Università di Pavia, 2026

Crypto, DeFi, Fintech

Massimo Morini

Digital Economy Research Lead, ADIA Lab
Professor at USI Lugano and Bocconi University
Head of Interest rate and Credit Models at Intesa San Paolo (2008-2019)
Chief Economist at Algorand and Cardano blockchains (2019-2025)

Executive Summary

- Distributed Ledger/Blockchain tech is an evolution of bank ledger money and assets
- It is also an evolution of Internet tech, and could be a foundation for long overdue digital identity
- Regulations like MiCAR are too conservative for this tech, and the Digital Euro design misses some points
- Blockchain tech allows more efficient automated risk management than traditional finance, but this has happened only in DeFI
- Recent Stablecoin regulations addressed blockchain as a new asset class, but is not progressing and looks like a broken promise
- Tech like zero-knowledge proofs that helps make blockchain scalable could be an answer to some of the challenges of AI

LEDGERS: A LONG JOURNEY FROM BANKS TO BLOCKCHAINS

- Around 3000 BC, Mesopotamians began using clay tablets to keep an account of goods stored in the temple's warehouses of the first cities. It's the beginning of accounting - *single entry accounting*, reporting quantities of goods in and out of the warehouse – but also of writing, numbers, arithmetic.

- In the Renaissance, *double entry accounting* is developed, adding giver and receiver (credit and debit) to each entry. This makes verification easier and allows multiple accounts and interconnected ledgers. This creates modern banks and dematerialized money, now represented and transferred through bank ledger entries, triggering the expansion of global trading and lending.

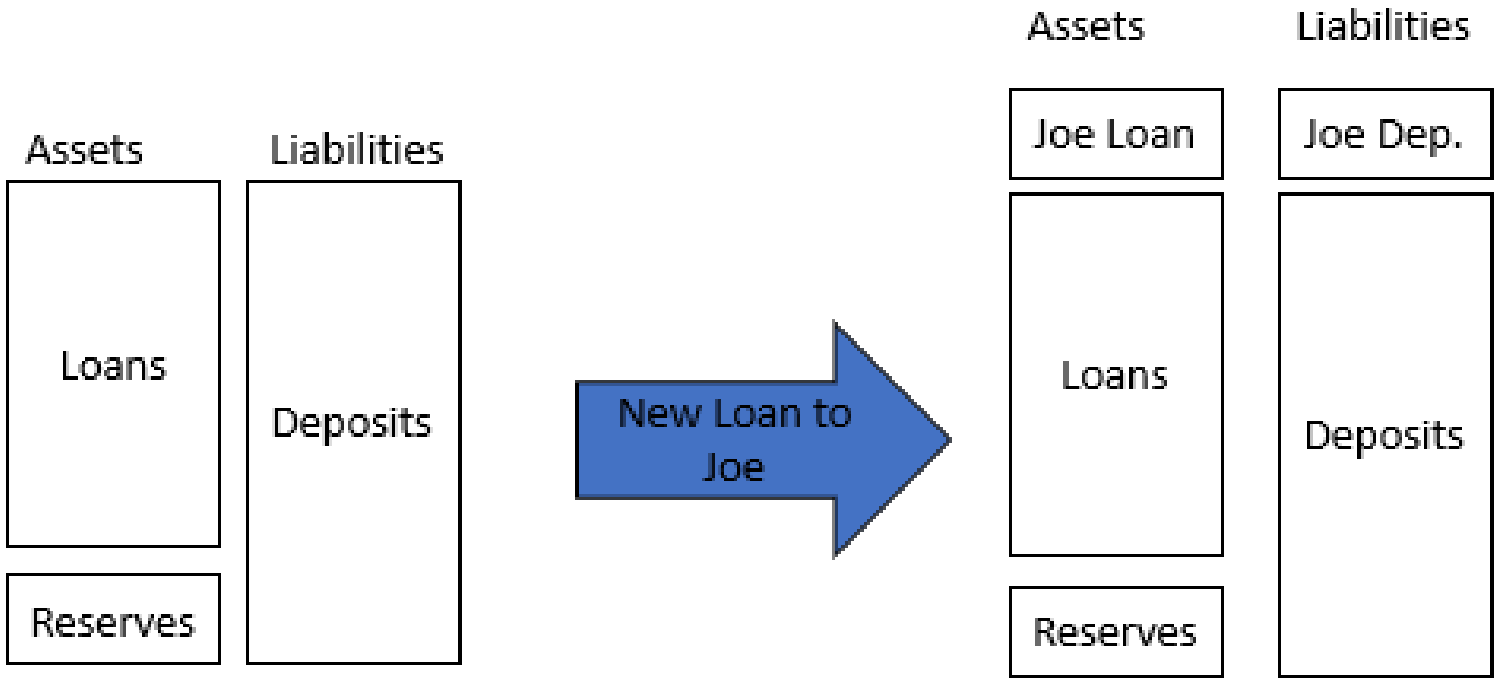
- From 1989 (Yuji Ijiri) to 2005 (Ian Griggs) *triple-entry accounting* is proposed: adding digitally signatures to each ledger's entry. This is implemented in 2008 by Satoshi in a public immutable decentralized ledger, the Bitcoin Blockchain. It creates a digital asset with all balances and signatures on a shared ledger, allowing ownership and trading without external info or intermediation.

- From 2008: *smart contracts* extend capabilities, sustainable versions like *proof-of-stake* blockchains are introduced, digital assets and *DeFi (Decentralized Finance)* are introduced at same time as *DAOs* and *Layer-2s.*

Unlike bank deposits, blockchain enables digital money independent from creating credit, that transfers in real time without intermediaries, neither correspondent banks nor central banks.

Understanding this requires reminding a few fact about commercial bank money

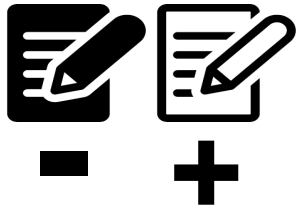
How banks create Money



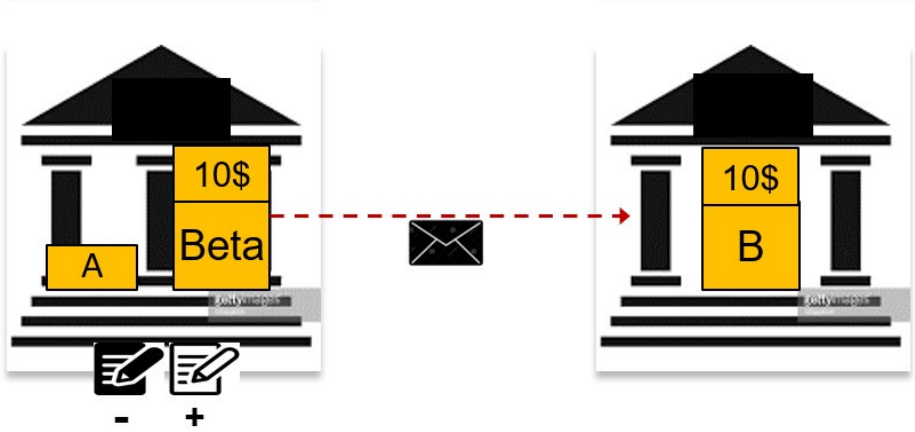
"Commercial banks create money, in the form of bank deposits, by making new loans… not typically do so by giving them thousands of pounds worth of banknotes. Instead, banks credits the company's bank account with a bank deposit of the size of the mortgage…both sides of the commercial banking sector's balance sheet increase as new money and loans are created". *McLeay et al. 2014, "Bank of England: Money in the modern economy"*

How banks transfer Money

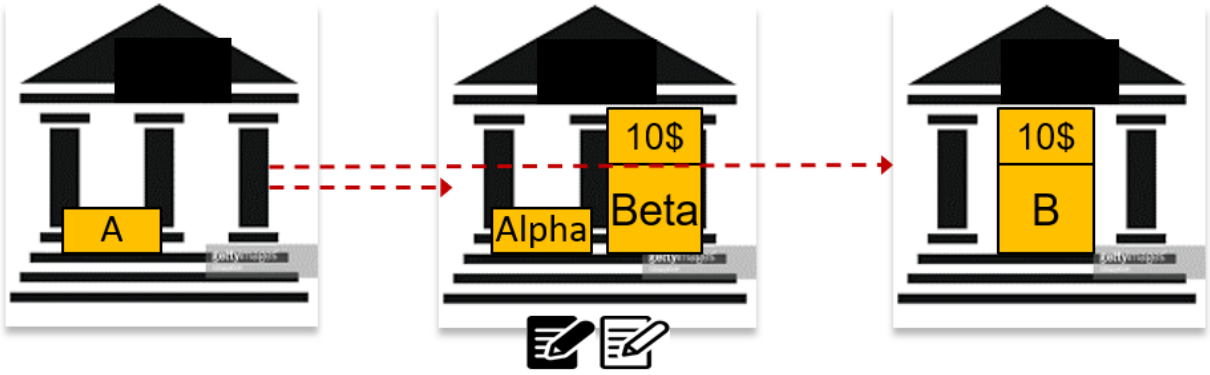
Transfer money to an account held at the same bank is simple double-entry accounting on one internal database:

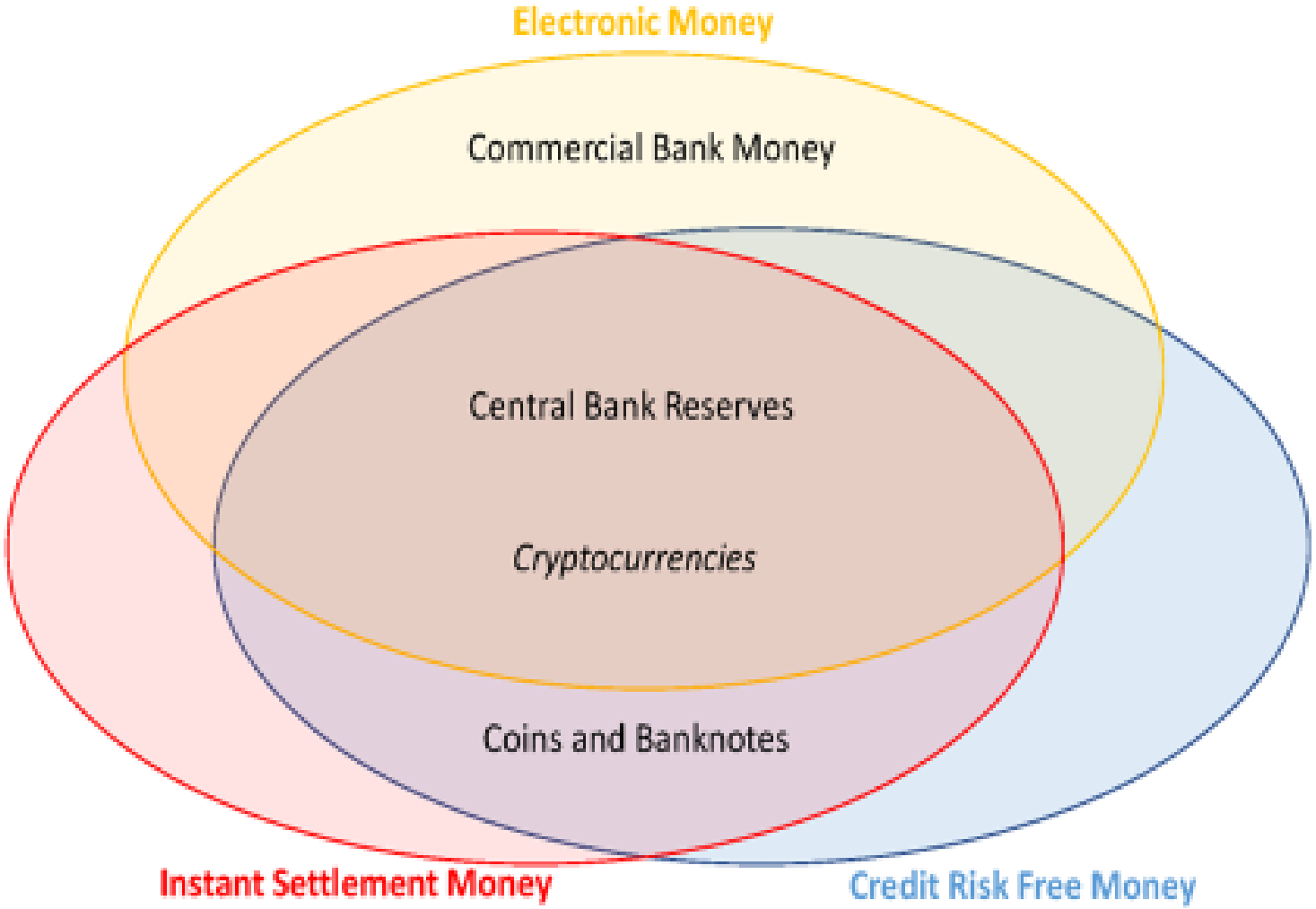


Transfer money to an account held at a different bank is much more complex (correspondent banking):



Things get even more complicated when the banks do not have a correspondent banking relation:





But research in the field did not start to change banks. The original issue was addressing some features of the internet that made it quite dangerous if used, beyond its nature of a network of information, as a network for native digital value

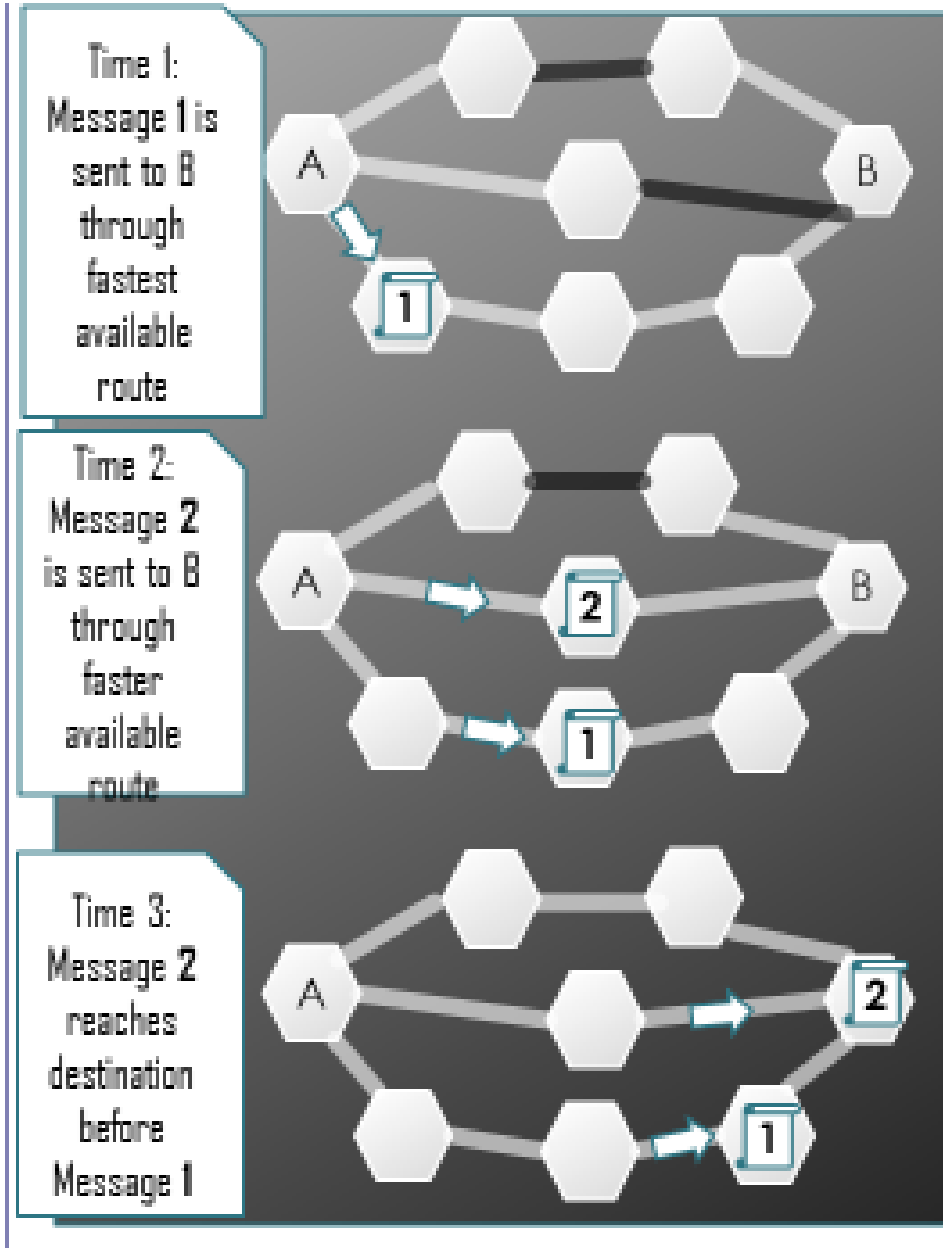
FROM INTERNET TO BLOCKCHAIN

Internet is a wonderful network for information, but some features make it a bad network of value.

1. **A client-sever architecture** that, in spite of a decentralized low-level layer, makes applications normally centralized and privatized. Who owns the servers controls everything.

2. **Lack of a layer of identity** to use globally and persistently, particularly when it comes to our digital properties and rights. The web is still based on usernames & passwords.

3. **Lack of an objective time-stamping**, and of an objective order in the transfer of information. An obstacle when messages are transactions.



FROM MONEY TO CRYPTO

Three pillars of blockchain

1. **A Peer-to-peer decentralized Ledger enables users' ownership and control.**

2. **Public-private keys provide a persistent identifier, and allow digitally sign transactions**

3. **A consensus algorithm allows to order transactions with unique time-stamping and sync the network**

This makes the Internet a network of value and incidentally gives rise to assets that can now be very volatile and not yet governed, but from a technical point of view has very good properties

Some issues with Regulations

- **MicA: «Crypto-assets are a digital representation of a value or of a right that is able to be transferred and stored electronically using DLT or similar technology**
  - But Bitcoin, or cryptos, or DeFi products based on Smart Contracts, are not «digital representations of a value». They are digital values, directly.
  - Transferring a token is a technical possibility allowed by PRIVATE KEYS. This is true even when key are stolen so there is no correspondece with the legal concept of «right».

- **MiCA: "Regulation should be guided by the principles of same activities, same risks, same rules" and of "technology neutrality"**
  - If properly applied, decentralized tech necessarily changes activities and rules. The first principle favours products that do now use the tech in an innovative way.
  - Tech neutrality makes not sense for disruptive technology. For example, MiCA regulates "operators of the trading platforms" that do not exist for public distributed ledgers

A worrisome Red Flag

This reminds a bit of the famous «Red Flag Act» that delayed the Automobile industry in the UK for long enough to stifle it for ever, giving the US, Germany, and other European countries an everlasting advantage.

In 1865 a law required all road locomotives, which included automobiles, to travel at a maximum of 4 mph in the country and 2 mph in the city, and most vehicles to be accompanied not only by a driver, but also by a “stoker” (a role needed on oldsteam locomotives, completely useless with cars, that were almost immediately powered by petrol) and even by a man carrying a red flag that was required to walk in front of road vehicles. The law was repealed only in 1903.

Chart from Perez (2002) “When the automobile was first invented, the first examples were like motorized versions of a horse and cart. It took time for people to grasp the possibilities of the new technology, independently of what had gone before”.

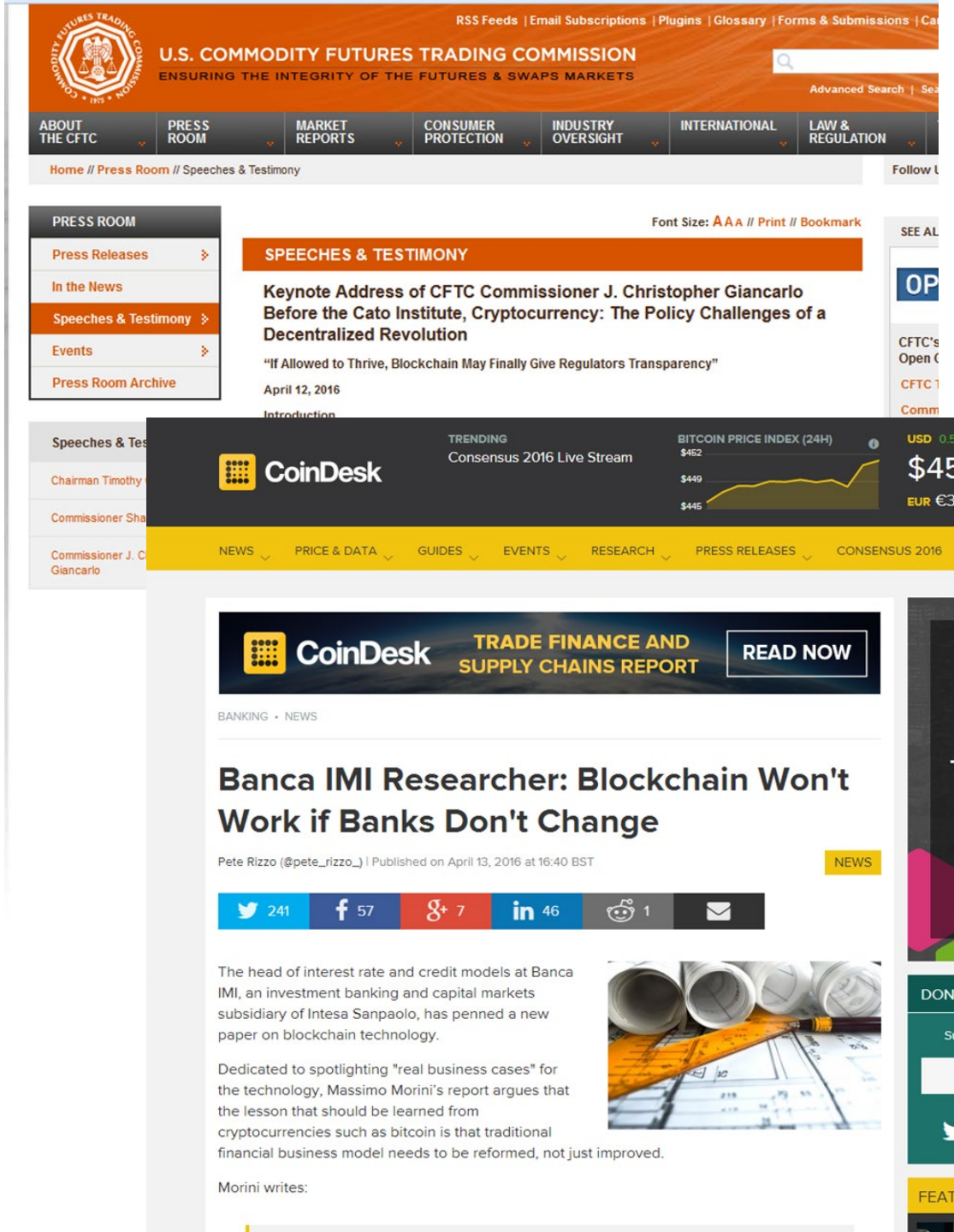
AN EARLY QUEST FOR DECENTRALIZED FINANCE

In the aftermath of the crisis, many problems of financial products came from credit risk: lack of trust among banks, higher funding costs, counterparty default risk, extra capital to cover risks

We know collateral has been the main answer

-Variation Margin: equal in every moment to the value of a derivative, through frequent and efficient collateral exchange

-Initial Margin: overcollateral, segregated and made immediately available to the counterparty at defaults



But collateral does not work as planned:

Technical Complexity. Top collateral agreement requires mastering liquidity across special accounts, access to all market data, experience with valuation/risk models. Corporates and institutions usually don't have these things, only large banks.

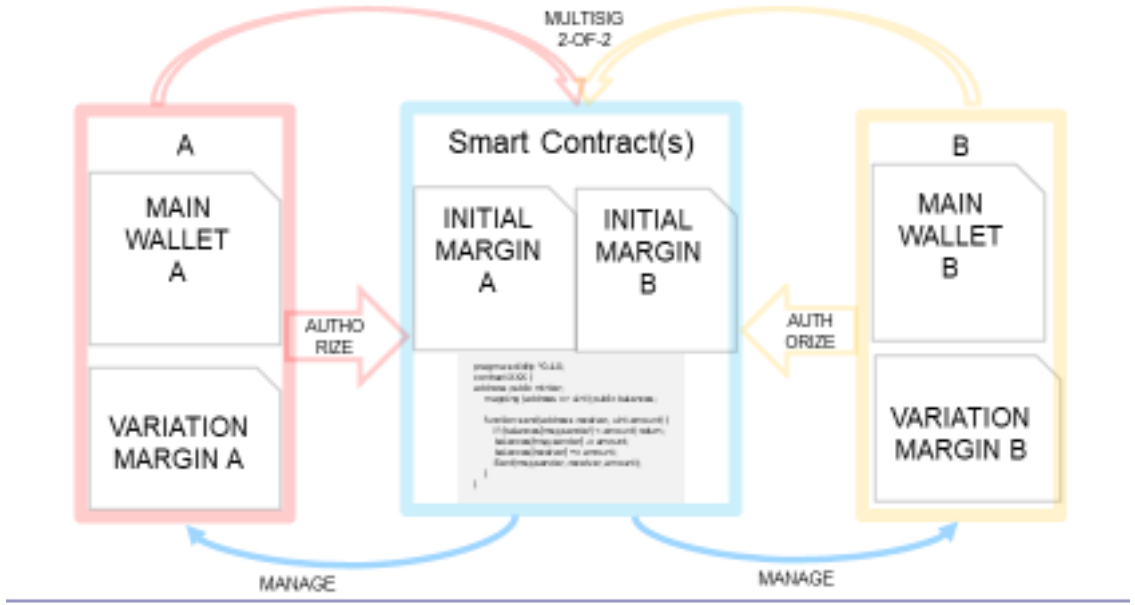
Collateral Misalignments. Even banks use different data and models, and at times can interpret contracts differently, leading to costly reconciliation processes.

Settlement Delays. Collateral settles in 1 to 3 days. Collateral received is aligned with the market of 1-to-3 days ago, not with current market.

Default Uncertainty and Delays: if a counterparty stops paying, the process do declare default takes several days. Then a complex valuation procedure (close-out) is started, adding additional delay and uncertainty.

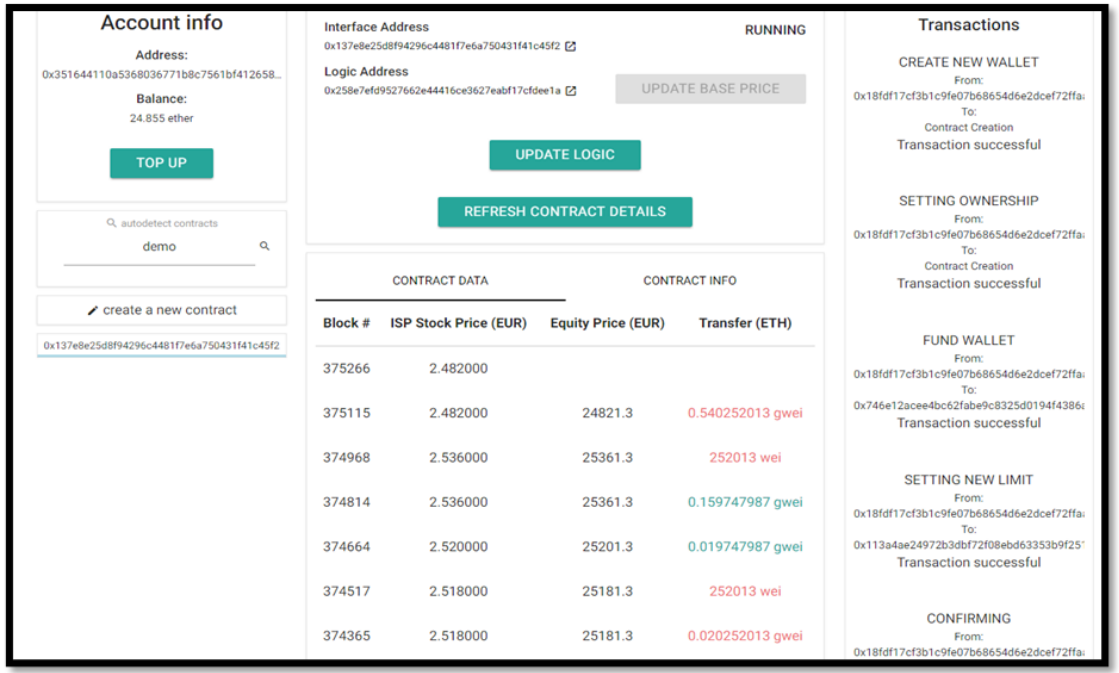
Why looking at blockchain technology?

- **Same tech platform for everyone**
- **Smart contracts execute their code directly**
- **More efficient settlement by consensus**
- **Automation and programmability**



In the Smart Derivatives Dapp, a system of smart contracts managed collateral, treating Variation (delegated to Smart Contract but under full user control) and Initial Margin (overcollateral segregated by smart contract) separately.

When there are payment or collateral delays, after a grace period there is automatic unwinding and transfer of variation margin and right part of initial margin to cover losses.

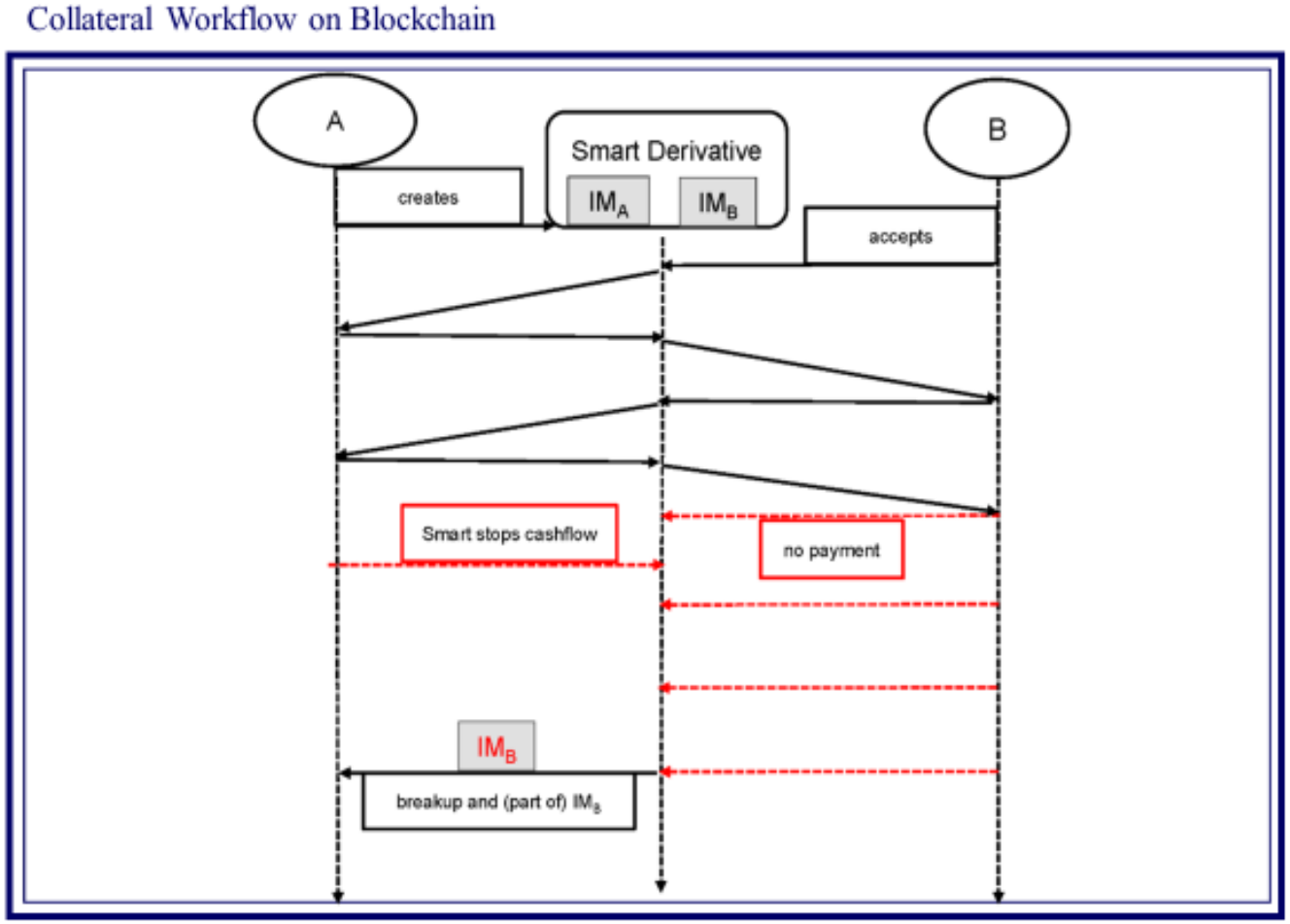


How that could solve the issues:

Technical Complexity: blockchains level the playing field, same payment and account technology for all parties.

Collateral Misalignments: all parties agreed on the smart contract code, ruling out misalignments

Settlement Delays: Delays down from few days to few minutes. Costs and time depend on protocol.



Default delays and uncertainty: smart contract covenants and unwinding reduces dramatically delays and uncertainty.

The idea of automated (over)-collateral and unwind was adopted by DeFi for basic borrowing-lending products, and currency stability by collateral. Makes some sense.

From decentralizing finance to Decentralized Finance (DeFi)

Lack of digital money, protocols, regulatory uncertainty prevented tests by banks from becoming reality. DeFi implements these principles easily

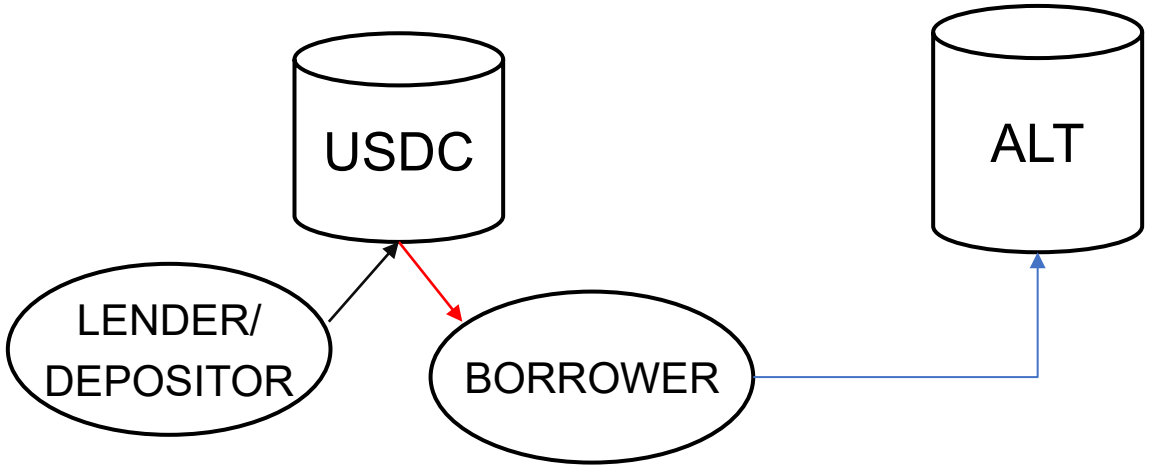
- **Transparency and Inclusion (open and same conditions for all)**
- **Level-playing field (same platform and smart contracts for all)**
- **Immediate Settlement and Finality (in protocol with speed, finality, and low tx fees)**
- **Over-Collateral managed by Smart Contracts via automated Risk Management**

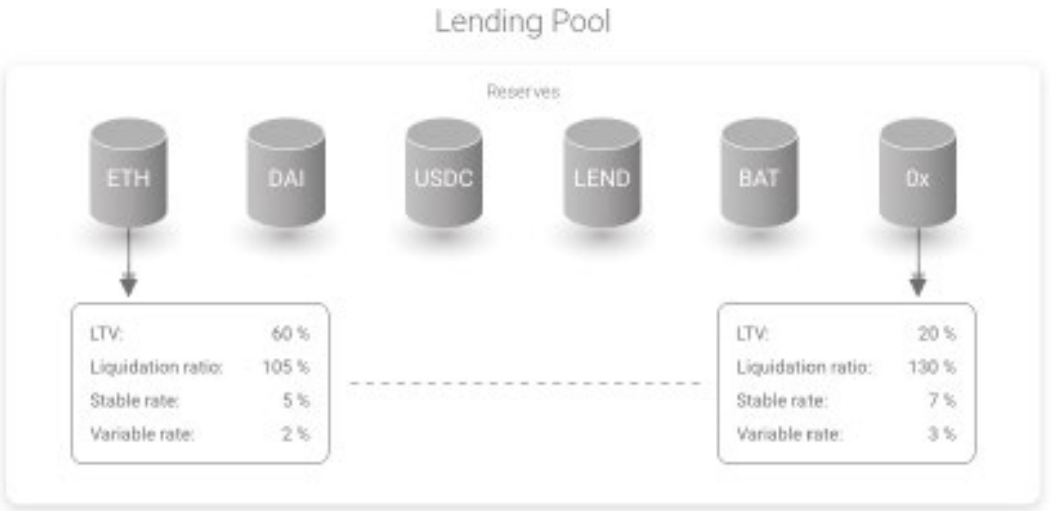
Default risk is so small that not knowing the borrower is ok. But we have new risks

- **Technical Risk (bugs in dapps)**
- **Financial Risk (complexity and vol)**
- **Not all protocols are the same in terms of fees, speed, forks.**
- **Not all projects are reliable (rug pulls, centralization, no transparency)**

1st risk is disappearing. 2nd would be reduced by institutional presence, that could eliminate the third one. The 4th one could be addressed by regulators and central banks.

Decentralized Borrowing-Lending

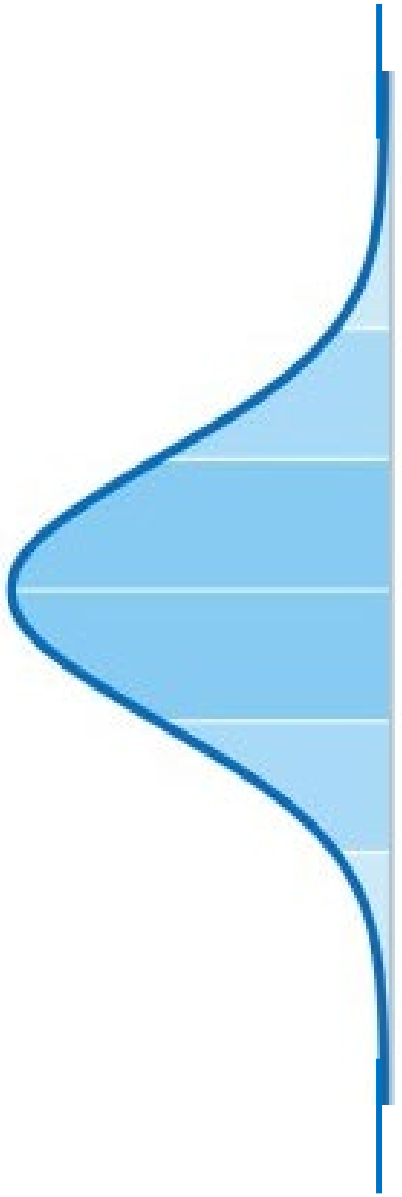




The fundamental idea of Borrowing-Lending in DeFi is that Lenders deposit a currency that Borrowers can withdraw as a loan guaranteed by Borrowers depositing other coins as collateral, for a larger value.

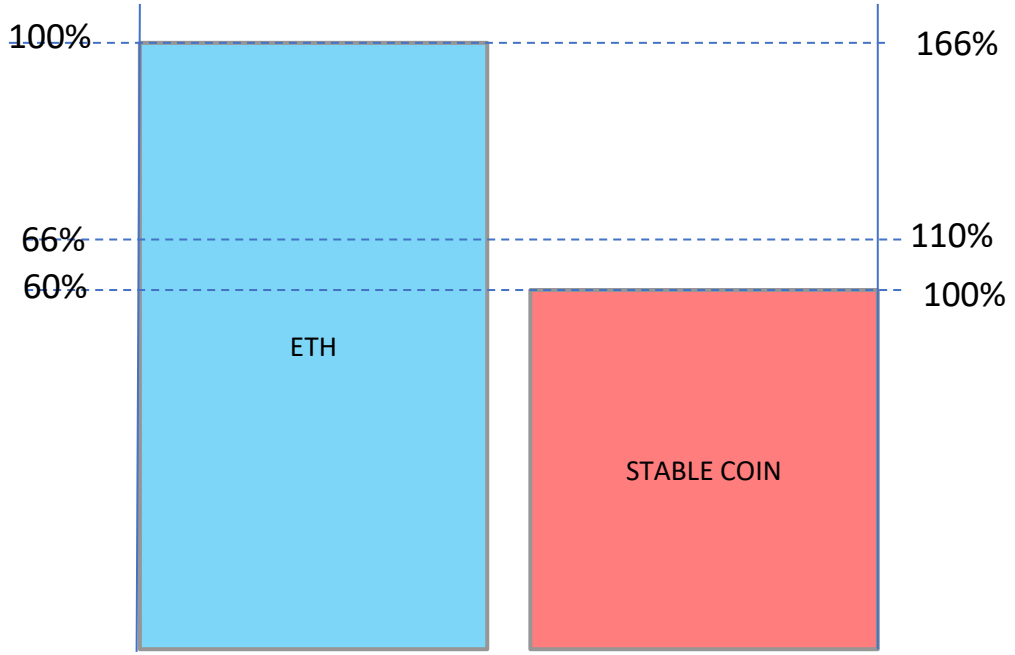
This allows borrowing-lending to happen even if the lender does not know the borrower and has no guarantees on its solvibility. In fact they have collateral.

In the last 2 business model, the same Collateral Automation seen for Derivatives is applied, see example:



Collateral is 166%=1/60% of the borrowed asset. This covers rather large swings of value.

If collateral falls below 110% of the borrowed value, collateral will be liquidated and the value given to the lender to make sure he has no losses. Liquiditation is decentralized and can be just for a part of collateral and loan, till collateral is again at least 110% of borrowed amount.



DEX, Lending, Algorithmic Coins

In a **decentralized exchange (DEX),** everyone can be a Liquidity Provider by putting two assets in a liquidity pool in a desired proportion. This proportion works as the exchange price. The market participants buy and sell assets according to their needs, altering the liquidity pool composition and therefore the exchange price. Liquidity providers will earn fees and will suffer market-makers-like 'impermanent losses' when the price changes, based on smart contract algorithms.

In a **decentralized lending protocol**, borrowers have to over-collateralize their borrowing of Asset A with another asset B. For example, borrowing 100 digital dollars can require $200 worth of a cryptocurrency, with margin calls if collateral loses value, till automatic unwinding using collateral to prevent losses. Smart-contract-based algorithms manage pooling of different borrowers, over-collateralization and liquidation based on collateral value.

Decentralized stable coins should be based on the same principle: overcollateral contributed by creators to keep a stable value for a created asset. 100 units of a created dollar coin may require at least $200 worth of collateral, with automatic redemption if collateral falls below the 2X overcollateralization. Reducing collateralization requirements can make the model fail (Terra-Luna example). Marker DAO, based on the above algorithms, was created in 2017 and still largest DeFi.

The new USA regulated stablecoins

In July 2025 we see something different. USA regulated stablecoins on public chains as a separate asset-class with bipartisan approval of GENIUS Act, making them a new form of legally protected digital cash for settlement, accounting and collateral.

Genius Act

- Stablecoins as cash for
  - Accounting
  - Settlement
  - Collateral
- Treasuries as Reserves
- Reserves Transparency
- Priority in default
- No interest to users

Much easier cross-border transactions. Risks for AML?

Cash equivalent to commercial bank money for finance.
Disintermediation Risk?

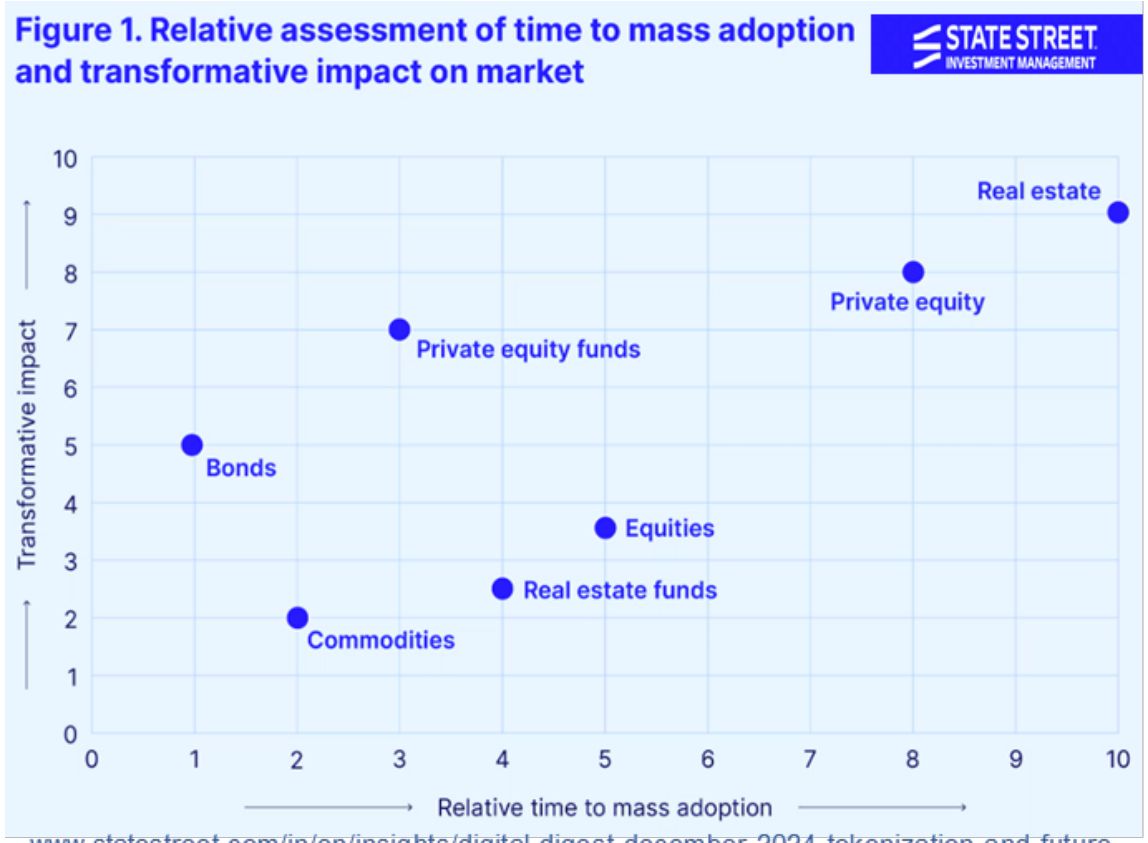
Seniorage to private issuers. Monetize treasuries easily.
Risk of exploding public debt and systemic risk?

Priority helps specialized stablecoin issuers.
Less good for big tech (Meta) and banks?

This gives back advantage to banks. But what about staking?

From Stablecoins to Tokenization

- This could eventually help Tokenization of traditional financial products or commodities:
  - regulated digital money will bring liquidity on public chains
  - allow real-time on-chain convertibility
  - serve as cash leg
  - provide a basis for compliant tokenization of different assets
  - Genius itself is an effective approach for the tokenization of treasuries
- Yet, it seems a broken promise. The operative guidelines are not coming out as expected and the necessary sister regulation, the Clarity Act, is not progressing. Some good news came out on March 20, 2026…



www.statestreet.com/in/en/insights/digital-digest-december-2024-tokenization-and-future

THE CBDC CONUNDRUM

CENTRAL BANKS (ECB, BoE…):"If cash were to disappear, the general public would not have access to central bank money anymore. Central bank money must be made available in digital form to all."

Reasonable, but won't it make depositors to flee banks, being digital and fully guaranteed by the state? Isn't it going to increase dramatically of SVB-style bank runs?

"The digital euro would be issued as a digital version of cash and conceived to preserve, rather than disrupt, current monetary arrangements"

-"Effective limits to the amount of digital euro individual users can hold: BoE "Uk citizens will be allowed 10-20k digital pounds per person" "ECB: for European Citizens, no more than 3000-4000 euros each" ABI "Too much, if like cash just 600-800 euros per person allowed"

-"Supervised intermediaries (banks) will open digital euro accounts or wallets and make the associated payment operations, as is currently the case for the bank accounts (ECB)"

- "The CBDC will likely be a centralized App managed by the Central Bank (ECB)"

THE CBDC CONUNDRUM

This may awkward, could still create a conflict with deposits, being too similar, and misses all the tech changes that could make it really a "digital cash"

- Digital identity through digital signatures
- Transactions and custody not (or at least less) dependent on intermediaries
- Immediate Settlement
- A decentralized setting

This features woud be available if the tech was blockchain on an institutional network

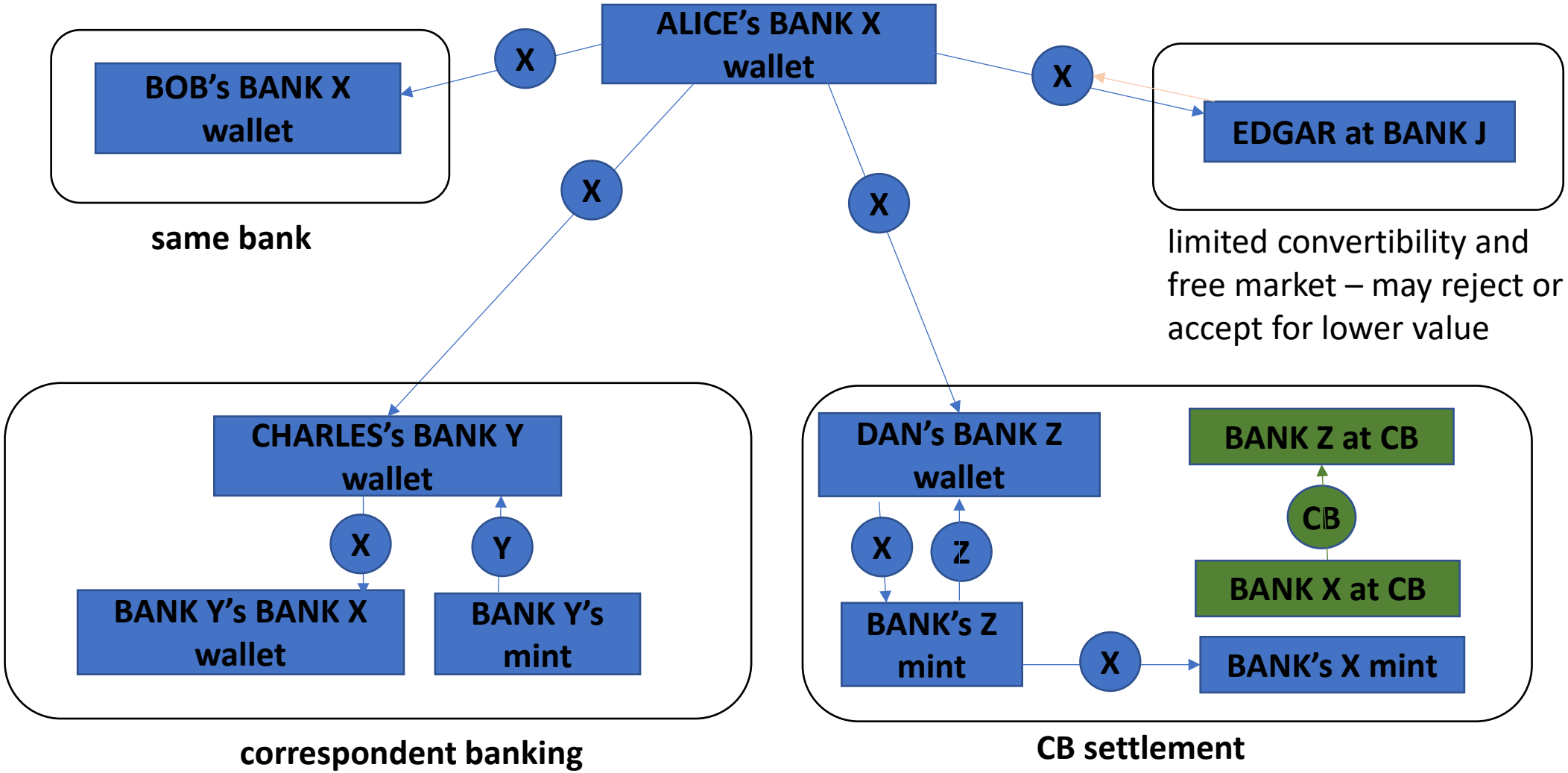
But in this case, won't it make depositors to flee banks, being digital and fully guaranteed by the state? Isn't it going to increase dramatically of SVB-style bank runs?

No. Risk of losing or being stolen the keys (similar to actual cash), usage will never be as easy as intermediated usage, privacy would be different. Banks would become custodians for most people and most amounts. And deposits would remain safer, easier.

And as for the doing away with credit cards for instantaneous payments, even just wholesale DLT would allow ECB with banks to offer a mean of payment using instantenouys settlement and central bank money. Limits would apply to card, not money.

TOKENIZING DEPOSITS

Tech could also be used for tokenized deposits, that could be as hybrid as desired due to the intermediation of regulated entities.



Thank you!