# Blockchains, Banks, CBDCs, and DeFi

Massimo Morini

Where we are now?

- Terra and FTX shaked the blockchain world

- SVB and Credit Swiss shaked traditional finance

- Blockchain tech growing stronger, more and more DeFi and Digital Assets

- Issues due to lack of standards and bad CeFi

- Banks keep financing the economy and are more and more interconnected with central banks and governments

- Yet their model is 500 years old and sclerotic

- Never been a better moment to dialogue and get the best of both worlds
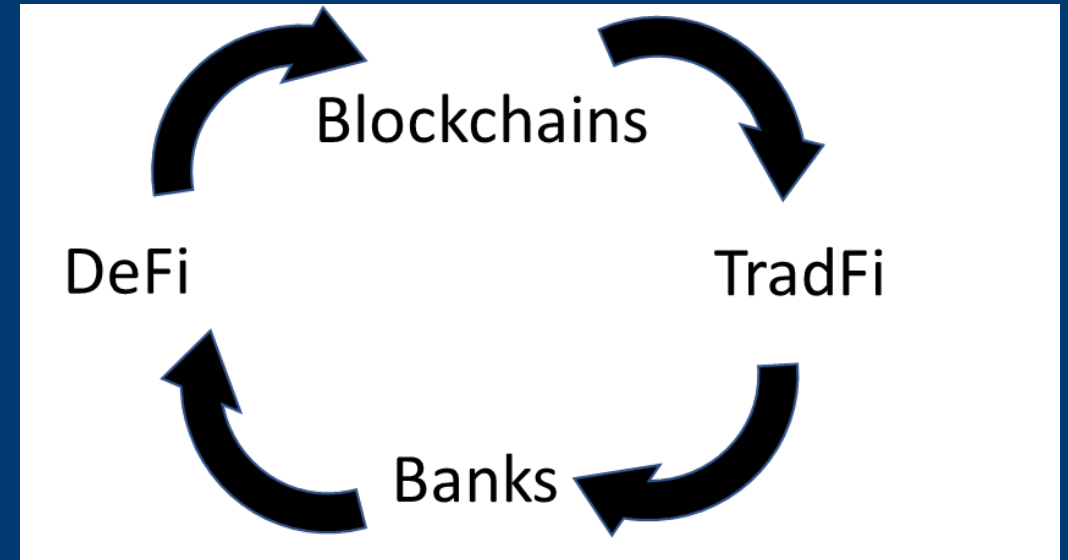
A LONG JOURNEY

- Around 3000 BC, Mesopotamians began using clay to count their agricultural goods. It's the beginning of writing, of numbers, of accounting (single entry).

- In 1494 during the Renaissance double entry accounting is developed. Bank ledgers start allowing international transactions. It is the 1st digitization of money.

- In 1989 Yuji Ijiri invents triple-entry accounting: each ledger's entry is digitally signed. In 2008 'Satoshi' creates the 1st public immutable decentralized ledger.

- Few years ago: a sustainable and efficient mechanism, Proof of Stake, is brought to high standards, smart contracts become effective, NFTS and DeFi can run fast with immediate finality

3

We have not yet transitioned to the new tech

3 kinds of money:

- *Currency* consisting of banknotes and coins
- *Commercial bank money* comprised of bank deposits
- *Central bank reserves* used exclusively by banks.

Commercial bank money is more than 90% of money.

Banks are not intermediaries that take deposits from the public and lend them out to companies.

They decide to lend out, and they create deposits out of this choice

How <u>Banks</u> really create money
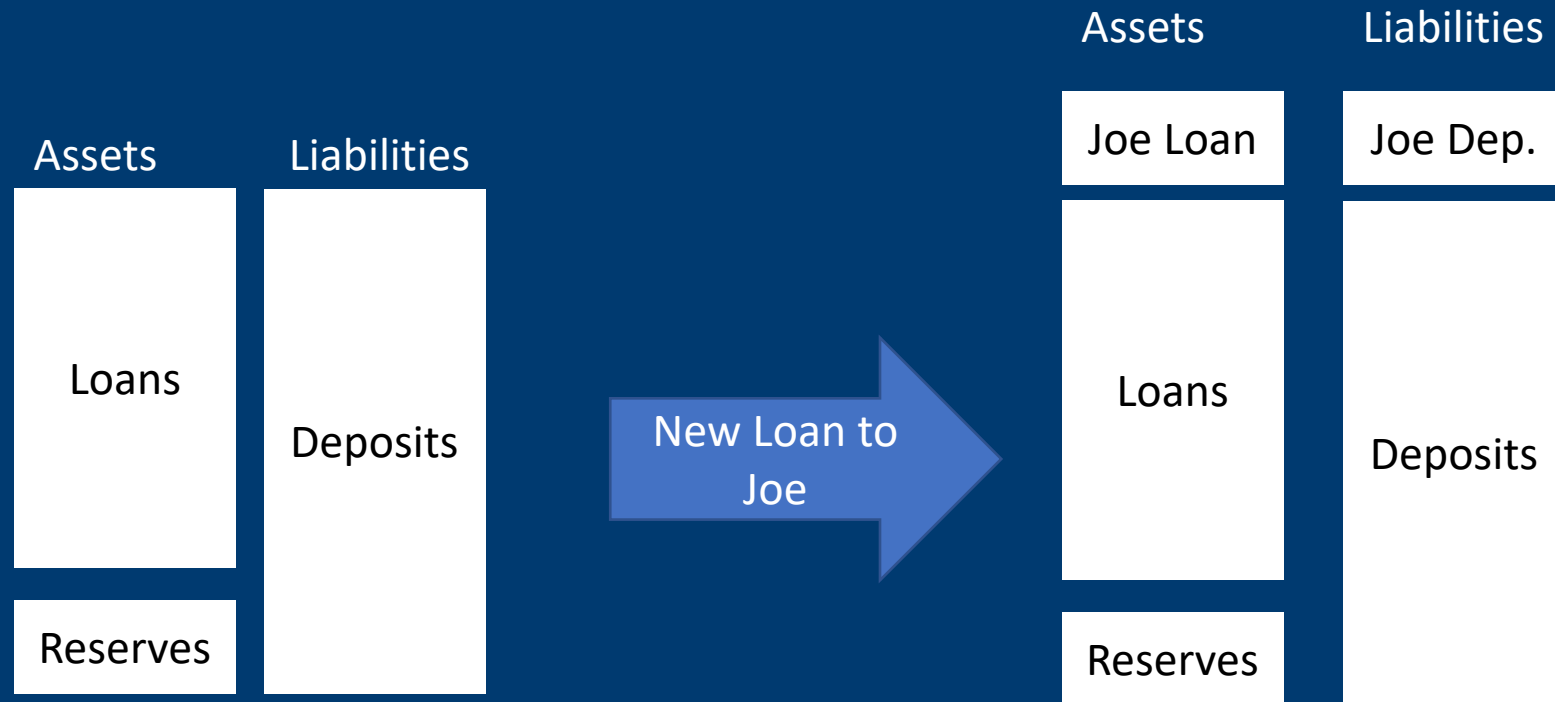
- The reserve is no rigid limitation, because normally reserves are, supplied 'on demand' by Central Banks to commercial banks in exchange for risky assets on their balance sheets.

- A risk of default exists since liquid liabilities are backed by risky illiquid assets, as confirmed by the state guarantee itself.

How Banks money is transferred

- **To an account held at the same bank**: just updating one database. Fast and inexpensive

- **To an account at another bank**. If A with account at Alpha bank wants to send money to B with account at Beta bank, and the bank are in correspondent banking relation, then Alpha has an account at Beta and Beta has an account at Alpha (Nostro-Vostro accounts in the international payment jargon).
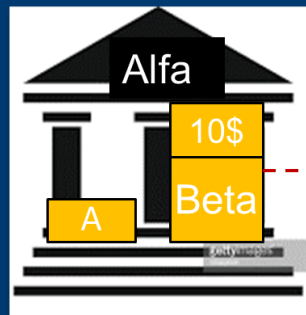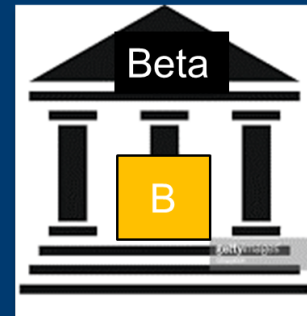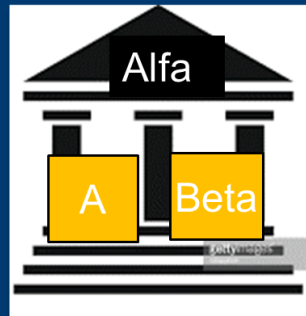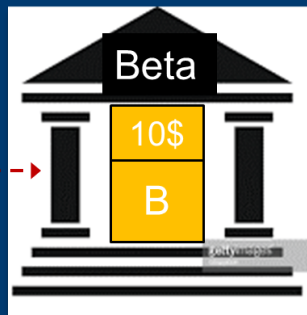
- **Transfer money to a bank which is not in correspondent banking relation is more difficult.** The two banks have to find an intermediary
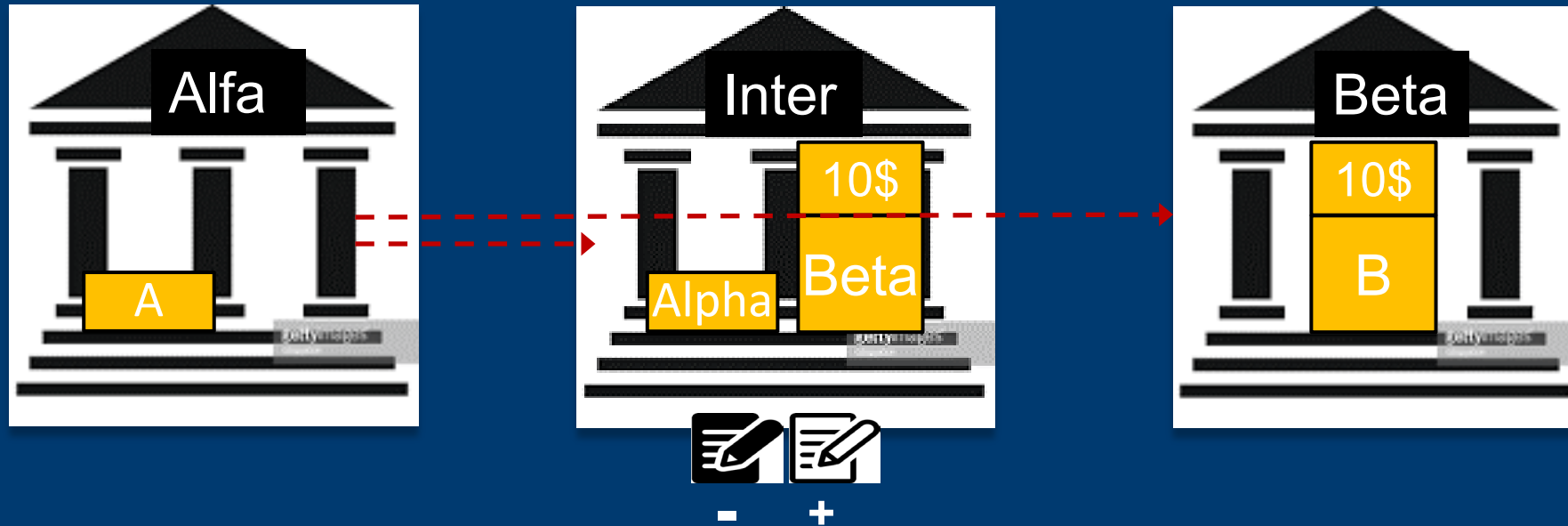
- Alpha bank will first send a message to Beta bank announcing the incoming transfer. Then Alpha can reduce the account of A and ask the Intermediary bank to reduce its own (Alpha's) account at the Intermediary bank and to increase the account of Beta, asking Beta to increase B's account.
- For international trades, messages go through SWIFT system. KYC and AML controls have to be done at all steps. Banks have to manage the credit and liquidity risk of all these accounts, will use EoD settlement at each step.
- Settlement is slow and fixed cost is high, reasonable only for large payments.

Central Bank Money

Central Bank electronic money changes the picture: interbank settlement becomes more similart to cash.
In the US, with Fedwire, its increasing usage for interbank settlement may explain the modern fast runs.
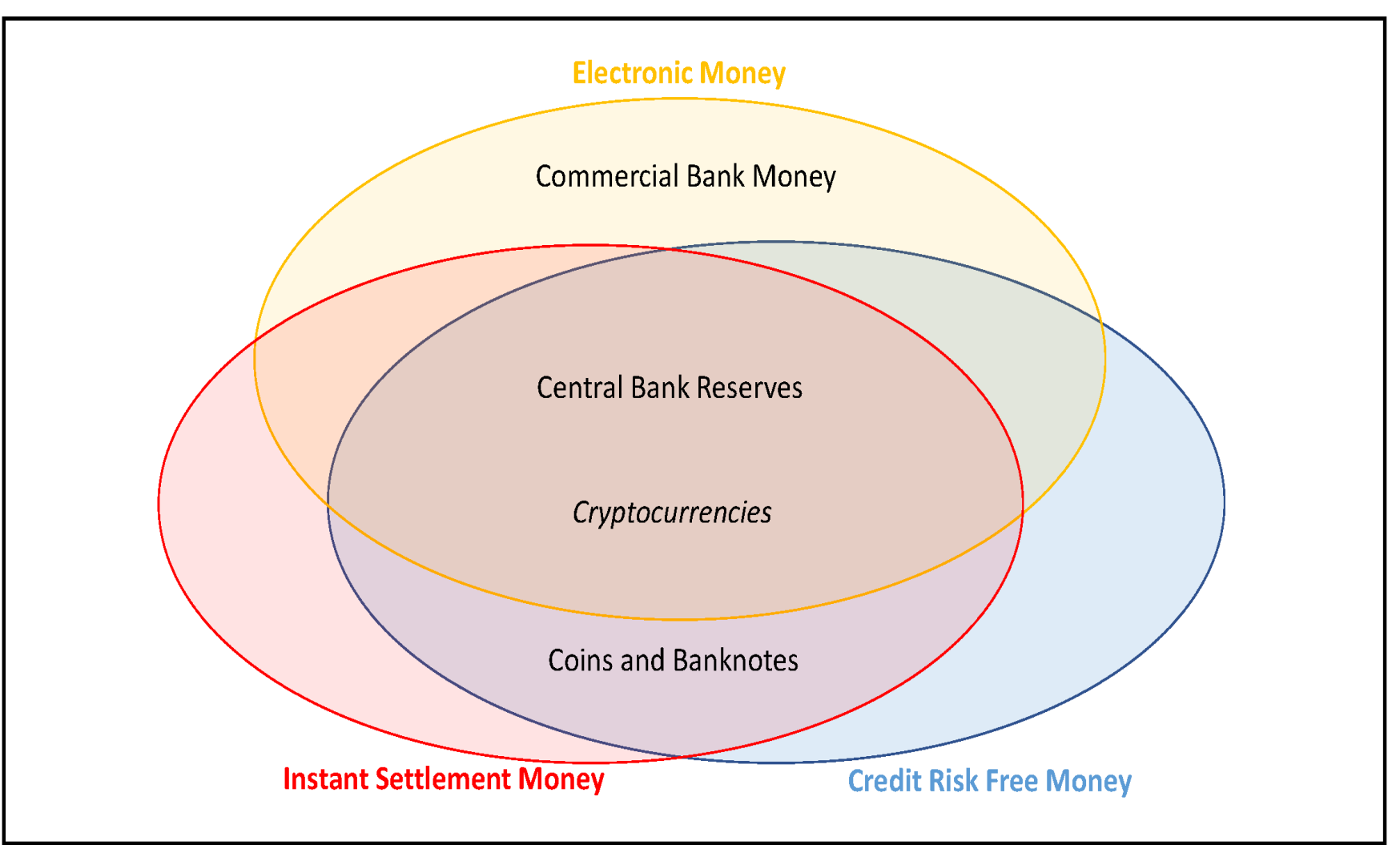
When banks have accounts at the same central bank, they can transfer central bank money through the central bank system.

It is an RTGS system (real time gross settlement). For the Euro area, it involves several countries and it is called Target 2.
•Bank A and Bank B both have accounts with a central bank
•Bank A submits the payment instructions to TARGET2
•Bank A's account is debited, and Bank B's account is credited – the payment is settled
•TARGET2 transfers the payment information to Bank B

See recent paper linking central bank money and Algorand blockchain to eliminate counterparty risk in fiat-crypto transactions (atomic swap or Delivery-vs-payment)
https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2022-026/index.html?com.dotmarketing.htmlpage.language=1

Different Forms of Money, and their Properties

FROM INTERNET TO BLOCKCHAIN

Internet is a wonderful network of info.
Not yet of value.
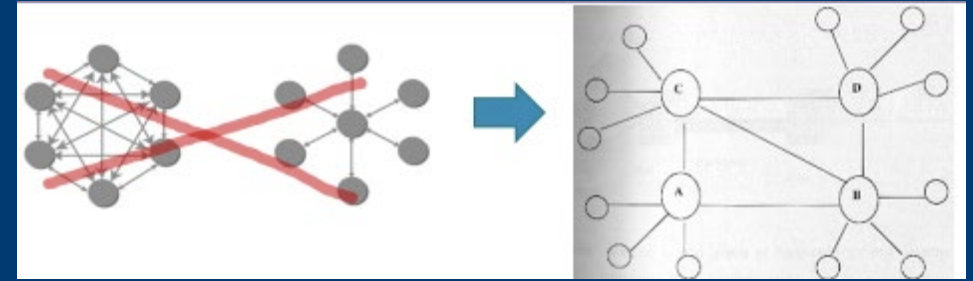
1. **A client-sever architecture** that, in spite of a decentralized low-level layer, makes applications normally centralized and privatized.

2. **Lack of a layer of identity** to use globally and persistently, particularly when it comes to our digital properties and rights.

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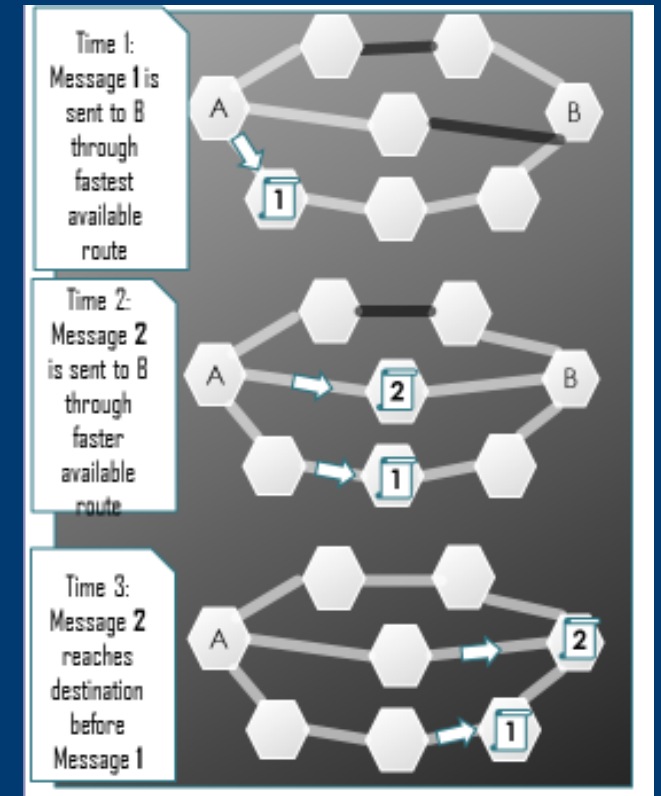
FROM MONEY TO CRYPTO

Blockchains address the Internet issues above through

1. **A Peer-to-peer decentralized Ledger**

2. **Public-private keys to digitally sign tx messages**

3. **A consensus algorithm to order transactions and sync the network**
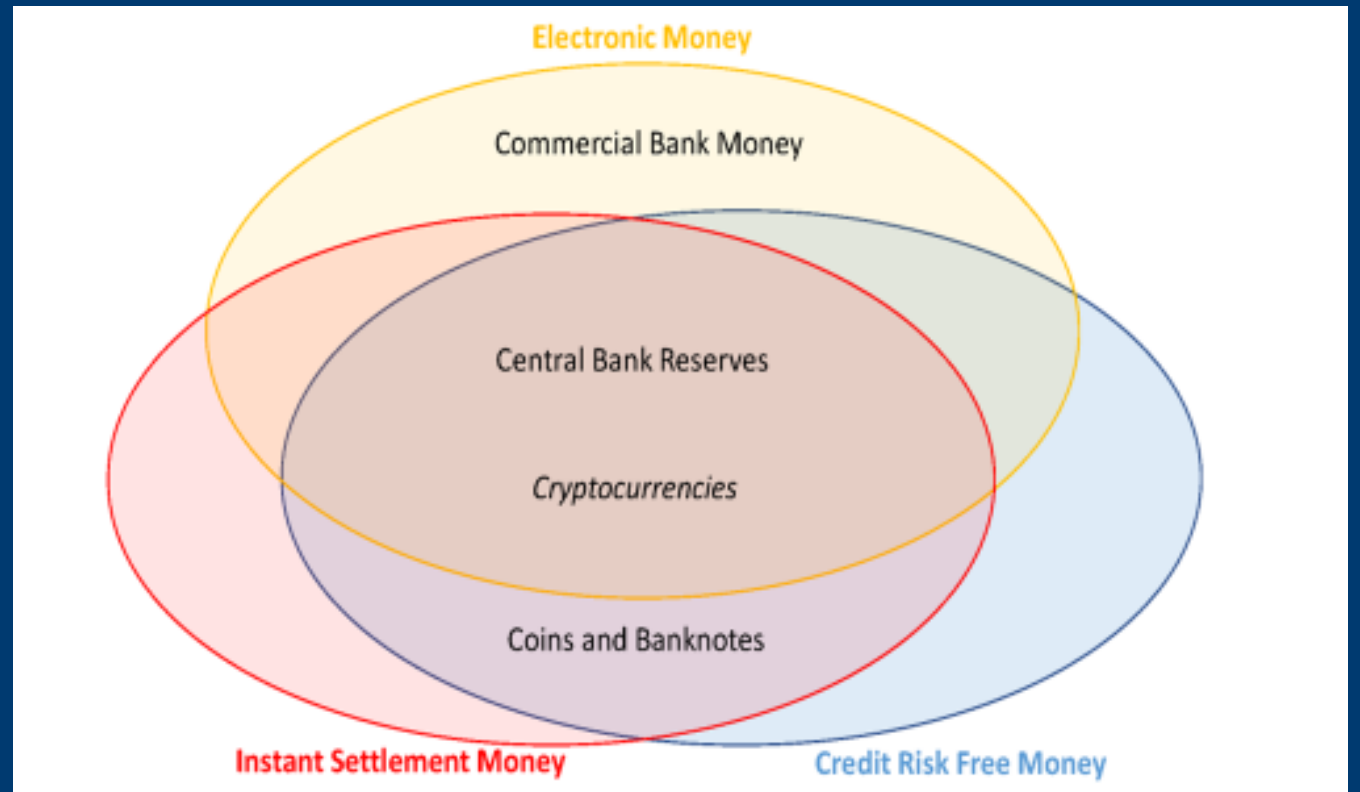
This makes the Internet a network of value. Incidentally it gives rise to assets now very volatile but with the same tech features of Central Bank Reserve money: electronic money free of credit risk and settled rapidly.

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 in all parts of the economy and society"

Won't it make depositors to flee banks, since it will be more modern and efficient, and yet fully guaranteed by the state? Isn't it going to increase dramatically of SVB-style bank runs?

"We favour a solution of continuity, where the digital euro would be issued as a digital version of cash and conceived to preserve, rather than disrupt, current monetary arrangements"

How can you obtain this?

-"Effective limits to the amount of digital euro individual users can hold: BoE "Uk citizens will be allowed no more than 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 have the contractual account management relationship, open digital euro accounts or wallets and make the associated payment operations, as is currently the case for the bank accounts"

THE CBDC CONUNDRUM

A CBDC cannot be a replacement of some features of cash

- Not for the secrecy which can be obtained by cash
- Not for the possibility to use cash also where or when tech in not available
- Yes for the lack of bank credit risk
- Yes for the possibility to do self-custody and disintermediated transactions, if blockchain is used

If the management will be given by banks with the same tech as deposits, last property is missed.

Without blockchain tech, it would be just digital money without bank credit risk, likely to crowd out deposits with a completely centralized, state-owned financial system. Will governments be able to replace banks in tuning money for financing the economy, with banks as their intermediaries? There are proposals for this (Brunnermeier's narrow banking).

If the crowding-out of deposits is prevented by state-imposed limits to ownership of money, the project will hardly succeed in a free economy.

There are a few less dystopic scenarios:
- more limited 'wholesale' CBDC on blockchain tech to give banks real-time settlement
- cash-like 'retail' CBDC on blockchain tech that naturally balances deposit features

WHOLESALE CBDC

If banks could use state-guaranteed tokenized money on a distributed ledger, they could settle also retail payments instantaneously and without direct involvement of the central bank. Incorporated in a payment system, this would male credit-cards redundant for payments.

This seems to be the more economic and less political goal of central banks in Europe.

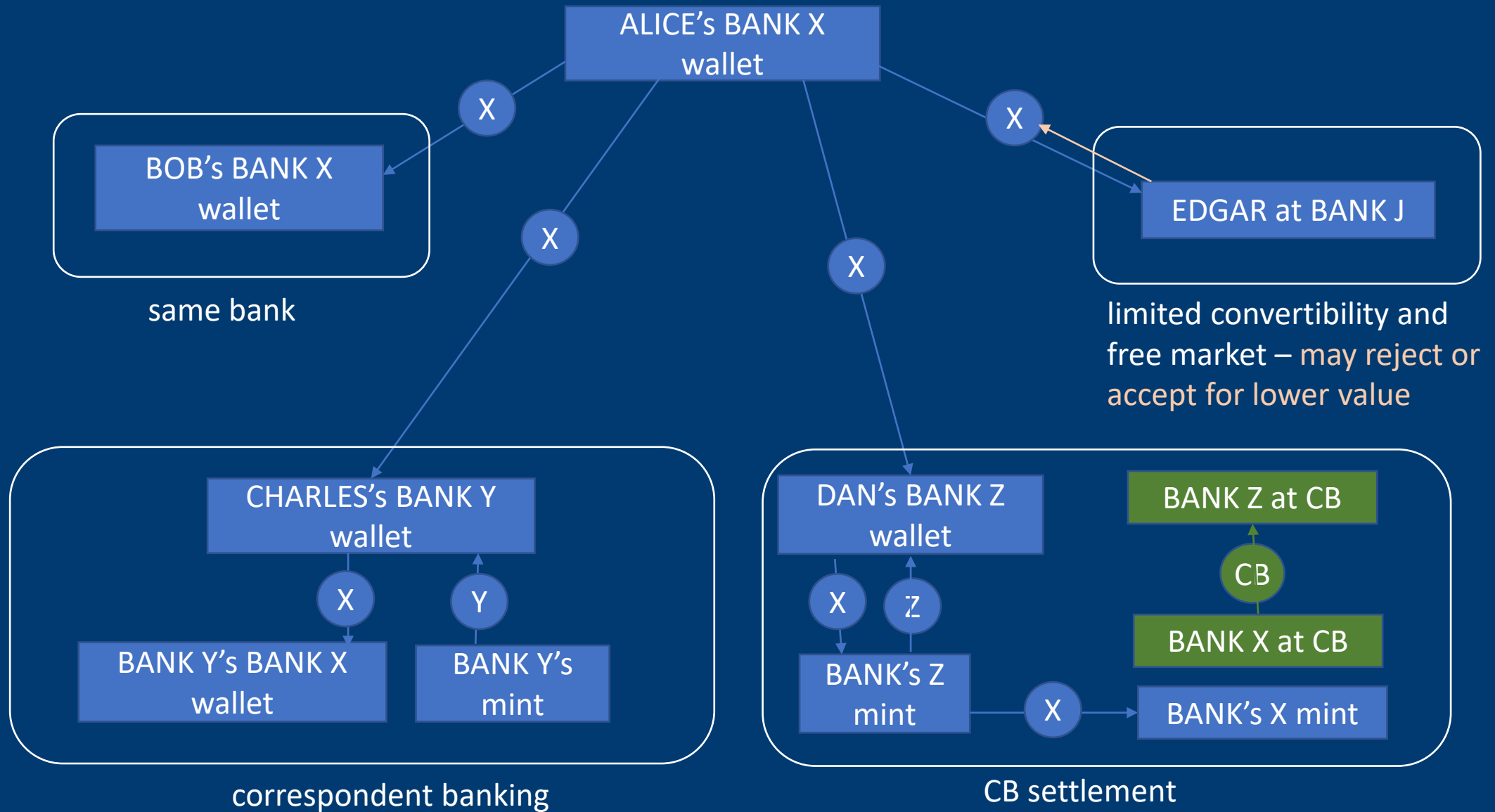In this context, unlikely that deposits remain on old tech.

RETAIL CBDC

If money is issued on a public blockchain infrastructure with individual key management and self-custody, with a link with legal identities but with the privacy features that are already technologically possible, it can really open a digital era for Europe.

It will not crowd deposits out, since the unease of self custody and the balance between privacy and transparency will keep a role for deposits.

It will create a custody business for banks and push to tokenize deposits as well.

TOKENIZING DEPOSITS

ALICE's BANK X wallet

X

BOB's BANK X wallet

same bank

X

X

X

EDGAR at BANK J

limited convertibility and free market – may reject or accept for lower value

CHARLES's BANK Y wallet

X

Y

BANK Y's BANK X wallet

BANK Y's mint

correspondent banking

DAN's BANK Z wallet

X

Z

BANK's Z mint

X

BANK's X mint

BANK Z at CB

CB

BANK X at CB

CB settlement

AN EARLY QUEST FOR DECENTRALIZED FINANCE

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

The most popular way to address credit risk in derivative products (options, swaps…) has been collateral (margin, guarantees…)

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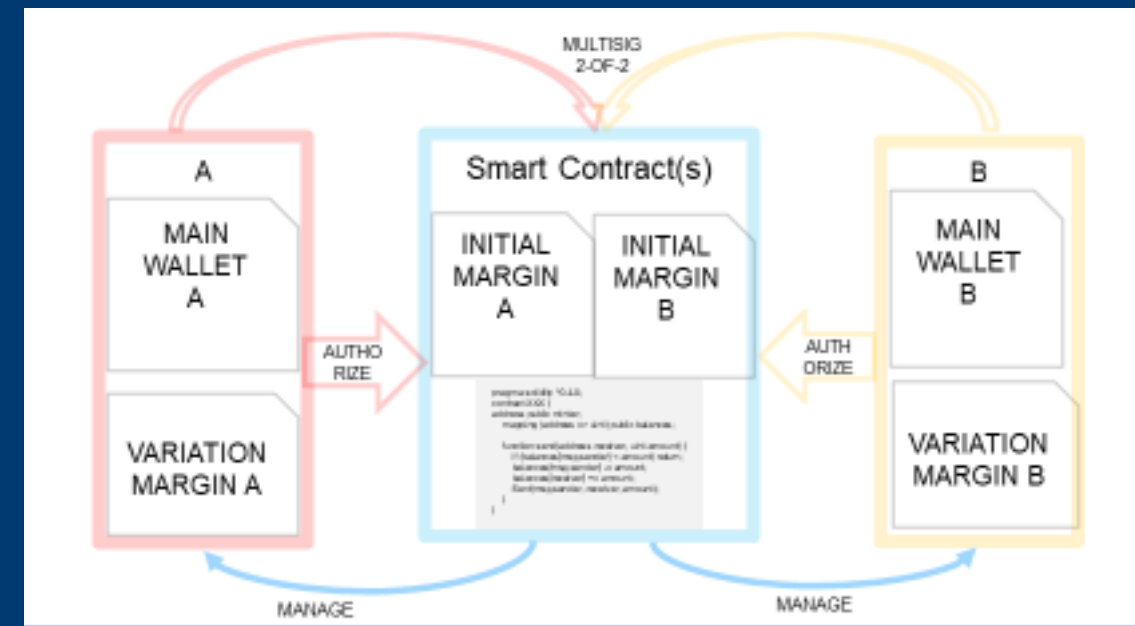
Default Uncertainty and Delays: if a counterparty stops paying, the process do declare default takes several days. Then a complex valuation procedure (close-out) is started, adding additional delay and uncertainty.

Why looking at blockchain technology?

- Same tech platform for everyone
- Smart contracts execute their
- 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, more efficient and effective on Algorand than Ethereum.

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

Collateral Workflow on Blockchain
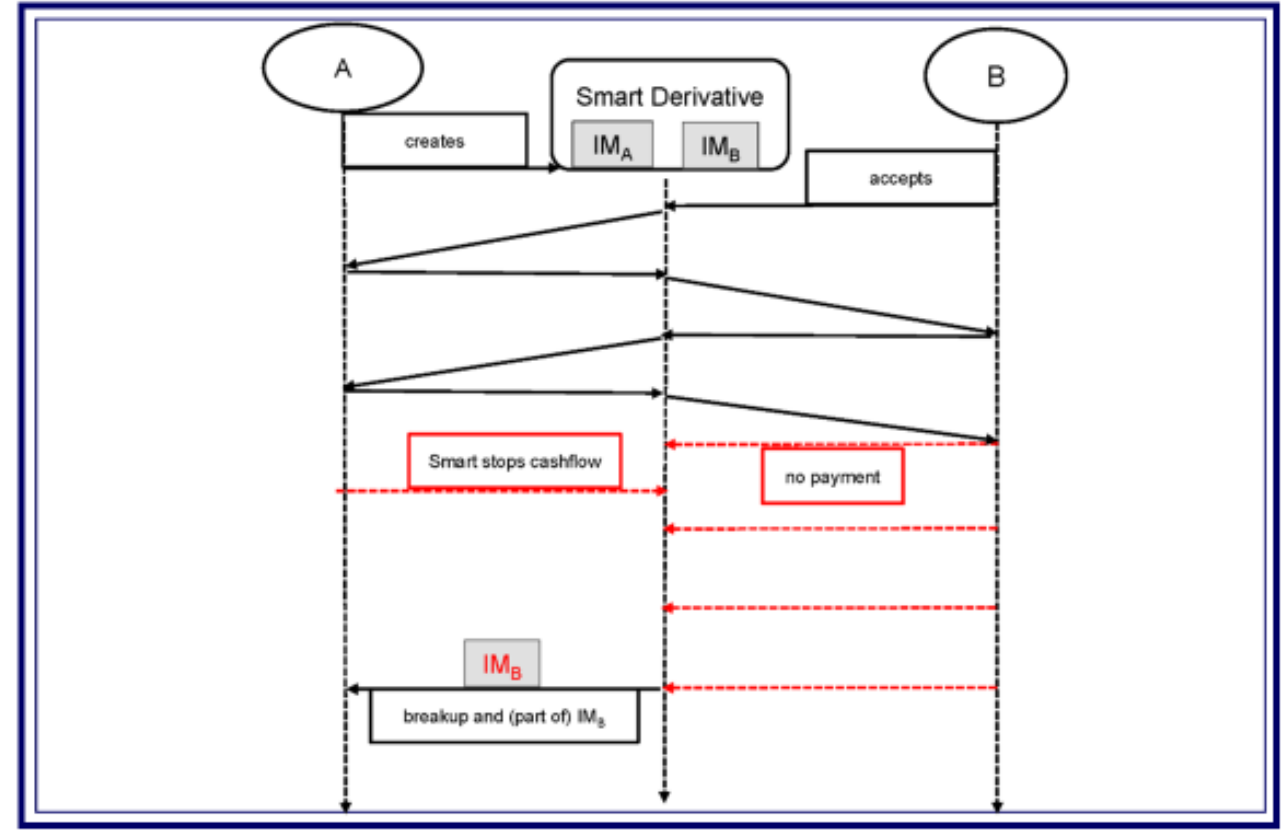
From decentralizing finance to Decentralized Finance (DeFi)

Lack of digital money, inefficient protocols, regulatory uncertainty prevented tests by banks from becoming reality.

Now the time has come. DeFi, running on public blockhains, implements these principles in reality:

- **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 (on reliable platforms)**

From decentralizing finance to Decentralized Finance (DeFi)

DeFi involves risk

- Technical Risk (bugs in dapps)
- Financial Risk (complexity and vol)
- Not all protocols are the same in terms of fees, speed, forks. Algorand has minimal fees, thousands of tx per seconds, no forks and no downtime. This is not always the case and it can impact DeFi activity.
- Not all projects are the same in terms of reliability (rug pulls, centralization, no transparency)

Don't trust, verify!

Do your own research!

- In spite of this DeFi is proposing some a business models based on algorithms that is attracting interest also from institutional players, and new protocols and platforms in a new regulatory setting can reduce the gap between old and new finance.

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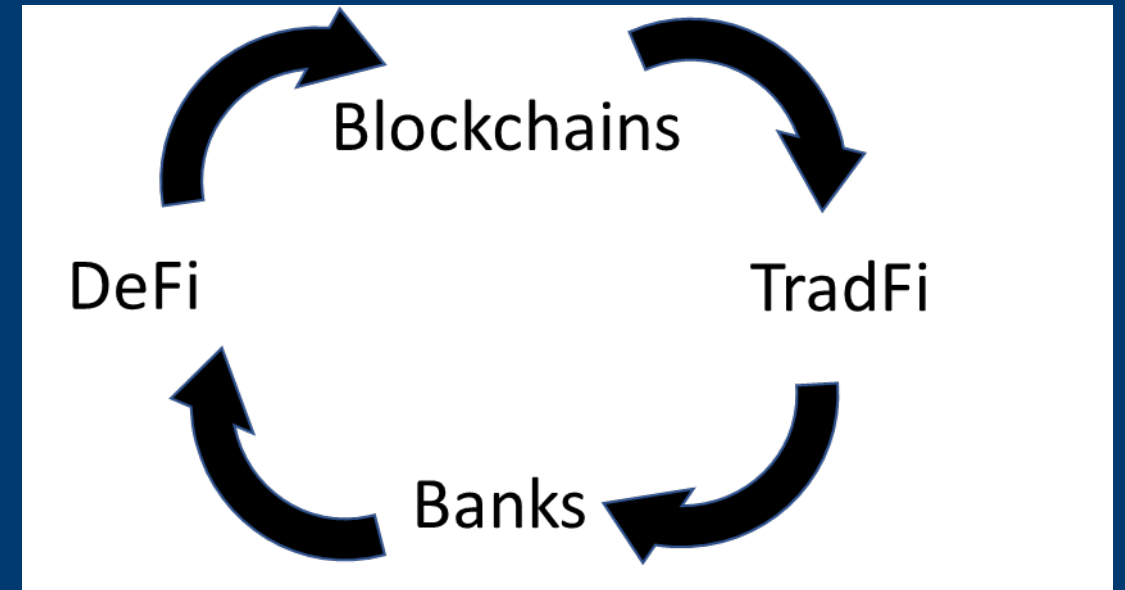
Decentralized stable coins should be based on the same principle: overcollateral contributed by creators to keep a stable value for a created asset. 100 units of a created dollar coin may require at least $200 worth of collateral, with automatic redemption if collateral falls below the 2X overcollateralization.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

Some flaws in the Terra-Luna final period risk-management setup

- The asset that serves as collateral must keep a value higher than the stable asset (otherwise, banking parlance, there's variation but not initial margin or overcollateral)

- There needs to be a resource of liquidity in the system

- Promising a fixed 20% return on the stable asset was contrary to the equilibrium of the system

From Morini 2014 "Inv and Sav wallets"
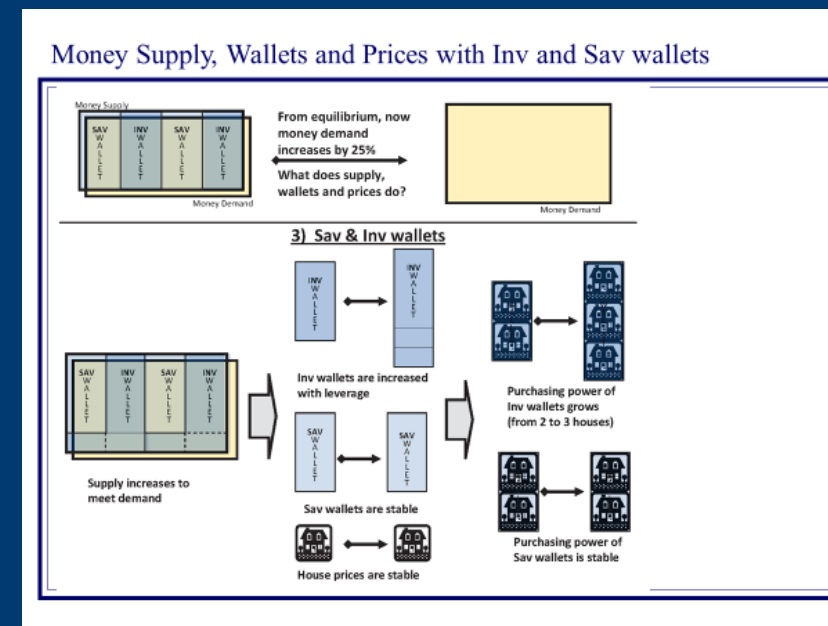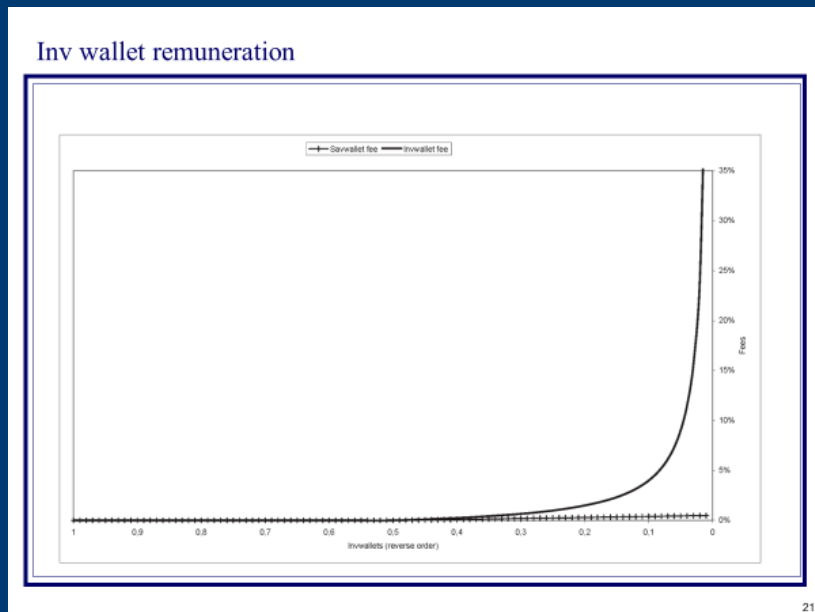
Where we can we go?

- We see that traditional and blockchain payments systems can work together.

- What could be the role of CBDCs? Can they work if banks, that create 90% of existing money, remain behind?

- What would happen if money could be completely digital and flow with less need of intermediaries and strong automation? Maybe on a blockchain that has finality in 4 seconds and was never down in 4 years like Algorand.

Thank you!