

United States House of Representatives
Committee on Financial Services
The Task Force on Financial Technology
2129 Rayburn House Office Building
Washington D.C. 20515

April 28, 2022
Written Testimony of
Mishi Choudhary

Chairman Stephen Lynch and Ranking Member Warren Davidson and distinguished Members of the Committee, I am pleased to appear before you today on this hybrid hearing entitled, “What’s in Your Digital Wallet? A Review of Recent Trends to Mobile Banking and Payment”.

My name is Mishi Choudhary and I am the Legal Director of the New York based Software Freedom Law Center that works to protect and advance Free and Open Source Software (FOSS) . Much of the world’s most important and most commercially significant software is distributed under copyright licensing terms that give recipients freedom to copy, modify and redistribute the software (“free and open source software”). One could not send or receive e-mail, surf the World Wide Web, perform a Google search or take advantage of many of the other benefits offered by the Internet without free and open source software. FOSS developers create and advance solutions to complex problems that are decentralized, open and accessible to everyone. Several of the world’s crypto currencies are built on FOSS and principles of this ecosystem. I would like to note that views presented here are my own.

Money and Digital Technology

In a rapidly evolving technological environment, consumers seek payment methods that are convenient, inexpensive, and secure. Our legacy transaction systems have suffered from high fees, limited access and modest innovation that have beset many financial inclusion efforts. Non-traditional players in the market have attempted to address some of these issues through use of mobile devices to improve access to financial products and services. Digital wallets that use mobile device’s wireless capabilities to transmit payment data securely from a mobile device to a point of sale designed to read such data are one such example. Digital wallets may act as either (or both), a storage mechanism for payment details and a storage mechanism for actual funds. In general, they are linked to a bank account, credit, debit or a prepaid card but don’t have to. They can hold money and other wallet users can make payment to a user that can be used without involvement of any bank or financial intermediary. These wallets, including but not limited to Apple Pay, Google pay, CashApp, Venmo, Alipay, and others store funds, make transactions and track payment histories. Some of them also store documents like driver’s licenses, giftcards, membership cards, hotel reservations inter alia. Mobile solutions that do not rely on bank account access including mobile wallets are particularly attractive to those who don’t have access

to a bank account. There are several other peer to peer (P2P) payment services that allow customers to send and receive money electronically between two users that may not fall under the definition of the term wallet. One such popular service is Zelle, operated by Early Warning Services, a company created and owned by seven banks: Bank of America, Capital One, JPMorgan Chase, PNC, Truist, U.S. Bank and Wells Fargo. Some of the features of such apps have also made them a prime target of fraud with little clarity on liability issues, in particular, the application of Regulation E .

Cryptocurrencies are currently stored in hot and cold wallets. Hot wallets come in three forms: Desktop, Mobile and Web and are connected to the Internet, therefore, “hot” in nature. The funds in a hot wallet can be spent at any time, online. Cold storage wallets do not require online servers and can store the assets in the wallets, which are physical devices. Hardware wallets store your cryptographic keys on a piece of hardware that has been specially designed for cryptocurrency transactions. The software program of hardware wallets allows users to keep their assets safe offline and only allows access via private key once the device is connected to the main computer system or device. This adds a security layer reducing the possibility of any cyber-attacks and the absence of a third party ensures that nobody can dictate transactions or access the user’s transaction history.

The transition to digital payments was already underway, but the COVID-19 pandemic accelerated adoption to new levels. Despite an uptake in the adoption of these forms of payments, unlike the Chinese or Indian markets that are mobile first, U.S. market still relies heavily on credit cards. A U.S. customer does not necessarily have the same motivation as their Indian or Chinese counterparts especially as credit cards are backed by various laws like the Fair Credit Billing Act, Electronic Funds Transfer Act (EFTA), Credit Card Accountability, Responsibility and Disclosure (CARD) Act amongst others.

We are seeing rapid development and experimentation in cryptocurrencies and various other digital forms of payments, with and without the need of traditional intermediaries. There are growing pains and volatility in these areas but the lessons they offer can help expand the frontiers of digital payment technologies.

Central Banks around the world are considering issuing digital equivalent forms of their currency to the public known as Central Bank Digital Currency (CBDC). Per the Atlantic Council, 87 countries (representing over 90 percent of global GDP) are exploring a CBDC. 14 countries, including China and South Korea, are now in the pilot stage with their CBDCs and preparing a possible full launch. 9 countries have now fully launched a digital currency. ¹

Challenges

As the popularity of these digital payment systems continues to increase, they are increasingly becoming targets of threat actors. In cases, where customers have been targets of fraud, they have not been afforded protections by underlying banks owing to the ambiguity of regulations.

Privacy and Data collection challenges have plagued such wallets. None of the existing offerings can replicate the privacy-respecting features of physical cash. Venmo, owned by PayPal that entered into a settlement with the Federal Trade Commission in 2018 keeps transaction history public by default.

¹ Central Bank Digital Currency (CBDC) Tracker, <https://www.atlanticcouncil.org/cbdctracker/?params=3f:f:7:f:f&country=&selected=> (last visited April 25, 2022)

These can be made private but contact lists remain visible. This feature was what led to the reporters discovering President Biden's account details on the application.

The Chinese example is a cautionary tale with respect to linking of the social credit system and data collection policies where the lines between the Government and private sector are increasingly blurred.

Most of the current solutions cater to the banked customers and don't address those that primarily work in the informal economy or are paid in cash. Such part of the American population also desires the modern conveniences that technology offers without losing the privacy offered by cash.

Opportunities

As we think about money in the age of the Internet, we must design for a future that is in the public's interest, incorporates privacy by design and facilitates financial inclusion. The super apps that are popular in countries like China are gaining popularity around the world, underscore the fact that concerns about data protection and privacy have not been adequately addressed and the current market options lack privacy-oriented messaging system integrated with payments. We need a currency or electronic token that is equivalent in functionality to cash, offers all of its benefits including anonymity, privacy, autonomy, no transaction fee and addresses all of its flaws. Such a design finds support in history as presented by David Chaum² in the 1990s and the recently introduced The Electronic Currency and Secure Hardware (ECASH) Act by Rep. Stephen F. Lynch (D-MA) that directs Treasury to commence a two-stage pilot program to test a variety of e-cash technologies and determine the optimum alternative for circulating this electronic currency.

The unique element of the ECASH idea is hardware wallets containing the equivalent of coins created by and managed by the United States Treasury which is as close a way of universal access just like the cash. This idea imagines how everybody can have, store and pay with money without the banking system being involved in any way at all. An idea is to have electronic tokens that are equivalent in functionality to cash and no more traceable. The risk of hard money for working class people has always been loss, inconvenience or inflation. Working people, back to the Jacksonian era in the United States have large experience with ways payment systems chosen by employers have hurt them. So they favor hard money, government coin that is deep in the fabric of democratic finance in the United States, as deep as the importance or role of the elite in the banking system. The questions of identity management like KYC is of great interest to everybody except to ordinary people whose preference is for cash. They live in a world in which informal economy is as important as the formal economy. In the 21st century, it should not matter whether what you are waiving at the cash register is a card issued to you by a bank or a credit union or is a hardware object that United States Treasury has certified, is the way that ECASH is carried around. This structure of ECASH does not have the quality of traceability and preserves privacy. The software underlying any of these technologies must be Free and Open Source to enable public review and audit of the source code for potential security issues.

If used correctly with adequate guardrails, digital money presents an opportunity for financial inclusion for those with little access to formal banking systems. Any such efforts must provide consumer protection and data privacy, aspects often found to be woefully lacking in several such offerings around

² David Chaum, *Achieving Electronic Privacy*, August 1992, <https://www.chaum.com/publications/ScientificAmerican-AEP.pdf>

the globe. What we need is to have more multi-disciplinary research in development of technologies that work for those that are most disadvantaged by the current system, those who don't have bank accounts and have to pay high fees to access their cash built with privacy by design.

Thank you for the opportunity to appear before you today, and I look forward to your questions.