

Discussion of

Global Stablecoins in 2030: A European Perspective

Ulrich Bindseil Romain Meuwissen Giorgio Mondini Martin Rohar

Discussant: Eric Budish
University of Chicago, Booth School of Business

The Future of Market Liquidity and Functioning Workshop
Federal Reserve Bank of New York · Clark Center for Global Markets, Chicago Booth

July 9, 2026

Overview: Global Stablecoins in 2030

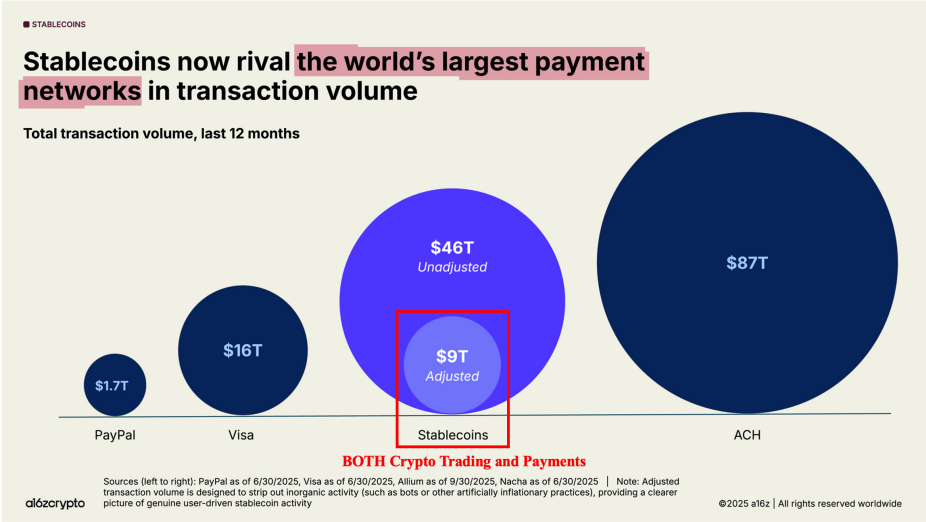
- ▶ Great paper on a confusing subject.
- ▶ Really two papers for the price of one.
- ▶ Sections 2-3, “The Nature and Uses of Stablecoins” and “Market and Financial Stability Impact”, are a terrific overview of the technology, terminology, policy issues and regulatory issues related to stablecoins
 - ▶ Essential reading.
 - ▶ Cuts through a lot of B.S. on the topic. (Fn. 3 alone is worth the price of admission: “According to ISO704 (2022, 42) circularity occurs if ... ”)
 - ▶ Best organized and executed overview I have seen.
- ▶ Sections 4-6: Analytical heart of the paper, scenario-based flow-of-funds analysis.
 - ▶ Focus of Ulrich’s presentation, I won’t rehash.
 - ▶ Overall: very thoughtful, clear, reasonable.
 - ▶ I will make two related substantive points about the analysis.
 - ▶ And then build off of Ulrich’s last bullet point: “Illicit use and regulatory arbitrage deserve close attention”
- ▶ Key distinctions: Legal vs. Illegal Stablecoin Uses; Permissioned vs. Permissionless Blockchains

Comment: Legal vs. Illegal Uses of Stablecoins

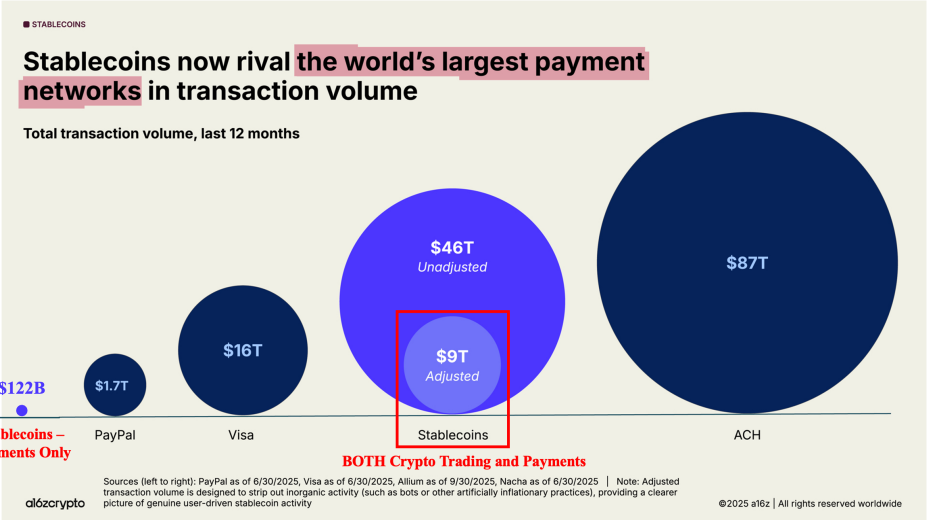
- ▶ Clearly: there are both legal and illegal potential use cases for stablecoins.
- ▶ More subtly: there are many use cases for stablecoins that are potentially legal but where the anonymity of stablecoins makes it easy to circumvent the law.
 - ▶ Leading example: crypto trading (DeFi). Does the user pay taxes?
- ▶ My read of the data so far is that by far the largest use case of stablecoins is crypto trading.
- ▶ Lots of remarkable reporting on the usefulness of stablecoins for crime (Zeke Faux on pig butchering, WSJ on funding terrorism).
- ▶ Use for payments, remittances, etc., is real but comparatively modest to date.

Stablecoins: The Data So Far

Stablecoins: The Data So Far

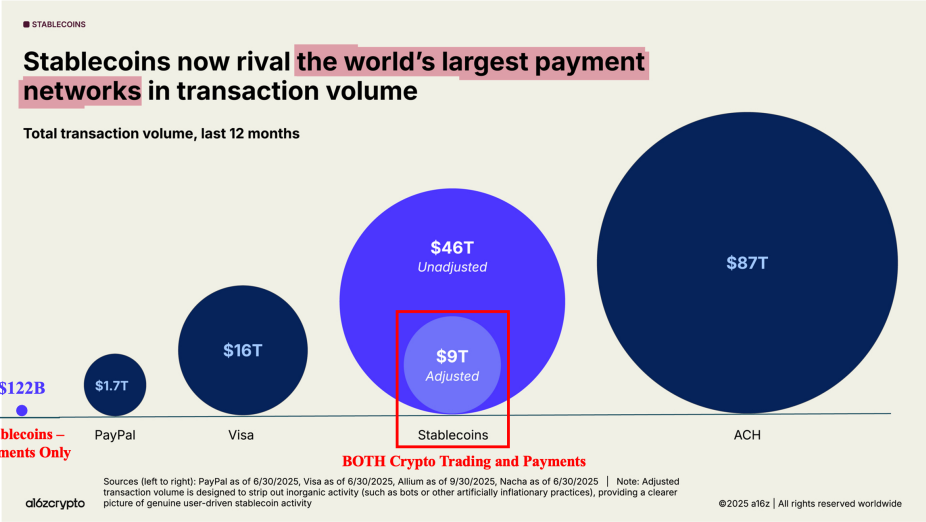


Stablecoins: The Data So Far



Source: Artemis bottoms-up analysis of 33 stablecoin payments companies. Includes P2P, B2B, Card, B2C and Prefunding payments. Artemis's methodology does not attempt to include DIY on-chain payments (e.g., using a MetaMask wallet). \$122B figure in the slide represents annualized run-rate based on most recent month of data (\$10.2B in the month of Aug 2025). This number is of the right order of magnitude when we look at the annualized run-rates of some of the largest stablecoin payments companies including Binance Pay, BVNK, Orbital and Conduit.

Stablecoins: The Data So Far



Source: Visa press release.

Stablecoins: The Data So Far



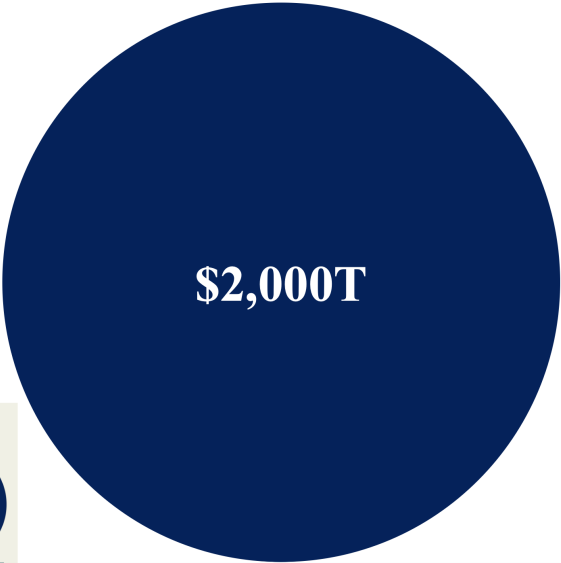
Stablecoins: The Data So Far



Fedwire Funds Service

Source: Federal Reserve Banks.

Stablecoins: The Data So Far



Global Payments Volume



Source: McKinsey 2025 Global Payments Report.

Comment: Legal vs. Illegal Uses of Stablecoins

- ▶ Comment #1: Flow-of-Funds analysis not really set up to distinguish between legal vs. illegal use.
- ▶ Comment #2: Does the USD 4.0 trillion “bull case” for stablecoin circulation capture the actual bull case in which stablecoins become dramatically more useful for legal payments?
- ▶ My policy worry
 - ▶ Stablecoins become really useful for legal purposes (asides from crypto trading).
 - ▶ In a form that also continues to be hyper-convenient for illegal purposes (electronic suitcases of cash).
 - ▶ And that creates an unappreciated systemic attack risk to boot.
- ▶ Policy has an opportunity to allow the useful without the hyper-convenient illegal and the attack risk.

Comment: Permissioned vs. Permissionless Stablecoins

- ▶ Crucial Distinction: Nakamoto's (2008) invention consists of both (i) a data structure, and (ii) a trust model
- ▶ Data structure ("blockchain")
 - ▶ Append-only distributed database.
 - ▶ Clear rules about what parties can add what transactions.
 - ▶ Cryptography to prove that past data has not been deleted or tampered with.
 - ▶ Not that novel/impressive from a technical perspective to computer scientists, but potentially useful for finance (Budish and Sunderam, "Blockchain Technology for Traditional Finance", NBER WP 2026).
- ▶ Trust model ("permissionless consensus")
 - ▶ Anonymous, decentralized set of participants collectively maintains the blockchain data structure (proof-of-work, stake, etc.).
 - ▶ Agrees on state and adjudicates disputes. Without any trusted party.
 - ▶ Boils down to an elaborate anonymous majority voting procedure.

Comment: Permissioned vs. Permissionless Stablecoins

- ▶ The trust model is where the scientific novelty lies ...
- ▶ And where two big vulnerabilities lie:
- ▶ Vulnerability #1: Intrinsically anonymous at the account level.
 - ▶ No amount of KYC/AML can fully overcome this.
 - ▶ Analogy: suitcases of cash.
- ▶ Vulnerability #2: Intrinsically vulnerable to majority attack at the system level.
 - ▶ Permissionless consensus relies on anonymous majority voting.
 - ▶ As the financial magnitudes increase ...
 - ▶ The incentives to obtain a majority and steal money increase too.
 - ▶ (Budish, “Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains”, QJE 2025)

Budish “Trust at Scale” (QJE, 2025) in Graphic Novel Form



Traditional Trust



Traditional Trust



Traditional Trust



Traditional Trust Model:

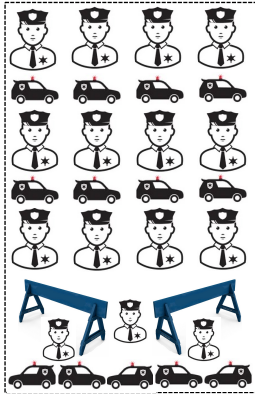
Traditional Trust



Traditional Trust Model:

- ▶ Security Guards

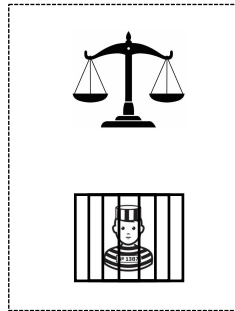
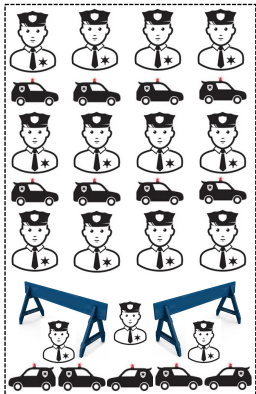
Traditional Trust



Traditional Trust Model:

- ▶ Security Guards
- ▶ Police Reinforcements

Traditional Trust



Traditional Trust Model:

- ▶ Security Guards
- ▶ Police Reinforcements
- ▶ Punishment via Rule of Law

Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust Model:

Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust Model:

- Large amount of Security Guards

Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust Model:

- ▶ Large amount of Security Guards
- ▶ But no additional layers (Police, Rule of Law)

Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust Model:

- ▶ Large amount of Security Guards
- ▶ But no additional layers (Police, Rule of Law)
- ▶ So, guards alone must deter attack

The Core Policy Conundrum

- ▶ Permissionless consensus poses a huge conundrum for policy makers.
- ▶ Conundrum: There is a lot of implicit legal protection for the anonymous trust if you look around (“legal puts”)
 - ▶ Ex: if an individual’s crypto wallet is stolen by a mugger -> they can call the cops
 - ▶ Ex: if a financial institution gets double spent -> they can call the FBI
- ▶ So, honest users get some implicit legal protection
- ▶ Which enhances the value of the permissionless system.
- ▶ Which provides more cover to black-market users.
- ▶ Have your cake and eat it too: anonymous, decentralized trust — unless there is a large attack, then call in the Feds

The Core Policy Confusion

Public Law 119–27
119th Congress

An Act

To provide for the regulation of payment stablecoins, and for other purposes.

July 18, 2025
[S. 1582]

*Be it enacted by the Senate and House of Representatives of
the United States of America in Congress assembled,*

SECTION 1. SHORT TITLE.

This Act may be cited as the “Guiding and Establishing
National Innovation for U.S. Stablecoins Act” or the “GENIUS
Act”.

Guiding and
Establishing
National
Innovation for
U.S. Stablecoins
Act.
12 USC 5901
note.
12 USC 5901.

SEC. 2. DEFINITIONS.

In this Act:

(1) **APPROPRIATE FEDERAL BANKING AGENCY.**—The term
“appropriate Federal banking agency” has the meaning given
that term in section 3 of the Federal Deposit Insurance Act
(12 U.S.C. 1813).

(2) **BANK SECRECY ACT.**—The term “Bank Secrecy Act”
means—

(A) section 21 of the Federal Deposit Insurance Act
(12 U.S.C. 1829b);

(B) chapter 2 of title I of Public Law 91–508 (12 U.S.C.
1951 et seq.); and

(C) subchapter II of chapter 53 of title 31, United
States Code.

(3) **BOARD.**—The term “Board” means the Board of Gov-
ernors of the Federal Reserve System.

(4) **COMPTROLLER.**—The term “Comptroller” means the
Office of the Comptroller of the Currency.

(5) **CORPORATION.**—The term “Corporation” means the Fed-
eral Deposit Insurance Corporation.

(6) **DIGITAL ASSET.**—The term “digital asset” means any
digital representation of value that is recorded on a crypt-
tographically secured distributed ledger.

(7) **DIGITAL ASSET SERVICE PROVIDER.**—The term “digital
asset service provider”—

means a person that, for compensation
conducts the business in the United
States.

The Core Policy Confusion

Public Law 119–27
119th Congress

An Act

To provide for the regulation of payment stablecoins, and for other purposes.

July 18, 2025
[S. 1582]

*Be it enacted by the Senate and House of Representatives of
the United States of America in Congress assembled,*

SECTION 1. SHORT TITLE.

This Act may be cited as the “Guiding and Establishing
National Innovation for U.S. Stablecoins Act” or the “GENIUS
Act”.

Guiding and
Establishing
National
Innovation for
U.S. Stablecoins
Act.
12 USC 5901
note.
12 USC 5901.

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE FEDERAL BANKING AGENCY.—The term
“appropriate Federal banking agency” has the meaning given
that term in section 3 of the Federal Deposit Insurance Act
(12 U.S.C. 1813).

(2) BANK SECRECY ACT.—The term “Bank Secrecy Act”
means—

(A) section 21 of the Federal Deposit Insurance Act
(12 U.S.C. 1829b);

(B) chapter 2 of title I of Public Law 91–508 (12 U.S.C.
1951 et seq.); and

(C) subchapter II of chapter 53 of title 31, United
States Code.

(6) DIGITAL ASSET.—The term “digital asset” means any
digital representation of value that is recorded on a cryp-
tographically secured distributed ledger.

ons a person that, for compensation
he business in the Unit
tame

The Core Policy Mistake

- ▶ Policy to date hasn't distinguished between permissionless and permissioned rails for stablecoins. If anything, GENIUS Act puts a thumb on the scale for permissionless.
- ▶ This is a mistake.
- ▶ Permissionless
 - ▶ Intrinsically vulnerable to 51% attacks -> so dangerous for financial markets.
 - ▶ Intrinsically anonymous at the account level -> so good for illegal activity.
- ▶ Permissioned rails backed by rule of law do not have these issues.
- ▶ Important note: there are some sympathetic use cases that take advantage of the anonymity too, such as international remittances.
- ▶ As Bindseil et al (2026) write: “first best in a democracy should be to amend inefficient regulation, and not to let regulatory arbitrage be the solution.”

Conclusion: Two Scenarios

- ▶ Optimistic scenario
 - ▶ Permissionless stablecoins put pressure on banks/TradFi firms to improve costs / reduce intermediary rents in the traditional, legal financial system.
 - ▶ Permissionless stablecoins put pressure on regulators to improve inefficient regulation (as Bindseil et al call for).
 - ▶ Permissionless stablecoins stay relatively small/contained.
 - ▶ Permissioned stablecoins become genuinely useful in some form (possibly as CBDC; possibly as variants of Zelle/Venmo; etc.).
- ▶ Pessimistic scenario
 - ▶ Permissionless stablecoins grow unchecked.
 - ▶ Permissioned stablecoins hindered by law (“Anti-CBDC Surveillance State Act”).
 - ▶ Bad actors around the world enjoy a much more convenient alternative to suitcases of \$100-bills.
 - ▶ The traditional financial system becomes intertwined with a technology that is intrinsically vulnerable to large-scale anonymous attacks.