Digital Asset

Testimony of
Yuval Rooz
Co-Founder and Chief Executive Officer
Digital Asset Holdings, LLC

Before the
U.S. House Committee on Financial Services
Subcommittee on Digital Assets, Financial Technology and Inclusion

Hearing on
Digital Dollar Dilemma: The Implications of a
Central Bank Digital Currency and Private Sector Alternatives

September 14, 2023

Thank you Subcommittee Chair Hill, Ranking Member Lynch, Full Committee Chair McHenry, and Ranking Member Waters for the opportunity to appear before you today. My name is Yuval Rooz. I am the Co-Founder and CEO of Digital Asset.

I helped found Digital Asset in 2014. Digital Asset is at the forefront of modernizing the infrastructure of the financial system with our privacy-focused blockchain technology. For nine years, we have worked hard to carefully and responsibly innovate to solve real problems in financial services.

Today, our clients are using our privacy-focused Daml application platform and Canton blockchain protocol to reduce the time to issue stocks, bonds,[1] and other financial products[2] from days to seconds, reducing settlement risk and increasing efficiency. One client is using our technology to process over $1 trillion of tokenized Treasury repo agreements per month.[3] And our technology was recently used in a pilot project with the New York Federal Reserve's Innovation Center to demonstrate how blockchain technology can modernize the infrastructure for global dollar-based settlements.[4] To promote interoperability, we recently announced (along with 29 market participants), the launch of the Canton Network to help connect institutions and move value globally.[5] Attached as an appendix is additional background on Daml, Canton, and the Canton Network.

Our success is in no small part due to the fact that our technology is built with privacy at its core—specific privacy rules can be configured for each party in a transaction, making our technology well-suited for financial services.[6]

I am here today because as we embark upon a new digital era in finance, I believe that the global financial competitiveness of the United States—including the dollar's position as the world's reserve currency—is at stake. This is a critical national security issue that demands innovation led by the private sector. But private sector innovation alone is not sufficient. As we've seen with the invention of the Internet, without a proper policy framework and absent a strong partnership between the public and private sectors, private sector initiatives may displace activities properly considered public goods—specifically money—that are due the protections offered by our Constitution. We

[1] https://www.euromoney.com/article/2bpedlxbptouac1934m4h/awards/awards-for-excellence/financial-innovation-of-the-year-2023-gs-dap-by-goldman-sachs
[2] https://www.regulationasia.com/deutsche-borse-goes-live-with-digital-securities-platform/
[3] https://www.mckinsey.com/industries/financial-services/our-insights/tokenization-a-digital-asset-deja-vu.
[4] https://www.newyorkfed.org/aboutthefed/nyic/facilitating-wholesale-digital-asset-settlement
[5] https://www.canton.network/press-release
[6] https://docs.daml.com/concepts/ledger-model/ledger-privacy.html

expect our financial transactions to be afforded the privacy protections of the Fourth Amendment and this should not change as payments become digital.

History has shown that technology is inseparable from finance. And today, we stand at yet another technological inflection point for the financial system: blockchain technology. As our successful client deployments demonstrate, blockchain technology—when built around configurable privacy—can provide the financial system with increased efficiency and reduced risk by eliminating the need for maintaining multiple copies of the same information—which is the case with today's payment systems—and by allowing value to be represented digitally.

Leveraging blockchain technology to modernize financial infrastructure is critical to ensuring our continued global financial competitiveness and the dollar's status as the world's reserve currency. It is the rails on which digital value will be transferred.

Of course, innovation alone is not sufficient for the United States to maintain its global competitiveness, but our role today as a global financial leader—with the dollar as the world's reserve currency—does require innovation. There is nothing inherent or inevitable about the inefficiencies in today's financial system and, as other countries' financial systems eliminate those inefficiencies through blockchain technology, the United States risks being left behind and losing our leadership position. A global economic order aligned with our values is in our national interest.

We have two critical advantages that can help us maintain our leadership position—vibrant private sector innovation, and the rule of law enshrined in our Constitution and protected by its system of checks and balances. And our advantages are strongest when wielded together. While private sector innovation is important—and is the engine that drives our economy—in an area as critical as finance, innovation needs to occur within a deliberate policy framework to ensure that innovation does not outrun or undermine our values and national interests.

As this Committee deliberates on how best to bring the dollar into the digital era, I am here to make two requests. First, that Congress ensures that any digitally-represented dollar, whether a stablecoin or a central bank digital currency, lives within our Constitutional framework—Americans using this digitally-represented dollar should have the assurance that their privacy rights are protected under our Fourth Amendment framework. And second, that Congress works closely with the private sector, and leverages technologies already built and proven, to serve as the rails for any digitally-represented dollar. Any solution that ignores private sector innovation risks technological stagnation and will undermine our global competitiveness.

Thank you for your time and I look forward to answering your questions.

***

Appendix

The Canton Network: A Regulatory Perspective[1]

(Working Paper)

May 2023

The Canton Network provides the financial system with the modern technological infrastructure necessary to handle its growing complexity and enable truly digital value transfer across traditional asset classes. At the same time, the Canton Network provides market participants with the control over data necessary to work within existing regulatory frameworks to build a safer and sounder financial system.

I. The Financial System is a Complex, Adaptive Network with an Inadequate Technological Foundation

> It would be hubris, however, to think that the current model represents the end of monetary history.
>
> —*Mark Carney, The Art of Central Banking in a Centrifugal World*[2]

The financial system is a complex, adaptive network.[3] Intranational and international flows of money and assets occur on a daily basis at a scale that can be hard to comprehend. However, while the financial system continues to increase in complexity, the technology inside the financial system—the technology that runs the financial system—has not kept pace.

Up until the 1960s, the backbone of the financial system was paper-based record keeping. But a drastic increase in trading volumes in the late 1960s triggered a "paperwork crisis" where financial institutions were overwhelmed by the sheer volume of paper required to process transactions, triggering adoption of computer-based record keeping.[4] The financial system today is still supported by technology that emerged as a stopgap solution to the paperwork crisis. While we may have moved away from paper records, the technology used as a replacement unfortunately simply mimics the structure of old paper-based record keeping systems. Information remains siloed both among and within institutions, resulting in data that remains unsynchronized across participants. Transaction settlement remains dependent on costly and slow reconciliation among participants. And though assets are now recorded on electronic ledgers, they remain as static ledger entries. Moreover, subsequent crises such as the 1987 stock market crash and the 2008 financial crisis have resulted in further stopgaps rather than deliberately designed technological solutions.

The financial system will only grow more complex as time goes on. We need to ask ourselves whether the technological band-aids we have been using for the last 50 years can hold up in

---

[1] Manoj Ramia, General Counsel, Digital Asset Holdings, LLC.

[2] Speech by Mark Carney, The Art of Central Banking in a Centrifugal World (June 28, 2021) https://www.bis.org/events/acrockett_2021_speech.pdf.

[3] Speech by Andrew Haldane, Rethinking the Financial Network (April 28, 2009) https://www.bis.org/review/r090505e.pdf.

[4] The Remaking of Wall Street, 1976 to 1971, by Wyatt Wells in the Harvard Business History Review (October 2, 2000) https://hbswk.hbs.edu/archive/the-remaking-of-wall-street-1967-to-1971.

the face of this continually increasing complexity and whether the compounding costs of information silos, unsynchronized data, and costly reconciliation are sustainable.

And, we need to ask ourselves whether the technological band-aids we have been using for the last 50 years are ultimately holding back the financial system from delivering more fully on its promise of creating shared prosperity.

There is an inherent risk in not having systems to manage and control assets that are as equally advanced as the assets themselves. And right now, we have a material gap between these assets and their underlying systems.

We shouldn't consider the current technological foundation for the financial system to be the end of history for innovation in financial technology; by no means is the financial technology we have today the logical end point of innovation.

II. The Promise and Pitfalls of Blockchain

Blockchain has been held out as a solution to the financial system's antiquated, patchwork, siloed technological infrastructure. To understand blockchain's promise, it's important to remember that at the core of the financial system are ledgers—the records of the assets held by financial institutions and the parties that own those assets. The fundamental innovation enabled by blockchain technology is the ability for market participants to work from a shared ledger rather than—as is the case today—each market participant having its own ledger. The obvious benefit of having a shared ledger is the accuracy gained by synchronized data and the efficiency gained by no longer having to reconcile transaction data among many individual ledgers.

And blockchain technology enables an arguably more important innovation: the ability to rethink how value is transferred. Today, because an asset is represented on multiple, disparate ledgers, any transfer of that asset requires manual processes prone to error, creating inefficiencies and settlement risk. But when an asset is instead modeled in code (and so is intrinsically tied to that code) using "smart contracts" on a blockchain-based shared ledger—this is what it means for an asset to be "tokenized"—the asset is no longer a static record, but rather becomes dynamic. Any rules underlying transfers of the asset can then be specified in the code representing the asset, making the asset "programmable." This can eliminate inefficiencies and reduce settlement risk. Moreover, with the rules for transfer now specified within the record of the asset, complex workflows involving multiple assets can easily be created; in other words, the workflows become "composable."

While shared ledgers are appealing, the problem is that they can pose serious privacy and data control challenges. A shared ledger where all of its contents are both visible to everyone and in everyone's possession is not a workable solution for the financial system. This type of a shared ledger would present not just privacy risks but also cybersecurity risks and, to the extent a shared ledger is available to everyone, risks around illicit finance.[5] Instead, each market participant needs to have granular control over who can see each aspect of a transaction and also needs to be able to ensure that only those entitled to see data are in possession of it. Unfortunately, most blockchain technologies do not provide this privacy and granular data control and so are not suitable for the financial system.

[5] U.S. Department of Treasury, Illicit Finance Risk of Decentralized Finance (April 2023) https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

III. Daml and Canton—Blockchain Technology Purpose-Built for the Financial System

Digital Asset's Daml and Canton technologies, however, have unmatched privacy and data control capabilities that make them unique in their ability to deliver the benefits of blockchain.

Daml is a smart contract language that enables assets to be modeled in the context of rights and obligations and that allows for workflows to be defined with granular control over data; the collection of these asset models and workflow definitions is a Daml application. This preserves privacy and makes Daml well-suited for digitally representing assets and financial workflows. With Daml, a developer can specify different privacy rules for each asset in a transaction that is handled in that Daml application. And using a set of Daml libraries we call Daml Finance, traditional assets can easily be tokenized while meeting the privacy requirements of the financial system. Daml applications fully realize these privacy capabilities by running on a Canton blockchain.

Canton (the name is a reference to Switzerland's cantonal, federalist governance structure) is a blockchain technology that takes a unique approach to creating a shared ledger. While most blockchains today replicate the *entire* ledger across parties on a network, with Canton, each user of a Daml application maintains a ledger of only the data it is permissioned to see by that Daml application. The Canton protocol ensures that this data is valid and current and that all data is encrypted. As a result, everyone works from a shared ledger without being in possession of the entire shared ledger and without that shared ledger actually existing; each user is only in possession of its portion of the shared ledger. This provides privacy as well as scalability and performance.

IV. The Canton Network—A Privacy-First Blockchain Network Designed to Meet the Business and Regulatory Requirements of the Financial System

Daml and Canton are powerful technologies. But their true potential is unlocked when Daml applications running on Canton ledgers connect to each other and move assets across their applications. Only then can digital value transfer match, and exceed, the manner and scale of today's analog financial system.

The Canton Network is designed to bring true digital value transfer to the financial system. Like the Swiss federalist governance structure from which it takes its name, the Canton Network is not one monolithic network or ledger where everyone is connected to everyone else and where all data is visible to everyone, as is the case with public blockchain networks. Nor is it a closed system limited to a single use case like many private blockchain networks. Instead, it is a collection of Daml applications running on Canton ledgers that *choose* to connect to each other; it is an interoperable network of networks.

The key to understanding why this is so powerful—and so different from any blockchain network available today, public or private—is in the structure of the Canton ledger itself. As discussed above, unlike other blockchains, with Canton there is no single ledger that is replicated across all of the parties utilizing the ledger. Instead, each user maintains a ledger of only the data it is permissioned to see (as defined in the relevant Daml application). This ensures that each participant has complete control over the parties they transact with, which parties can see what data, and where data resides.

While other blockchain networks have their ledgers as their focal point, with the Canton Network, the Daml applications are the focal point. Market participants develop Daml applications to suit their needs, defining down to the sub-transaction level which parties can see what data. Market participants are already doing this with Daml- and Canton-based systems in production today.

The Canton Network is simply the universe of these and other Daml applications that are connected to each other. And as these Daml applications connect, assets can be transferred across institutions like they are today. The result is an interoperable network that will allow market participants to achieve truly digital value transfer and realize the benefits of tokenization, programmability, and composability.

But, importantly, these connections happen only to the extent the operators of these Daml applications choose to connect to others. And the extent to which these connections happen—and the data seen by each party connecting to an application—is also solely controlled by the application operator. As a result, market participants operating Daml applications as part of the Canton Network will be able to control which parties they transact with—allowing for KYC/AML compliance—and will also be able to control where the data for each transaction resides and who can see that data—mitigating cybersecurity concerns.

With the Canton Network, market participants now have a technological solution that enables truly digital value transfer across traditional asset classes, allowing for data synchronization—eliminating reconciliation—while also providing control over data that no other blockchain network can deliver.

Traditional assets digitally moving across the Canton Network will run on modernized, interoperable technological infrastructure while arguably retaining the same risk profile they have today or even potentially a better risk profile given the faster issuance and settlement times (reductions from days to seconds) enabled by data synchronization.

As a result, regulators should continue to be able to apply existing regulations to the underlying participants, assets, and activities on the Canton Network "based on the principle of same risk, same activity, same regulation."[6]

V. Conclusion: The Canton Network—Technological Innovation to Build a Safer and Sounder Financial System

The Canton Network provides the financial system with the modern technological infrastructure necessary to handle its growing complexity and enable truly digital value transfer across traditional asset classes. At the same time, the Canton Network provides market participants with the control over data necessary to work within existing regulatory frameworks to build a safer and sounder financial system.

[6] Speech by Michael Barr, Making the Financial System Safer and Fairer (September 7, 2022) https://www.federalreserve.gov/newsevents/speech/barr20220907a.htm.