



Dr Geoffrey Goodell
Department of Computer Science
University College London
66-72 Gower Street
London WC1E 6EA
England
g.goodell@ucl.ac.uk
+44 2031087568

Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna VA 22183
United States of America

Re: Docket Number FINCEN-2020-0020, RIN 1506-AB47

Dear FinCEN Regulatory Support Team:

I am a researcher in the Financial Computing and Analytics Group in the Department of Computer Science at University College London, and I am also a citizen of the United States of America. I have spent a decade working in the financial industry and have advised financial regulators in the UK and abroad. My research concerns complex systems at the interface of finance, information technology, and public policy. Over the past four years, my work has specifically focussed on digital currencies and the future of payments. My brief comments in this letter concern the current FinCEN consultation on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets.

Specifically, my comments concern restrictions related to the use of non-custodial wallets. Most importantly, I emphasise that it is possible to introduce regulation of digital currency transactions involving non-custodial wallets while still allowing non-custodial wallets that protect the privacy of end-users. For this reason, I applaud the fact that the proposed regulation does not prohibit the use of non-custodial wallets. I also applaud the fact that the obligation for financial institutions to identify the counterparties to transactions would apply only to the transactions, as opposed to the non-custodial wallets themselves, and only to a limited set of transactions that meet specific criteria. Finally, I applaud the fact that the criteria can be determined in advance by the counterparties to a transaction before the transaction is attempted. These decisions are reasonable and appropriate.

At the same time, I am concerned about the use of language in the proposed rules and its associated documents that equates non-custodial wallets to anonymous bank accounts. This analogy is not appropriate: While anonymous bank accounts involve a specific relationship between a bank and a customer over some period of time, non-custodial wallets require no such relationship and are essentially tools that allow individuals to be custodians of their own money. A more appropriate

analogy would compare non-custodial wallets to physical wallets that hold physical cash. For this reason, I argue that non-custodial wallets should offer to their users the same affordances as cash and consequently are essential to individual privacy and human rights.

Unfortunately, the proposed thresholds for reporting and recordkeeping rules involving non-custodial wallets do not match the requirements for cash. First, the recordkeeping rules for cash transactions are not the same as the recordkeeping rules for bank wire transfers, and the requirement for a bank or money services business to maintain records identifying the counterparties to any transaction involving \$3,000 or more is not consistent with the fact that cash transactions in excess of this amount are not subject to the same recordkeeping requirement in the US. The requirement for recordkeeping must therefore involve either a significantly higher threshold or a test that depends upon the specific use case. Second, under some circumstances it is also possible for individuals to conduct legal cash transactions in excess of \$10,000 without incurring regulatory reporting obligations in the US. Therefore, it would be more appropriate to apply the corresponding reporting requirement to the withdrawal or deposit of funds between a bank or money services business and a non-custodial wallet, rather than to the transaction itself.

Although retail digital currency transactions are currently perceived as something of a niche market, reason exists to believe that the scope and set of use cases for such transactions will expand in the decades ahead. One important reason relates to the secular decline in the use of cash in much of the developed world. Indeed, many retailers have come to conclude that accepting cash is optional, and for this reason legislation to compel retailers to accept cash exists in many jurisdictions around the world, including Denmark, Norway, China, and several US states [1, 2]. However, such legislative protections might not be enough to sustain cash as a viable payment option. As retail transactions increasingly take place electronically, the variable revenues associated with operating cash infrastructure fall relative to the fixed costs, and the marginal cost of handling cash increases. This logic applies without distinction to retail users, including both customers and vendors, as well as banks and operators of ATM networks. In the UK, ATM networks and bank branches that facilitate the circulation of cash are facing pressure that has led to a downward spiral in cash services [3].

Cash affords certain important advantages to its bearers that modern retail payment infrastructure does not, including but not limited to:

- **Owner-custodianship.** The absence of a custodian means that the bearer cannot be blocked by the custodian from making a remittance or charged differentially by the custodian on the basis of the counterparty to a transaction. Self-determination is an essential feature of ownership, and a critical prerequisite to ownership is the ability to withdraw and use cash in a multitude of transactions without a custodian.
- **True fungibility.** Because cash does not require any particular identification or imply any particular relationship with a financial institution, users of cash know that their money is exactly as valuable as anyone else's. Absent this property, counterparties to a transaction would be able to discriminate on the basis of the identity of the bearer or the custodian, and the same amount of money would have a different value in the hands of different people.
- **Privacy by design.** It is no secret that retail payments leave behind a data trail that can be used to construct a detailed picture of an individual's personal lives, including travel, financial circumstances, relationships, and much more. The fact that electronic payments can be used for surveillance and population control has been known for many decades [4, 5]. I further note that data protection, which relates to the access and use of private information once collected,

is not the same as privacy by design, wherein users of a technology do not reveal private information in the first instance. The principle of favouring privacy by design to data protection is well-understood [6], and the continued inability of governments and corporations to prevent unauthorised access, both by (other) government authorities and by malicious adversaries, underscores a greater need for private information to not be collected [7]. I have also elaborated this argument specifically in the context of value-exchange systems [8].

Non-custodial wallets offer a way to preserve cash-like characteristics in digital transactions, and I have argued that the popularity of cryptocurrencies largely follows from the pursuit of privately held digital cash [9]. The increasing preponderance of online and digital transactions must not be viewed as an opportunity to expand the scope for surveillance and control over individual persons by monitoring or restricting what they do with their money.

Fortunately, it is possible to regulate financial transactions without collecting data that could be used to profile the behaviour of individual persons. The solution proposed by my team introduces a government-backed digital currency infrastructure to ensure that every transaction is registered by a bank or money services business, and it relies upon non-custodial wallets backed by privacy-enhancing technology such as zero-knowledge proofs to ensure that transaction counterparties are not revealed [10]. Please refer specifically to Sections 3.3, 3.4, and 4.4 for details relevant to the proposed regulation.

In principle, it should be possible to accommodate such solutions by adapting the proposed regulation to protect the rights of individual persons. For the proposed regulation to avoid infringing upon essential privacy and human rights, specific measures must be taken to ensure:

- that non-custodial wallets must not be expected to carry persistent identifying information such as a unique identifier or address that would be associated with multiple transactions,
- that non-custodial wallets must not be expected to reveal information, including keys or addresses associated with previous or subsequent transactions, that can be used to identify their bearers, owners, or sources of funds,
- that the obligation to identify the counterparties to a transaction can only be imposed at the time of a transaction, and
- that the process for providing information to the requesting banks or money services businesses for the purposes of recordkeeping or reporting must not involve the non-custodial wallet itself and would be carried out only with the consent of both counterparties.

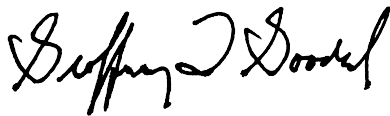
It can only be possible for ordinary users of non-custodial wallets to have confidence that their routine activities will not be profiled if the relevant thresholds are sufficiently high and circumstances are sufficiently rare for which counterparty information is requested for recordkeeping or reporting. Such requests must involve the explicit consent of the owner or bearer of the digital tokens on each separate occasion, must not be routine for ordinary persons carrying out ordinary activities, and must not require a non-custodial wallet or other personal device to reveal any information identifying its owner or bearer.

In all cases, it is critical to separate the regulatory requirements for identification (the 'policy') from the underlying protocols and technology that facilitate payments (the 'mechanism'). Such separation

must be seen as a requirement for non-custodial wallets. The mechanism by which custodial retail electronic payments are implemented enables surveillance as an artifact of the custodial relationship. For owners of money to truly use it freely, they must have a means of using money outside custodial relationships and without the risk of profiling. To impose requirements upon non-custodial wallets that essentially proscribe such uses would only serve to ensure that digital money is never truly owned, as its users would be forced to accept a more limited set of rights.

Please feel free to contact me if you have any questions related to the contents of this message or would like to discuss my research in greater depth. I welcome your thoughts and would very much welcome the chance to speak further with you on this important topic.

Yours sincerely,



Dr Geoffrey Goodell

References

- [1] Access to Cash Review (UK), Final Report, March 2019.
<https://www.accesstocash.org.uk/media/1087/final-report-final-web.pdf>
- [2] M Sadeghi. "Fact check: No US law requires businesses to take cash, but local laws may mandate it." USA Today, 2020-09-16. <https://eu.usatoday.com/story/news/factcheck/2020/09/16/fact-check-cashless-businesses-banned-only-some-local-state-laws/3330804001/>
- [3] D Tisher, J Evans, K Cross, R Scott, and I Oxley. "Where to Withdraw? Mapping access to cash across the UK." University of Bristol, November 2020.
- [4] P Armer. "Privacy Aspects of the Cashless and Checkless Society." Testimony before the US Senate Subcommittee on Administrative Practice and Procedure. 1968-02-06, as published by the RAND Corporation, April 1968. <https://www.rand.org/content/dam/rand/pubs/papers/2013/P3822.pdf>
- [5] P Armer. "Computer Technology and Surveillance." *Computers and People* 24(9), pp. 8–11, September 1975. https://archive.org/stream/bitsavers_computersA_3986915/197509#page/n7/mode/2up
- [6] H Nissenbaum. "Deregulating Collection: Must Privacy Give Way to Use Regulation?" May 2017. <https://doi.org/10.2139/ssrn.3092282>
- [7] A Rychwalska, G Goodell, and M Roszczynska-Kurasinska. "Management of Big Data in the public sector: System-level risks and design principles." Presented at Conference on Complex Systems (CCS), Singapore, September 2019. To appear, *Surveillance and Society*. Available at SSRN: <https://ssrn.com/abstract=3455123>.
- [8] G Goodell. "Privacy by Design in Value-Exchange Systems." Discussion Paper, June 2020. <https://arxiv.org/abs/2006.05892>
- [9] G Goodell and T Aste. "Can Cryptocurrencies Preserve Privacy and Comply with Regulations?" *Frontiers in Blockchain*, May 2019. doi:10.3389/fbloc.2019.00004. Also available at SSRN: <https://ssrn.com/abstract=3293910>
- [10] G Goodell, H Al-Nakib, and P. Tasca. "Digital Currency and Economic Crises: Helping States Respond." London School of Economics Systemic Risk Centre Special Paper SP 20, September 2020. Presented at the 6th Annual Peer-to-Peer Financial Systems Workshop (P2PFISY 2020), December 2020. Available at SSRN: <https://ssrn.com/abstract=3622089>