CIRCLE

First Principles of Interoperability

Lessons from traditional US payments systems

Zach Wong // Oct. 6, 2022 // Chicago, IL

Note (10/11): These slides supported a live discussion. As such, they may be incomplete or lack context.

I've added some of my speaking notes in blue-background bubbles like this.

Table of Contents

1. Introduction

Circle, public policy, and interoperability

CIRCLE

OUR MISSION

To raise global economic prosperity through the frictionless exchange of value

Circle is a global financial technology firm that enables businesses of all sizes to **harness the power of digital currencies and public blockchains for payments, commerce and financial applications worldwide**. Circle is the sole issuer of USD Coin (USDC) and Euro Coin (EUROC).

Founded in 2013, Circle's **transactional services, business accounts, and platform APIs** are giving rise to a new generation of financial services and commerce applications that hold the promise of raising global economic prosperity for all through the frictionless exchange of value.

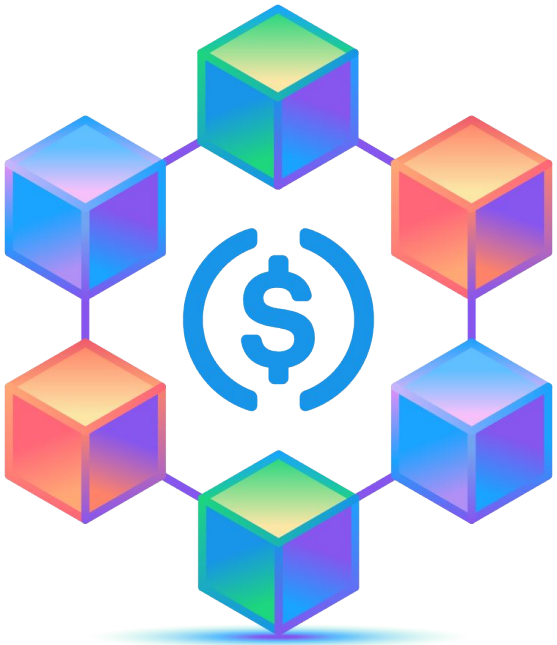
USDC itself has a multichain strategy

Native USDC today:

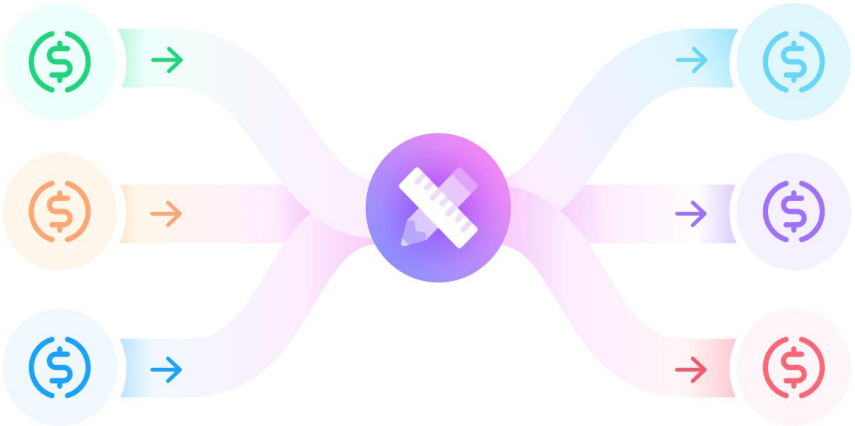
ETHEREUM	SOLANA	ALGORAND
STELLAR	TRON	HEDERA
AVALANCHE	FLOW	POLYGON

Intended soon:

ARBITRUM	OPTIMISM	COSMOS
NEAR	POLKADOT	



Developers can swap native USDC permissionlessly with the new Cross-Chain Transfer Protocol



With Circle's Cross-Chain Transfer Protocol, developers building wallets, bridges, payments apps, financial services tools and more can soon **enable users to send and transact USDC natively across chains**. Cross-Chain Transfer Protocol will effectively teleport USDC from one ecosystem to another, maximizing capital efficiency and streamlining the user experience.

Allbridge and **Wormhole** are among some of our launch partners!

About Me

Policy & Strategy // Market Conduct & Competition

Previously: Consumer Financial Protection Bureau, Congress

My team:

- Meets with policymakers
- Responds to requests for information
- Advocates for how Circle and its products should be regulated
- Contributes to corporate strategy and roadmap

Regulators are concerned about interoperability

As a nascent industry, chains, products, and services are fragmented right now.

Regulators worry that crypto will fracture financial services and lead to less efficient markets.

OCC Acting Comptroller Michael Hsu

> *Without interoperability amongst USD-based stablecoins, the risk of digital ecosystems being fragmented and exclusive (with walled gardens) is heightened.*

Federal Reserve Board Vice Chair Lael Brainard

> *More broadly, it is important for the United States to play a lead role in the development of standards governing international digital finance transactions involving CBDCs consistent with the norms of privacy, accessibility, interoperability, and security.*

Bridges are essential for smooth user experiences

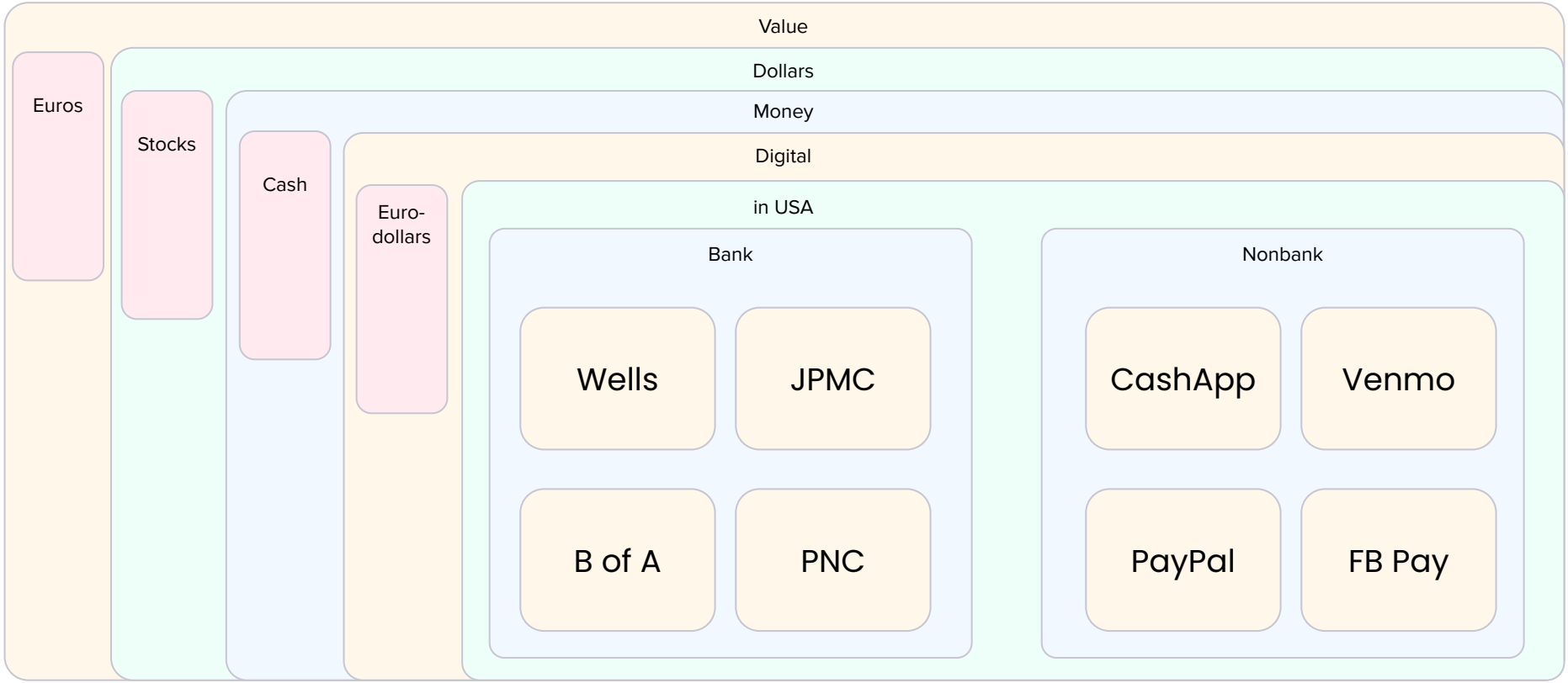
- Optimize use cases for protocol design choices
- Unify liquidity and utility
- Avoid product replication and promote innovation
- Consolidate around effective development standards

Interoperability protocols - and apps building xChain - will help onboard billions of users

Table of Contents

2. Reality: Everything is Fragmented

Everything is a network



When you're trying to pay someone, you need to agree how to do it. That's the establishment of a network. If we both have access to the same network, that reduces friction for our cooperation.
Not coincidentally, payment costs and complications generally increase as you go wider in this diagram.

Every company is its own network

Every financial services company is its own network.

Many consumer fintechs are based on trying to create a new, proprietary payments network.

These disparate systems only interoperate because of coordinating infrastructure (bridges!).

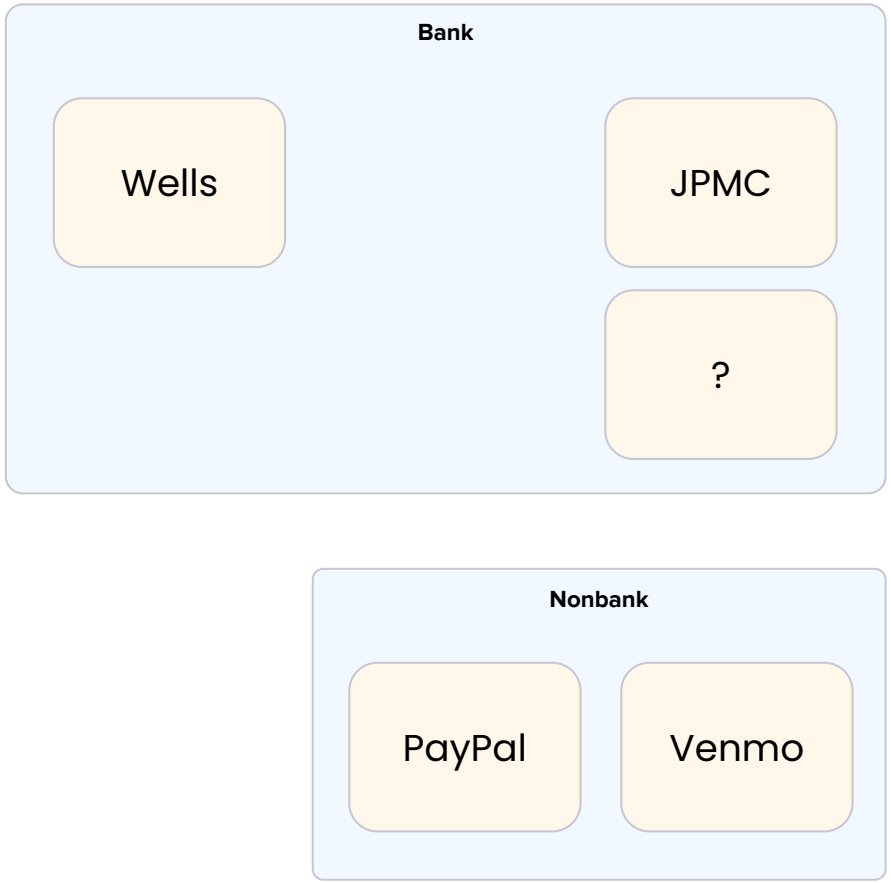


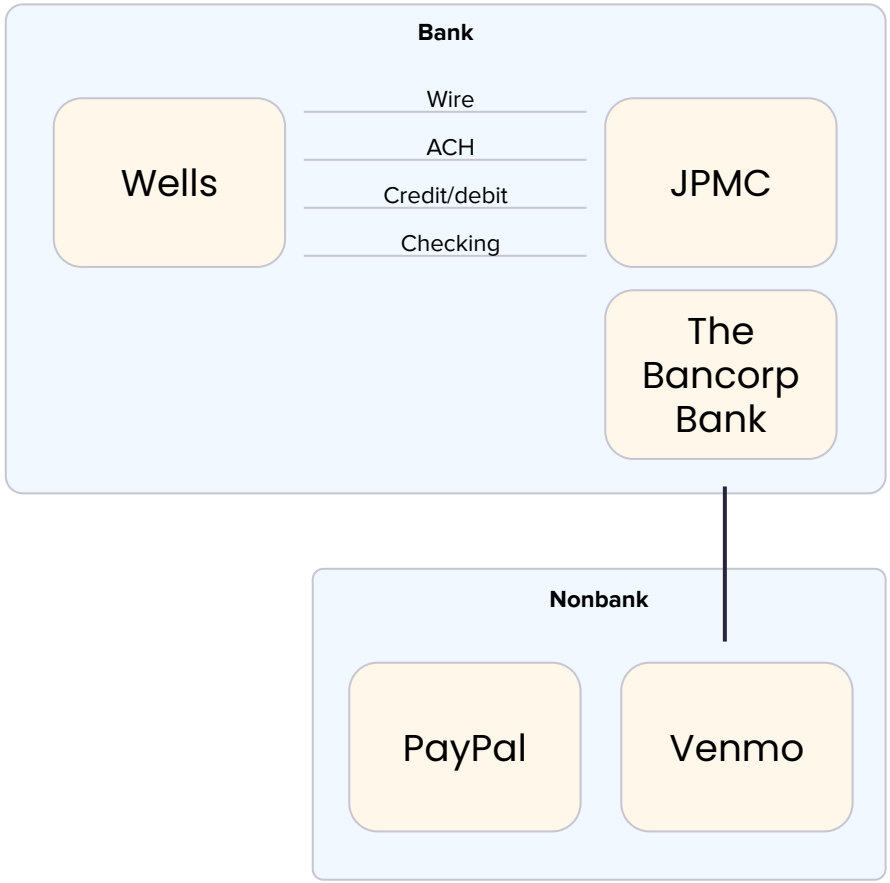
Table of Contents

3. Perception: Everything is Unified

Backend systems enable interoperability

Traditional financial services had to go through the exact same process of bridging to enable smooth financial services experiences.

Even today, nonbank financial institutions are segmented from the bank financial services ecosystem; they have to go through a bank.

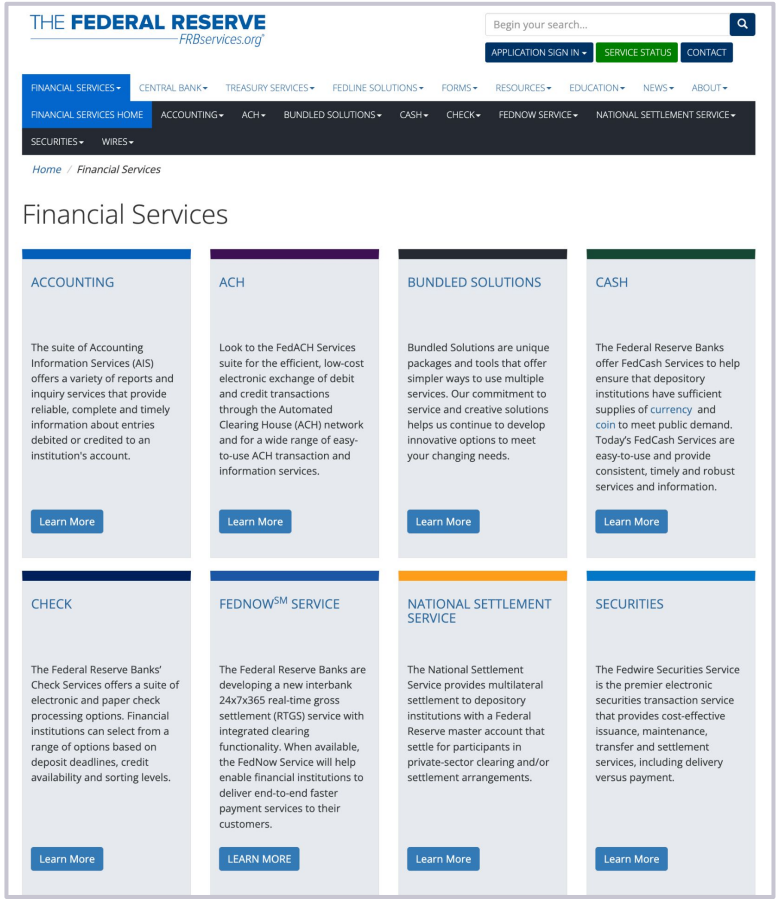


Most things go through the Federal Reserve

In addition to setting monetary policy, other parts of the **Federal Reserve System** also supervise banks and provide genuine *financial services* to banks.

Almost all domestic payments clear through Federal Reserve systems.

An interesting question to think about is what are the implications of the Federal Reserve serving as the central clearing system? Why did Congress make the *policy* decision for the Federal Reserve to provide central services in this way? What advantages and disadvantages does that provide? Is that replicated in crypto and, if not, is it important to do so?



My favorite Federal Reserve webpage

Nonbank services add additional functionality

Certain private companies have carved out niches for providing specific interoperability services.

Opportunities for crypto are abundant

For example, cross-border payments are awful

Domestically, merchants and businesses suffer

High fixed costs render micropayments impossible; ads take their place

Innovation in TradFi is slow, if not almost nonexistent

Table of Contents

4. Lessons for Crypto

Lessons for Crypto

If, as the critics quip, crypto is rebuilding the traditional financial system from scratch, let's at least do it better.

Technical infrastructure is not the only thing that matters

What social, economic, or political structures do you need to put in place to ensure a quality UX? What mechanisms or functions from tradfi must be replaced?

Network effects trend toward consolidation; are we still early, or are standards set?

It's helpful to converge on standards, but once set they are hard to modify. Let's get them right at the start.

What are the implications of a system built on bearer assets vs. central clearing?

Bearer assets are good for some purposes, but they may cause challenges in certain situations. Consider the relative advantages and disadvantages of the tools you're using.

Studying TradFi systems exposes user experience obstacles that **I have not heard of being addressed** in crypto.
Have a different opinion? Please reach out: zachrwong.info/contact.

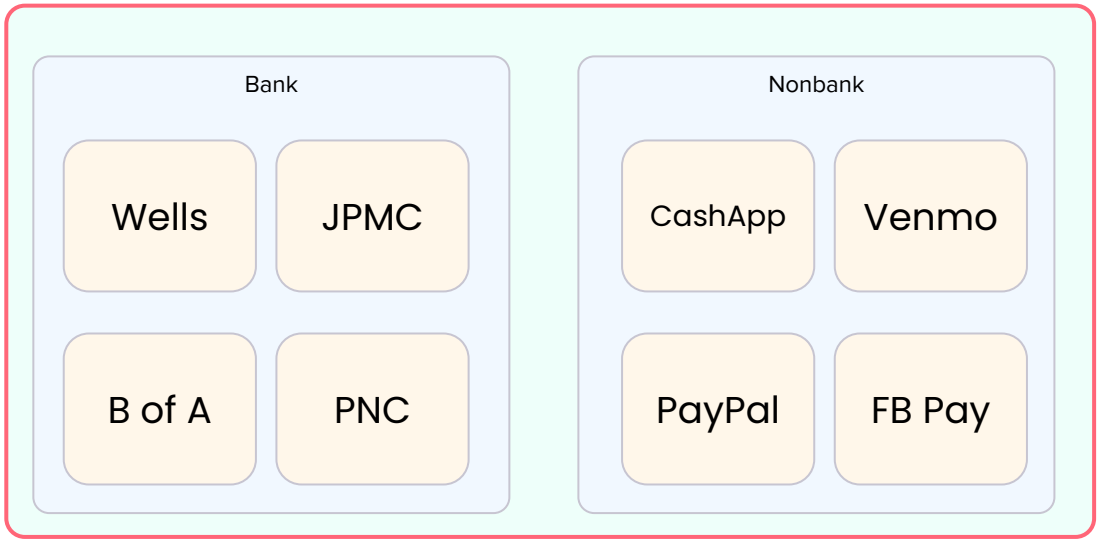
Legal and social systems ensure a consistent experience

Financial institution supervision

Private network rules

Consumer protection regulations

Unified currency zones



When you get to this point, you generally do not have to worry about what specific system you're using.

FI supervision. Both bank supervision and public company reporting. Consumers don't have to implicitly discount their assets based on some unclear, asymmetric assessment of financial institution integrity.
Network rules. e.g., allocation of liability for fraud means consumers have a smooth experience without having to track down every FI in the chain. Textbook coordination problem; not solvable by a single FI.
Consumer protection regulations. Consumers bear no mental overhead of deciding what system to use based on what is safer or not; generally pretty consistent protections.
Unified currency zones. Use USD in the US. Consider in crypto how you buy NFTs with ETH on Ethereum but SOL on Solana; other asset payment options also offered but not used frequently. Is that the best UX?

INDEMNIFICATION AGREEMENT
REQUEST FOR RETURN OF FUNDS FROM ACH TRANSACTION

This Indemnification Agreement (this "Agreement") is made and entered into by _____ ("ODFI") and _____ ("RDFI").[1]

On _____ [date of transaction], the following (e.g. erroneous, improper, unauthorized, or fraudulent) ACH transaction (the "Transaction") occurred, resulting in funds (the "Funds") being credited to a deposit account (the "Account") at RDFI:

- Requested Amount: $_____
- Indemnifying Bank customer name: _____
- Originating Company Identifier: _____
- Indemnified Bank Account number: _____
- Trace Number: _____

ODFI hereby requests that RDFI block access to the Funds in the Account, and/or in any other bank account to which any portion of the Funds have been transferred ("Subsequent Account"), in an amount equal to (i) the Requested Amount listed above, or (ii) the amount of the Funds still on deposit in the Account and/or Subsequent Account, whichever is lesser ("Restrained Amount"). ODFI further requests the RDFI return the Restrained Amount to ODFI via R06 code or other mutually agreed means of payment. In consideration of the foregoing, ODFI agrees to indemnify the RDFI from and against any and all claims, demands, losses, liabilities and expenses, including attorneys' fees and costs, resulting directly or indirectly from compliance by RDFI with ODFI's request. This indemnity is intended to be consistent with and in addition to the indemnity stated in Article 2, Subsection 2.12.3 of the *NACHA Operating Rules*.

This Agreement may be executed electronically or by facsimile signature of ODFI. This Agreement shall be governed by and construed in accordance with New York law.

We simply give the money back to the person who sent it.

Model form from NACHA, 2019

Example of an enforced social convention. *See* Patrick McKenzie, Finality doesn't exist in payments discussing hold harmless agreements.

The legal system seems core to the enablement of certain features

Reversibility

Uncollateralized lending

Certain NFT rights

Reversibility. Citigroup case is an example of a payment that was final from a technical perspective but was reversed. When is reversibility a desirable or undesirable trait?
Uncollateralized lending. “Unsecured” loans are underwritten based on one’s current reputation (credit score, an asset) and then collateralized against one’s future reputation. If borrower defaults, the lender can force her into bankruptcy, possibly obtaining some assets back but also decrementing the borrower’s future reputation.
Certain NFT rights. A16z’s CantBeEvil encodes creative commons-like licensing rights into on-chain data; ostensibly helps with legal enforcement, e.g., of music NFT rights.
I’m **NOT** claiming that these features are always desirable; only that if one does desire them, then the legal system seems helpful.

Citigroup’s $500 Million Blunder Ends in Victory for the Bank

- Appeals court says Revlon lenders can’t keep errant payment
- Panel vacates lower ruling; one expert cites ‘Twilight Zone’

Research

Paradigms for On-Chain Credit

written by
Lucas Baker

Reversible Transactions on Ethereum: ERC-20R and ERC-721R

```
pragma solidity ^0.8.13;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import "@a16z/contracts/licenses/CantBeEvil.sol";

contract MyToken is ERC721, CantBeEvil {

    constructor() ERC721("MyToken", "MTK") CantBeEvil(LicenseVersion.CBE_CC0) {}

    // Rest of the NFT code

    // This contract inherits these functions from the CantBeEvil contract:
    //      getLicenseURI()
    //      getLicenseName()
}
```

Lessons for Crypto

If, as the critics quip, crypto is rebuilding the traditional financial system from scratch, let's at least do it better.

Technical infrastructure is not the only thing that matters

What social, economic, or political structures do you need to put in place to ensure a quality UX? What mechanisms or functions from tradfi must be replaced?

Network effects trend toward consolidation; are we still early, or are standards set?

It's helpful to converge on standards, but once set they are hard to modify. Let's get them right at the start.

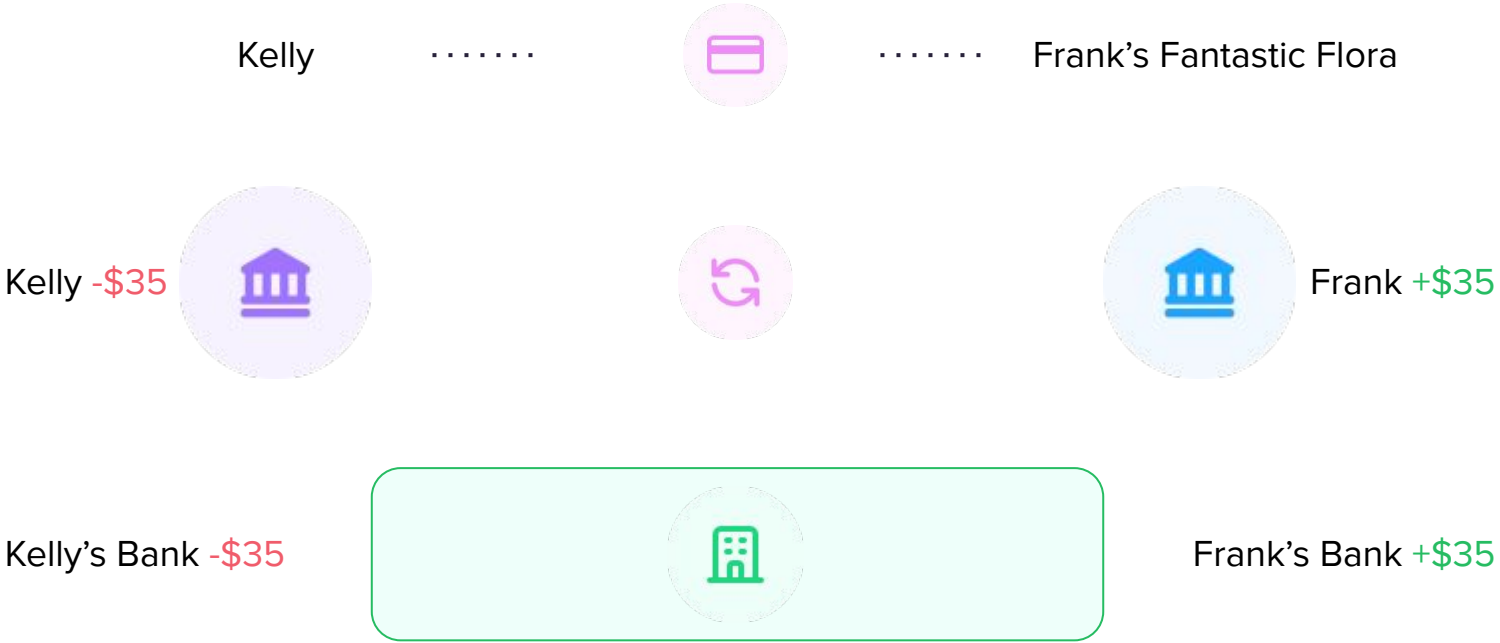
What are the implications of a system built on bearer assets vs. central clearing?

Bearer assets are obviously good for some purposes, but they may cause challenges in certain situations. Consider the relative advantages and disadvantages of the tools you're using.

E.g. what chain should I build on, what programming language should I use, should I limit myself to EVM or something else, etc.

Central clearing means net settlement

A “payment” from one person to another takes places on the back end as an alteration of depository institution liabilities.



What costs and benefits does central clearing offer vs bearer asset systems? For what specific use cases could it be helpful to introduce elements of central clearing, if any?

Thank You & Questions

Circle: @circlepay | circle.com/usdc | discord.gg/buildoncircle

Me: @mud2monarch

Last point: PERCEPTION VS REALITY. TradFi has abstracted away much of the complexity and cost to the user. For example, cards sap revenue from merchants, who pass on costs, but consumers love cards. Crypto might build better backend infrastructure, but it also has to distribute a competitive user experience.