For example, the Basel Committee on Banking Supervision (BCBS) capital rules for holding cryptocurrencies and Stablecoins are based on the conviction that public blockchains are more dangerous than private blockchains, but regulators in certain jurisdictions (including the United Kingdom) do not share that view. Regulatory divergences of this kind are not going to be reduced (or arrested) because assets are digital rather than conventional.

Is the United States ceding legal and regulatory leadership of the global custody industry to the EU?

Historically, the United States has shaped the evolution of the global custody industry, notably through Sections 17(f) 5 (which obliges American asset managers to hold assets abroad with custodians that meet certain criteria only) and 17(f)7 (which obliges global custodians to manage the risks of customer assets held in CSDs) of the Investment Company Act of 1940. But the passage of MiCAR, and the renewed commitment of the European Commission to the Capital Markets Union (CMU), suggests the EU can shape the regulatory environment of the digital asset custody industry on a global as well as a regional basis. Certainly, EU regulations are followed closely by foreign regulators and often adapted by them. However, national implementations of EU law mean the European markets themselves are yet to be harmonised, because national regulatory authorities guard their prerogatives jealously. It follows that regulatory divergence is likely to remain a persistent feature of the European marketplace, which in turn makes it difficult for European regulators to assume global leadership. That said, the pioneering of difficult regulatory areas by the European Commission does ensure that EU initiatives are widely monitored and partially imitated around the world.

What the Audience Said

Why Are Traditional Custodian Banks So Cautious About Safekeeping Security and Fund Tokens?

Data Presentation

Some insights from the Future of Finance digital asset custody database

Presenters: Dominic Hobson, Co-founder of Future of Finance; and Piers Cardew, Director of Research at Future of Finance.

The origins of the digital asset custody industry

Digital asset custody emerged within the cryptocurrency industry as a solution to the risk of retail investors losing the private keys that determine ownership of the asset. This gave the cryptocurrency exchanges the opportunity to develop the first successful digital asset custody services.

But exchanges are not suitable custodians for institutional investors, which require independence, proper customer due diligence processes and robust safekeeping procedures. So institutional investors encouraged the global custodian banks they use in their traditional business to provide a service as well.

At the same time, professional traders of cryptocurrencies began to demand custody (and financing) services that could support their activities across multiple cryptocurrency and token exchanges, and their use of Stablecoins as a substitute for fiat currency on-chain.

Lastly, technology vendors also developed " wallets" for retail investors to self-custody their holdings of cryptocurrencies. Self-custody remains the default choice for retail investors, who continue to value the original, un-intermediated promise of blockchain technology.

The current structure of the digital asset custody industry

The result is a complex and fragmented digital asset custody industry which poses questions for buyers of its services. Potential customers need to establish who the providers are, what assets they are prepared to safekeep, which types of clients they seek and how resilient they are. Answering these questions entails understanding the digital asset custody industry along several dimensions.

The dimensions include *ownership* (where the key distinction is between banks and non-banks); *industry sector* (banks, exchanges, technology vendors, hybrids of technology vendors and bank-owned custodians and hybrids of technology vendors and custodians not owned by banks); *digital asset class* (cryptocurrencies, non-fungible tokens (NFTs), security tokens, fund tokens, native tokens and non-native tokens); *client type* (retail investors, institutional investors, professional traders); *services offered* (custody only or custody plus staking, lending and borrowing and “prime brokerage”); and *regulatory status* (especially whether a firm is registered or licensed as a bank or securities house).

The elucidation of any one of these dimensions quickly runs into some basic data challenges (see Chart 1). The most formidable is the lack of disclosure by the digital asset custodians themselves, about their regulatory status, business objectives and assets under custody (AuC).

Then there is the variation in the regulatory regimes that apply in different jurisdictions. A custodial licence in one jurisdiction might be less meaningful than mere custodial registration in another. In terms of regulation, it is challenging to analyse which custodians are entitled to custody which assets, and which custodians can service which types of clients, while remaining compliant.

Digital asset custodians have also sought and secured a variety of audited accreditations whose value needs to be understood. Technical and technological capabilities manifestly differ, but it remains difficult to distinguish between valid claims and

marketing strategies, and providers are at different stages of development. There is also a constant reshaping of the structure of the industry by merger and acquisition.

Chart 1

Challenges to Understanding Digital Asset Custodians

1. Lack of disclosure
2. Variation in regulatory regimes/lack of regulatory standards
3. Who can custody what in terms of asset classes
4. Who can custody assets for whom (while remaining compliant)
5. Variations in licences and accreditations
6. Differences in technical capabilites and technologies
7. Providers are at different stages of development
8. Constant M&A in the sector

The importance of regulatory information in understanding digital asset custodians

These obstacles cannot be circumvented but must be confronted using whatever resources are available. To work out which custodians are providing services to institutional clients, the right starting point is to sift official registers of service providers. This is easier in some countries than in others.

Germany, for example, has a list of licensed providers for all "cryptographic assets," including cryptocurrencies and Stablecoins as well as security and fund tokens. In Germany, banks must also be approved explicitly as digital asset custodians.

In the United States, the New York Department of Financial Services (NYDFS), whose Special Trust licences have emerged as the default licence of choice for digital asset custodians in the United States, also maintains a useful list of approved entities.

These entities almost certainly hold the bulk of institutional cryptocurrency and tokenised assets globally. A Bank for International Settlements (BIS) report of December 2023 estimated major banks hold a total of just US$6.4 billion in cryptocurrency, whereas the firms on the NYDFS list were at the time holding US$350 billion worth.

Custodians in other countries are trickier to assess. Banks may, for example, provide digital asset custody services in a jurisdiction but not under a fresh licence. Instead, they are providing the service under a pre-existing banking licence.

In such cases, the fact that a bank is offering a digital asset custody service at all must be gleaned from sources other than official registers. It is safe to assume that, if a regulated bank is providing a digital asset custody service, it is doing so with the approval of the regulator.

Some countries also maintain corporate registers with dozens or even hundreds of names registered as digital asset custodians. This is true of France, Italy, Spain, Lithuania and especially Poland. Most of the names on these lists are yet inconsequential, though they can include household name banks with a demonstrable commitment to digital assets in general, and not just custody.

In the United Kingdom, the Financial Conduct Authority (FCA) maintains a register for non-banks.[5] In 2023, the previous Conservative government announced plans to legislate for a future financial services regime for "crypto assets," and the decision was confirmed by the new Labour government in November 2024.

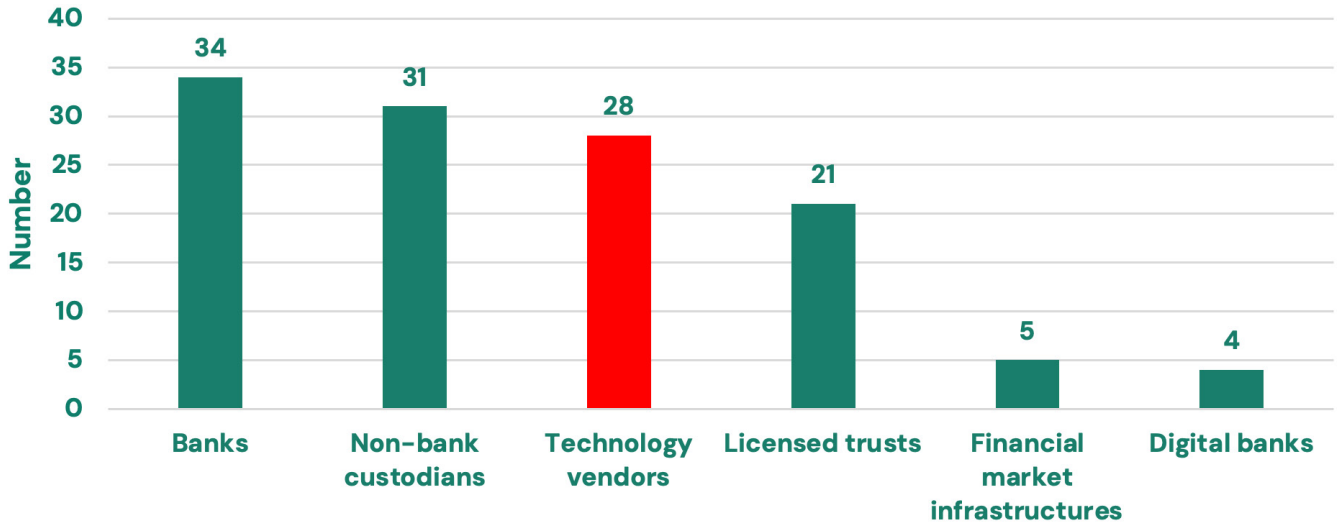
This legislation will extend the digital assets regulatory remit of the FCA from Anti Money Laundering (AML), Countering the Financing of Terrorism (CFT) and sanctions screening into a more comprehensive conduct regime covering digital asset trading, including security and fund tokens, Stablecoins, and digital asset custody. It is not yet clear whether banks offering digital asset custody services will have to apply for a special licence.

A snapshot of the digital asset custody industry

The combination of official data sources and other public information has yielded enough information for Future of Finance to identify 123 firms engaged in institutional quality digital asset custody (see Chart 2). The largest groups are banks and specialist non-bank custodians but 28 of the 123 are technology vendors.

Chart 2

Types of Digital Asset Custody Service Providers



Although it is tempting to conclude that technology vendors should be disregarded – after all, they are selling software, not a service - that would be a mistake. Technology companies are also seeking regulatory permissions. Four are known to have secured regulatory licences already (see Chart 3).

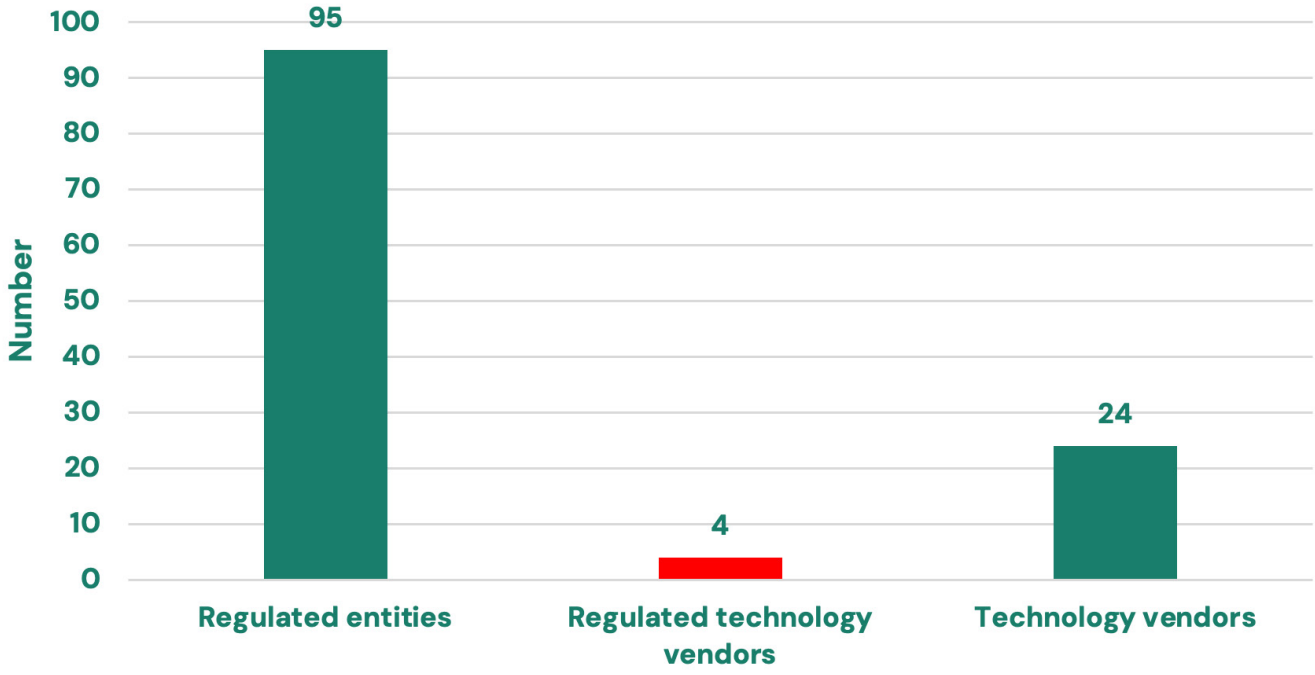
Fireblocks, for example, now offers a custody product under an NYFDS licence. It is structured as a synthetic global network, in which Fireblocks effectively sources the custodians.

Technology vendors are also important in the sense that their software lends credibility to bank and non-bank digital asset custodians. Almost 40 bank and non-bank custodians are known to have in-sourced the technology they use from the top tier of digital asset custody vendors such as Taurus, GK8, DFNS and Fireblocks, and the real number is almost certainly higher.

5. See the Chart on page 19.

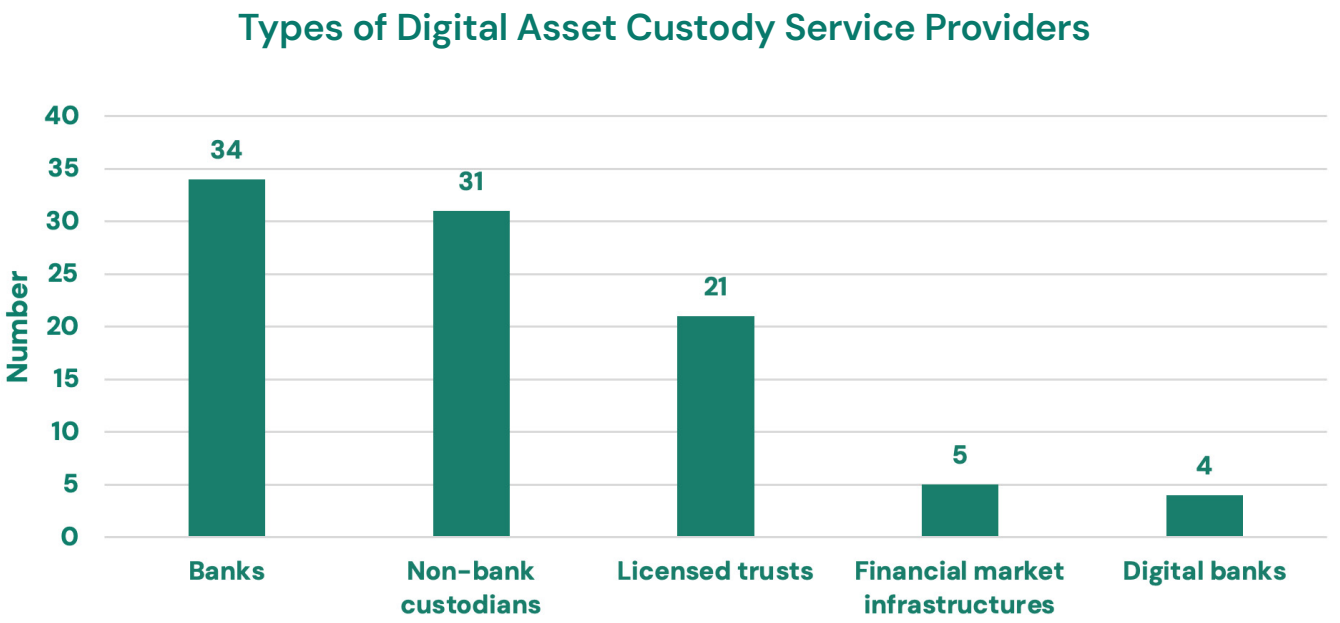

Regulators of Digital Asset Custodians

Chart 3


Technology Vendors Are Getting Regulatory Licences
Number
100
90
80
70
60
50
40
30
20
10
0
95
4
24
Regulated entities
Regulated technology vendors
Technology vendors

The 95 digital asset custody service providers that are not technology vendors divide into five separate categories (see Chart 4). The largest group is bank custodians, many of them household names involved in conventional global custody such as BNY, Société Générale or Standard Chartered Bank.

Chart 4



The second largest group is non-bank custodians that have emerged from providing services to cryptocurrency investors, such as BitPanda (which acquired the United Kingdom-based digital asset custodian Trustology in 2022) and Copper.

The third largest non-technology group is the licensed trusts. Their number includes the BitGo Trust Company, Inc. which is a qualified custodian regulated by the South Dakota Division of Banking and registered as a Money Services Business (MSB) with the Financial Crimes Enforcement Network (FinCEN).

The custody arm of the leading cryptocurrency exchange, Coinbase Custody Trust Company, LLC is chartered as a limited purpose trust company by the NYDFS.[6] The Coinbase exchange has money transmission licences in 46 of the 50 American states.

One of the two smallest groups of non-technology digital asset custodians is financial market infrastructures such as SIX, the stock exchange, central counterparty clearing house (CCP) and central securities depository (CSD) group in Switzerland, and the innovative Börse Stuttgart Group, which is active in Germany as well as Switzerland.

The smallest non-technology group of digital asset custodians consists of digital banks. Their number includes Anchorage Digital Bank N.A., the only federally chartered "crypto" bank in the United States and Sygnum Bank, which holds a banking and securities dealer licence from the Swiss Financial Market Supervisory Authority (FINMA) and a Capital Markets Services (CMS) licence from the Monetary Authority of Singapore (MAS).

The digital bank group also includes Solaris Bank, which has a full banking licence from the German Federal Financial Supervisory Authority (BaFin) and e-money institution licences from the FCA in the United Kingdom and the Bank of Lithuania.

6. For assets in custody with Coinbase see the chart on page 33.

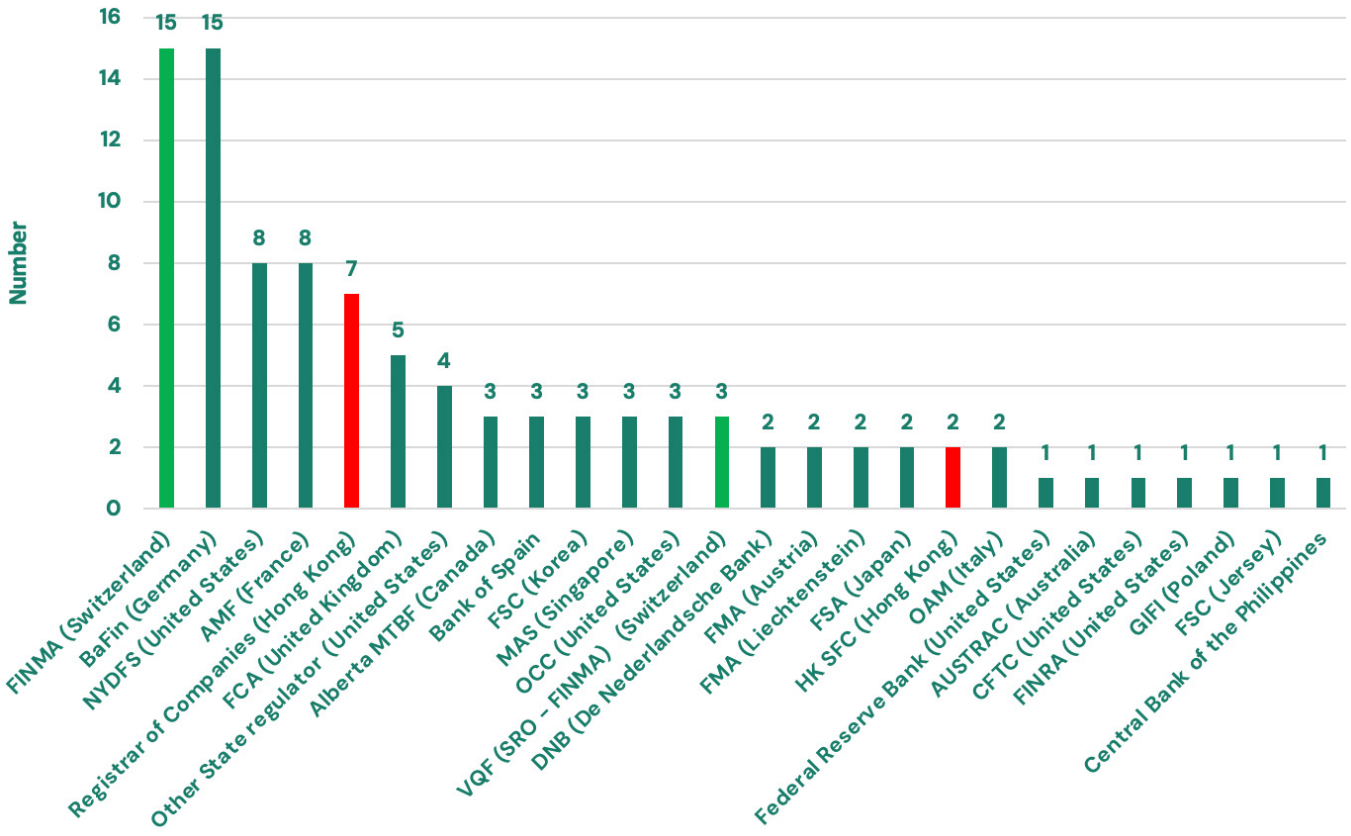
How digital asset custodians are regulated

Who regulates a digital asset custodian is a useful proxy for the quality of the institution and its services. Although it would be helpful - especially in matching custodians to customer needs - to assess custodians by other criteria such as product capabilities, range of services, the number of blockchains and tokens supported, wallet types and features and target customers, this information is difficult to obtain from public sources. The work is under way but not yet complete.

In the interim, the regulatory status of a custodian is the best guide to quality. But even with a group as small as the 99 regulated entities – 95 digital asset custodians plus the four regulated digital asset custody technology vendors - the number of regulators involved is large. The 99 firms answer to 27 separate regulators (see Chart 5).

Chart 5

Primary Regulators of Digital Asset Custodians and Regulated Technology Vendors



That said, more than a third of regulated digital asset custodians are supervised by the major securities market regulators in just three European jurisdictions: Switzerland (FINMA), Germany (Bafin) and France (Autorité des marchés financiers (AMF)).

The Swiss regulators are highlighted in lime green in Chart 5 because providers are regulated not only by FINMA but also by a self-regulatory organisation (SRO) called Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF), an independent but lesser degree of regulatory authorisation.

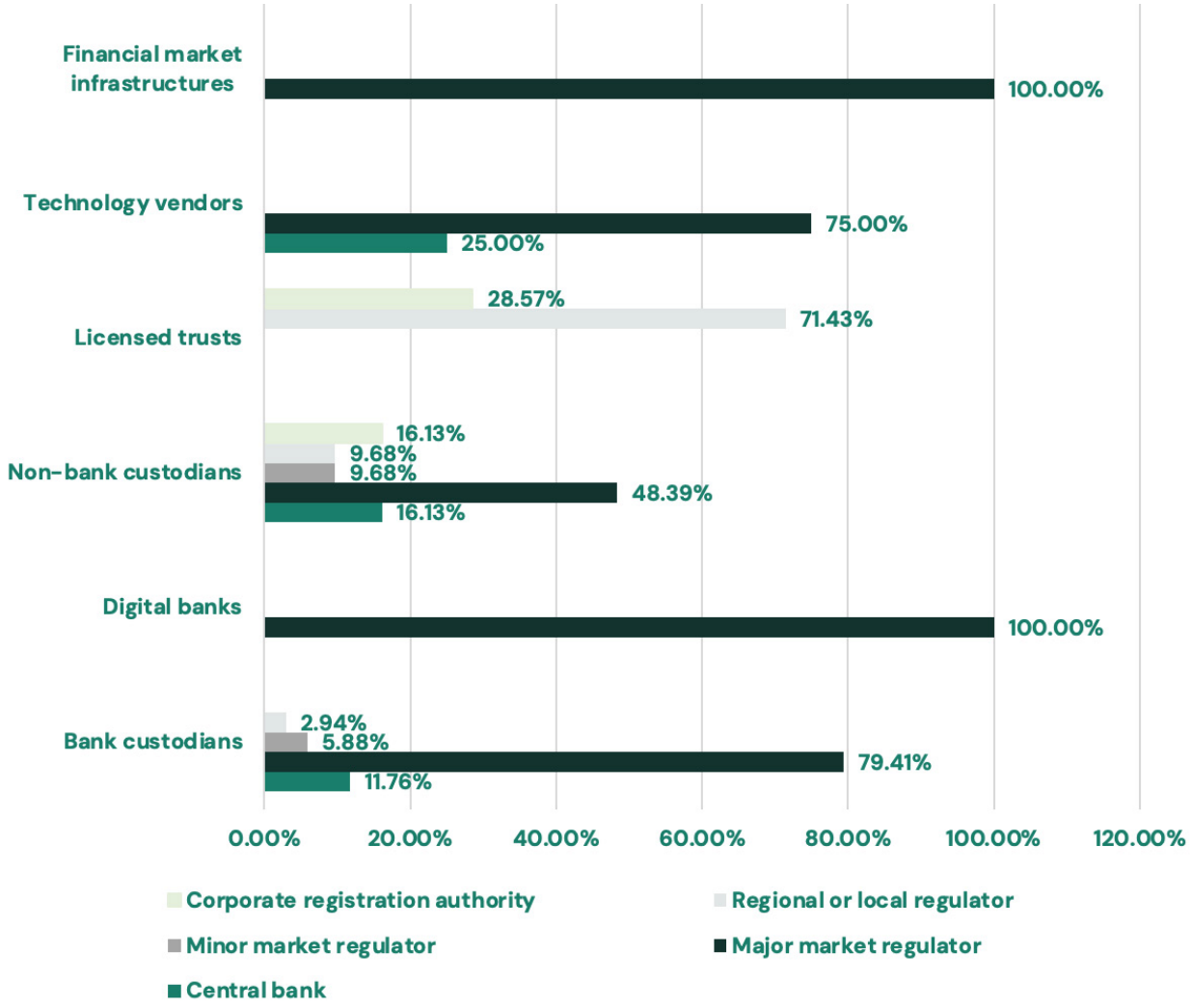
On the other hand, the Hong Kong regulatory authorities – where the Registrar of Companies and the Securities and Futures Commission (SFC) are highlighted in red in Chart 5 – issue different licences of equal quality for different types of services.

The different types of regulator matter. In Chart 6 the primary regulators of digital asset custodians are divided into five different types. The most prestigious is a central bank, closely followed by securities market regulators in a major jurisdiction. Minor market, or regional or local, regulators are less reassuring.

Appearing on a corporate registration list is rarely informative about quality. In general, any type of licence is superior to corporate registration, which tends to be a function of the universal need to comply with AML, CFT and sanctions screening obligations.[7]

Chart 6

Primary Regulators of Digital Asset Custodians



The message of Chart 6 is clear. As primary regulators of digital asset custodians, major securities market regulators predominate in all cases except non-bank custodians and licensed trusts. Less than half of non-bank custodians are supervised by a major securities market regulator.

None of the licensed trusts is regulated by a major securities market regulator. They are instead regulated overwhelmingly by either a local or regional regulator such as the NYDFS or reside on a corporate register only.

It is not clear how deeply corporate registrars delve into entities on the register. In the United Kingdom, investigations are probing. In other jurisdictions, such as Poland, it is relatively easy to register without addressing a lot of questions.

7. The Financial Action Task Force (FATF) Recommendations on measures countries should implement to combat money laundering and terrorist financing are the only regulatory obligation laid universally on cryptocurrencies (see footnote 1 on page 16).

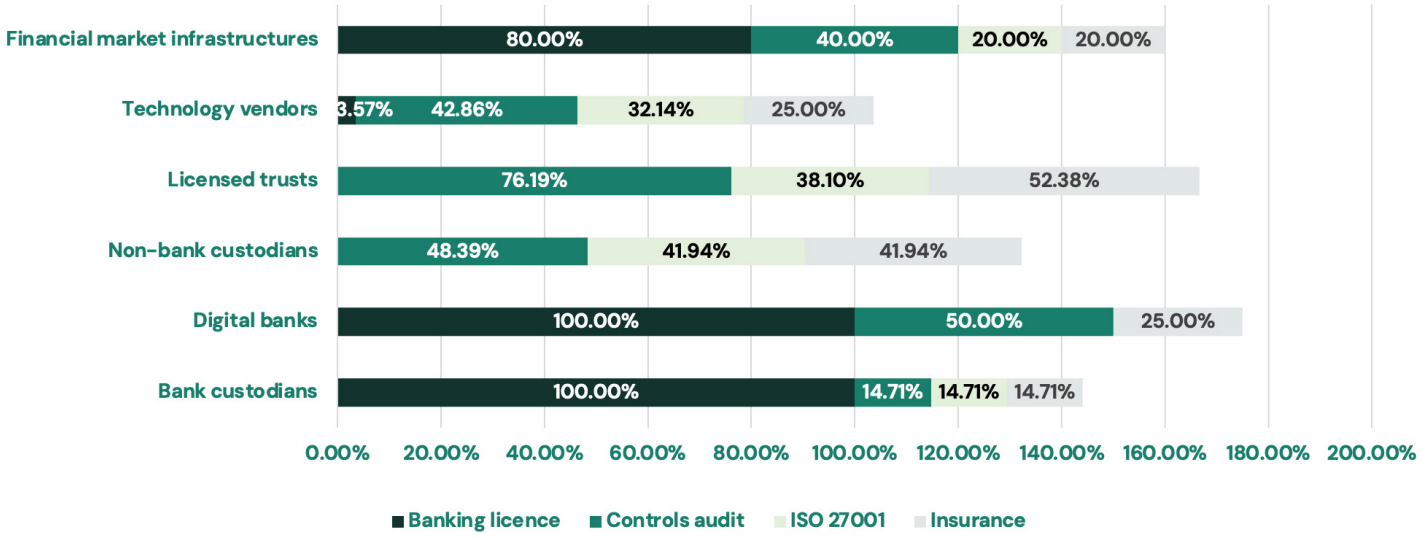
Overall, the most popular licences are being issued by FINMA in Switzerland, the MAS in Singapore, the Financial Services Agency (FSA) in Japan, the BaFin in Germany, NYFDS in the United States and the SFC in Hong Kong. The new licences being issued by regulators in the United Arab Emirates (UAE) are increasing in popularity too.

Other sources of credibility for digital asset custodians

A banking licence is obviously the sternest test, and 100 per cent of banks have one, as do 80 per cent of financial market infrastructures (see Chart 7). If non-banks cannot obtain recognition from a major market regulator, they look for other sources of credibility. Options include insurance but also accreditations from auditors confirming internal controls are sound or the firm meets, say, the International Organisation for Standardisation (ISO) 27001 standard for information security management (see Chart 7).

Chart 7

Licences and Accreditations of Digital Asset Custodians and Technology Vendors



More than half licensed trusts have insurance cover. Four in five have had their controls audited, and two in five have passed the ISO 27001 test. Non-bank custodians and technology vendors are following the same logic.

Every type of digital asset custodian has these accreditations, but they are more important to licensed trust banks, non-bank custodians and technology vendors than they are to banks. Without the option to secure a banking licence, non-bank custodians are (understandably) acquiring other certificates of their soundness.

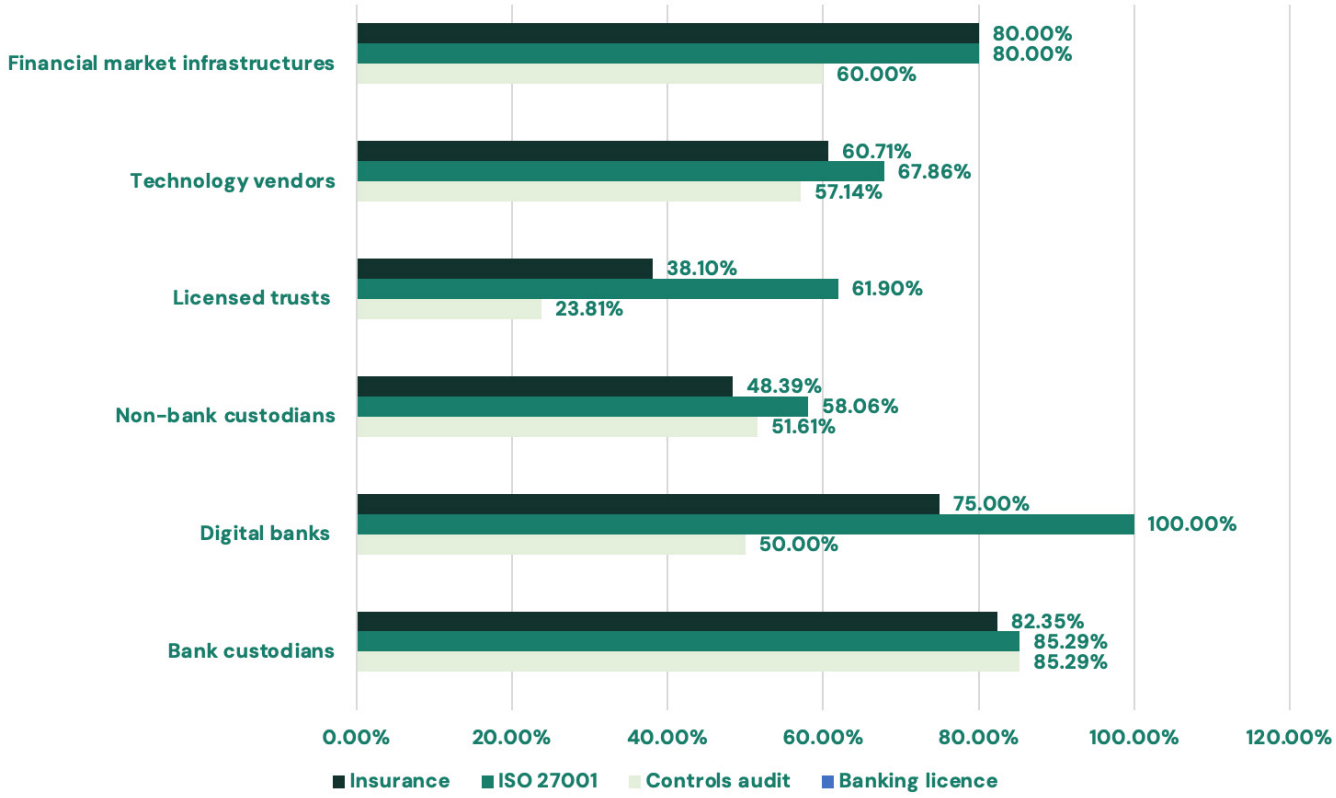
The industry needs a method to help investors choose digital asset custodians

This does not mean banks are not seeking the same forms of accreditation. In the case of more than 80 per cent of the bank-owned custodians, the database cannot yet confirm whether they have ISO 27001 accreditation, or have had their controls audited, or whether they have taken out insurance to protect customer assets. There are similar data gaps at most of the other types of digital asset custodian (see Chart 8).

Only in the case of the non-bank custodians is there a high degree of confidence about accreditations. If the charts are not showing accreditations, the providers do not have them. In other categories, the necessary information is proving elusive.

Chart 8

What We Don't Know About The Licences and Accreditations of Digital Asset Custodians



As a result, the preliminary nature of this classification of digital asset custody service providers is obvious. Much of the information needed to help investors choose a digital asset custodian is either not disclosed or is hard to find. But devising an effective methodology to enable buyers to distinguish intelligently between digital asset custodians is a goal to which the industry should aspire.

Panel 3

Who is offering to custody what for whom?

Panellists: James Pollock, EMEA Sales Director at Digital Asset; Kara Kennedy, Head of Digital Asset Product at J.P. Morgan Securities Services; Jürgen Hofbauer, Global Head of Strategic Partnerships at Taurus SA; Adam Groom, Head of Revenue and Exchanges EMEA at Copper; Thilo Derenbach, Head of Sales and Business Development, Digital Securities Services, at Clearstream; and, as moderator, Monica Summerville, Head of Capital Markets Technology Research at Celent.

How is the digital asset custody industry evolving?

The origins of digital asset custody lie in the initial cryptocurrency boom of 2015-2017. Retail investors needed digital wallets to hold the private keys to their coins, and the cryptocurrency exchanges provided them. Independent digital asset custodians, and vendors of independent digital asset custody technologies, proliferated in 2017 and especially 2018, as the first cryptocurrency bubble inflated and then deflated. At the time, these so-called "crypto custodians" were servicing mainly retail clients investing their own money in Bitcoin, Ether and other cryptocurrencies. The established global custodian banks did not come under serious pressure to provide a digital asset custody service until pioneering wealth managers, private banks and asset managers started to invest in cryptocurrencies with money that was not their own. Managing and safekeeping assets for third parties demands not only a higher standard of service but entails meeting regulatory obligations as well. This demand for digital asset custody services of institutional-grade quality, provided by regulated financial institutions to end-investors and asset managers active in the traditional financial markets already, will only increase as securities and funds are tokenised. This is a major factor in attracting institutional money to digital asset markets, because the custodian banks are already servicing end-investors and asset managers in their traditional business. Those global custodian banks that have engaged with digital assets have also identified opportunities for businesses other than custody, including payments and debt and equity capital markets. Digital asset custody technology vendors report interest from custodian banks in integrating digital asset activities with other services provided by the bank. Interestingly, this will undermine a conspicuous advantage of independent, specialist non-bank custodians, which have succeeded partly because they can offer customers access to asset services such as staking and lending as well as trading. At regulated banks, trading and lending tend to take place in siloes that are separate from custody and regulated in a different way from custody. Integration will blur those siloes.

Should regulated custodian banks offer cryptocurrency staking, lending and borrowing services?

At present, the division of labour between non-bank, specialist digital asset custodians and traditional custodians means that regulated banks experience less demand to provide cryptocurrency services. Conversely, non-bank providers lack the regulatory licences to contest asset servicing by banks in the traditional financial markets. The division of labour is likely to persist. The servicing of tokenised securities and funds will continue to be dominated by banks and the servicing of cryptocurrencies will continue to be dominated by non-banks. That is because few non-bank custodians have yet obtained the regulatory licences they need to provide services under extant securities and fund laws.

Will the banks displace the independent digital asset custodians?

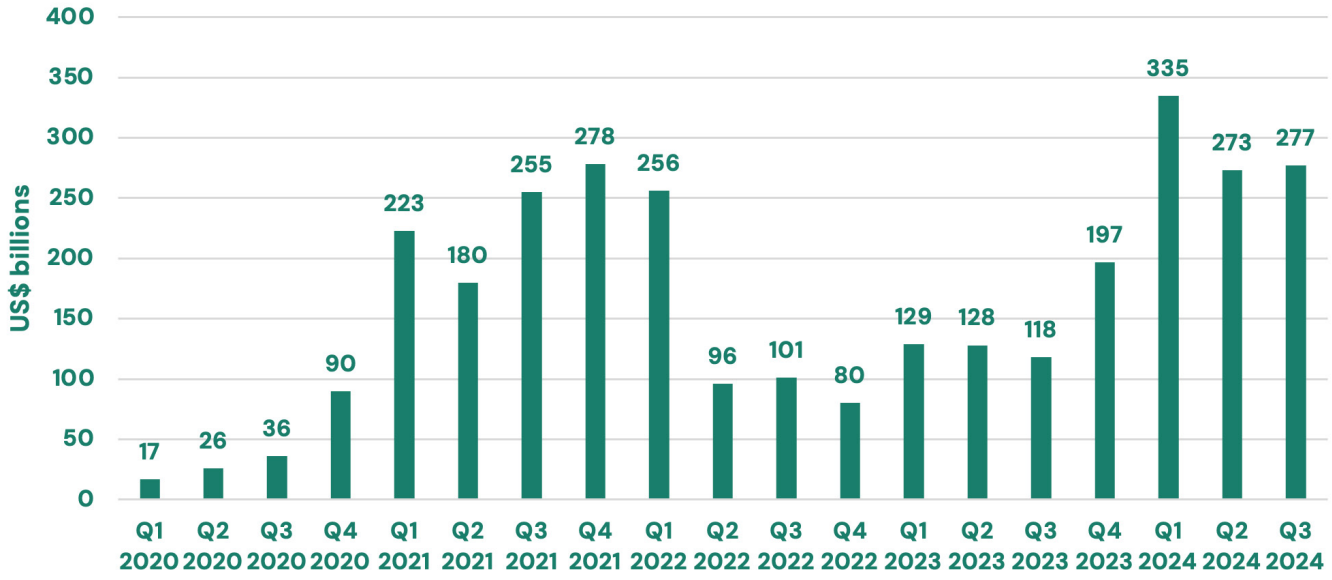
There will be convergence rather than displacement. The current fragmentation of digital asset custody services, and especially the bifurcation between the independent specialist "crypto custodians" and the global custodian banks, will diminish over time. Both will converge on a single regulated model. Regulatory measures such as the Markets in Crypto Assets Regulation (MiCAR)

of the European Union (EU) are encouraging convergence already by enabling independent specialists to secure regulatory licences and allowing traditional global custodian banks to expand their services - initially into cryptocurrencies – without taking undue compliance risk.

Which custodians are securing the biggest market share?

The data needed to make a confident assessment does not yet exist. The market is not big enough for any provider to achieve genuine, measurable scale. But the opacity is also deliberate to the extent that many potential digital asset custodians have yet to go live with their offerings. When it comes to market share, the bifurcation of the industry between "crypto custodians" and global custodian banks with conventional custody businesses and ambitions to grow revenue from servicing tokenised securities and funds as well as cryptocurrencies also makes it difficult to compare like with like. Only Coinbase, as a public company, publishes a regular valuation of customer assets in custody in its quarterly and annual reports (see the Chart below). These assets consist largely of the major cryptocurrencies (Bitcoin, Ether, Solana), Stablecoins and cash used by their customers in cryptocurrency trading and financing activities. Coinbase, which has secured business from the issuers of spot Bitcoin Exchange Traded Funds (ETFs) that traditional custodians might expect to secure, is undoubtedly the market leader in the cryptocurrency custody field. But it is better compared with digital asset custodians such as BitGo and Copper (which also support clients trading cryptocurrency across multiple venues) than traditional global custodians such as BNY or J.P. Morgan (which are more inclined to support buy-and-hold investors). In the longer term, cryptocurrency clients are likely to become less important than investors in tokenised securities and funds.

Customer Assets in Custody at Coinbase



However, the industry is likely to remain relatively fragmented for the foreseeable future, with different providers servicing different asset classes and market participants, if only because one-stop-shops are too ambitious at this stage in the evolution of digital asset custody services. Convergence will occur, and market shares shift rapidly, once the digital asset markets (Decentralised Finance, or DeFi) mature and become interoperable with the conventional financial asset markets (Traditional Finance, or TradFi). That is not just because global custodian banks and financial market infrastructures such as central securities depositories (CSDs) will bring existing relationships and business volumes to bear but because their involvement will accelerate the tokenisation of securities and funds.

What is the safest choice as a digital asset custodian?

The audience was bearish about cryptocurrency exchanges. This is an obvious lesson of the past, from Mt. Gox to FTX, which the "prime brokerage" products of certain digital asset custodians are also designed to address by keeping encumbered assets in custody with an independent, bankruptcy-remote entity. Yet somewhat counter-intuitively, the audience still favoured independent non-bank specialists over regulated banks (see the Chart below). This bias reflects the continuing domination of digital asset markets by cryptocurrencies, where the involvement of banks in custody remains limited. In other words, regulated banks are not yet servicing the cryptocurrency industry, and especially not its more esoteric asset classes, or providing unfamiliar services such as staking, chiefly because they lack the regulatory certainty to proceed confidently. The value of the assets to be custodied on behalf of most market participants is also trivial, both absolutely and relative to the size of the portfolios they maintain in traditional markets, so anxiety about the resilience of the custodian is less intense. Again, regulated banks and financial market infrastructures with banking licences are likely to become a more popular choice as the regulatory environment becomes clearer. Ultimately, firms managing money for third parties, which treat digital assets as a commercial opportunity like any other, want to work with regulated banks because they value a bank as a counterpart in their existing business. In effect, the independent, non-bank specialists are an adequate choice for early adopters content to speculate rather than invest. Institutional money seeking consistent profits will always favour regulated banks.

What services are regulated banks developing?

Virtually every custodian bank is exploring digital asset custody, and several have launched services. By purchasing digital asset custody technology from vendors that have developed state-of-the-art systems in the cryptocurrency markets, banks are becoming formidable competitors to independent non-bank specialists. They combine technology with the assurance of a bank with a banking licence and a balance sheet. Partnerships between global custodian banks and digital asset technology vendors are commonplace already. Indeed, banks are often content to leave custody of esoteric digital assets to technology partners, which act as sub-custodians while the bank focuses on, say, the top three or five cryptocurrencies. However, this sub-custody solution is limited to cryptocurrencies. It cannot work with tokenised securities and funds, whether they are native or non-native. Custodian banks will be concerned about their responsibility to keep customer assets safely and their liability for lost customer assets if a token is issued, settled and safekept on a decentralised blockchain, and traded between parties that hold digital wallets on other blockchains. Decentralised networks of networks of that kind make it difficult for custodians to monitor the transactions that determine who owns what. In traditional markets, custodians value CSDs precisely because they provide a centralised venue where all securities are issued, all parties can settle transactions, and a register of all owners is maintained. Custodians have always struggled to support assets that are not issued and maintained in a CSD.

Could CSDs help custodians develop digital asset custody services?

If custodians value the work of CSDs in traditional markets, an obvious implication is that CSDs could accelerate the growth of the digital asset markets by making it easier for regulated banks to provide digital asset custody services. CSDs would, by definition, improve integration between the digital and traditional asset markets. They could overcome a major retardant of progress - the high cost of adopting an altered or new operating model – by providing their existing users with a familiar point of entry to the digital asset markets. In this context, the experiments with new CSD models being conducted in the United Kingdom Digital Securities Sandbox (DSS) set up by the Bank of England and the Financial Conduct Authority (FCA) are unusually important. Their long-term success will depend on adoption, and that depends in turn on ensuring any new models that emerge from the DSS are not restricted to a small proportion of the potential market in digital assets. One obvious opportunity for CSDs, which some are already exploring, is to extend their repo services to digital assets, enabling banks to raise commercial bank money and central bank money against digital asset collateral. That would create a direct and profitable link between traditional financial and money markets and digital asset markets, with the potential to enhance liquidity in both. The risk for established CSDs is that, if they do nothing, others will emerge to provide the digital asset equivalents of the services they provide in the traditional markets today: issuance, settlement, registration, asset servicing and financing. Specialist digital

asset custodians are already providing the "prime brokerage" services that enable cryptocurrency market participants to post cryptocurrencies, staked cryptocurrencies and tokenised money market funds as collateral across a range of trading venues hosted on private, public and public permissioned blockchains without the assets ever leaving custody. Even if a CSD in a national market does not provide all these services it could act as the "orchestrator" or monitor – what Blockchain Law IV in Luxembourg calls the "control agent"[8] - of their provision to market participants by other service providers.

Does self-custody ever make sense?

Self-custody is sometimes the only choice. An end-investor seeking exposure to digital assets via a venture capital fund or fund of funds invested in promising but risky blockchain start-ups, for example, will struggle to find a custodian at all. It takes months to complete the due diligence on each Layer 1 blockchain or Layer 2 network and then insulate customers from the differences between them, so custodians cannot achieve the necessary scale quickly. In addition, some hedge and proprietary funds trading their own money have built custody solutions in-house. But as soon as a market participant raises external capital, or starts to manage money for third-party clients, self-custody ceases to be an option.

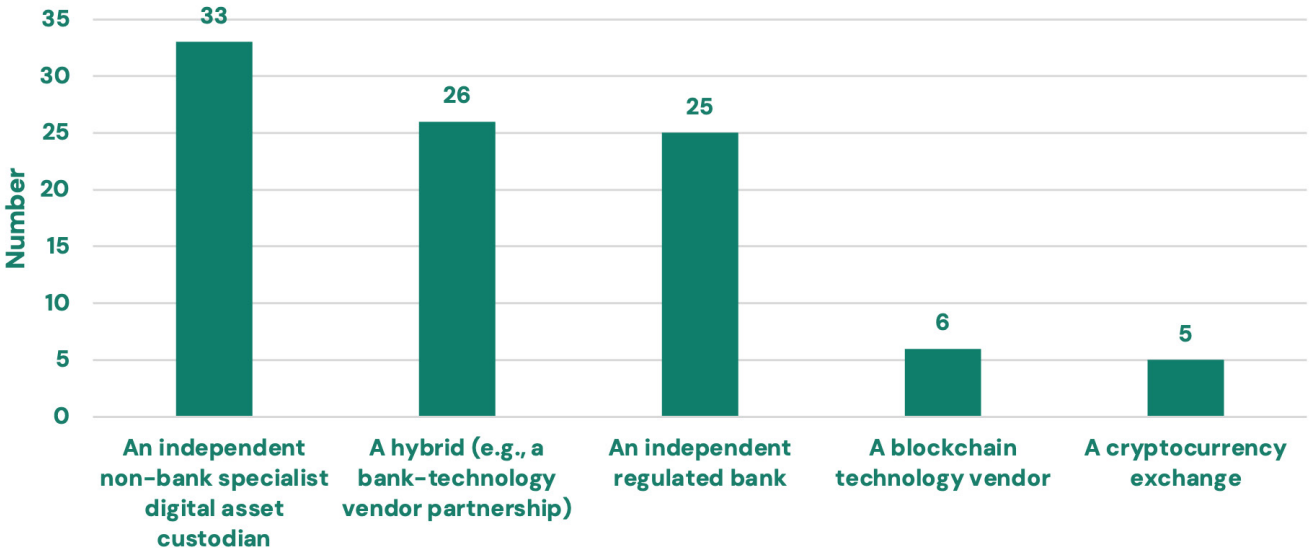
What will the digital asset custody industry will look like in 2030?

By 2030 the different types of custodians will have converged on a common operating model, and the consolidation of the industry will have begun. More capital will flow into the industry. Partnerships between specialist providers will flourish. All digital asset custodians will benefit from a wider degree of regulatory clarity and consistency across jurisdictions. Services will be provided mostly to customers on permissioned public blockchains rather than wholly private or wholly public blockchains. Blockchain technology, including standards to facilitate interoperability, will be much less prominent in industry discussions and the types of digital asset being issued, traded and safekept much more prominent. By 2030, atomic settlement will also have reduced settlement risk in capital markets to zero.

8. Under the fourth iteration of the Blockchain Laws passed by the Luxembourg government, a "Control Agent" can be appointed. Its duties include monitoring the digital assets held in custody and reconciling what is held with what is issued. Maintaining the integrity of an issue in this way is a classic function of a CSD.

What the Audience Said

Which Type of Digital Asset Custodian Is Best Placed to Protect Customer Assets?



Panel 4

What should you look for in a digital asset custodian?

Panellists: Glenn Morgan, Senior Vice President and Digital Asset Practice Leader at Aon; Anya Nova, Director of Sales, Europe at GK8 Custody; Donald Brouwer, Vice President of Business Development at Dfns; and Tom Pikett, Director and Digital Assets Product Manager at BNY.

How do the risks of digital asset custody differ from the risks of traditional custody?

Digital assets are not the same as conventional financial assets, so custodians must master familiar risks in unfamiliar guises, and entirely new risks. The fact that ownership of a digital asset depends on possession of private keys is an obvious difference from registered securities or funds. The keys are routinely sharded into multiple parts which must not only be reassembled as needed but may be in jurisdictions that a traditional custodian is under a regulatory obligation to avoid. In the case of tokenised securities (and Stablecoins) stolen private keys can be used to mint large quantities of the assets. But theft of private keys is not the only risk. One risk that is poorly understood is that it is possible to steal assets by adding malicious code to a transaction that is in flight, replacing the recipient address without any need to steal the private keys. Digital wallets, where assets are held, are not like custody accounts either. They are anonymous and change and multiply rapidly all the time. Atomic settlement is also different from settlement by Payment versus Payment (PvP) or Delivery versus Payment (DvP) on trade date plus two days (T+2). It is not clear whether atomic settlement achieves legal settlement finality (legal irreversibility, even if a party goes bankrupt) because there is a risk that transactions will be unwound. Smart contracts rather than paying agents or custodians transfer value automatically but might be prompted to send tokens by defective or compromised data oracles. The issuance, dilution and buyback of digital assets is controlled not by corporate hierarchies organised under company law but by decentralised autonomous organisations (DAOs), which are often captured by a minority of large holders. Corporate actions are not just dividend payments or rights issues but "airdrops" and "forks." Assets are lent but also "staked." Of course, not all users of digital asset custody services experience these risks in the same form or have the same attitude towards them, but that only adds another layer of complexity for digital asset custodians. Venture capital funds, for example, prefer to assume the risk of self-custodying private keys so they can act fast when an opportunity arises. Bank-owned digital asset custodians, on the other hand, recognise the need to ensure private keys are as invulnerable as possible. This is why they rely on expert digital asset custody technology vendors rather than building infrastructure in-house and insist on extensive testing and auditing processes before going live with a service.

Is sending and retrieving fiat currency cash to and from blockchains particularly risky?

Keeping cash in custody does not create a risk greater than safekeeping any other tokenised asset. However, using cash in the form of a Stablecoin or tokenised deposit or tokenised money market fund to settle a transaction on-chain does create a risk while a payment is en route from the payer to the payee. The risk is not high if cash is moved on- and off-chain by members of a private, permissioned blockchain network, where the counterpart that is the source or destination of the cash is also expected to do due diligence on the underlying client. Moving cash on and off public blockchains is obviously riskier. One solution is to avoid using on- and off-ramps altogether. In November 2024 SWIFT, UBS Asset Management and Chainink announced that they had completed a successful pilot test in which investors subscribed and redeemed shares in tokenised mutual funds entirely off-chain by using the SWIFT payments network. GK8 also offers a service in which Application Programme Interfaces (APIs) are used to confirm a payment is in a bank account, with confirmation triggering the minting of a token to a blockchain.

Are traditional custodian banks struggling to manage digital asset custody risk?

Not yet. Nevertheless, traditional global custodian banks must avoid the temptation to attempt to do everything in-house. They must understand their own limitations and be willing to work with specialist partners in specific areas. That said, the proportion of the work completed in-house is likely to increase as internal knowledge expands. The crucial consideration, however, is not the ability of a traditional custodian bank to build a digital asset centre of excellence. It is to distribute knowledge of digital assets throughout the institution.

In safekeeping digital assets, is technical excellence more valuable than financial strength?

Two in five members of the audience ranked technical and technological excellence above a strong balance sheet as a desirable quality in a digital asset custodian (see Chart below). If custody was a purely off-balance sheet business, this would make sense, but it is not. The financial crisis of 2007-08 proved that some ostensibly off-balance sheet risks could still impact bank balance sheets. Operational risks, of the kind custodian banks incur, have long carried a capital weighting. In March 2022 the Securities and Exchange Commission (SEC), via Staff Accounting Bulletin No. 121 (SAB 121), prescribed that digital assets held in custody on behalf of customers should be shown on the balance sheet of the entities it regulates[9]. The Bank for International Settlements (BIS) has also imposed capital requirements on banks to cover their exposures to digital assets, with especially punitive capital weightings for digital assets issued on to public blockchains. Obviously, non-banks do not bear any of these balance sheet costs, which means they can focus on the technicalities and the technology, and offer cheaper, more flexible and more creative digital asset custody services. Custody clients that value technical ingenuity attach a higher value to those capabilities than financial strength. Other clients, and especially those managing third party assets as a fiduciary, will take the opposite view.

9. On 23 January 2025, subsequent to the Future of Finance event, the SEC confirmed in Staff Accounting Bulletin 122 (SAB 122) that it was rescinding the guidance in SAB 121."

Is technical excellence the right criterion for choosing a digital asset custody technology vendor?

No. The digital asset custody technology sector suffers from a high risk of merger or acquisition or outright failure. If financial strength and longevity are important when choosing a digital asset custodian, they are even more important when choosing a digital asset custody technology vendor. Blockchain technology that worked well in a Proof of Concept (PoC) or Pilot Test may be technically excellent but also be hard to scale. As the digital assets markets grow beyond cryptocurrencies, it will be important to choose a vendor whose technology can scale with the market. Speed of settlement is an obvious case in point. Proof-of-work blockchains have notoriously limited capacity to settle transactions quickly, so vendors must find ways to massively increase the number of transactions per second (TPS) their technology can process. As transaction volumes and trading counterpart numbers increase, digital asset custody technology vendors will also be under pressure to increase the number of digital wallet addresses their technology can support. Buyers of digital asset custody technology are also finding that working with one vendor is not enough, because different vendors cover different segments of the digital asset markets. Working with more than one vendor is also a form of risk management. If one vendor fails, the other can pick up the slack.

Is there demand for custody services that span both traditional and digital assets?

Yes. There is growing interest in a consolidated custody service from institutional clients which have exposure to more than one type of asset. An asset manager holding cryptocurrencies, native and non-native tokenised assets and traditional securities and funds does see advantage in the ability to manage all the assets as different parts of a single pool. The assets can be lent and financed and posted as collateral interchangeably as well as being bought and sold. However, it is difficult for banks to integrate such a rapidly evolving technology as blockchain into their legacy banking systems.

Are digital asset custodians struggling to optimise quality and price?

Traditional global custodians have a self-defeating tendency to customise their services to the wants and needs of institutional clients in exchange for miserly fees that are better suited to a pile-them-high-and-sell-them-cheap commoditised service. This has made it difficult to scale the global custody business as a standardised offering. The digital asset industry is not yet large enough for global custodian banks to have experienced similar dilemmas. Clients are as yet focused not on value-adding services but purely on asset protection. As a regulated institution, global custodians must also be mindful of the uncertain legal and regulatory environment, which limits the range of services they can offer for fear of inadvertent compliance breaches. It is difficult for banks to customise such a narrow range of services. The number of blockchains they can support is limited too. New services, such as staking, must be assessed not just as commercial opportunities but from a risk management and control, cybersecurity, resilience and contractual perspective as well.

What can be done to reassure traditional custodians that staking is safe?

A dozen firms involved in the cryptocurrency industry have with the assistance of PwC developed the Node Operator Risk Standard (NORS) to certify the level of security and operational efficiency of Ethereum node operators via staking risk management standards and third-party certification. It helps holders of cryptocurrencies choose staking counterparts that are safe. The success of initiatives such as these depends on industry-wide adoption, which in turn depends on the robustness and scalability of the standard and its adaptability to changes in both the technology and the way the underlying markets work.

What is the value of insurance to a digital asset custodian?

Independent specialist digital asset custodians, including some controlled by banks, use insurance to reassure customers that they can be made whole if assets are lost. The ability to demonstrate that an insurer considers the risk insurable has sales and marketing value. However, the terms of insurance policies vary. For example, insurance cover is sometimes pooled. This means that, in the event of a catastrophic loss, multiple clients must compete for a share of a single pot of money. Cover tailored to individual clients is superior. Policies can also vary by custodial method. One digital asset custodian offers customers that use a "cold" vault cover worth eight times as much (US$1 billion) as it offers to customers that hold assets in a "warm" infrastructure (US$125 million). Interestingly, the audience attach little value to insurance (see Chart below). This is sensible. Insurance cover *is* less important than the technical knowledge, processes and controls, regulatory status and financial strength of a digital asset custodian. The ability of any insurance policy to protect the policyholder client against loss is subject to underwriting caps, capacity limits and contractual terms and conditions that may not be fulfilled in every case. Limits vary according to the impregnability of the method by which the digital asset is safekept. Large custodial clients find that there is insufficient capacity in the market to cover the whole of their risk, so they must spread their business across several custodians. Likewise, insurers must share the burden of a large underwriting risk with other insurers. Although the digital asset custody insurance market is maturing and becoming more sophisticated, as both the underwriters and the custodians learn from each other about risk and risk management, the market still lacks capacity. All digital asset custodians are currently safekeeping assets whose value is greater than the value of their insurance cover.

Do jurisdictional differences and legal and regulatory uncertainty increase the cost of insurance?

The novelty of the digital assets industry means there is not a long claims history on which insurers can base their policies. Insurance underwriters see legal and regulatory uncertainty in a jurisdiction as making it harder to get an enforcement action if assets are missing. They also prefer digital asset custodians to be licensed or regulated. But the risk of an organisation getting sued successfully is the major deterrent to the provision of insurance.

How much weight do audited accreditations carry with insurance underwriters?

Both specialist, non-bank digital asset custodians and digital asset custody technology vendors have accumulated audited accreditations such as ISO 27001 (an international standard of information security), System and Organisation Control (SOC) I and II certificates (financial and information controls assurance) and International Standard on Assurance Engagements (ISAE) 3000 and 3402 certificates (which certify that controls are in place). They are evidence of institutional-grade internal controls, which can be reassuring for potential buyers when the company is selling an innovative product, especially if the auditor that issued the certificate is a Big Four brand. Insurers are interested in which firms audit a potential risk, and a brand name auditor improves the profile of a risk in much the same way that it improves sales prospects, even if a Web 3.0-savvy start-up firm specialising in digital assets would be better qualified to judge the capabilities of the business. In effect, and perhaps contrary to the audience conviction that technical knowledge is the most important factor in choosing a digital asset custodian (see the Chart below), buyers are purchasing Brand as much as Knowledge. That said, possessing certifications prepared by a Big Four firm is not a sine qua non of obtaining insurance. It helps mainly in reducing the number of questions a digital asset custodian must answer because underwriters do ask potential clients directly why they do not have certain accreditations. Insurers are interested mainly in identifying potential points of failure, and especially whether losses are more likely to be occasioned by the behaviour of the custodian than the customer. Experience shows that losses tend to be caused by customer misuse of technology and processes rather than by weaknesses in the technologies or processes themselves.

Do insurers rely on standardised questionnaires when assessing digital asset custodians?

No. There are many variants. Insurers tend to rely on detailed statements of facts rather than questionnaires. These are highly prescriptive and sometimes so detailed that they must be completed by multiple individuals at a digital asset custodian because certain information cannot be shared between colleagues. There are dedicated questionnaires for other lines of coverage, such as financial crime, cybersecurity and blockchain technology but, in these cases, insurers decide what they care most about. They often accept information generated by the activities of their peers.

Are there standard Request for Proposals (RFPs) questionnaires for digital asset custodians and digital asset custody technology vendors?

No. The standardised questionnaires prepared by trade associations such as the Association for Financial Markets in Europe (AFME) and the industry consultants that intermediate RFP processes for end-investors and asset managers in the traditional custody industry are not yet evident in digital asset custody. On the technology side, banks ask vendors different questions, partly because they must respond to regulatory demands, and these vary between jurisdictions. The questions they do not ask are often more important than the ones they do. It is an area in which the buyers are learning by doing.

What the Audience Said

What is the Most Important Factor in Choosing a Digital Asset Custodian?

Panel 5

Digital asset custody: What can possibly go wrong?

Panellists: Laurent Kssis, Board Member and Strategic Advisor to Issuance.Swiss AG; Philip Rage, Director of Strategic Initiatives at Soter Insure; Tariq Rasheed, a Partner at Reed Smith; Jeet Singh, Partner and EMEA Blockchain Leader at EY; and, as moderator, Ed Pugh, Development Director, Fintech and Digital Assets, at Aon.

"Not your keys; not your assets." Is this true of all digital assets?

Private keys are multi-digit numbers which investors entrust to digital asset custodians under a power of attorney. If the private keys to a digital asset are stolen from the custodian, the extent to which the thief has stolen something that they can turn into money varies by asset type. "Native" cryptocurrencies and tokens are indeed lost, with illicit proceeds run through "mixers" or "tumblers" that help hackers hide the trail of transactions by associating them with unrelated funds. Non-native security or real-world asset (RWA) tokens, on the other hand, are protected by the continuing existence of the underlying assets, so the registration function enables the missing token to be burned and a replacement minted.

How are digital asset custodians managing "not your keys; not your assets" risk?

Multi-signature ("multisig") wallets are the most common solution. By requiring two or more private keys to sign off on any transaction, they increase the security of the funds stored in the wallet. Multisig processes work fast enough not to disrupt the market by slowing transactions down, and regulators see them as a useful way for independent custodians to manage, on behalf of institutional investors, the critical source of failure in digital asset markets. The real challenge for custodians (and regulators) is how to mitigate the same risk for retail investors, most of which continue to self-custody. Though apps are now available which obviate the need for cold storage in a locked vault, private keys remain vulnerable to the hacking and theft of mobile telephones. It is a good example of how digital assets change the form (theft of a wallet on a mobile phone) rather than the substance (theft of a physical wallet) of safekeeping risks. Retail investors remain resistant to third party custody because being able to transfer value without the intermediation of a financial institution is a foundational principle of the blockchain industry. Eventually, private keys will be built into the retail user experience of apps in the same way that anti-virus software is now built into computers.

Which matters more in risk mitigation: technology or processes and procedures?

Though much time, money and effort are expended on auditing what is novel about digital assets – such as smart contracts and the private key ceremonies used to generate and distribute private keys securely – the main source of vulnerability is not the blockchain technology. Indeed, the traditional assets safekept by traditional global custodian banks would benefit from the protections blockchain technology affords digital assets. Customer asset protection processes and procedures are more important. Here, digital asset custodians can and should follow the precedents set by the traditional custody industry. Making a single individual responsible for approving transactions, for example – as a number of digital asset custodians have proposed – is not a good idea. There is another reason to implement sound processes and procedures to approve transactions. They are now audited and reviewed not just by issuers and investors but by insurers when providing Directors and Officers (D&O) liability insurance as well as theft cover for customer assets. Firms with excellent processes and procedures pay less for insurance.

Do digital asset custodians have to manage entirely new risks?

Yes and no. At a private key generation ceremony, for example, what matters is not what happens but whether the people at the ceremony are trustworthy and will not steal the keys as they are generated. Which is not unlike checking the individuals given access to a bank vault full of physical securities. The 80:20 Rule applies. Four fifths of the risks digital asset custodians must mitigate and manage are familiar from traditional custody, and the remaining fifth are familiar risks that manifest themselves in unfamiliar ways. In other words, the experience of traditional custodian risk managers is entirely relevant to digital asset custody.

Smart contracts are often identified as a truly novel risk. Are they?

Yes and no. Smart contracts are hackable and offer rewards that are attractive to criminals in the same way as many conventional assets. They are vulnerable at the point where value is being transferred, and not just where value is being held in custody, but the same is true of conventional settlements. However, smart contracts are self-executing agreements written in code and embedded in blockchains. This means that, unlike traditional corporate code, once a smart contract is issued on to a public blockchain, it can be accessed by anyone, including bad actors that seek to exploit coding flaws to steal funds. Once issued, a smart contract is also unchangeable; it cannot be upgraded. This is why smart contracts are audited before launch, to check their code, logic and security measures and fix any potential vulnerabilities before the contract is deployed, but this protection is not foolproof. Smart contracts also execute on receipt of information received. If that information is out-of-date or corrupted or prepared by a calculation agent whose methodology is not standardised, this could create losses and subsequent litigation. In addition, the main reason that smart contracts appeal to issuers - they dispense with costly intermediaries – is also their greatest weakness. If something goes wrong with a smart contract there is no intermediary, such as a broker, paying agent or escrow agent, to sue for recompense.

Should the industry persist with smart contracts?

Smart contracts have yet to optimise how they are governed. But solving the governance problem has enormous potential value, because smart contracts can automate operational processes that are inefficient and expensive. The insurance industry could use smart contracts to automate documentation, credit and funds checks. In the securities and trade finance industries, linking smart contracts to digital identities could transform transaction reporting. Legal certainty would make it easier to broaden the use of smart contracts in operational automation because it would mean all parties to a smart contract are agreed on the source of the information that triggers a pay-out, what should happen if that source fails and what should happen when a trigger event occurs. Ultimately, legal certainty means beneficiaries will always be entitled to their pay-outs, irrespective of the technical performance of the smart contract. If a smart contract is designed well enough to deal with multiple eventualities algorithmically, and all parties to the contract are aligned on a single interpretation of how those eventualities will eventuate, it can add efficiency to operations. But there remains a risk of an unexpected event that even the best-designed smart contract fails to anticipate, just as issuers of Collateralised Debt Obligations (CDOs) and their investors failed to anticipate the events of 2007-08. This risk is especially high with such an immature instrument as a cryptocurrency. It is amplified by the fact that the same smart contract function can be processed differently on different blockchains, creating legal as well as practical uncertainty as to who owns what and who owes what when something goes wrong.

Staking is often identified as another truly novel risk in digital asset custody. Is it?

No. Staking is analogous to re-use of securities for lending or financing purposes, in which an asset is put at risk to generate a return. Many digital asset custodians see staking as a potentially useful revenue stream while they wait for tokenisation of securities and funds to accelerate. But potential buyers of the service are inhibited by uncertainty about the consequences if a staking investment goes wrong. Documentation has not yet settled whether custodians are acting in a fiduciary capacity and assuming liability for any losses or on a title transfer basis, in which the investors own nothing but an unsecured claim. Decentralised apps (DApps), which run autonomously through smart contracts on Decentralised Finance (DeFi) networks, will struggle to attract institutional support as long as investors lack trust in the ability of smart contracts to secure entitlements and ownership. That lack of confidence reflects a lack of confidence in the legal underpinning of DApps and the smart contracts they rely on to clarify who owns and owes what when something goes wrong. This matters when the number of digital asset custodians that offer or are planning to offer staking services is increasing.

Are data hacks a risk in digital asset custody?

Yes. Digital asset custodians collect a lot of personal and corporate information about their customers when conducting due diligence as part of the on-boarding process. Hackers do steal this information, which then allows criminals to attempt social engineering frauds in which they exploit the knowledge they have stolen. These are the same as the phishing, vishing and SMShing emails, text messages and telephone calls that follow hacks of any database that contains customer information.

Do institutional investors have different expectations of digital asset custodians?

No. Investors seek the same benefits from a digital asset custodian as they do from a traditional custodian. They want their assets safekept from loss, theft and fraud; to be made whole if assets go missing; their entitlements, such as interest and dividends and distributions, collected; their transactions settled; to obtain additional earnings from lending or re-using assets in custody; to remain in compliance with relevant laws and regulations; and to be insulated from the operational, technological and technical complexities of obtaining these benefits. Much of what sounds novel is in fact familiar. An “air drop” or a “fork,” for

example, is a corporate action, and investors will find their custody agreement is a good guide to how their custodians will treat them.

How do retail investors choose digital asset custodians?

Retail investors in cryptocurrencies tend to entrust their assets to the cheapest service provider. This gives the cryptocurrency exchanges where retail investors buy and sell cryptocurrency a distinct advantage. Many exchanges still commingle proprietary and customer assets rather than segregate them. There are incentives to commingle, especially lower "gas" fees to settle transactions. Commingling is also what enables exchanges to offer retail investors low prices for custody. But it puts customer assets at risk if the exchange fails. Though regulations such as the European Union (EU) Markets in Crypto-Assets Regulation (MiCAR) do aim to ensure that assets are segregated, there are no independent due diligence agents capable of empowering retail investors to choose custodians on an informed basis.

Are regulators also treating digital asset custodians in the same way as traditional custodians?

Yes. MiCAR, for example, regulates cryptocurrency custodians as Crypto-Asset Service Providers (CASPs) in much the same way the EU regulates traditional custodians. The focus on authorised entities, prudential requirements, governance, asset segregation arrangements, authorised sub-custodians and insolvency regimes are familiar. MiCAR also makes custodians liable for actual losses of customer assets attributable to them, but this is in line with the obligations EU-based custodians assume in the mutual and hedge fund sectors. Where regulatory approaches might move away from past practice is in confronting issues not previously experienced, such as an "air dop" or "fork" or smart contract that goes wrong.

Is there a risk that the courts will treat the role of a digital asset custodian differently from a traditional custodian?

The courts will expect custodians to protect the assets of customers in the same way that they expect traditional custodians to protect conventional forms of property. They will assess whether the custodial relationship is a pledged or title transfer one, whether and how the assets were segregated, where the custodian is based, what sub-custodians were used and so on. So the principles the courts will apply in tracing responsibility are familiar. The issues that are likely to arise with digital asset custody are not entirely novel and they will be addressed in completely traditional ways. Case law on "forks," for example, is already quite developed in the United States, though less so in the United Kingdom.

What are the fundamental requirements that investors should seek from any digital asset custodian?

At a high level, proper due diligence on a digital asset custodian should focus on five issues. These are ensuring that private keys are kept securely, customer asset segregation arrangements are appropriate, records of client transactions and assets are kept, private and public records of customer assets are reconciled, and contractual arrangements maximise protection of customer assets. These considerations apply equally to traditional custodians. Yet the temptation to make unreflective comparisons between digital and traditional custody offerings should be resisted. In digital asset custody, the risk-reward ratio of the choices an investor makes is much higher than in traditional custody. It is easier for a traditional custodian to offer a keen price because costs can be spread over a much larger volume of business. The same is not true of the as yet relatively small digital asset markets. Nor is blockchain technology as mature or as thoroughly tested as conventional technologies. This affects the safety of services such as staking as well as safekeeping services. Not all digital asset custodians are equally equipped to look after any type of digital asset either. A buy-and-hold investor needs a different service from an investor that trades cryptocurrencies round-the-clock across multiple venues, necessitating continuous movements of collateral. Innovation is constant too, and the ability of custodians to keep abreast of innovations in digital assets will vary.

What are the legal and regulatory priorities for buyers of digital asset custody services?

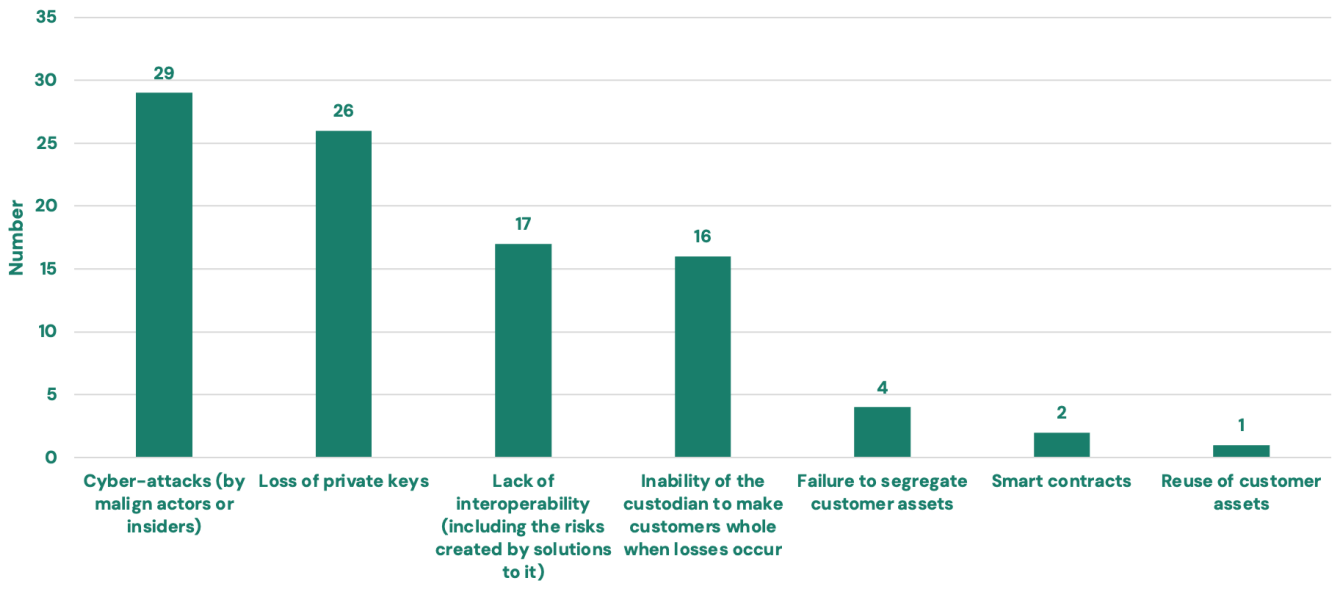
If a custodian fails, the first consideration is location. Digital asset custodians do engage in regulatory arbitrage, and buyers must be mindful of the risks. Even if the custodian is ostensibly located in the United Kingdom, assets may be held by a sub-custodian in Bermuda, which means the insolvency proceedings will take place in Bermuda. The second consideration is the custody agreement: What does it say will happen to the assets if the custodian fails? Wherever the assets have ended up, the courts must proceed from where they should be rather than where they are. Obviously, a respectable jurisdiction with a higher cost of compliance, such as Switzerland or a major EU member-state that has implemented MiCAR and accepts supervision by the European Securities and Markets Authority (ESMA), implies that the provision of a digital asset custody service will cost more. But in principle a successful draft custody agreement must seek to maximise legal customer asset protections, even if they cost more. The third consideration is what the custodian can do to the customer. A customer acting on their own account is in a less vulnerable position than one acting on behalf of third-party clients. If a third-party client is a money launderer or financier of terrorism or a sanctions evader or a criminal, the custodian will have claims against the customer. If the custodian is based in a jurisdiction where it is incentivised or comes under regulatory pressure to freeze customer assets, that can lead to a loss of control by the customer.

What sorts of losses have customers of digital asset custodians incurred so far?

Losses are not visible until they are large. Custodian banks are hacked every day but absorb small losses. Even large losses are never fully explained. It follows that the best way to manage the risk of assets being lost is to appoint a regulated custodian backed by a major bank that subscribes to industry-wide customer asset protection insurance programmes and, if these fail to make customers whole, that is also capable of absorbing unexpected losses on its own balance sheet.

What the Audience Said

What is the Biggest Single Risk Incurred by Investors in Digital Assets?



Upcoming Events in 2025

Digital Asset Exchanges	March 13 2025
Digital Money	June 16 2025
Future of Finance Award Ceremony	June 19 2025
Tokenisation	October 16 2025
Digital Asset Custody	December 3 2025

**Dates are subject to change*


Future of
Finance