



Amber Baldet
Cofounder & CEO, Clovyr

Committee on Agriculture
United States House of Representatives

July 18, 2018

Cryptocurrencies: Oversight of New Assets in the Digital Age

Chairman Conaway, Ranking Member Peterson, and Members of the Committee, thank you for the opportunity to be here this morning. I'm Amber Baldet, co-founder and CEO of Clovyr, a company building tools that make it easier to build decentralized applications on top of both publicly accessible blockchain networks and access-controlled distributed ledgers.

From 2015 to April of this year, I led the blockchain program for JPMorgan's Corporate & Investment Bank, though I'd like to note that my comments today do not represent my former employer. I also currently sit on the Board of the Zcash Foundation¹, a non-profit organization seeking to advance the state of the art for privacy technology as applied to Internet infrastructure and privacy-preserving cryptocurrencies.

Technical research & development, corporate and financial industry transformation, digital privacy and public cryptocurrency advocacy: these various hats might sound incongruous, but I see them as interconnected pieces of a larger puzzle. The puzzle we are trying to solve is the design for the next-generation fabric of both macro and micro-economies.

Email allows you to send a digital version of a birthday card to a grandchild instantly. Cryptocurrency like Bitcoin gives you the ability to put the digital equivalent of ten dollars inside that card. No need to attach a code for a gift card redeemable at a single retailer or buy a clunky prepaid cash card from a credit card company. Whereas you might attach the same family photo to three different birthday cards, you can't send the same ten dollars more than once. The revolutionary proposition of cryptocurrency - or more broadly, cryptoassets - is the ability to send something you own across the Internet and then irrefutably not have it anymore, without relying on a third party to intermediate or otherwise witness the event.

So far, money seems to be the "killer app" for blockchain. Much as the early Internet's killer app, e-mail, continues to be a cornerstone of how we communicate online, peer to peer payments will likely grow into and persist as a ubiquitous part of our personal and professional daily processes. And even now, it's easy to imagine a world of utility beyond that first use case. The ability to spend, trade, rent, or license unique digital bearer assets could be applicable to many things we own:

¹ <https://z.cash.foundation/>



Decentralized networks, growing together.

mortgages, securities, collectibles, intellectual property rights, unused disk space on your home computer, personal data, etc.

Imagining a mature, interconnected global ecosystem of such markets feels like standing in the 90s, looking at a pre-World Wide Web electronic bulletin board system and trying to imagine Netflix streaming on your phone. The prospect seems so fanciful as to be impossible, but here we are. And yet, my concern is not getting to that end state, it's the choices that we make along the way. As evidenced by the debate around, and impact of, legislation like the DMCA (Digital Millennium Copyright Act), Net Neutrality, FOSTA/SESTA (Fight Online Sex Trafficking Act / Stop Enabling Sex Traffickers Act), or sporadic discussion of state-mandated weak cryptography since the 1990s (e.g. Compliance with Court Orders Act of 2016), the government greatly impacts how we are all able to use Internet and communications utilities which are inexorably woven into the vast majority of Americans' daily lives.

The peer-to-peer protocols which underpin cryptoasset networks are not much different than those that underpin the Internet; they are just rules for how to route bits and bytes. They do not care about the legality or morality of what crosses the wire and can be used in service of business as usual, political action, commission of crimes, facilitating human rights, or sharing funny photos of cats. Everything old is new again, and we are at the precipice of the same concerns for cryptoasset networks as for the Internet – balancing protections of free speech with concerns about undesirable content and activity, fraud and crime prevention, extension of law enforcement capabilities into a new domain, tax enforcement more fluid interstate and global commerce, etc.

The difference, of course, is that we did not previously need to decide if every e-mail message was possibly a security with potential for capital gain and loss, or report the number of emails we sent on our tax returns. The discussion today concerns the financial classification of the assets that cross the wires, which is important, but cannot be completely decoupled from the treatment of the internet any more than litigation about a car crash can be divorced from observations about the condition of the road, timing of traffic lights, speed limit signage, and driver compliance with traffic laws. It is critical that while we spend time sorting the sports cars from the SUVs, we don't lose focus on building solid infrastructure that reaches neighborhoods of all types.

It's not just about our banking sector, not just corporate supply chains, not just consumer payment rails, but how all these things might be connected both here and abroad to reduce friction and open new possibilities for economic growth. It is recognition that we are building next-generation systemically important infrastructure for the American economy. It's also about learning how to balance the enormous potential value of this technology with the need for consumer protections and national security, and how to achieve this while respecting human and Constitutionally-protected rights.

There are many stakeholders in this emerging universe who sometimes have fundamentally divergent philosophies. Yet, they are in near unanimous agreement that when it comes to cryptographically unique digital bearer assets, the genie is out of the bottle. As science fiction author William Gibson said, "The future is already here, it's just not very evenly distributed." While



Decentralized networks, growing together.

we struggle to overlay existing regulatory frameworks onto new technology that is useful precisely for its fluidity - sometimes it may act like a medium of exchange, sometimes a store of value, a commodity, a security, etc. - while we wrestle with that flexibility, other areas of the world are embracing the ambiguity and learning by doing.

In Afghanistan, for example, Code to Inspire² helps train young women for technical careers and pays them in Bitcoin, which they can use in local shops as well as global marketplaces. In a place where women's banking and even physical agency is limited, financial autonomy and digital inclusion is a powerful force for equality and Democracy.

Another example is that in some African countries and places with less legacy financial infrastructure, companies are using cryptoassets to enable farmers to properly track and register their commodities³, enhance supply chain transparency and increase their bargaining power in downstream commodities market pricing. Not only can end consumers "tip their farmer" in support of fair and sustainable working conditions, but every other factory or wholesale retailer along the way can make more informed decisions about the provenance of inputs to their products.

The sticking point in such registries might be the perfection of these cryptoassets, in that while we can represent a real-world good on a blockchain, processing of claims in the case of a default requires enforcement practices external to the network. Relatedly, while tokenized physical assets have been proposed as a response to government corruption (for example, forced re-allocation of land rights during a change in leadership), credible threat or use of physical violence still holds more sway over allocation of resources than any ledger ever will. Ironically, then, these sorts of token registries might work best in places that want to leapfrog a generation of banking technology, but already have well-functioning rule of law.

In the United States, early adopters are excited to connect their cryptocurrency wallets to both new and traditional e-commerce experiences. For example, payments startup Square⁴, whose strategy is already based on disrupting traditional payments processors, has added the ability buy, sell, and transfer Bitcoin into its mobile app, dependent on users having already moved US Dollars into the app via a transfer from a connected bank account. While only a small percentage of Square's Cash app user base has used the feature, over 7 million people have downloaded the app⁵. It's integrations like this, which spread awareness to consumers who didn't go out looking for a cryptocurrency experience, but now have access via workflows of equivalent simplicity to what they expect from other products, that stand to drive rapid adoption among everyday users rather than just investors.

² <http://codetoinspire.org/>

³ <https://www.forbes.com/sites/dantedisparte/2018/01/28/one-thing-is-clear-from-davos-blockchain-is-out-of-beta/#5ba1a829d4fe>

⁴ <https://squareup.com/help/us/en/article/6307-getting-started-with-bitcoin-in-cash-app>

⁵ <https://www.recode.net/2018/2/27/17059182/square-cash-app-monthly-active-users-customers-seven-million-december-venmo>



Decentralized networks, growing together.

There are also several more experimental projects that are interesting, for example: using economic incentives to battle fake news, cryptocurrency micropayments as an alternative business model to data-hungry online advertising, and fluid marketplaces for unused disk space on home computers as a disruptive force to centralized cloud storage. These projects, all launched as initial coin offerings (ICOs) either on a new single-purpose blockchain network or as a token on top of an existing network like Ethereum, are often compared to the internet startup boom of the 90s. Because these are “blockchain native” assets rather than tokenized representations of real-world assets, it may be possible to more closely approximate today’s dispute resolution frameworks entirely as programmatic rules within “smart contracts,” but only if explicitly coded to do so, and only assuming there are no bugs in the code which cause unintended and possibly irreversible outcomes.

The ability to “code oneself out of business” is a novel property of decentralized blockchains, but most experiments today invoke a variety of human-controlled workflow checkpoints or escape hatches to allow intervention if necessary. Along with understanding who controls access to the network and who can modify the rules of the system, identifying these escape hatches and who controls them might be helpful in sorting tokens into various asset classes once a sensible taxonomy has been established.

Of the myriad applications currently under development, it’s hard to tell what’s going to take off and what will be most transformative. Nonetheless, the sheer number of people globally working on these projects⁶ make it likely that it’s only a matter of time until they are no longer considered experimental. The question is how long it will take for distributed ledgers of various incarnations to be considered a legal system of record in enough places that interacting with them is the norm rather than a novelty. Clarity around legal and regulatory treatment in various jurisdictions is, perhaps, the most important factor in the speed of that evolution.

As a counterpoint, and to temper what might sound like unbridled enthusiasm, blockchain is not the answer to every problem. For example, I recommend caution with exploration of blockchain based e-voting. Ensuring one-person-one-vote while keeping ballot selections private, is an incredibly complex computer science and human coordination problem we’re not ready to tackle yet. It is one thing to experiment with making decisions about a blockchain network’s governance processes using the network itself, it is quite another to talk about electronic voting processes for something like U.S. elections, where even traditional electronic voting machines are continually demonstrated to be vulnerable to being hacked.⁷

But when it comes to more promising near-term use cases, the oft-referenced regulatory position of Do No Harm⁸ is a helpful signal but is perhaps not strong enough. Recently, new entrants Coinbase

⁶ <https://www.computerworld.com/article/3235972/it-careers/blockchain-moves-into-top-spot-for-hottest-job-skills.html>

⁷ <https://www.newscientist.com/article/2142428-hacking-a-us-electronic-voting-booth-takes-less-than-90-minutes/>

⁸ <https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo37>



Decentralized networks, growing together.

and Gemini launched cryptocurrency custody solutions^{9,10} for retail and institutional investors, and this week Coinbase made further strides in SEC approval to list on its exchange tokens which are considered securities¹¹. As more traditional assets become tokenized, they may be able to challenge incumbents not because the incumbents are too outdated to understand the technology or unable to develop new products and services quickly enough, but because they are held back from competing due to regulatory uncertainty.

Similarly, as the Federal Reserve and commercial banks take a wait-and-see approach to exploring tokenized representations of the U.S. Dollar, we risk missing the larger picture of what a next-generation Internet of Value means for geopolitics and the future of nation-state economic competition and power projection. It's no surprise that some of the central banks most aggressively investigating cryptocurrency as an alternative or enhancement to their existing currencies are in Venezuela¹², Russia¹³, and China¹⁴. As we begin to explore domestic strategy in this area, it will be important to clarify how existing FinCEN, OFAC, and other relevant rules can be applied, modified, or interpreted to not stifle innovation.

Interestingly, the anonymous, censorship resistant features of open blockchain currencies may turn out to be a helpful reference when creating a digital U.S. Dollar equivalent that is as well regarded around the world as the physical dollar is today. There is no technical reason we cannot have both centralized (FedCoin-like) and decentralized (Bitcoin-like) digital assets in circulation, to provide consumer choice and allow risk diversification. Going forward, I encourage more discussion of strongly encrypted, privacy-preserving digital currencies coupled with opt-in selective disclosure¹⁵, as opposed to options like mandatory cryptographic backdoors or "golden keys," which make our systems attractive targets for nation-state sponsored cyberattacks and hackers¹⁶.

In conclusion, even – and hopefully if – this Committee's guidance is simply a strong commitment to non-interventionism, safe harbors for innovators, and work toward resolution of the patchwork fabric of state laws, the time it takes to come to such a commitment may have the unfortunate effect of eroding America's early mover advantage in technical innovation and entrepreneurship. We take for granted that much of the Internet as we know it was developed here at home, and the immense benefits accrued to us because of it. I appreciate your ongoing work to come to consensus on a way to repeat the successes of the early Internet era while learning from the things we can do better this time around. Thank you for your time.

⁹ <https://custody.coinbase.com/>

¹⁰ <https://gemini.com/custody-services/>

¹¹ <https://www.coindesk.com/coinbase-claims-it-now-has-regulatory-approval-to-list-security-tokens/>

¹² <https://www.theverge.com/2018/3/21/17146764/venezuela-petro-cryptocurrency-russia>

¹³ <https://www.nytimes.com/2018/04/29/technology/blockchain-iso-russian-spies.html>

¹⁴ <https://www.coindesk.com/state-digital-currency-still-on-agenda-says-china-blockchain-research-lead/>

¹⁵ <https://blog.z.cash/viewing-keys-selective-disclosure/>

¹⁶ <https://www.nytimes.com/roomfordebate/2016/02/23/has-encryption-gone-too-far/a-key-for-encryption-even-for-good-reasons-weakens-security>