

**Testimony of John Collins before the
Maryland Financial Consumer Protection Commission
Tuesday, June 5, 2018**

Thank you Chairman Gensler for inviting me today and thank you to the members of the Maryland Financial Consumer Protection Commission for the opportunity to be here and for your commitment to protecting Maryland consumers and interest in exploring emerging financial technologies.

My name is John Collins. I am an Affiliate with the Berkman Klein Center for Internet and Society at Harvard University, where I focus on emerging public policy issues surrounding the increased digitization of finance. Specifically, I concentrate on issues surrounding cryptocurrencies, open blockchain networks and distributed ledger technologies. I'm former Head of Policy for Coinbase, the world's leading digital currency platform, where I led strategy and external engagement on a variety of policy, legal, and compliance issues. Prior to my time at Coinbase I served as Senior Advisor to the U.S. Senate Homeland Security Committee Chair, Senator Tom Carper, and led Congress' first oversight work into digital currencies and blockchain technologies in 2013. I'm also the founder of the First State Fintech Lab, a nonprofit organization focused on strengthening Delaware's position in the financial technology sector via innovative public private partnerships, novel educational opportunities and curricula, and fostering greater diversity in the financial technology industry.

Today, I hope to broadly discuss the landscape of digital finance, or "fintech" as it is often referred, explore cryptocurrencies and blockchain technologies' roles and activities within that landscape, and, finally, speak to what governments are doing to both foster innovation and protect consumers.

Financial Technology

It's important to recognize that the issues being faced by policymakers today are not new.

In 1995, the Financial Services Committee of the U.S. House of Representatives held a hearing held titled "The Future of Money". The Chair of this hearing, former Congressman Mike Castle, who is actually from my home state of Delaware, said the following:

"The future of money contains the potential both for great commercial promise and for enormous risk of undermining the system of exchange and the administration of justice. This is true whether the media of exchange enter electronic commerce using computers linked into networks or via computer chips embedded in cards or other devices."

That hearing was held twenty-two years ago, but we see and hear those same words today. In 1995, they were discussing the very first iterations of electronic payment cards. Today, we talk about digital currencies, blockchain, or artificial intelligence, or machine learning.

These all make up the larger universe of financial technologies - or “fintech” as it is often referred. The definition of “fintech” will differ from person to person but very simply it is financial services delivered via technological channels, whether that be an ATM, a laptop, or a smartphone.

In 1995, one could barely imagine the overwhelming role that the internet would play in our lives today, especially as it relates to financial services. And technology is continuing to reshape how financial products and services are being developed and delivered to consumers. Automation through algorithms and machine learning or artificial intelligence are fundamentally changing our relationship to finance and how we as a society govern and manage financial systems. It’s even changing how citizens themselves interact with those products. This technological shift presents enormous commercial promise but also new challenges - and opportunities - for policymakers the world over.

Enabled by the internet and empowered by mobile computing, technology platforms and protocols are rewiring traditional financial relationships on a global scale. And these technologies and relationships have the potential to dramatically improve customer lives and drive economic growth.

Mark Carney, Governor of the Bank of England, puts it succinctly:

“The biggest prize arises from FinTech’s potential to combine seamless, real-time payments, distributed commerce, more sophisticated client targeting and more accurate credit scoring.”¹

Fintech solutions are providing greater access to capital for consumers, lower transaction costs, and greater entrepreneurship among all sectors of the economy. And, like the internet itself, financial technology and internet banking are creating entirely new products and behaviors that we weren’t even able to imagine before.

According to a major study by the consulting group Price Waterhouse Cooper, legacy financial institutions who invest in financial technology products and services can expect to gain an annual Return on Investment of 20%.² These gains come not only from more efficient processes but also from partnering with entrepreneurs and embracing new ways of thinking to create novel products for consumers.

¹ Mark Carney, “The Promise of FinTech – Something New Under the Sun?,” 2018, <https://www.bis.org/review/r170126b.pdf>

² Price Waterhouse Cooper, “Global Fintech Report 2017,” 2017, <https://www.pwc.com/jg/en/publications/pwc-global-fintech-report-17.3.17-final.pdf>

There are five major factors that are driving the popularity and adoption of these technologies, as identified in a white paper published by the Electronic Transaction Association³, a major U.S. based trade association representing a number of large and small financial technology companies:

- The first is Access. These new technologies are allowing consumers to access funds and financial services wherever and whenever they're needed. This, of course, has been made much easier by the advent of mobile computing.
- The second is Affordability. Fintech products help customers better select from various affordable products and services. Technology is increasing competition and driving down the cost of goods and services, which makes products more affordable, and thus accessible to more consumers.
- The third is Convenience. Fintech products are providing consumers with multiple payment options that save time and money.
- The fourth is Security. These products are helping protect consumer funds from physical and electronic fraud or theft.
- And the fifth is Control and Financial Management. These products are helping consumers gain better control over their finances through financial literacy and various other financial management tools.

These are just some of the reasons we're seeing the prevalence and adoption of these products grow. In turn, we're also seeing tangible results for the commercial marketplace and for overall economic growth.

A good example of this is online lending platforms, which represents one of the most mature and popular segments within the financial technology sector. A comprehensive analysis of small business loans from Paypal Working Capital and Kiva, an online marketplace lender, found two key results that are important for local and national economies⁴:

- 1) First, online loan products have potentially significant economic benefits. Based on increased sales of businesses that received Paypal Working Capital loans, it is estimated that these programs have the potential to boost economic activity in the U.S. by about \$698 billion, or about 3.98 percent of the country's 2015 GDP.

³ Electronic Transactions Association, "How Fintech is Addressing the Financial Needs of the Underserved," July 2016, <http://www.electran.org/wp-content/uploads/2016-ETA-WP-How-Fintech-is-Addressing-the-Needs-of-the-Underserved.pdf>

⁴ Usman Ahmed et al., "Filling the Gap How Technology Enables Access to Finance for Small- and Medium-Sized Enterprises," 2016, https://publicpolicy.paypal-corp.com/sites/default/files/policy/PayPal-Policy-Paper_Access-to-Finance_0.pdf

- 2) Second, young and minority-owned businesses with low and moderate income are benefiting particularly from these products. In fact, nearly 35 percent of Paypal's working capital loans went to low and moderate-income businesses during the time period observed. That's compared with 21 percent of retail bank loans. And 61 percent of Paypal working capital loans go to entrepreneurs and young firms that have been in business for less than five years. And more than half (53 percent) of Kiva's loans go to women-owned businesses and 63 percent to minority-owned businesses; this compares to 36 percent and 14.6 percent, respectively, of traditional retail bank loans.

The reasons for these results are varied but two stand-out:

- 1) First, in the wake of the 2008 financial crisis, financing for small business was particularly hit hard. In 2014, small business lending by the ten largest U.S. banks was down 38 percent from its peak in 2006 and retail branches were shuttered by the thousands across the country.
- 2) Second, providing financing to small businesses - in particular, very small ones - is viewed as too high risk and too expensive. And the businesses themselves often don't apply because the costs on their side are too high or they fear rejection.

Financial technology, leveraging the global communications network that is the Internet, combined with advanced analytics, are being used to break down some of these barriers to access. Indeed, as the study points out, the need for small working-capital loans, which a traditional retail bank often considers too risky or low profit, can be filled by an online lender that can leverage that technology and scale to overcome these difficulties.

This is financing and business growth that would simply not be happening without these new products and services. Further, they are reaching markets and individuals that otherwise been traditionally underserved by the financial system, promoting greater opportunity and access across race, gender, and socio-economic class.

Blockchain technologies

The Commission has been tasked with studying cryptocurrencies, initial coin offerings, cryptocurrency exchanges, and other blockchain technologies. So, the question is how do these technologies fit within the larger universe of financial technology or fintech offerings.

The term 'blockchain' has become nearly ubiquitous in daily life. There is not an industry conference where the term is not the basis of keynotes and panel sessions. This enthusiasm has resulted in an explosion of curiosity, exploration, investment and development in industries ranging from diamond mining to real estate.

It's clear that blockchain technology has potential in at least two major areas relative to financial services. Richard Gendal Brown, Chief Technology Officer at R3, a well-known enterprise blockchain software company, wrote:

"...the blockchain revolution is so fascinating because it could actually be TWO completely different revolutions... both profound in their implications:

- Censorship-resistant digital cash providing a new platform for open, permissionless innovation driven from the margins
- And industry-level systems of record driving efficiencies for incumbents."⁵

The latter "revolution" is the one often discussed by enterprises such as banks, major retailers, and other institutions. In simple terms, these "industry level systems of record" are often times closed-loop blockchains - or blockchain-"like" software implementations - where the participants are known, validated, and given permission to participate. The terms "permissioned ledger" or "distributed ledger technology" (DLT) are often used, interchangeably, to describe such implementations. This software is most akin to a corporate intranet versus the wider, public internet, which is more comparable to open blockchain networks such as bitcoin.

When approaching blockchain or blockchain-like technologies, one should recognize that the elements of this technology which make it so interesting and useful are also what make it so confusing. Namely, in most cases, they represent entirely new open networks or systems architecture upon which individuals and organizations are creating, testing, and building solutions - and everyone is doing it for the first time. Some of these solutions have failed, are failing, or will fail. Some of these solutions will be massively successful. And others will pivot and change based on business and organizational needs, and needs of the users who are consuming the products being constructed.

Institutions around the globe continue to test blockchain technology implementations in a variety of ways to drive operating efficiencies. It remains unclear where the "killer app" may lie, but it likely won't result in a tangible difference for the end consumer, outside of potentially quicker or cheaper results. In truth, in the United States, much of these new processes can likely be covered under existing laws. These innovative institutions should be supported and if laws, regulations, or rules are found to be inhibiting potential efficiency-driving innovation, policymakers should work with industry to deal with those concerns, while maintaining important consumer and financial systems protections.

Again, it's important to remember that technology's iterative nature results in products, experiences, and markets that are often difficult to forecast. The Apple app store would not have been possible without the Iphone. And Snapchat - a company now worth \$25 billion wouldn't be possible without either.

⁵ Richard Gendal Brown, "Bitcoin and Blockchain: Two Revolutions for the Price of One," July 23, 2015, <https://gendal.me/2015/07/23/bitcoin-and-blockchain-two-revolutions-for-the-price-of-one/>

Cryptocurrencies

Gendal Brown describes the first blockchain revolution use case as “censorship-resistant digital cash”. This is a good description of one of cryptocurrencies’ primary use cases. The best known example of a cryptocurrency is Bitcoin. Bitcoin is an open blockchain network and the first real and well-known application of blockchain software. It was released in 2008 as an open-source project by an unknown developer or group of developers. The title of the whitepaper accompanying the release was: “Bitcoin: A Peer-to-Peer Electronic Cash System.”⁶

While the first cryptocurrency, Bitcoin certainly wasn’t the last. While the total number of cryptocurrencies is difficult to validate, as of early June 2018, there were over 1600 cryptocurrencies listed on CoinMarketCap.com, a well-recognized industry reference site.⁷ The total market capitalization of these cryptocurrencies hovers around \$350 billion.

Fundamentally, cryptocurrencies, enabled by blockchain, represent a shift from an internet of data or information to an internet of ownership. Before blockchain technology, one could not truly transfer ownership via the internet. Files and information could be shared but not actually transferred, meaning one user give another user some digital element and no longer possesses it. This enables a number of potential applications but digital cash would be the most developed and popular to date.

Open networks - networks that allow for participation and collaboration by anyone with an internet connection - tend to be unpredictable. That said, as evidenced by the number of cryptocurrencies, the market prices of these cryptocurrencies, and of private and public investment in cryptocurrency related ventures, it is dramatically clear that there is significant interest in these technologies on the part of the public.

The question you may have is: Why? Who is buying and using cryptocurrencies?

There’s little in the way of actual publicly available data but from my own experience and observations there is some commonality among groups of users. This is certainly not a comprehensive list, but it aims to give a sense of the types of individuals who are involved in this new and unique industry:

- **“Early adopters” or “true believers”**: These are individuals who, either because of technical or political interest, buy, use, or build cryptocurrencies. These individuals tend to have more libertarian political leanings and are drawn to the ability to serve as their “own bank” and to hold a self-sovereign, deflationary asset and to experiment with new and innovative technologies.
- **Hobbyists**: These are individuals who are curious about cryptocurrencies and buy them to experiment and participate in a new technology at a very basic level and with not a great deal of investment.

⁶ Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008, <https://bitcoin.org/bitcoin.pdf>

⁷ Coin Market Cap, 2018, <https://coinmarketcap.com/>

- **Speculators:** These are individuals who buy cryptocurrencies as an investment and hold them over time hoping for their value in dollars to rise.
- **Traders:** These are individuals who spend a great deal of time buying and selling cryptocurrencies across markets in order to (hopefully) realize financial profits in dollars.
- **Illicit actors:** As with any new tool or technology, there are individuals who will utilize it for ill. These individuals acquire and use cryptocurrencies as a means to purchase illegal goods on “darknet markets”, exploit ransomware to acquire cryptocurrencies, or use the technology for other nefarious purposes.

It’s worth noting that we have seen a shift in the predominant use case for cryptocurrency over the course of the past several years. While early businesses and users were focused on bitcoin’s potential to serve as a global, decentralized payment rail to provide transactions cheaper and faster than wire transfers, credit cards, and other means of payment, the “currency” element of cryptocurrency has diminished. The most popular use case today is as a digital asset or commodity, thus the success and focus on investment and exchange platforms.

From a consumer perspective, users need to understand that this is a nascent technology and the value of cryptocurrencies is extremely volatile. Many states require strict disclosures to the consumer, warning them of the financial risks inherent in putting money into digital assets, as with any investment. Further, some states require strict cybersecurity and other standards for companies who hold cryptocurrencies on behalf of consumers.

Ransomware is a growing concern for both public and private organizations, as well as individuals. Most often, ransomware software is placed within a computer or computer network via an outside malicious actor or hacker. The software locks up the system, disallowing users across accessing it, until a ransom is paid to the attacker. Cryptocurrencies are the preferred method of payment in such attacks and we’ve seen a rise in such attacks, commensurate with the rise in the price of cryptocurrencies.

It is important to remember that ransomware predates bitcoin and cryptocurrencies. Further, ransomware is more a problem of network cybersecurity and hygiene than it is a problem of cryptocurrencies. Even so, some cryptocurrency companies work hand-in-hand with law enforcement and affected organizations to remediate and prevent such attacks. Continued investment and education, as well as improved cybersecurity standards and diligence will be required to combat this problem.

Cryptocurrency exchanges

Cryptocurrency exchanges serve as the on-ramps between the digital and “real” worlds. They are online platforms that take fiat money (dollars, euros, etc.) and exchange it for cryptocurrencies. In some cases these exchange platforms function as brokerages, whereby the company buys and sells cryptocurrencies via their own stock and charge a fee. In other cases they function as pure spot exchanges, matching buyers and sellers via a centralized order book and charge a fee for the service.

Since the Financial Crimes Enforcement Network's (FinCEN) landmark guidance in 2013⁸, cryptocurrency exchange platforms have been required to register as a Money Service Business (MSB) with the Department of Treasury and comply with the requirements of the Bank Secrecy Act. Further, these platforms must be granted money transmitter licenses in the states in which they wish to operate. The FinCEN guidance has proved effective, provided regulatory clarity for companies and served as the basis for similar rules adopted by other nations across the world.

Most states have interpreted current money transmission statutes to apply to cryptocurrency businesses without modification. In one notable exception, New York State developed a license specific to digital currency businesses, the "BitLicense".⁹

Over the course of the past few years, however, the limitations of state-based licensing regimes for these companies have revealed themselves.

First, having to acquire and maintain an individual license in each state is expensive and time consuming. This is a problem not just for cryptocurrency companies but for all financial technology companies who are deemed to be MSBs. The result is a regulatory moat by which only incumbents and well-funded startups can operate nationwide. Compare that with the European Union (EU) where an "E-Money License" allows for passporting across countries in the EU.

The result is a less competitive business environment in the United States, driving companies and consumers outside the country to foreign-based platforms. In some cases, these platforms do not afford the same security and protections as American based businesses. This has the potential to put consumers at great risk.

Second, as the predominant use case for cryptocurrencies has shifted from payments to use as a digital asset or commodity, the most popular and successful businesses have become cryptocurrency exchanges. It is unclear whether or not state money transmission statutes are adequate to regulate these exchanges to prevent market manipulation and other concerns. This issue was raised by Chairman of the Securities and Exchange Commission (SEC), Jay Clayton, at a recent U.S. Senate Banking Committee hearing.¹⁰ The SEC and the Commodities and Futures and Trading Commission (CFTC) continue to discuss how best to regulate cryptocurrency markets, but it's clear that the states have a significant role to play as the primary regulator of these markets.

⁸ FinCen, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013, <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>

⁹ New York Department of Financial Services, BitLicense, June 24, 2015, https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

¹⁰ Jay Clayton, Chair of the SEC, Testimony before the U.S. Senate Banking Committee, February 6, 2018, <https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission>

Responding to the concerns above, the Conference of State Bank Supervisors (CSBS) began their “Vision 2020” initiative to modernize and simplify state supervisory practices for all fintech companies, with the input of industry.¹¹ This is important work that all parties should continue to support and strengthen.

To be clear, there is significant need to ensure the safety and soundness of cryptocurrency platforms that hold digital assets on behalf of their customers. Around the world we have seen the result of unregulated or poorly regulated exchanges who are hacked or otherwise fail, resulting in the loss of their customer funds. The question is how to provide this necessary oversight and who is best suited to ensure the security and safety of these customers and keep compliant and safe platforms here in the United States.

Initial Coin Offerings

Initial Coin Offerings (ICOs) represent a new method of crowdfunding using the sale of digital tokens or coins. To date these ICOs have raised nearly \$10 billion in 2018 alone.¹² ICOs tend to not be native cryptocurrencies operating on their own blockchain network. Instead, the overwhelming majority of tokens are built using smart contracts on the Ethereum network, an open blockchain similar to bitcoin.¹³

ICOs represent a novel method to crowdfund for particular products, initiatives, or companies. That said, it has also become an attractive place for scam artists and outright criminals.

A recent study by the Wall Street Journal examined 1,450 ICOs and found that 271 were purportedly found to be exhibiting “red flags” including “plagiarized investor documents, promises of guaranteed returns and missing or fake executive teams.”¹⁴

The SEC continues to grapple with how to best to address the ICO boom. It is clear that many ICOs are likely to be interpreted as securities and thus subject to the relevant securities laws. In some cases the SEC has already taken action against specific individuals and organizations who have committed fraud or other crimes. State securities administrators and Attorneys General have taken similar actions and have issued a number of consumer warnings.

It is in the best interest of both government and industry to work together and come to agreement on common definitions and treatment of ICOs. Further, it is incumbent on industry to do what it can to regulate itself and develop a base-level code of conduct for such activities. There are numerous such initiatives under way and they should continue, or else risk further consumer harm or regulators’ over correction.

¹¹ CSBS, Vision 2020, <https://www.csbs.org/vision2020>

¹² CoinSchedule, “Cryptocurrency ICO Stats,” <https://www.coinschedule.com/stats.html>

¹³ Consensus, “The State of the Ethereum Network,” June 1, 2018, <https://media.consensus.net/the-state-of-the-ethereum-network-949332cb6895>

¹⁴ Shane Shifflett and Coulter Jones, *Wall Street Journal*, “Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud,” May 17, 2018, <https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115>

Government's' role in financial innovation

Hong Kong, Singapore, the United States, the United Kingdom, Australia, and some individual U.S. states, are establishing centralized offices of innovation, regulatory sandboxes, and private-public partnerships to build out their respective financial technology sectors.

The United Kingdom, which has been a leader in this space, is currently working with 18 FinTech firms whom they are hosting in a regulatory sandbox. This allows these firms to test products in collaborative fashion with regulators at the table. This gives them space, comfort, and advice to build products that are new, valuable, and safe for consumers, without worrying about adverse regulatory action. It's an attempt to meld the "move fast, and break things" mentality of Silicon Valley with the more conservative nature of financial regulators. Given their success, the UK recently announced the creation of a "Global Regulatory Sandbox" to formalize partnerships with other jurisdictions.¹⁵

In the U.S., a national sandbox is difficult to implement given our fragmented financial regulatory structure. That said, the Director of the Consumer Financial Protection Bureau (CFPB), Mick Mulvaney, recently announced they were exploring establishing a U.S. based regulatory sandbox on consultation with the CFTC and some states.¹⁶ Arizona recently passed legislation to establish a regulatory sandbox and other states are expected to follow suit.¹⁷ Blockchain technology and related cryptocurrency products are prime candidates for a regulatory sandbox program that structures experiments to be "small enough to fail".

While the structure of fintech innovation initiatives vary from jurisdiction to jurisdiction, there are some common themes:

- First, governments are choosing to accept the opportunities before them and embrace innovation.
- Second, they are forming collaborative relationships with legacy institutions and FinTechs, in some cases driving those relationships.
- Third, they're enabling testing of new products and services through things like sandboxes.
- Fourth, they're breaking down barriers between regulators and businesses through improved communication of expectations, decisions, and making resources more readily available to firms.
- And fifth, they're moving to simplify regulatory processes for firms that, to date, have been onerous and opaque, especially for very small startups.

¹⁵ United Kingdom Financial Conduct Authority, "Global Sandbox," February 14, 2018, <https://www.fca.org.uk/firms/regulatory-sandbox/global-sandbox>

¹⁶ Neil Haggerty, American Banker, "CFPB looking to hop on fintech sandbox bandwagon," May 29, 2018, <https://www.americanbanker.com/news/cfpb-looking-to-hop-on-fintech-sandbox-bandwagon-mick-mulvaney>

¹⁷State of Arizona, "Arizona Becomes First State in U.S. to Offer Fintech Regulatory Sandbox," <https://www.azag.gov/press-release/arizona-becomes-first-state-us-offer-fintech-regulatory-sandbox>

In closing, the problems and concerns raised by cryptocurrency and blockchain technologies are not new. They are simply exhibiting themselves via new means. Companies have a responsibility to protect and be honest with their customers. Governments have a responsibility to protect their citizens and the overarching financial system upon which we all rely.

Regulators and policymakers should recognize that the purpose of regulations, laws, and other guidance is to achieve certain policy outcomes. In some cases it's to prevent money laundering, or terrorist financing, in other cases it is to protect consumers from scams. In all cases, these desired outcomes have developed over time, from a variety of well-researched inputs in the policymaking process. Regulators should recognize the letter of the law may not fit the behavior of recent technological developments. In these cases they should be flexible and work towards what the law or policy is intended to accomplish rather than remain intransigent to outdated modalities. Not only will this nurture innovation, it will provide consumers access to potentially valuable new products, and allow regulators to better accomplish their mandates.

The internet as a living, breathing, ever changing communications network has changed society by making it ever more connected. As we view its potential to change financial services, there is little doubt it will have the same effect: it will drive collaboration and efficiency, while driving down costs and serving more people in more places . It will strengthen markets and products, bringing them to people who didn't have access to them before and desperately need and want them. And again that's just what we know today. Who knows where we will be in another twenty-two years.

Thank you for your time today and I look forward to answering any questions you may have.