Comments to the Office of the Comptroller of the Currency on National Bank and Federal Savings Association Digital Activities

Peter Van Valkenburgh
July 29, 2020

Introduction

Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing digital currency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

Our comment letter will primarily describe various cryptocurrency activities that are within the core or incidental activities that banks should be able to perform (Question Four of the Advanced Notice of Proposed Rulemaking—ANPR)[1]. After these activities are characterized and their benefits to bank customers are described, we will offer suggestions relating to legal standards for electronic operations at National Banks that can clarify the bank-permissibility of these activities (Questions One through Three of the ANPR)[2].

As the OCC has already recognized in the recent Interpretive Letter dated July 22, 2020,[3] cryptocurrency technology is an important innovation in financial technology, and safekeeping of cryptocurrency is and ought to be a core banking activity.[4] We would argue, one step further, that cryptocurrency and public blockchain networks are a fundamental evolution in money for both private currencies (*e.g.* Bitcoin) and potential future public currencies (*e.g.* central bank digital currency). These networks afford the public significant advantages that are not available

[1] Department of the Treasury Office of the Comptroller of the Currency, "National Bank and Federal Savings Association Digital Activities," Advance Notice of Proposed Rulemaking, OCC-2019-0028, RIN 1557-AE74, June 4, 2020, https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-76a.pdf.
[2] *Ibid*.
[3] Jonathan V. Gould, "Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customer," Department of the Treasury Office of the Comptroller of the Currency, Interpretive Letter #1170, July 22, 2020, https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf..
[4] *Ibid*. *See also*: Peter Van Valkenburgh, "Comments to the Office of the Comptroller of the Currency on Exploring Special Purpose National Bank Charters for Fintech Companies," *Coin Center* (Apr. 2017) https://www.coincenter.org/comments-to-the-office-of-the-comptroller-of-the-currency-on-exploring-special-purpose-national-bank-charters-for-fintech-companies/ (explaining how cryptocurrency activities are direct analogs to existing bank-permissible activities).

within legacy digital money systems. Their ledgers are freely auditable to determine total supply and rate of new money creation.[5] Such networks are open to all comers just as physical cash is a transaction tool available to all (and in contrast to commercial bank money that is available only to those able to obtain banking relationships).[6] Transactions on these networks are mathematically verifiable such that each individual can be assured of settlement finality without trusting a third party, and such that machines can be programmed to engage in transactions free from regular human chaperoning.[7]

Contrary to some misguided criticisms, recent improvements to these networks allow them to work at global scale and for tiny transactions that are non-economical for intermediated systems.[8] Contrary to common belief, these networks are not entirely anonymous but can afford law enforcement the tools necessary to forensically track criminals.[9] Contrary to common belief, these networks can also be built to accommodate transactions that protect the privacy of transaction participants while affording granular levels of information sharing with counterparties, regulators, or law enforcement when, and only when, appropriate and lawful.[10]

Open blockchain networks and the cryptocurrencies they make possible are the future of money, and, accordingly, this comment will advocate that banks should be permitted to engage in any and all activities that might be commonly performed to use and maintain these networks.

Six New Activities

As the OCC recently recognized, cryptocurrency safekeeping is within the scope of activities enumerated by the National Bank Act as core banking functions.[11] We applaud that interpretation and advocate that all of the following activities are similarly within core functions or else incidental functions as described in the National Bank Act,[12] and that banks

[5] Andrea O'Sullivan, "What is cryptocurrency good for?" *Coin Center* (Jul. 2018) https://www.coincenter.org/education/blockchain-101/what-is-cryptocurrency-good-for/.
[6] Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.
[7] *Ibid*.
[8] Elizabeth Stark, "Lightning Network," *Coin Center* (Sep. 2016) https://www.coincenter.org/education/key-concepts/lightning-network/.
[9] Jason Weinstein, "How can law enforcement leverage the blockchain in investigations?" *Coin Center* (May2015) https://www.coincenter.org/education/policy-and-regulation/how-can-law-enforcement-leverage-the-blockchain-in-investigations/.
[10] Andrea O'Sullivan, "What are mixers and 'privacy coins?'" *Coin Center* (Jul. 2020) https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/.
[11] Jonathan V. Gould, "Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customer," Department of the Treasury Office of the Comptroller of the Currency, Interpretive Letter #1170, July 22, 2020, https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf.
[12] 12 USC §§ 21-216(d).

should be free to engage in these activities so long as they do them safely and with standards and guidance provided by the OCC:

1. **Safekeeping:** Fiduciary and non-fiduciary cryptocurrency safekeeping,
2. **Multisig safekeeping:** Safekeeping and use of a minority of keys associated with cryptocurrency held in multisig transactions,
3. **Node Operation:** Operation of network nodes that relay cryptocurrency transactions and store and validate copies of public blockchains,
4. **Payment Channel Operation:** Operation of network nodes that form payment channels for second layer scaling networks (*e.g.* the Lightning Network) and the provisioning of these channels with cryptocurrency liquidity,
5. **Privacy Services:** Provision of privacy enhancing services for cryptocurrency transactions such as CoinJoin transactions or zero-knowledge proof generation and validation, and
6. **Self-sovereign Identity Services:** Issuance of identity attestations and acceptance of third-party attestations of customer identity using self-sovereign identity systems powered by open blockchain networks.

Safekeeping

The Interpretive Letter dated July 22, 2020 already covers activities that we describe as safekeeping.[13] In general, banks should be free to offer cryptocurrency safekeeping services in either a non-fiduciary capacity (as with safe deposit box services) or a fiduciary capacity (as a trustee or executor). For clarity it must be stressed that these services do not encompass cryptocurrency lending or the hypothecation of customer cryptocurrency assets as deposits. These should be safekeeping services wherein the bank merely provides the infrastructure by which a customer can secure her own assets (*e.g.* a safe deposit box) or fiduciary services wherein the bank can hold the assets as a trustee, but must always act in the interests of the trust beneficiary and must assert no claim or right to hypothecate or otherwise alienate the funds from the trust or its beneficiaries.[14] In other words, banks engaged in safekeeping must either limit themselves to assisting customers in the physical storage and security of digital keys related to customer cryptocurrency, or else hold cryptocurrency in an omnibus wallet for the benefit of its customers on a 1:1 reserve basis. At this time we do not believe that it would be prudent for banks to engage in cryptocurrency deposit-taking or lending because of the absence of federal deposit insurance for cryptocurrency accounts and the general lack of highly liquid private insurance markets.

Multisig Safekeeping

[13] *Ibid.*
[14] *See e.g.,* New York Department of Financial Services, "Financial Services Superintendent Linda A. Lacewell announces grant of DFS trust charter to enable Fidelity to engage in New York's growing virtual currency marketplace," Press Release (Nov. 2019) https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1911191.

Multisig safekeeping should be understood as a subset of the simple cryptocurrency key storage described above. It is a lower risk activity than typical cryptocurrency custodianship because it involves the safekeeping of a minority number of keys in a multiple signature or "multisig" cryptocurrency transaction.[15] These transactions are sometimes referred to as M-of-N transactions wherein rules encoded in the cryptocurrency blockchain dictate that funds will be imobile unless M-of-N digital signatures accompany the transaction message. A simple example is a 2-of-3 multisig transaction where the customer has control of two keys and the bank has control of a third. Lacking a second key, the bank can never transact with the customer's cryptocurrency (which is why this is a lower risk activity) and serves only as a custodian of a back-up key in the event the customer loses one of her two other keys.

In this example the Bank could also provide a transaction screening service akin to credit and debit card fraud prevention. Imagine, for example, that the customer keeps one of her two keys on her phone and the other locked in a safe at her home. When she makes transactions using her phone the bank is alerted and asked to add a second digital signature to the transactions using its key. The bank can condition its second signature according to fraud prevention rules: *only sign if amount transacted is under $X, only sign if customer's phone can be geolocated to a typical home country or region, only sign if customer has not reported phone to be lost or stolen, etc.*

Many banks have already developed these fraud prevention services in the context of debit and credit cards. The general irreversibility of cryptocurrency transactions means that these services are even more important in this arena than in traditional payments systems. Additionally, the fact that a bank could provide these services while maintaining insufficient keys to transact without customer involvement reduces the risk inherent in the bank being hacked or otherwise losing or compromising its keys: the customer would still be free to transact using her keys alone.

Node Operation

In order to provide the safekeeping functions described above, banks will need to interact with public blockchain networks so that they may make transactions and confirm past transactions related to the cryptocurrencies being secured. Accordingly, banks will need to run the relevant node software for any cryptocurrency they choose to support.[16]

Typically cryptocurrency network nodes perform various functions beyond enabling the user to check and transact with her own specific balances. These include relaying transaction messages from strangers on the peer-to-peer network, declining to relay transaction messages that are invalid according to the rules of the network, as well as relaying and validating new blocks as they are appended to the blockchain. Node operators thus perform a valuable public service: they provide communications throughput for strangers transacting on the network and they act as a first layer of defense against attempts at passing fraudulent transactions (all honest nodes

[15] Ben Davenport, "What is multi-sig, and what can it do?" *Coin Center* (Jan. 2015) https://www.coincenter.org/education/advanced-topics/multi-sig/.
[16] *See e.g.* Bitcoin Core, accessed Jul. 2020, https://bitcoin.org/en/bitcoin-core/.

may refuse to relay a fraudulent transaction such that it never even reaches a miner or block creator who could put that transaction into a block), and nodes also store redundant copies of the blockchain and prevent fraudulent blocks from spreading through the network.

While no bank should be forced to perform all of these activities simply because it chooses to safekeep cryptocurrency, banks should be free to perform these activities to the extent they remain compliant with other laws. For example, banks should not relay transactions to or from cryptocurrency addresses on the US Treasury Department's Office of Foreign Assets Control (OFAC) list of "Specially Designated Nationals and Blocked Persons List" (SDN),[17] and simple filtering rules can be employed to ensure compliance with those laws. However, if a bank is relaying transactions on the peer-to-peer network between non-sanctioned addresses, it should not be obligated to obtain identifying information related to those transactions. The strangers making these transactions are not the Bank's customers any more than persons who visit the website of a bank without intention to open an account are the bank's customers. Just as banks today can already provide communications infrastructure related to remote banking, banks of tomorrow should be free to help provide communications infrastructure related to cryptocurrency networks.

Thanks to the technical nature of cryptocurrency networks, the bank should not be viewed as in any way liable for merely relaying transaction messages later determined to be illicit. The peer-to-peer nature of these networks means that a bank will never be the but-for cause of a transaction being made merely because it was one of several nodes that relayed the transaction message. Several other peers will relay that message as well, and no specific peer is essential to its transmission. Indeed, by relaying transactions, banks could gain enhanced visibility into the flow of funds on these networks, which could be valuable in their own compliance with KYC and AML rules related to their actual customers.

Payment Channel Operation

Payment channels allow several cryptocurrency transactions between parties within a channel to be made without each atomistic transaction being settled to the blockchain.[18] If Alice wishes to pay Bob but thinks she might make several transactions over the next month—perhaps Alice is, in fact, a water meter and Bob is a computer for the water utility provider in the city—then the two parties can enter a payment channel. Alice places an amount in the channel that she deems sufficient for the future payments she might want to make to Bob. This entails creating a multisig transaction with Bob where both signatures are needed to move funds out of the channel. In case Bob disappears, Alice will typically also include "timelock" on the transaction

[17] The full SDN list can be found in several formats on the OFAC website, e.g. US Treasury Department Office of Foreign Assets Control, "Specially Designated Nationals and Blocked Persons List," alphabetical listing (Jul. 2020) https://www.treasury.gov/ofac/downloads/sdnlist.pdf
[18] Chris Smith, "Micropayments," *Coin Center* (Jun. 2015) https://www.coincenter.org/education/key-concepts/micropayments/.

that allows her to reclaim any funds remaining in the channel after some set period of time even if Bob refuses to sign with his signature.[19]

Now, as Alice consumes water she signs several transaction messages (each updated for a larger payment as more water is consumed) and sends them to Bob. Bob holds on to these payment messages but, at any point, could add his signature and claim the amount owed on the blockchain. If Alice disappears, Bob stops the flow of water and adds his signature to the most recent transaction claiming the funds paid thus far on the blockchain. If Bob disappears and the water stops flowing, Alice stops sending signed payment messages, waits until the n-lock expires, and reclaims any funds left in the channel. If neither disappear they continue exchanging payment messages until all of the channel funds have been spent and then settle on the blockchain with the option to add new funds to their shared channel. Thus several thousand transactions can be made with only two transactions actually being sent to the cryptocurrency blockchain itself: the transaction that funded the channel and the transaction that emptied it according to the final respective balances of the participants.

At no point can either participant meaningfully cheat the other participant, so—despite the several transactions being exchanged without settlement to the blockchain—neither party ever suffers substantial counterparty risk.

Payment channels can be made to be bi-directional (Bob effectively cancels a past payment from Alice sending funds backwards) and several payment channels can be knit together in a web (Alice to Bob, Bob to Cynthia, Cynthia to David, etc.) such that (with sufficient participants) almost anyone can pay almost anyone else merely by exchanging these signed payment messages through a network of related parties rather than settling everything immediately to the blockchain. Networks of payment channels can therefore be scaling solutions for public blockchain cryptocurrencies.[20]

The Bitcoin blockchain, for example, is currently rate-limited by design in the software to between seven and twenty-seven transactions per second globally, shared amongst all users, which is a severe limitation.[21] However, if users are employing payment channels, such as Bitcoin's Lightning Network of payment channels, then each of those seven transactions a second could be the initial setup or final settlement of payment channels that enable or will enable thousands of individual transactions.

Metaphorically this is not dissimilar from batch settlement, although, significantly, no person or institution needs to be trusted to do the settlement honestly, because, as in our initial example of Alice and Bob and the water metering, every participant can always resort to

---

[19] "Timelock," *Bitcoin Wiki*, accessed Jul. 2020, https://en.bitcoin.it/wiki/Timelock#:~:text=A%20Timelock%20is%20a%20type,channels%20and%20hashed%20timelock%20contracts.
[20] Elizabeth Stark, "Lightning Network," *Coin Center* (Sep. 2016) https://www.coincenter.org/education/key-concepts/lightning-network/.
[21] Evangelos Georgiadis, "How many transactions per second can bitcoin really handle? Theoretically." *IACR Cryptol*. ePrint Arch. (Apr. 2019): 416, https://eprint.iacr.org/2019/416.pdf.

broadcasting her latest signed transaction messages to the network in the event her counterparties become unresponsive or corrupt.

Banks should be able to open these payment channels with their customers and between other banks. Thus a customer could make thousands of transactions with the bank, other customers of the bank, or other customers of other banks, all while making only two transactions that actually take up valuable and scarce space on the blockchain. The system should be humorously familiar to bankers as it is a mirror image of the correspondent banking network. Similar though they may be, however, cryptocurrency payment channel networks are significantly better technology than traditional correspondent banking networks: intermediary participants can never make transactions without the cryptographic signature of the originator and, therefore, can't arbitrarily redirect or misdirect funds. If intermediary participants become unresponsive, corrupt, or compromised, other parties can simply settle the accounts to the blockchain in their absence, inconvenient and expensive perhaps, but far better than truly lost funds.[22]

Privacy Activities

Banks have important legal and ethical obligations to protect the privacy of their customers.[23] Banks also have legal obligations to surveil the activities of their customers and, under certain circumstances, report details to regulators and law enforcement.[24] These obligations are in tension but they are not irreconcilable. Nothing in this balance should change merely because a bank is transacting with cryptocurrencies. Indeed, because of the need to strike a balance between privacy and surveillance, banks should be free and perhaps even incentivized to use privacy enhancing cryptocurrency technologies.

We use the umbrella phrase "privacy enhancing cryptocurrency technologies" to describe two broad areas of innovation: (1) trustless transaction mixing technologies like CoinJoin for Bitcoin transactions, and (2) privacy enhanced cryptocurrency networks like Zcash and Monero. [25] The specific operation of these technologies is beyond the scope of this comment and we direct the OCC to valuable resources elsewhere.[26]

---

[22] By way of comparison, the legacy SWIFT network that fuels transaction communications among financial institutions has been hacked several times, resulting in losses of millions of dollars in unrecoverable funds. *See*, Michael Corkery, "Once Again, Thieves Enter Swift Financial Network and Steal," *New York Times* (May 2016) https://www.nytimes.com/2016/05/13/business/dealbook/swift-global-bank-network-attack.html.
[23] *See, e.g.,* the Gramm-Leach-Bliley Act, 12 USC § 78, § 377; 15 USC § 80.
[24] *See, e.g.,* the Bank Secrecy Act, 31 USC §§ 5311-5332.
[25] *See generally,* Andrea O'Sullivan, "What are mixers and 'privacy coins?'" *Coin Center* (Jul. 2020) https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/; see also: .
[26] *Id*. *See also:* Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash (for a discussion of the moral and ethical importance of privacy enhanced cryptocurrency technologies) and Peter Van Valkenburg, "Electronic Cash, Decentralized Exchange, and the Constitution," *Coin Center* (May 2019)

Speaking generally, Bitcoin and similar early open blockchain networks have transparent blockchains. Batched payment channel transactions aside (see above), every transaction between users of the cryptocurrency will be described in plain text on the blockchain, and these public details will include the pseudonymous addresses of sender and recipient and the amount sent. If real identities can be associated with addresses as is often the case (*e.g.* when you pay your friend you will learn each other's addresses) then many if not all of the transactions of a cryptocurrency user can be tracked by third-parties.

This state of affairs is very poor for financial privacy, especially when address clustering and other big-data tools are leveraged to systematically unmask all addresses and transaction details for the viewing pleasure of paying customers of blockchain analysis firms.[27] To address this problem, technologists have focused on the two separate lines of innovation mentioned above: (1) trustless transaction mixing technologies like CoinJoin for Bitcoin transactions, and (2) privacy enhanced cryptocurrency networks like Zcash and Monero.

Mixing technologies allow several users to sign a single transaction together that obfuscates the details of any particular transaction within the mix. Importantly, like the payment channel technologies described above, no participant needs to be trusted in order to perform the mix; either everyone signs the transaction honestly and it is carried out, or else everyone gets their money back.

Privacy enhanced cryptocurrencies either have these mixing transactions enabled by default for all users (*e.g.* Monero with RingCT transactions as the default form) or use novel cryptography to build verifiable mathematical proofs of transaction validity that assure participants that they have received bona fide funds but do not allow third parties to glean any additional information about the transaction beyond that mathematical proof written to the blockchain (*e.g.* Zcash).[28]

While the naive initial reaction of financial professionals may be alarm at these new privacy enhancing tools, and an assumption that they are incompatible with the operations of banks and other regulated institutions, in fact the opposite is true. Banks have specific duties with regard to anti-money laundering, and those compliance obligations can be met while utilizing privacy enhancing cryptocurrency technologies to protect the privacy of bank customers. Indeed, employing privacy-enhancing technologies may be the optimal way to fulfill their obligations to both their customers and public authorities. This is because, if a bank chooses to assist a customer in making cryptocurrency transactions and does so without utilizing widely available privacy-enhancing technologies, then the bank will be revealing potentially sensitive information about their customer's financial transactions to the public at large.

---

https://www.coincenter.org/app/uploads/2020/05/e-cash-dex-constitution.pdf (for a discussion of the constitutional implications—First and Fourth Amendments—of regulating these tools).

[27] *See, e.g.* Chainalysis and Elliptic

[28] Zooko Wilcox and Peter Van Valkenburgh, "Zcash," *Coin Center* (Dec. 2016) https://www.coincenter.org/education/key-concepts/zcash/.

This is, of course, a large subject and we will not go into a detailed analysis of the Bank Secrecy Act, associated laws, and cryptocurrency technology at this juncture. The general principle is, however, as follows: Banks are obligated to know their customers and take reasonable "risk-calibrated" steps to prevent money laundering. Banks already meet these obligations adequately even though they deal frequently in fully anonymous bearer assets (*e.g.* cash). Even if any of the aforementioned privacy technologies were as anonymous as cash (and they are not owing to certain inevitable limitations in digital technologies), Banks should still be able to interact with these technologies while taking all of the same precautions they would take with respect to customers transacting with cash. Banks should thus rigorously identify their customers before providing any privacy enhancing cryptocurrency services for them, and they should perform heightened due diligence on any payments their customers initiate or receive if either the amounts involved are substantial or a suspicious pattern of behavior has emerged with respect to several smaller transactions.

Self-sovereign Identity Services

The easiest way to understand self-sovereign identity services is to begin with the problems inherent in traditional identity services. Typically a bank customer is identified by the institution from whom they seek an account. Some series of documents and statements are requested by the institution, provided by the customer, and authenticated by the institution. At the end of the process the customer is given an account and credentialing and authentication information: typically the customer chooses an username and a password, the password is hashed and the hashed password is stored by the institution to validate future login attempts. Additional factors like a recovery email address and/or phone number for receipt of one-time "two-factor" codes may also be recorded at this stage. The bank now has an identity for the customer and each time the customer wishes to transact she must re-identify herself using the password and other credentials matched to that identity upon account creation. If she loses her password or other credentials, some amount of recredentialing must be performed between bank and customer—often as elementary as responding to an email from the recovery email address previously recorded or offering the answer to some obscure question asked at sign-up. At the end of all this effort, there is a bespoke database at the bank that matches the real identity credentials and other due diligence performed by the bank on every customer to a login, hashed-password, phone number, email and emergency reset questions reported by each customer.

Note four important things about this identity system:

1. The identity is not portable. Unlike a physical driver's license or state-issued ID card, the customer is only able to use her login with the bank that established the match between the real documentation and the login credentials. She can't use that login at another bank or online service provider.
2. The identity is controlled by the bank rather than the customer. Unlike a drivers license that a user effectively owns and can share with any number of parties seeking identification, the bank owns the database that matches real credentials with logins.

Either for basic cybersecurity reasons or competitive advantage, the bank will not be opening up its database in order to identify customers for other third parties. This is why traditional online identity tools are not "self-sovereign," the customer relies on the institution for identity and does not own and possess the identity credential herself.

3. The identity will be vulnerable. Unlike a physical driver's license which would be difficult to steal from thousands of bank customers (a good deal of pickpocketing to do, indeed), the bank's database along with the thousands of identities described therein is a single attack surface for hackers to compromise. This is a grave vulnerability that's been exploited time and time again much to the agony of identity theft victims and compromised institutions alike.[29]
4. The identity will almost certainly be inefficient and redundant. We can assume that the customer will want to have several other online financial accounts as well as other online accounts with non-financial service providers like social networking, news and entertainment, or email providers. Each will have its own bespoke database matching originally provided user credentials with service-specific login credentials.

In the end we have lock-in (ID not portable), vulnerability (ID relies on institution), fragility (ID security only as strong as weakest identity provider), and redundancy (several ID providers and unique logins and passwords for each). Without portability the user faces costs creating new identities to open new accounts at alternative service providers. Without individual ownership of the credential the user is vulnerable when her information along with every other account holder is compromised by a high profile hack at one of her several service providers. And without interoperability the user ends up with her data spread across several providers and must manage unique passwords and login credentials for each and every one. It's a nightmare of complexity that we all experience intimately every day.

Parts of this system cannot and should not be innovated away. Trusted third parties like banks and governments will always need to play the role of initially requesting and verifying identity documents and attesting that they have been inspected recently and remain good sources of identifying information about a person. Nor should we expect or hope to one day have but one and only one entity making these attestations on our behalf. The federated or pluralistic identity system we have today in the U.S. has valuable resilience: I do not need to rely on one third party to prove my identity; I have a driver's license from my state government, a birth certificate from a hospital, a social security card and passport from the federal government, and a diploma from a private university. This diversity ensures that I will not ever be at the mercy of a single trusted party in order to prove my identity to another person or institution.

What we should do away with, however, are the several siloed, incompatible, and vulnerable databases that match an attestation of identity (we have checked the documents and this person exists and has these attributes) with a series of digital login credentials (username,

[29] Peter Van Valkenburgh, "Bitcoin: Our Best Tool for Privacy and Identity on the Internet," *Coin Center* (Mar. 2015) https://www.coincenter.org/bitcoin-our-best-tool-for-privacy-and-identity-on-the-internet/ (detailing the costs of identity theft and hacks of centralized web service providers).

password, email, and phone number) unique to each particular institution seeking identity assurances. Just as distributed ledgers begin to obviate the need to rely on siloed and incompatible databases of financial transactions at several independent financial institutions, so too do open blockchain networks begin to obviate the need for bespoke identity databases at several independent online service providers (including financial institutions).

A single shared database that links identity attestations from trusted parties to individually held cryptographic credentials would be superior to our current siloed systems. To be clear, those trusted parties who initially verify identity documents would still retain these proofs of identity and none of that sensitive information would be put "on a blockchain." Instead, the trusted parties whom we will call attestors, retain their proofs of a person's identity and publish a digitally signed attestation to a blockchain that says, "this blockchain credential (likely a public cryptographic address that has associated private keys which are retained by the person being identified) has been identified as *someone* by us." Then the person who wishes to prove her identity to another institution can point to the attestation on the blockchain and digitally sign a message with the associated private key in order to prove they are the person about whom that attestation was made and that the attestation was made at a certain date and time and has not since been revoked (hence the need for a blockchain or blockchain-like append-only public ledger).

Specific attribute information could be granularly shared between the original attestor institution and the institution seeking proof of identity, at the explicit request of the person being identified. Indeed, the person being identified could carry an encrypted statement of the identity attributes that were verified and signed by the attesting institution (a birth certificate with a name and age, a driver's license with eye-color and photo, a diploma with subject matter and degree-level attained) and selectively reveal those signed attributes (this is my age, this is my eye-color) to the institution seeking to identify the person. The institution need not then request this data from the original attestor but could, instead, simply ask the original attestor if the digital signature that was made on those attributes remains valid.

If at any point the original attesting institution discovers fraud or suspects the subject's credentials have been hacked, they can simply revoke those signatures and alert others that the attestation is no longer valid, indeed this too could be done using a blockchain wherein a new entry is made invalidating a prior attestation and creating a new attestation (just as an old Bitcoin unspent transaction output is replaced by a new one, thus preventing someone from "double spending" the original output). Attestations would be revoked if the person's cryptographic credentials are compromised or the original verified documents are later discovered to be bogus, and multisig technology (described above) could be implemented to decrease the risk of any credential ultimately being compromised (by forcing a would-be hacker to compromise multiple devices or parties rather than merely a single smartphone or computer of the victim).

This system as described is a self-sovereign digital identity system. It mimics the real physical identity system we use in off-line interactions: I still rely on several institutions to offer me

identity credentials, but I possess and carry these attestations in a wallet, on my person, or secured in my home. Before the advent of open blockchain networks, portable and self-sovereign identity credentials were not possible in a digital context unless some trusted third party was to provide the database infrastructure and make it available to any and all persons seeking an identity or seeking to verify an identity. With open blockchain networks, that single database can be provided by freely available, censorship resistant, public infrastructure, in other words, by open blockchain networks.

There are several parallel efforts underway to build and test these open-blockchain identity systems.[30] While it is premature to identify any particular effort as the imminent global standard, banks should be free to begin experimenting with these systems either as attestors of their customer's identity or as parties relying on another institution's digital attestations. This will require some standard setting as well as careful oversight from regulators, but the urgency of identity theft and cybersecurity risks inherent in existing identity standards argues in favor of beginning that experimentation as soon as possible. Therefore, the OCC should clear the way by emphasizing the value of these systems and by ensuring that banks are free to test them.

Six Cryptocurrency Activities in Summary

These six activities are, all of them, revolutionary computing activities made possible by open blockchain networks that can and will provide real and substantial benefits to Americans. We cannot overstate the significance of the recent work at the OCC to take a proactive and innovation-friendly approach toward cryptocurrencies and associated open blockchain technologies.

Digital asset safekeeping services will play an essential role alongside self-custody in ensuring that Americans are never dependent on any particular institution or personal device to protect their wealth and financial independence. Multisig safekeeping services can enable fraud-prevention techniques for digital asset transactions and further diversify options for digital asset safekeeping, ensuring that even if one institution or device is compromised no personal savings are lost.

Node and payment channel operation by major US financial institutions will add even more robustness to already decentralized open blockchain networks and ensure that American businesses play a significant part in maintaining these valuable networks as global public goods.

Privacy enhanced cryptocurrency services will help protect the dignity and autonomy of persons transacting online while still allowing some granular control over information sharing

[30] *See, generally* Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel, "A Survey on Essential Components of a Self-Sovereign Identity," (2018) https://arxiv.org/pdf/1807.06346.pdf; *see also*, "Decentralized Identity: own and control your own identity," Microsoft (2018) https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY; *see also, "Blockchain for digital identity,"* Consensys, accessed Jul. 2020, https://consensys.net/blockchain-use-cases/digital-identity/.

with law enforcement when and only when due process demands. Self-sovereign identity services will re-empower Amercians with portable digital credentials, substantially mitigating the risks of service lock-in, identity theft, and poor password management.

Importantly, all of these activities and services are integral to the core business of banking, and banks should be free and encouraged to pioneer all of these innovative open blockchain technologies safely and with appropriate guidance from regulators. Accordingly, in the following and final section of this comment we will highlight portions of current regulations that may be augmented to clarify permissible cryptocurrency activities for National Banks.

Clarifications to Legal Standards to Accommodate Activities

At § 7.5001 (d) (3)[31] we suggest adding a new item to the illustrative list of electronic activities incidental to the business of banking. This item should include the following activities,

- "Cryptocurrency network node operation including storage and validation of a blockchain as well as relaying of third-party transaction messages."
- "Cryptocurrency payment channel node operation including provision of liquidity for channels created with bank customers or with other banks."

To § 7.5001 (d) (3)(iv)[32] we suggest adding "cryptocurrency wallet software and hardware" to the list of equipment that may be sold by banks to customers.

To § 7.5002 (a)[33] we suggest adding the following to the illustrative list of banking services delivered through electronic means:

- "Providing fiduciary and non-fiduciary safekeeping services for customer cryptocurrencies."
- "Providing transaction fraud prevention and cryptocurrency key recovery services with multisignature cryptocurrency keys."
- "Providing microtransaction and other payment services by opening and funding cryptocurrency payment channels with customers and between other banks."
- "Offering privacy and anonymization services to obfuscate customer information on public cryptocurrency networks,"
- "Issuing customer identity attestations and validating existing attestations on public cryptocurrency networks or similar self-sovereign digital identity systems"

Because several state laws require licenses from those engaged in money transmission or virtual currency business activities (variously defined), we suggest that § 7.5002 (c) (dealing with preemption of state law) be amended to specifically mention money transmission and

[31] 12 CFR Subpart E - National Bank Electronic Activities
[32] *Id.*
[33] *Id.*

other licensing requirements for cryptocurrency activities as preempted for chartered national banks.

We suggest adding the following to the list of electronic capacity that banks may sell to third parties (§ 7.5004 (c)) "capacity for making, storing, and validating transactions on a cryptocurrency network."[34]

Because cryptocurrency network software is, almost without exception, released under open source licences rather than proprietary license,[35] we suggest adding to the end of § 7.5006 (c) (dealing with bank production and dissemination of software)[36] as follows: "A National Bank may utilize existing software including but not limited to open source software to perform banking functions and may develop derivative software from existing software in accordance with any existing licensing agreements including open source software licenses. A National Bank may publish banking software in third-party software repositories for public use and inspection."

Lastly, at § 7.5007 we suggest adding cryptocurrency safekeeping, software development, and networking services to the illustrative list of correspondent services.[37]

We thank you for this opportunity to comment, and look forward to continuing the discussion as the OCC continues to explore these important issues.

[34] *Id*.
[35] Peter Van Valkenburgh, "What is 'open source' and why is it important?" *Coin Center* (Oct. 2017) https://www.coincenter.org/education/advanced-topics/open-source/.
[36] 12 CFR Subpart E - National Bank Electronic Activities
[37] *Id*.