CHULALONGKORN
BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Cryptocurrency and Decentralized Finance (DeFi)

Assoc. Prof. Kanis Saengchote, Ph.D.
Department of Banking and Finance
Chulalongkorn Business School
www.dr-kanis.com

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

COINTELEGRAPH
The future of money

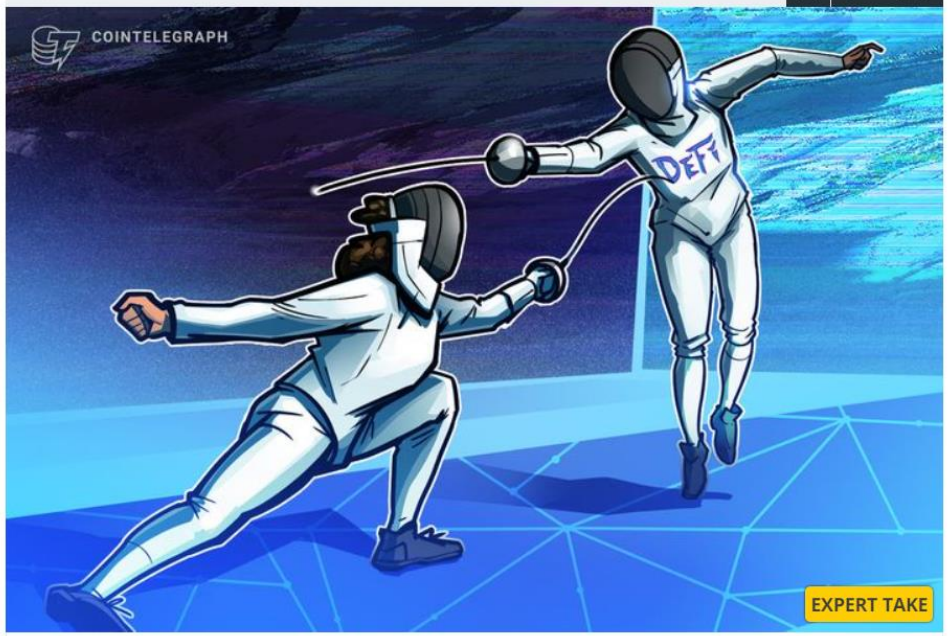
PIERS RIDYARD JUN 25, 2021

Better, faster, cheaper: How DeFi will kill the retail bank

disrupting commercial banking field

The battle for global consumer deposits is going to be the fight of the century. But to vanquish old-fashioned banks, the DeFi sector needs to up its game.

13567 Total views 19 Total shares Listen to article 4:28



Will DeFi destroy banking?

October 14, 2020 by Chris Skinner 2 Comments

It has been a while since I sat back to think about the future bank. I talk about the future bank all the time, but the overall view of a bank in its totality. What will it look like in 2030 and beyond?

I think it will still have branches. Not many, but there is a need for a physical presence. Maybe one branch in each regional hub. The branch will be a hi-tech hotbed, with great smelling coffee and humans available on demand.

Most of the branch traffic will be small to medium sized businesses (SMEs), as most people will deal with the bank through their devices. Their devices are not mobile telephones or notepads, although it does include those, but also their television, refrigerator, car and spectacles or whatever else is attached to the internet.

None of that thinking is particularly new. We were saying this twenty-five years ago.

What is new is that the bank won't be dealing with money anymore.

Money, at least money in its current form, will have disappeared. It will have been replaced with data. Again, I've said this for a while, but if money completely disappears and is replaced with digital central bank currencies, then the world is moving to a different place for definite.

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

blockchain-based digital money

Bloomberg

US Edition ▾ Sign In Subscribe

• Live Now Markets Economics Industries Tech AI Politics Wealth Pursuits Opinion Businessweek Equality Green CityLab Crypto More

What you need to know: Everything You Need to Know in Aftermath of Thailand Election

Politics

Thai Opposition Party Plans $15 Billion Digital Tokens to 'Resuscitate' Economy

- Pheu Thai to fund populist policies from budget, new revenue
- Boosting GDP to 5%, tripling farm income priorities: Prommin

Pheu Thai party supporters at a rally in Bangkok, Thailand, on April 5. *Photographer: Lauren DeCicca/Getty Images*

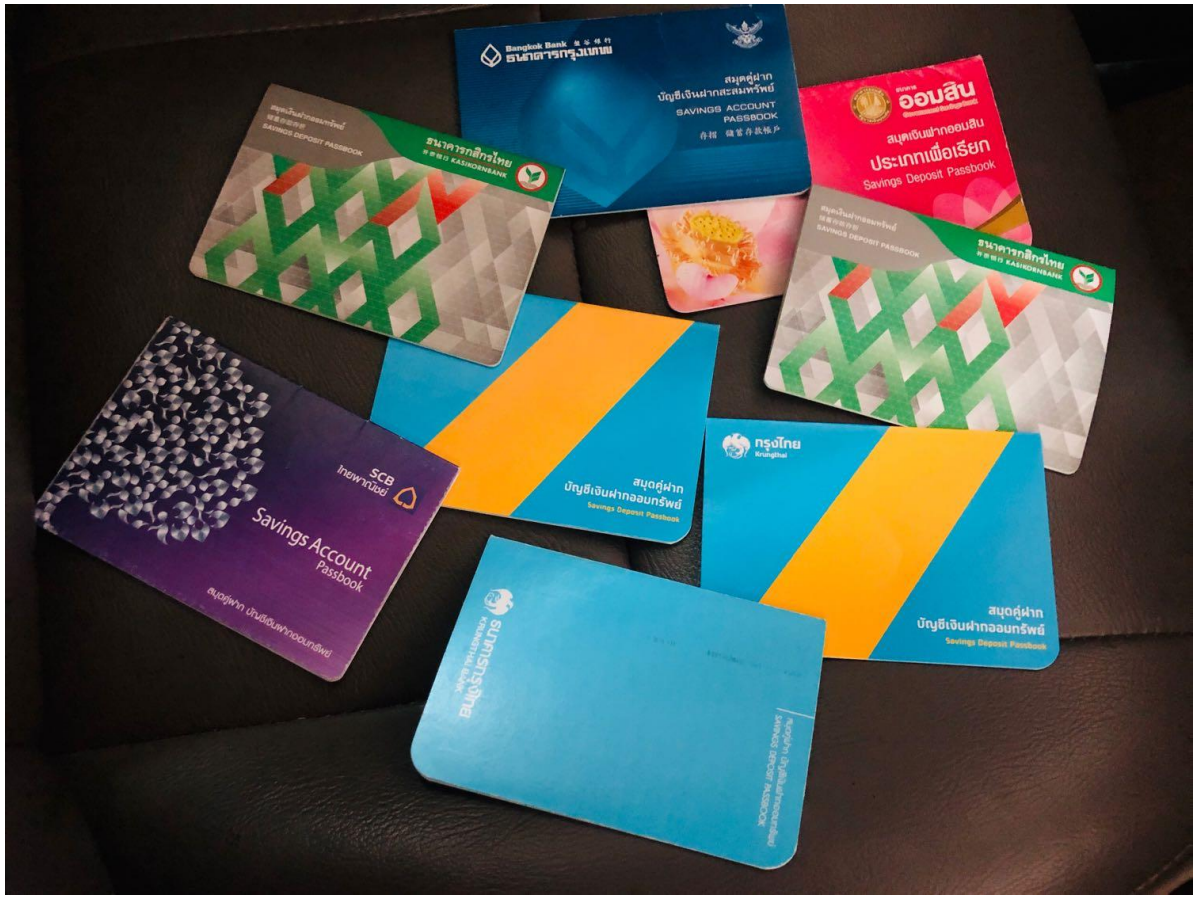
By Patpicha Tanakasempipat and Thomas Kutty Abraham
April 7, 2023 at 3:13 PM GMT+7

What is “Digital Money”?

Bank money is digital money

/ electronic

↳ not physical
↳ stored in electronic base



transfer physical money to digital money

Digital wallet is e-money

money can be changed to other form of money without any friction (1-on-1 basis)

need electronic money provider licence by BOT

regulated service

cannot lend money

digital wallet

Dolfin wallet

rabbit LINE Pay

S Pay

truemoney wallet

And money and credit coexist in our current financial system

transaction cost ; if customer paid in credit card → shop cannot use it immediately unlike paid in cash

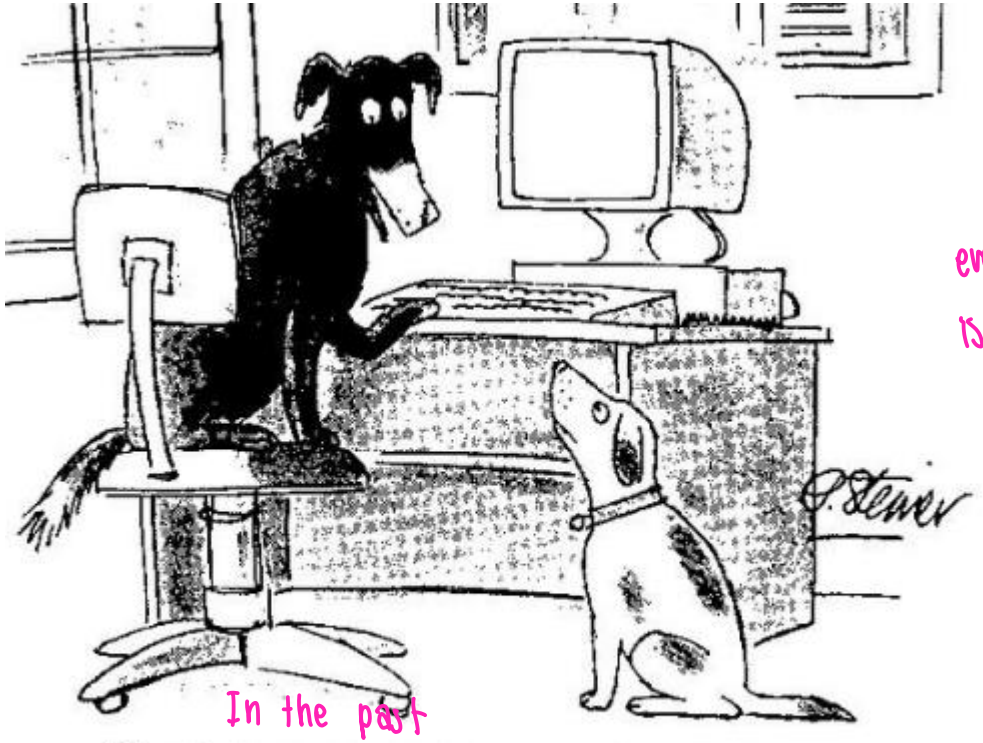
credit card has to create network for the cardholder to buy something without money

↓

charge fee to shops

Problems with the convenience of digital economy

internet movement



In the past

"On the Internet, nobody knows you're a dog."

everything you do is recorded as internet footprint

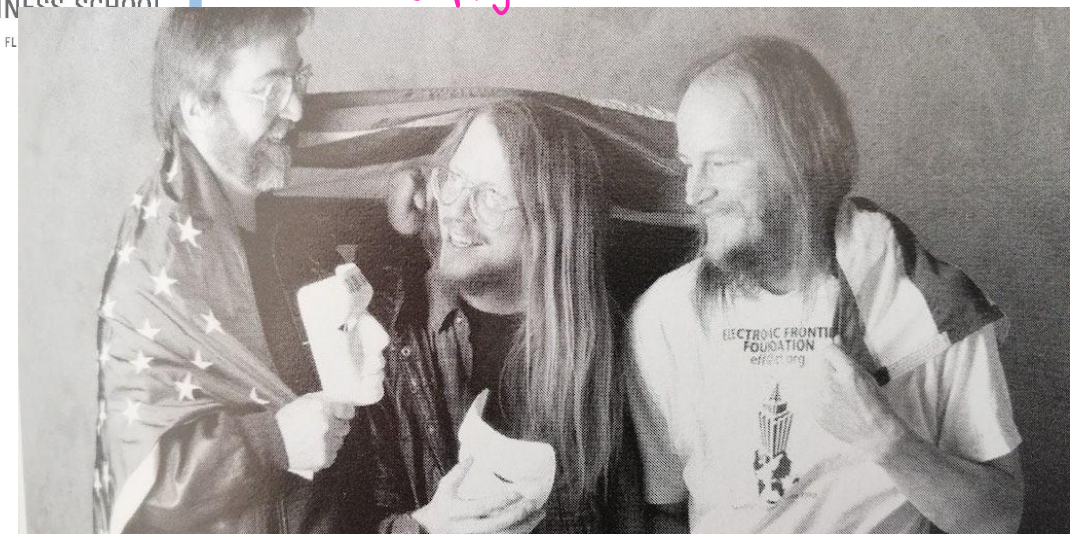
"Remember when, on the Internet, nobody knew who you were?"

try to encypt somethin

Cypherpunk's Manifesto (1993)

, afraid that people can lose their privacy

coding



Cypherpunk: any individual advocating widespread use of **strong cryptography and privacy-enhancing technologies** as a route to **social and political change**.

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must _always_ reveal myself.

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

transferring money from bank A to B is difficult
even there's Internet network

WIRED

STEVEN LEVY BUSINESS DEC 1, 1994 12:00 PM

E-Money (That's What I Want)

The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters – in your wallet. It's not only going to revolutionize the Net, it will change the global economy.

THE KILLER APPLICATION for electronic networks isn't video-on-demand. It's going to hit you where it really matters – in your wallet. It's not only going to revolutionize the Net, it will change the global economy.

Modern challenge:
digital "cash" is very difficult to create!

Modern money is information, so shouldn't it be easy to have digital cash?

Why is it hard to transfer informational money?

money deposit in KBank is different from SCB

KYC : banks need to know who you are

bank may ban you from making payment!

tells other people who you are & perfect money

account based money ← your money may not belong to you

That's because

Money ≠ Cash!

⇒ bitcoin is created

make digital money that still keep you privacy

↳ not content any memory

concensus algorithm → must be faired & not colluted

* permissionless system

↓

by decentralization

↳ use blockchain to achieve this

- Cash is bearer instrument.
- Cash is private.
- Cash needs no permission.

Digital money is account-based.

Digital information has perfect memory.

Digital database users have different rights.

How does a transaction get into the blockchain?

mining bitcoin
- people join as they can get bitcoin

↳ not too short → e.g. every 50 mins, new group of people + new transaction set need to be faired

↳ who win → can pick whatever transaction

everyone keep same set of data
↳ we want to decentralize the processing right to choose transaction

if that address acount is known → it can be banned by people who process the transaction if they don't like the account

A transaction is requested and authenticated → A block representing that transaction is created → The block is sent to every node (i.e. participant) in the network → Nodes validate the transaction

Cryptography allows "accounts" (addresses) to be independently created, accessible via the unique "private key".

Censorship resistance is achieved by decentralizing the authority to record new transactions.

Nodes receive a reward for Proof of Work, typically in cryptocurrency → The block is added to the existing blockchain → The update is distributed across the network → The transaction is complete

blank paper with the same fingleprint

time-stamping service → time-stamp data
↳ no way to change the previous record

© Euromoney Learning 2020

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System
```

Bitcoin: A Peer-to-Peer Electronic Cash System

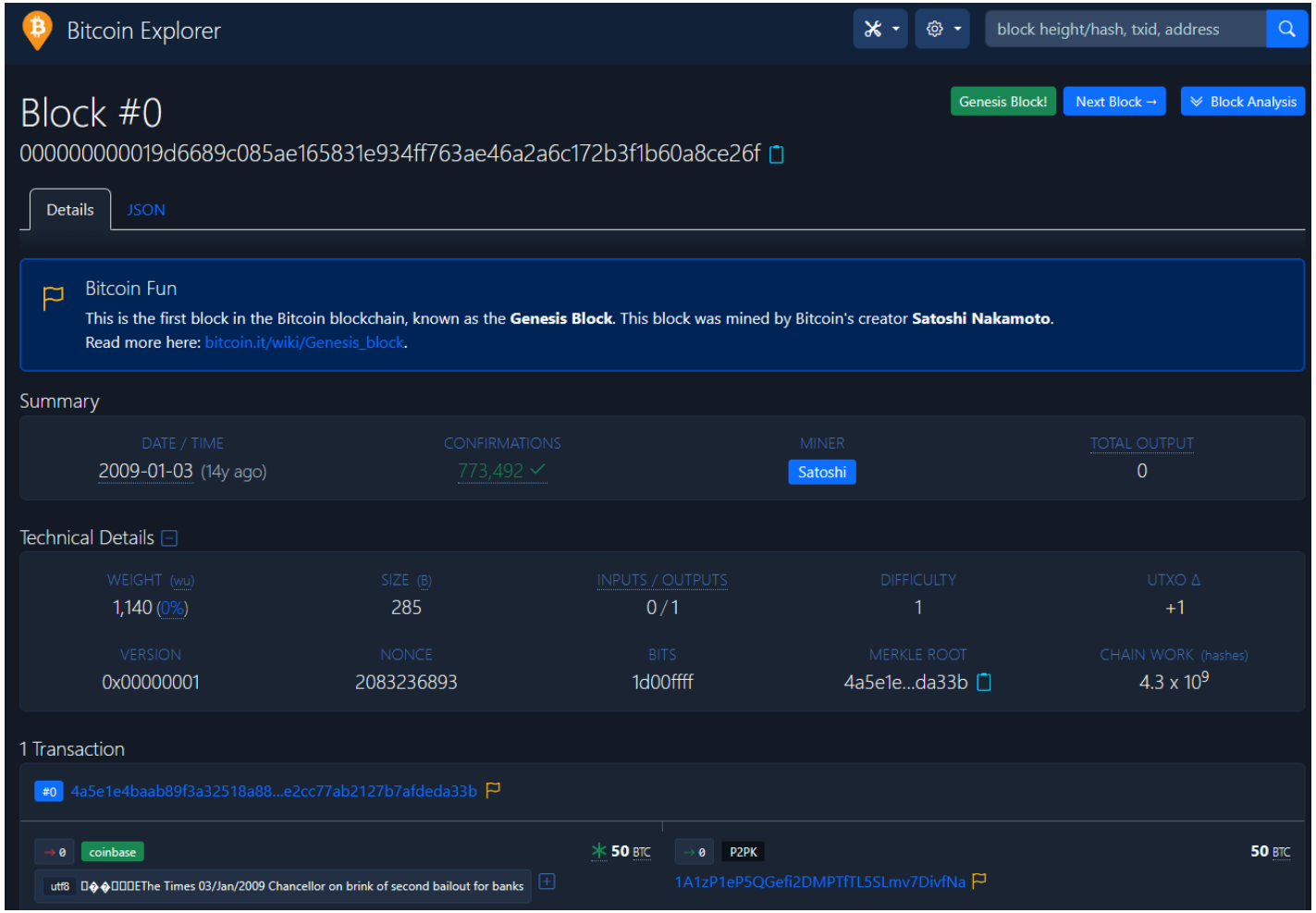
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

1. Introduction

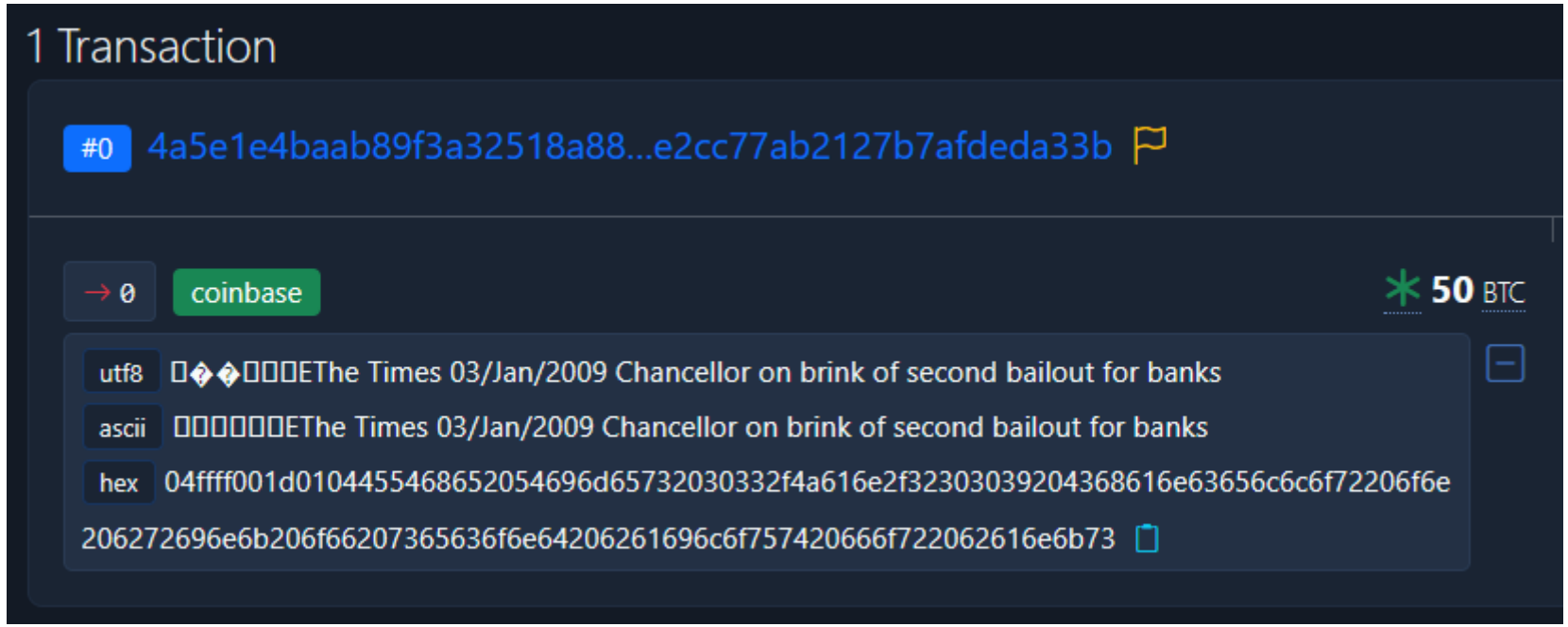
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Each block has a unique digital fingerprint (block hash)



New coins are created in coinbase transactions.



Is cryptocurrency like digital cash?

system of money that can value

system: will check whether you have bitcoin or not
who you want to transfer to

Decentralize: different groups that can be autorized and process the transaction

no identity is required
don't identify who you are

- Bearer instrument — Address is owned by holder of private key.
- Private — Txns are transparent, but address is anonymous.
- Permissionless — Instr. sent by private key and mined by random node.

  - Transparent and publicly auditable.
  - New accounts can be freely and anonymously created without the need to reveal the identity of the account owner, preserving privacy.
  - Transactions are processed by random nodes that can provide services freely and anonymously, making the system permissionless and censorship resistant.

Thus, the Bitcoin blockchain is a permissionless information system that does not require trusted third parties (i.e., corporations and governments).

But why is Bitcoin valuable?

cannot generate income

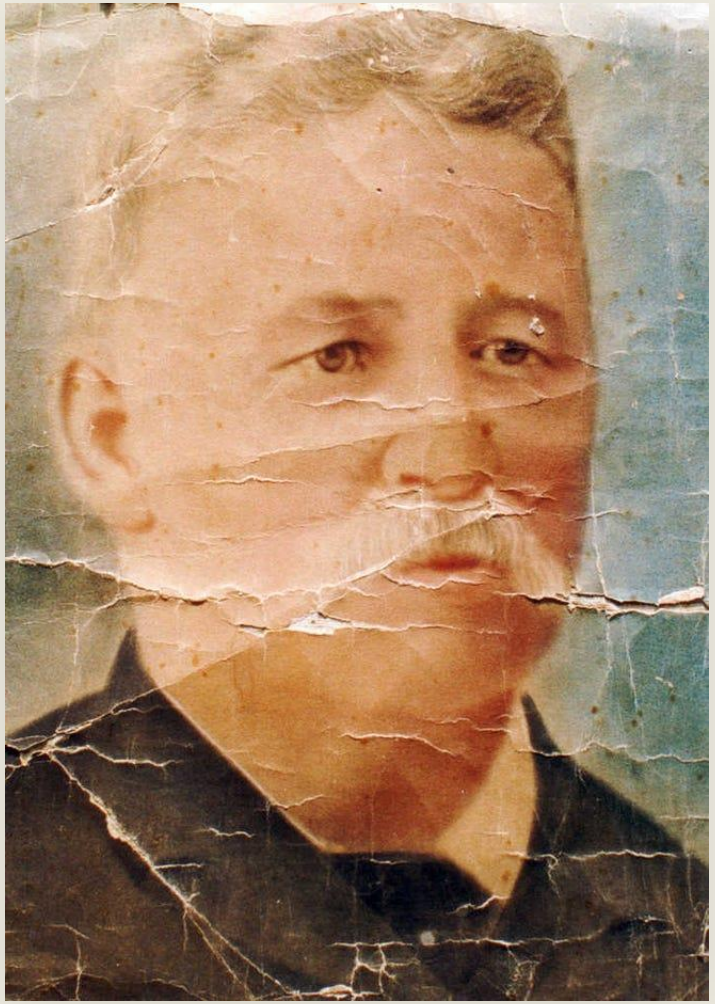
as long as people want it → it is valuable

What is money?

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Money is money because society believes it's money.

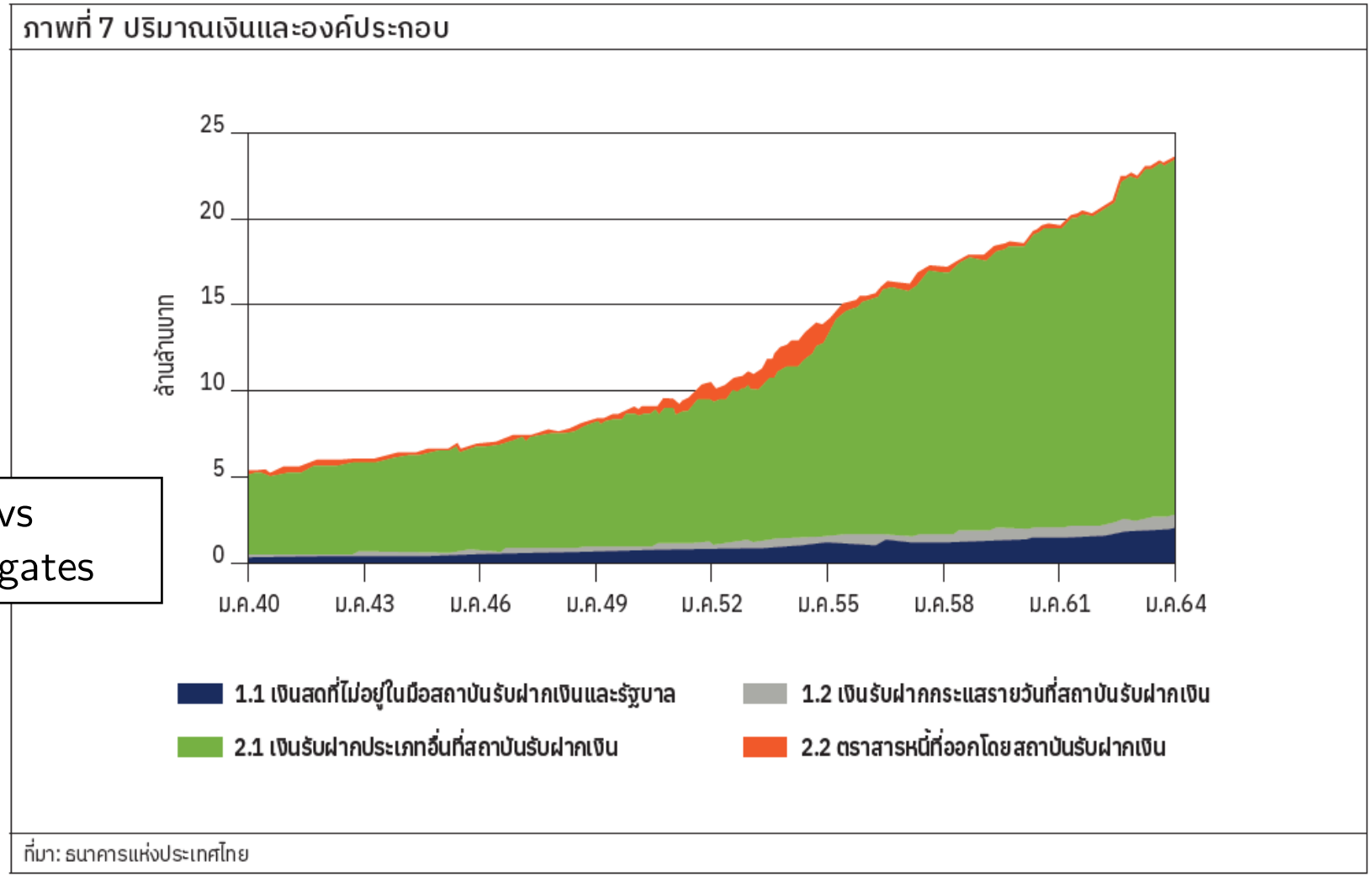
outside money : e.g. gold



Modern money is mostly information.

8% of “money” in circulation is cash and the rest is credit.

Monetary base vs monetary aggregates



ที่มา: เงิน: อดีต ปัจจุบัน และอนาคต (คณิสร์ แสงโชติ, 2565)

WESTERN UNION
WU
SM
moving money for better

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Sms → to send message

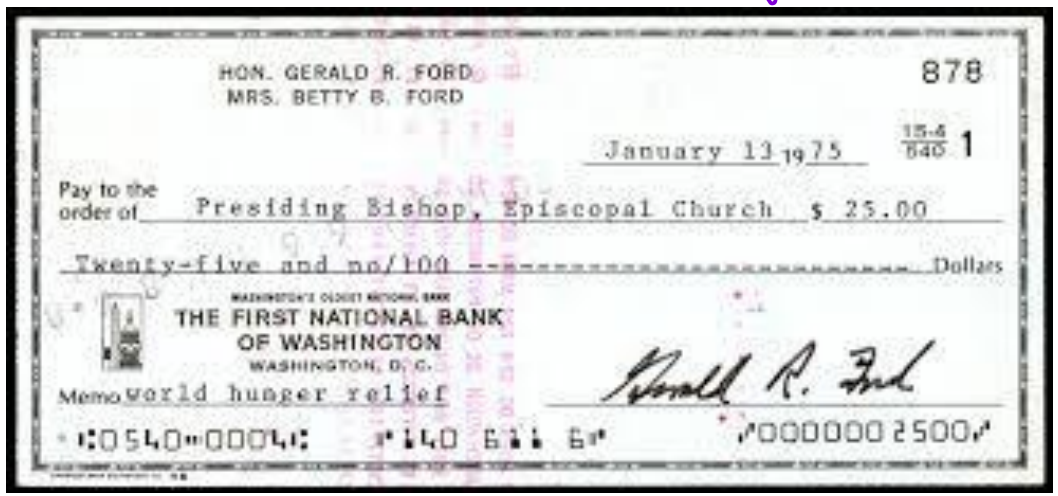
WU
↓
Counterparty
for people to transfer and receive money
↓
give money with equivalent value to receiver in different place

when you move money to different bank (A→B)
[bank's liabilities change]

first step to do money transfer
↓
start with <u>message</u>
↓
e.g. sent to message to bank to ask for permission to tranfer money

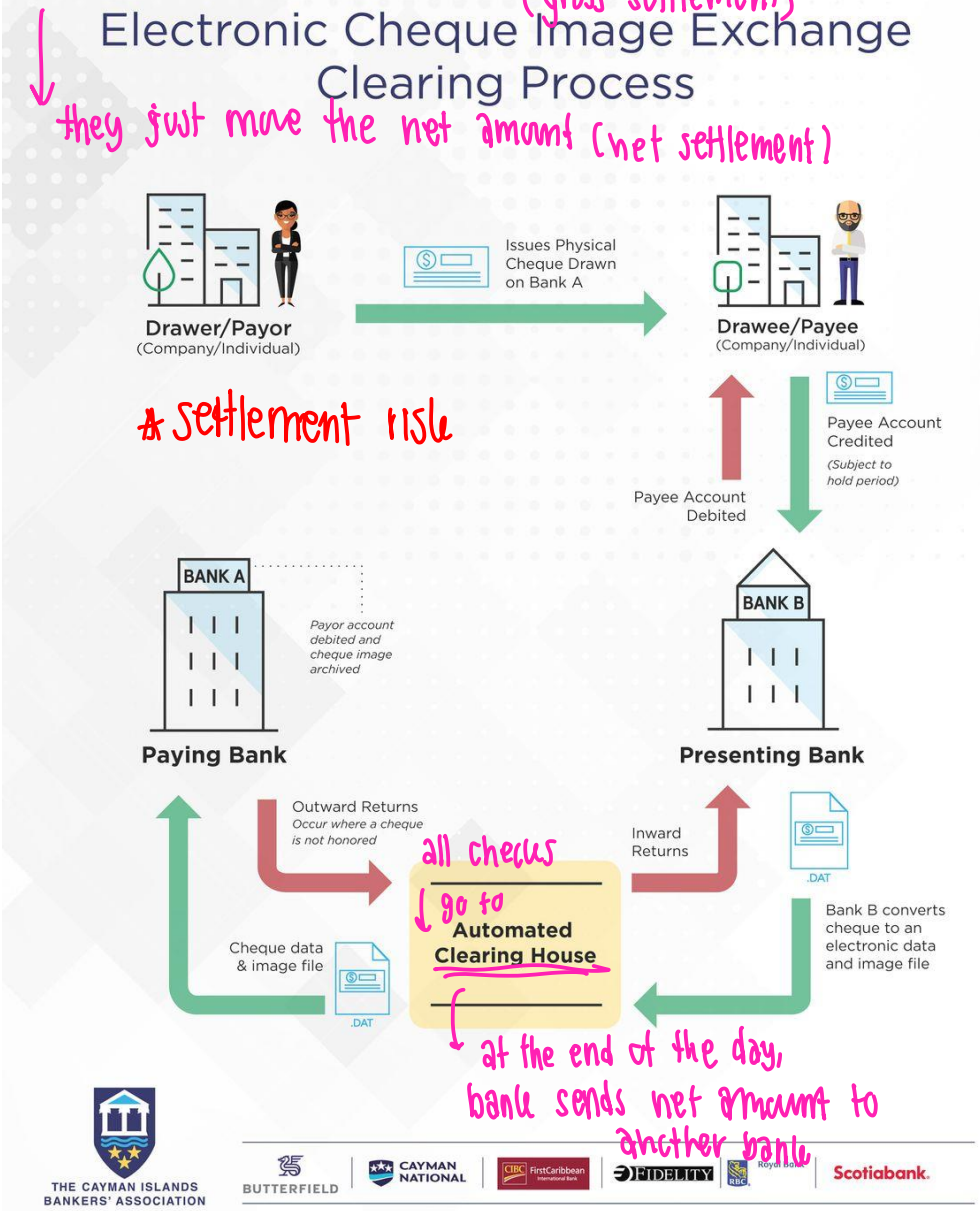
CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

check is like sms that inform the identity of receiver & receivee


HON. GERALD R. FORD
MRS. BETTY B. FORD
878
January 13 1975
15-4/640 1
Pay to the order of Presiding Bishop, Episcopal Church $ 25.00
Twenty-five and no/100 ---------- Dollars
THE FIRST NATIONAL BANK OF WASHINGTON
WASHINGTON, D. C.
Memo World hunger relief
⑆054000041⑆ 140 611 6⑈ ⑈000000 2500⑈

→ banks don't move their money every transaction: (gross settlement)

they just move the net amount (net settlement)



all checks go to

at the end of the day, bank sends net amount to another bank

* settlement risk

Banca, banchieri,

and the money lender

The role of the financial system

bank

Contemporaneous (form, space)

- Asset custody
- Payment and exchange

Intertemporal (time, state)

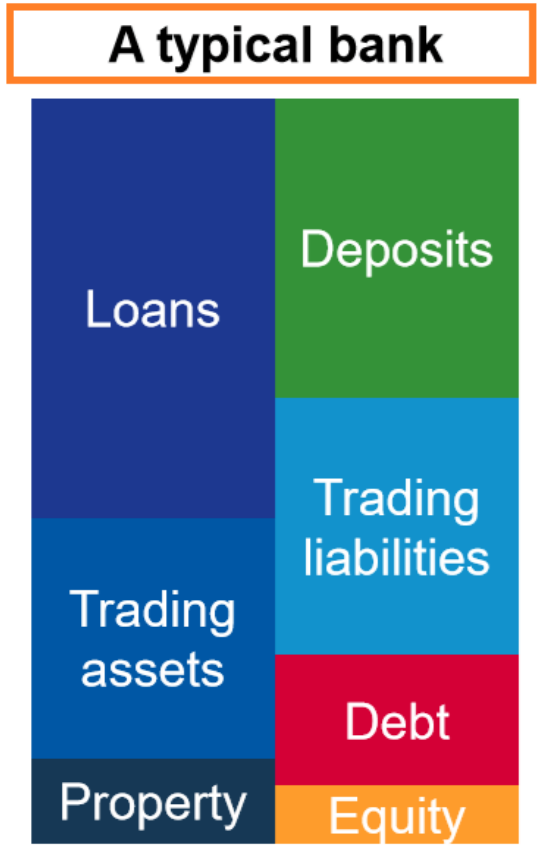
- Capital allocation
- *Wealth management*
- *Risk allocation*

Banking beyond asset custody

- borrow 10M from bank
- loan receivable?
- if the borrower uses the same account bank then, bank creates deposit - loan - based
  ⇓
  bank doesn't have to find other external source of money

The money lender's problem:

"Whose money" do I lend?



Money that that I cannot create (outside money)?

→ Intermediation banking

bank acts as medium

people deposit cash to bank:
bank owns assets cash ↑
liabilities ↑

Money that I can create? (inside money)

bank creates their own money and want others to use it

→ Credit creation banking

central bank requires them to have reserve

bank keeps some liquidity on hand so that people can withdraw cash

12th Century International Money Transfers and 16th Century Medieval Faire

The warrior monks who invented banking

By Tim Harford
50 Things That Made the Modern Economy, BBC World Service

30 January 2017

A merchant from Lyon who wanted to buy - say - Florentine wool could go to this banker and borrow something called a **bill of exchange**.

This was **a credit note, an IOU**, but it was not denominated in the French livre or Florentine lira.

Its value was expressed in the ecu de marc, a private currency used by this international network of bankers.

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

International Transfers

How do financial institutions facilitate value transfer today?

- While the current "rails" for value transfer between financial institutions are complex and involve many institutions a similar process is used for all transactions; from large institutional transfers to the settlement of retail payments

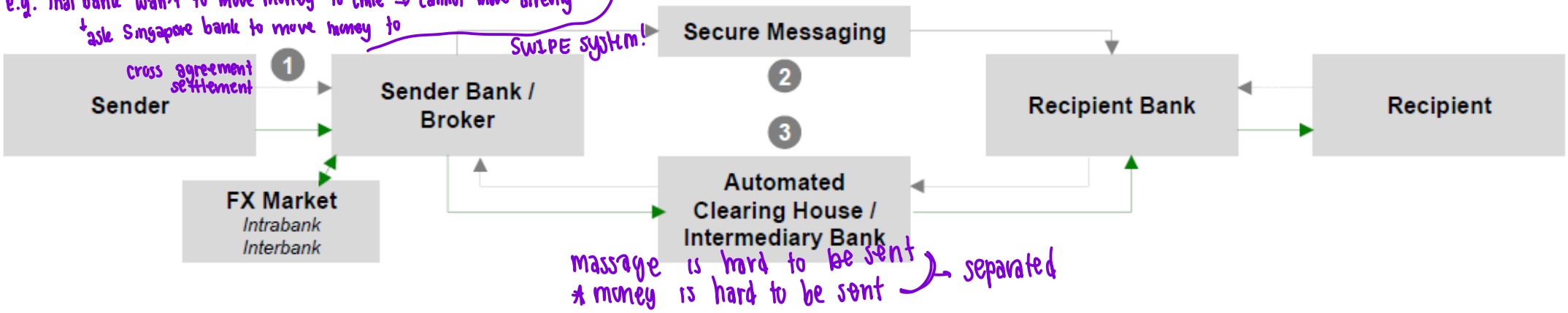
1 Sender Request
Sender asks their financial institution to transfer an amount to a specific address (using BIC or IBAN codes)

customer want to
e.g. Thai bank wan't to move money to China ⇒ cannot move directly
ask Singapore bank to move money to

2 Secure Messaging
Sending bank sends a secure message to the recipient bank requesting transfer of the specified amount

3 Flow of Funds
The recipient bank responds to the sender bank's request for funds via a clearing house or correspondent bank

Flow of Funds
Transfer Request / authorisation



massage is hard to be sent
& money is hard to be sent
separated

Evolution of money transfer schemes

- The basic elements of the current value transfer process have been in place for over 150 years
- The concept of "wire transfers" was originated by telegraph companies (e.g., Western Union) who would receive funds for transfer from a sending party and send a telegraph to correspondent branch instructing them to deliver the money to the intended recipient
- The digitisation of this process throughout the latter half of the 20th century improved the security of messaging services and improved the settlement time of clearing house activities

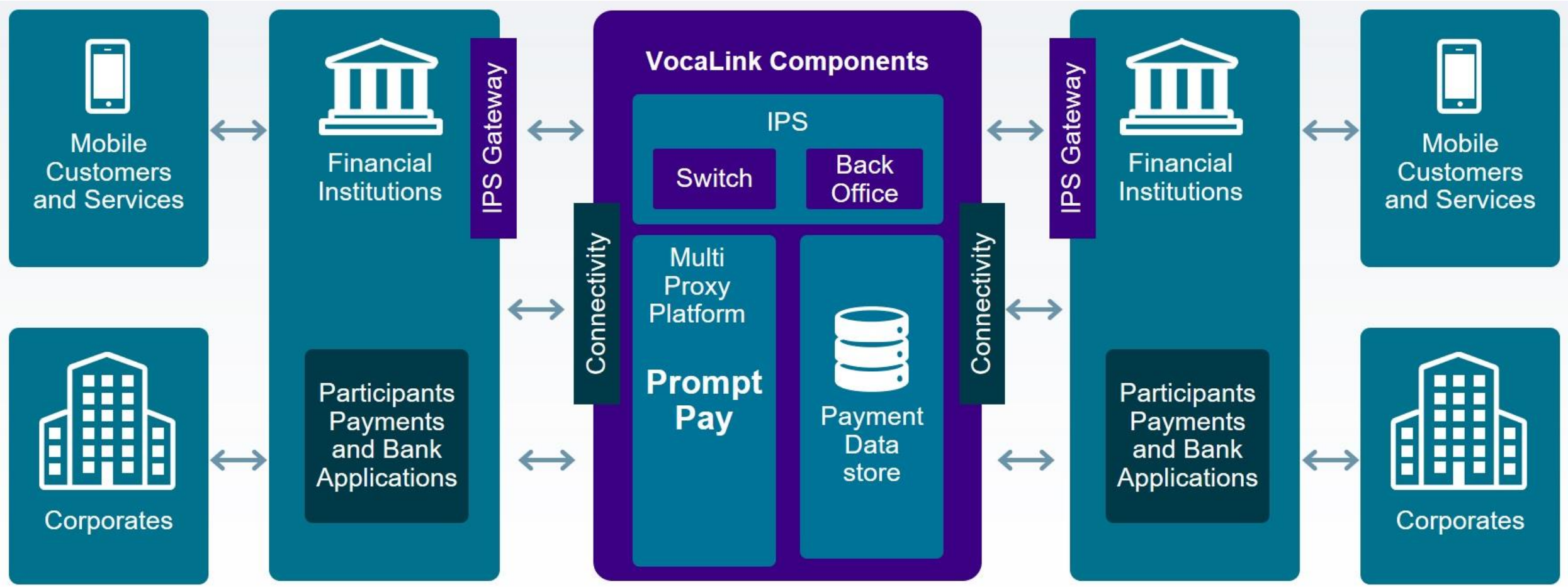
Key pain points with today's schemes

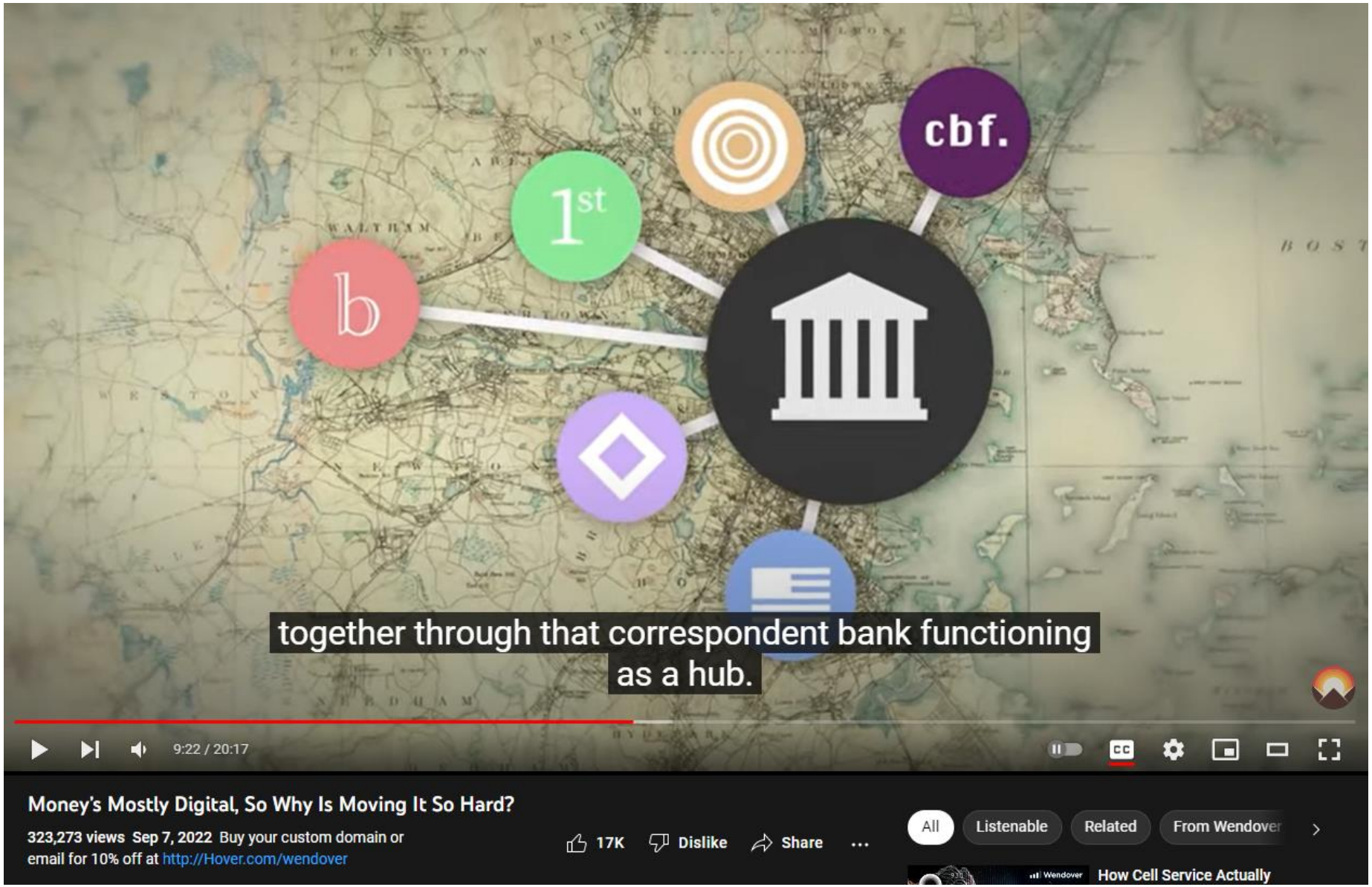
- The actual transfer is not instantaneous: funds may take several hours or even days to move from the sender's account to the receiver's account
- If the sending and recipient banks do not hold reciprocal accounts the payment must be sent to a clearing house or correspondent bank for the assurance of payment for the recipient, adding costs and delays
- The complex structure of requesting the recipient bank to demand payment makes the process more vulnerable to fraud using exposed sender credentials

Promptpay allows banks to reconcile with one another

low

↳ Banks in Thailand know each other → they're willing to receive settlement risk




cbf.
1st
b
together through that correspondent bank functioning
as a hub.
9:22 / 20:17
Money's Mostly Digital, So Why Is Moving It So Hard?
323,273 views Sep 7, 2022 Buy your custom domain or
email for 10% off at http://Hover.com/wendover
17K
Dislike
Share
All
Listenable
Related
From Wendover
How Cell Service Actually

Amsterdam: early 1600s

Reserve and settlement account
⇓
commercial banks do settlement to central bank

Forms of central bank's money
① CBDC : alternate form of CB money
② reserve & settlement account

to be used by commercial bank

use gold as money

set a bank
↓
if you come to this city
then you have to use Amsterdam money
↓
, you don't have to carry money
⇓
just tell the bank who you have to pay at the end of year
↳ just adjust the balance
⇓
become account-based transaction

central bank currency to be used by central bank

$\Downarrow$ can be done by decentralization

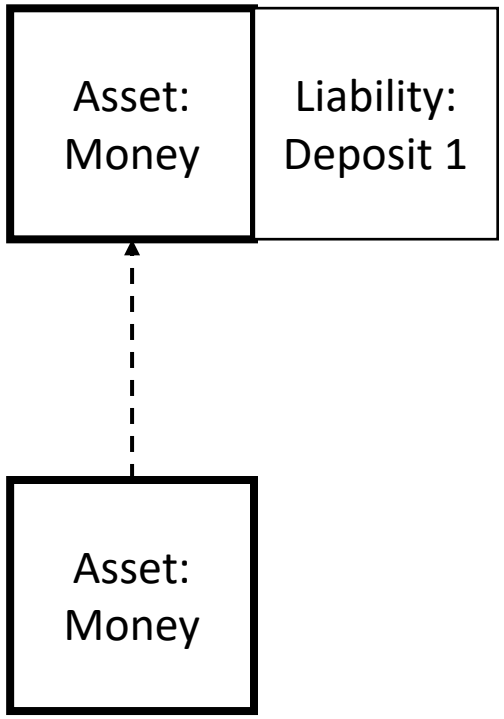
More examples of money throughout history

Most of the "Money" we use liquid, transferable debt issued by someone (not always government!)

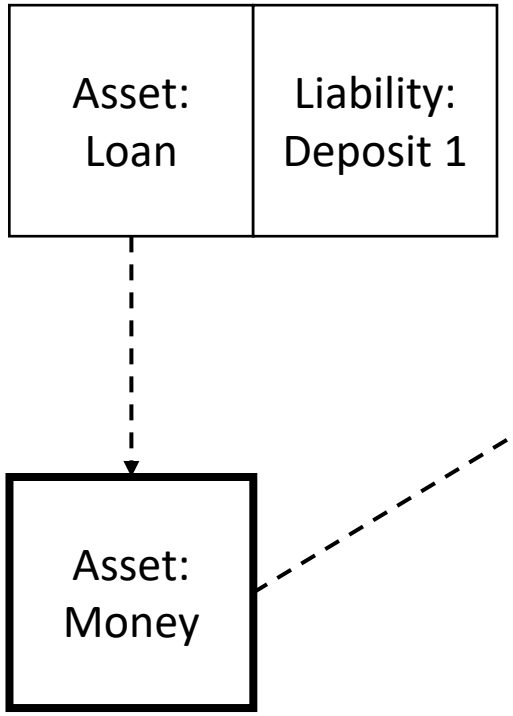
The money multiplier → "infinite" loan creation

As long as customers don't want their "money" back, it's fine to keep going.
It's even easier when you don't need to raise deposit and use private money!

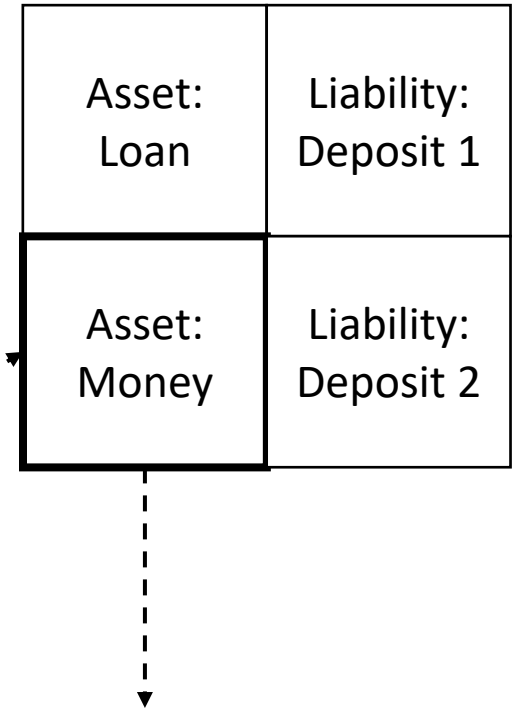
Step 1: receive deposit



Step 2: lend money



Step 3: receive deposit

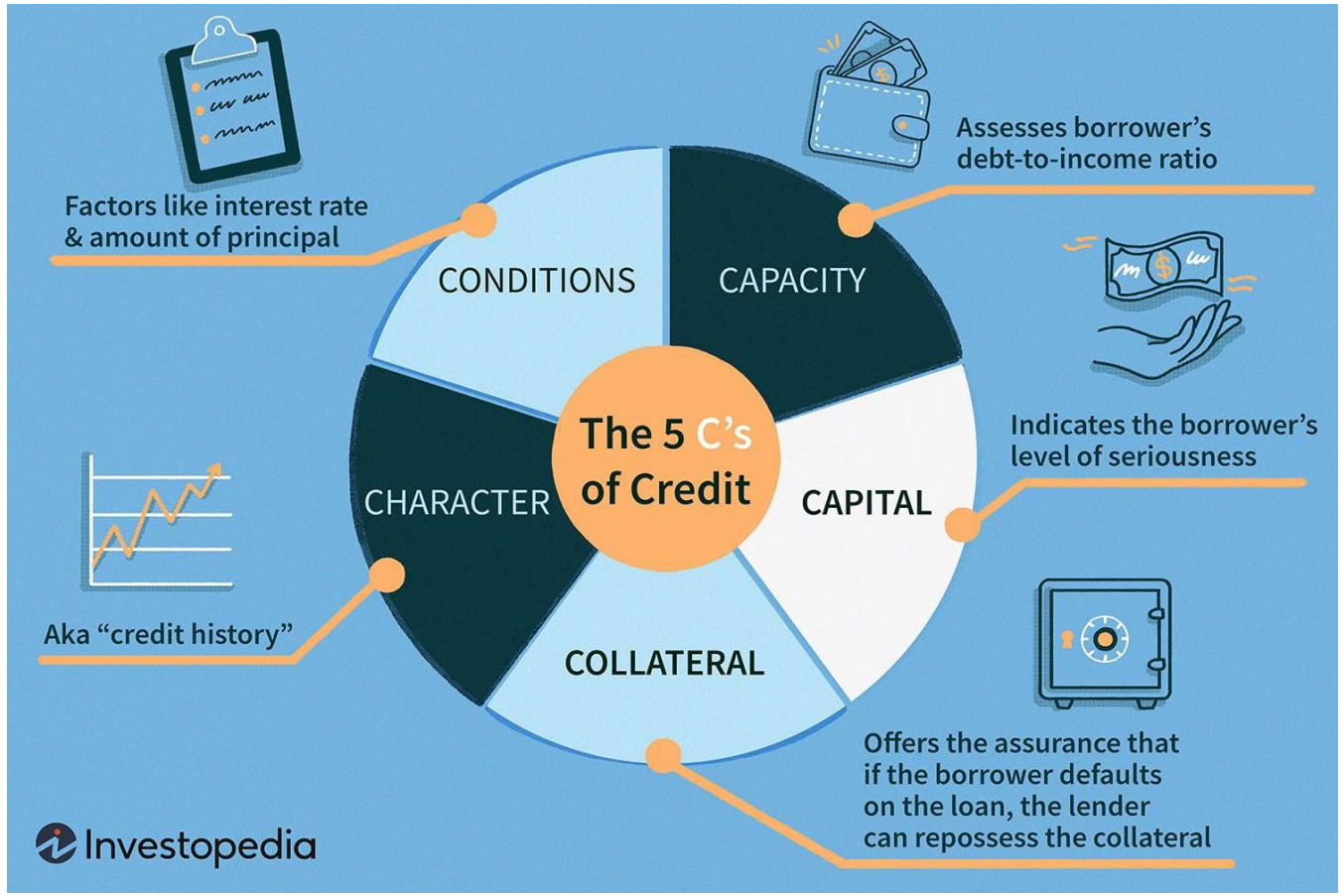


Step 4, 5, 6…

Bank as a data company

Fundraising is important it allows you to capitalize on opportunities and/or avoid catastrophes (time and state = uncertainty), and information is crucial.

Collateralization and repeated interactions to foster trust (across **form, space, time and state**) underpin the modern financial system.



Ability to pay – adverse selection

Willingness to pay – moral hazard

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Money and Currency

USD is not accepted in local shops in Thailand

Country's currency

interest rate is the price of money btw future & past

- self-ful believe equilibrium
  everyone believes that
  it has value

main store value

The Gold "Standard"

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Unofficial Translation

CURRENCY ACT B.E. 2501

BHUMIBOL ADULYADEJ, REX

Given on the 18th day of August B.E. 2501:

Being the 13th Year of the Present Reign

Section 26. For the purpose of maintaining the stability of the currency, the Bank of Thailand shall maintain a currency reserve, hereinafter to be called the "Currency Reserve".

Section 30.[18] The following assests shall be lawful components of the Currency Reserve:

(1) gold,

(2) foreign currencies which are convertible currencies or any other currencies prescribed by a Ministerial Regulation, which must be in the form of deposit with a bank outside the Kingdom or with an international financial institution,

(3) foreign securities payable in foreign currencies as stated in (2),

(4) gold and foreign assets paid as subscription to the International Monetary Fund,

(5) Reserve Tranche Purchase Certificate

(6) Special Drawing Right Certificate,

(7) securities of the Thai Government payable in foreign currencies as stated in (2) or in baht,

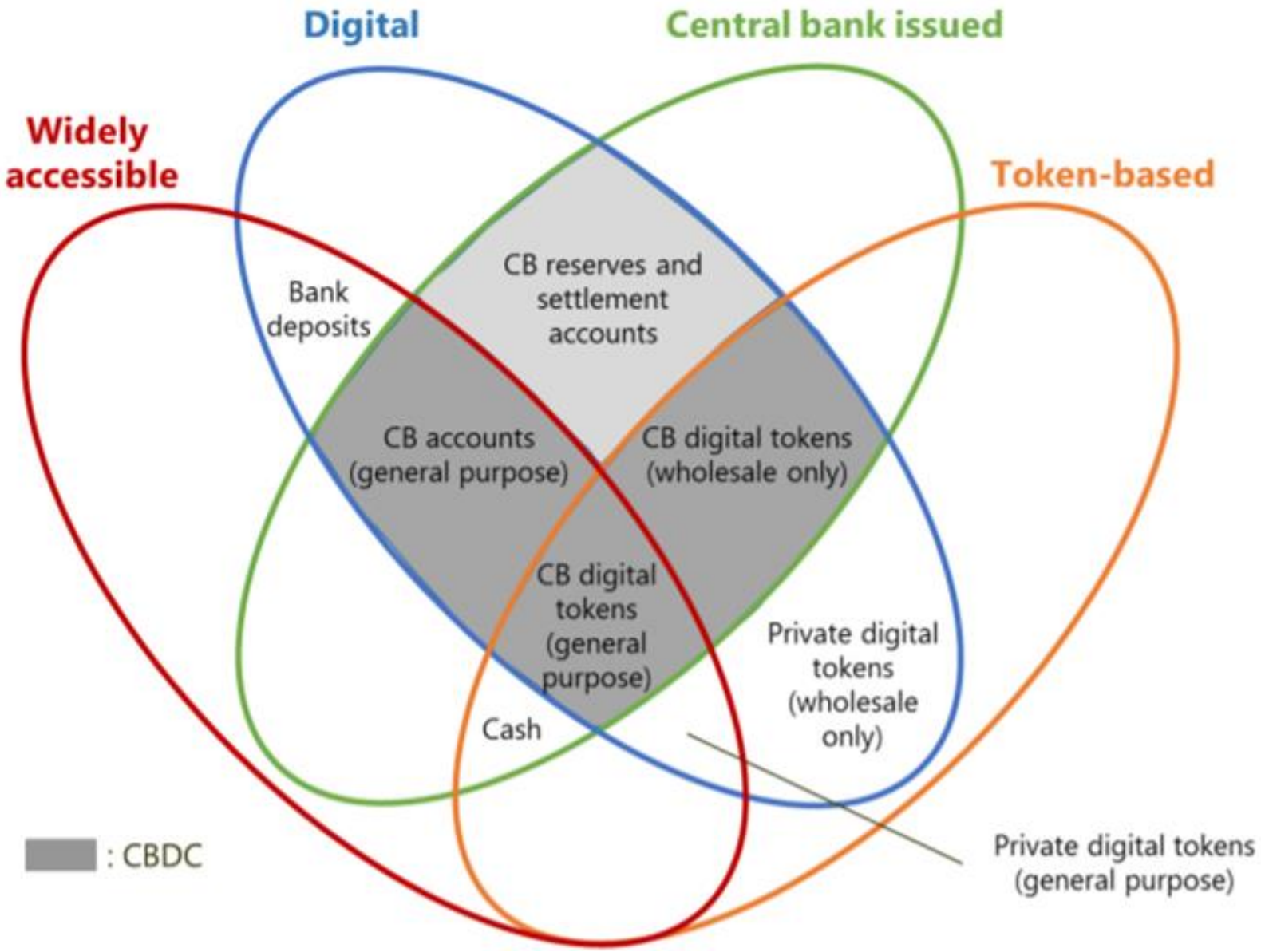
(8) domestic bills which the Bank of Thailand is permitted to purchase or rediscount, provided that the total value thereof does not exceed 20 per cent of the total amount of notes issued.

With respect to the assets stated in (1), (2), (3), (4), (5) and (6) above, the Bank of Thailand shall be required to maintain their total value at not less than 60 per centum of the notes issued.

[17] As amended by the Currency Act (No. 2) B.E. 2510

[18] As amended by the Emergency Decree Amending the Currency Act B.E. 2501 B.E. 2521

UNOFFICIAL



Source: Bech and Garratt (2017)

¥10.00
中国人民银行

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

	GOLD	BITCOIN	FIAT CURRENCY	
DURABLE	+	+	—	While all are physically durable, fiat currency over history has not maintained purchasing power durability
DIVISIBLE	—	+	+	Physical gold is only divisible to small pieces; bitcoin is divisible to eight decimals
FUNGIBLE	+	+	—	Gold and bitcoin are fungible, but fiat currency is not fungible with other fiat (US Dollar is not fungible with Canadian dollar)
PORTABLE	—	+	+	Gold has a high value to weight ratio, but compared to the others is still heavy and cumbersome to transport
VERIFIABLE	—	+	—	Both gold and fiat currency have been counterfeited; gold can be verified but only through cumbersome assay
SCARCE	+	+	—	Gold is scarce, bitcoin is scarce and finite; the only constraint on fiat currency is willingness of government or central bank
TRACK RECORD	+	—	—	Gold has the longest track record as money and maintaining purchasing power; bitcoin's history is the shortest; fiat currency has a poor track record[2]

Bitcoin First:

Why investors need to consider bitcoin separately from other digital assets.

Key question

What makes Bitcoin valuable?

Fidelity DIGITAL ASSETS™

Cryptocurrencies and stablecoins

#	Coin	Price	24h Volume	Exchanges	Market Capitalization	30d	Last 30 Days Circulation
1	Tether USDT	$1.00	$19,022,987,144	443	$83,182,981,854	-0.0%	
2	USD Coin USDC	$1.00	$4,452,574,181	418	$26,167,256,046	0.4%	
3	Dai DAI	$1.00	$86,026,114	223	$3,846,601,709	-2.1%	
4	TrueUSD TUSD	$0.999169	$278,987,467	55	$3,161,717,269	14.9%	
5	Binance USD BUSD	$1.00	$2,398,639,760	107	$2,500,892,717	-25.1%	
6	USDD USDD	$0.999905	$29,762,908	22	$726,140,039	0.3%	
7	Frax FRAX	$0.996813	$5,745,736	45	$669,913,445	-17.3%	
8	Pax Dollar USDP	$0.999814	$8,072,687	24	$507,535,214	0.3%	
9	PAX Gold PAXG	$1,905.24	$6,540,033	31	$473,123,046	0.2%	
10	Tether Gold XAUT	$1,919.40	$3,788,056	18	$473,453,510	0.9%	

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Blockchain and DeFi

bitcoin network

↳ can only trade bitcoin

DISRUPT
Crunch

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
By Vitalik Buterin (2014).

When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the "bitcoin", a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So far, the "bitcoin" as a currency unit has taken up the bulk of the public attention, both in terms of the political aspects of a currency without a central bank and its extreme upward and downward volatility in price. However, there is also another, equally important, part to Satoshi's grand experiment: the concept of a proof of work-based blockchain to allow for public agreement on the order of transactions. Bitcoin as an application can be described as a first-to-file system: if one entity has 50 BTC, and simultaneously sends the same 50 BTC to A and to B, only the transaction that gets confirmed first will process. There is no intrinsic way of determining from two transactions which came earlier, and for decades this stymied the development of decentralized digital currency. Satoshi's blockchain was the first credible decentralized solution. And now, attention is rapidly starting to shift toward this second part of Bitcoin's technology, and how the blockchain concept can be used for more than just money.

add, subtract, divide number

→ Programmable blockchain

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Ethereum 'Tokens' Are All the Rage. But What Are They Anyway?

At the root of a high-profile wave of mega-ICO fundraising efforts on ethereum is a token standard called ERC-20. So what is it anyway?

Amy Castor

Jun 17, 2017 at 5:08 p.m. Updated Sep 11, 2021 at 8:27 p.m.

Some ERC-20 smart contract functions

- Name
- Mint
- Burn
- Transfer
- TransferFrom

Token Systems

On-blockchain token systems have many applications ranging from sub-currencies representing assets such as USD or gold to company stocks, individual tokens representing smart property, secure unforgeable coupons, and even token systems with no ties to conventional value at all, used as point systems for incentivization. Token systems are surprisingly easy to implement in Ethereum. The key point to understand is that all a currency, or token system, fundamentally is, is a database with one operation: subtract X units from A and give X units to B, with the proviso that (i) A had at least X units before the transaction and (2) the transaction is approved by A. All that it takes to implement a token system is to implement this logic into a contract.

The basic code for implementing a token system in Serpent looks as follows:

```
def send(to, value):
  if self.storage[msg.sender] >= value:
    self.storage[msg.sender] = self.storage[msg.sender] - value
    self.storage[to] = self.storage[to] + value
```

This is essentially a literal implementation of the "banking system" state transition function described further above in this document. A few extra lines of code need to be added to provide for the initial step of distributing the currency units in the first place and a few other edge cases, and ideally a function would be added to let other contracts query for the balance of an address. But that's all there is to it. Theoretically, Ethereum-based token systems acting as sub-currencies can potentially include another important feature that on-chain Bitcoin-based meta-currencies lack: the ability to pay transaction fees directly in that currency.

Stablecoin = token + mechanism that incentivizes users to buy and sell at $1

Contract 0xdAC17F958D2ee523a2206206994597C13D831ec7

Bitfinex | Token Contract | Blocked

Buy | Exchange | Earn | Gaming

Featured: Etherscan API - Need higher call rates ? Sign-up for a dedicated plan today!

Contract Overview	Tether: USDT Stablecoin
Balance:	1 wei
Ether Value:	Less Than $0.01 (@ $1,314.89/ETH)
Token:	>$81,316.31 >109

More Info	More
My Name Tag:	Not Available, login to update
Contract Creator:	Bitfinex: Deployer 5 at txn 0x2f1c5c2b44f771e942a...
Token Tracker:	Tether USD (USDT) (@$0.9999)

Source: https://etherscan.io/address/0xdac17f958d2ee523a2206206994597c13d831ec7#code

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

code that you can read for free

Code | Read Contract | Write Contract

Read Contract Information [Expand all] [Reset]

1. name
2. deprecated
3. totalSupply
4. upgradedAddress
5. balances
6. decimals
7. maximumFee
8. _totalSupply
9. getBlackListStatus

Source: https://etherscan.io/address/0xdac17f958d2ee523a2206206994597c13d831ec7#code

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Code | Read Contract | Write Contract

Connect to Web3

[Expand all] [Reset]

1. deprecate (0x0753c30c)
2. approve (0x095ea7b3)
3. addBlackList (0x0ecb93c0) invalid
4. transferFrom (0x23b872dd)
5. unpause (0x3f4ba83a)
6. pause (0x8456cb59)
7. transfer (0xa9059cbb)
8. setParams (0xc0324c77)
9. issue (0xcc872b66) create
10. redeem (0xdb006a75) destroy, burn

Source: https://etherscan.io/address/0xdac17f958d2ee523a2206206994597c13d831ec7#code

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Contract Source Code (Solidity) **Audit Report**

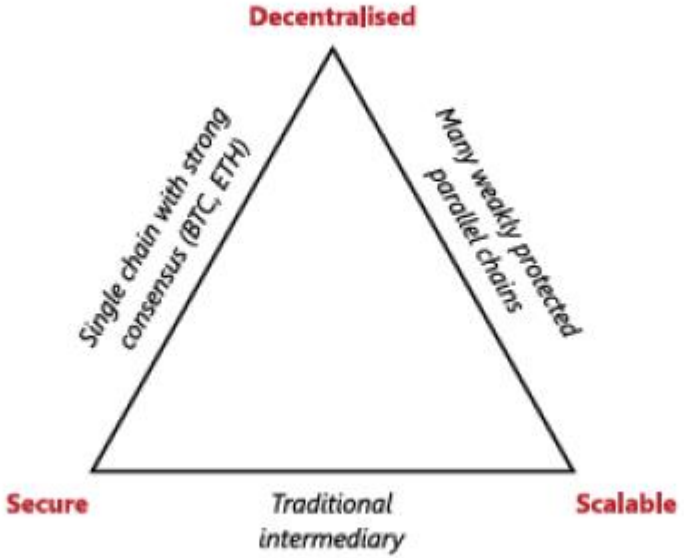
Outline More Options

```
    // @param _symbol Token symbol
    // @param _decimals Token decimals
    function TetherToken(uint _initialSupply, string _name, string _symbol, uint _decimals) public {
        _totalSupply = _initialSupply;
        name = _name;
        symbol = _symbol;
        decimals = _decimals;
        balances[owner] = _initialSupply;
        deprecated = false;
    }

    // Forward ERC20 methods to upgraded contract if this one is deprecated
    function transfer(address _to, uint _value) public whenNotPaused {
        require(!isBlackListed[msg.sender]);
        if (deprecated) {
            return UpgradedStandardToken(upgradedAddress).transferByLegacy(msg.sender, _to, _value);
        } else {
            return super.transfer(_to, _value);
        }
    }

    // Forward ERC20 methods to upgraded contract if this one is deprecated
    function transferFrom(address _from, address _to, uint _value) public whenNotPaused {
        require(!isBlackListed[_from]);
        if (deprecated) {
```

Source: https://etherscan.io/address/0xdac17f958d2ee523a2206206994597c13d831ec7#code

Q: Why do we need to pay gas to use smart contracts?
A: To keep the minimum spec for nodes as small as possible.

Buterin's "scalability trilemma" Graph 3



Sources: Auer et al (2021); Buterin (2021).

A permissionless blockchain that allows anyone to become a node must democratize the ability to become nodes. Otherwise, the authority will not be decentralized. Thus, the blockchain storage space (block size) and computing power per block (gas limit) become scare resources that users must pay for.

decentralize : change the right

If not, it's not true

A permissionless blockchain is NOT SCALABLE by DESIGN, otherwise nodes or a certain group behind nodes can retain the authority on which transactions to process or censor.

613,000 USDT transferred. $1.05 in gas.

Overview | Logs (1) | State | Comments

Transaction Hash:	0x032542ecb17fe9a16fd492682cac13a7204d9638a8a7d430effb73166f69f607
Status:	Success
Block:	15811321 9 Block Confirmations
Timestamp:	1 min ago (Oct-23-2022 02:10:59 PM +UTC) | Confirmed within 4 secs
From:	0x5d1a27d0dc2215906beb77604cc56b333ab1c03f
Interacted With (To):	Contract 0xdac17f958d2ee523a2206206994597c13d831ec7 (Tether: USDT Stablecoin)
ERC-20 Tokens Transferred:	From 0x5d1a27d0dc221... To 0x4e42e973d81e6... For 613,000 ($613,613.00) Tether USD (USDT)
Value:	0 Ether ($0.00)
Transaction Fee:	0.00079999115 Ether ($1.05)
Gas Price:	0.00000001735 Ether (17.35 Gwei)

price per unit of gas willing to pay

1.05 USDT transferred. $1.44 in gas.

Overview | Internal Txns | Logs (4) | State | Comments

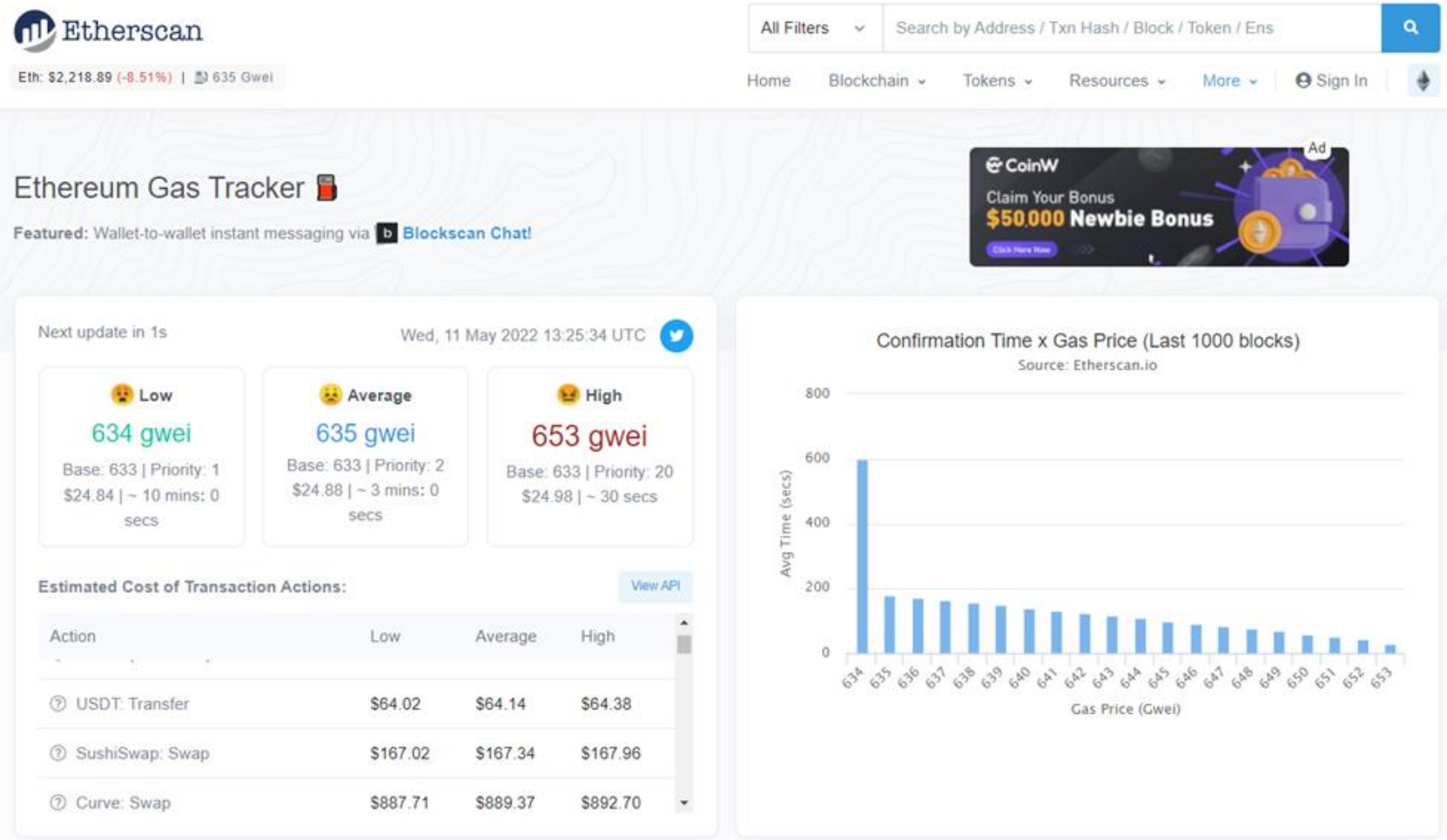
Transaction Hash:	0xe36007572d25ca5c49e3460a9e61925a04f11ea0b78948b92fa7e4e833d7d8bc
Status:	Success
Block:	15811326 14 Block Confirmations
Timestamp:	2 mins ago (Oct-23-2022 02:11:59 PM +UTC) | Confirmed within 5 secs
From:	0x29e8c93c8406727266cf2d577b91dd29b3991344
Interacted With (To):	Contract 0x7d655c57f71464b6f83811c55d84009cd9f5221c (Gitcoin: Bulk Checkout)
ERC-20 Tokens Transferred: 2	From 0x29e8c93c84067... To 0xeb439eed56426... For 1 ($1.00) Tether USD (USDT) From 0x29e8c93c84067... To Gitcoin: MultiSig For 0.05 ($0.05) Tether USD (USDT)
Value:	0 Ether ($0.00)
Transaction Fee:	0.001096961491777012 Ether ($1.44)
Gas Price:	0.000000013443814547 Ether (13.443814547 Gwei)

When the network is congested, gas cost can skyrocket.

What happened on May 11, 2022?

the day when terra and LUNA broke down

big increase in transaction cost



High level overview of DeFi protocols

01	Lending	• Suppliers deposit tokens and earn supply APY • Borrowers take out tokens and pay borrow APY • Rates are determined by smart contract and are accrued (compounded) in every block
02	Decentralized Exchange	• Token holders use their idle tokens to provide liquidity in pools of pairs or basket of tokens • Automated market maker (AMM) smart contract executes exchange orders in liquidity pools
03	Derivatives and Synthetics	• Smart contract creates structured product based on desired underlying asset (e.g. USD, TSLA) or states of the world (e.g. rainfall) • Counterparty risk is managed by margins
04	Asset Management	• Protocol identifies opportunities with maximum yield and smart contract executes trades • Smart contract rebalances portfolio according to desired objectives

There are only 2 types of variable revenue models in finance.

1. **Interest** (charged on notional principal and length of transaction.
2. **Fee** (charged on notional principal only)

DeFi 1.0 = basic provision with minimal computation (**low gas cost**)

DeFi transactions are not peer-to-peer, but **peer-to-contract** or **peer-to-pool**. Smart contracts act as the coordinator between different participants in the protocol. Liquidity is pooled to provide financial services without the need to know specific counterparties. The conditions governing each transaction are coded into contract and are visible to all since all smart contracts are information on blockchain state.

Putting this into our financial economics framework

The ability to store wealth and transact without relying on “trusted” third parties?

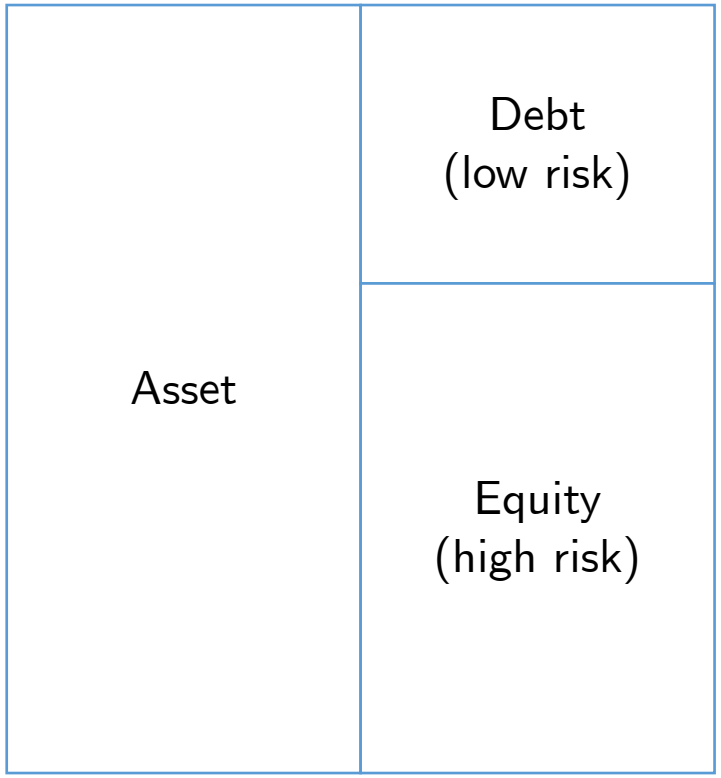
Contemporaneous (across form and space)

- Self-custody and permissionless payment
  → “self-sovereign” / “Not your keys, not your coins.”
- Exchange? – swap pools
  → trade directly at securities depositories

Intertemporal (across state and time) …?

- Capital allocation / fundraising? – lending pools
- Wealth management and risk allocation? – any multi-token pool

Mechanism design / financial contract is about **risk allocation**. Legal enforceability is often required for contractual commitment (helps lower transaction cost).



Risk in = risk out (ceteris paribus)

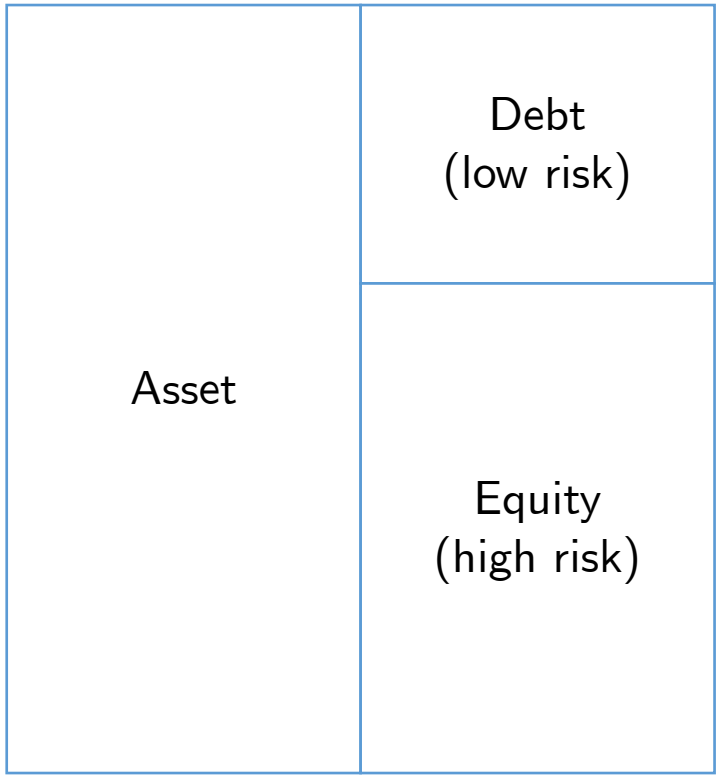
Redistribution of risk to those with greater capacity to bear risk can be value-enhancing.

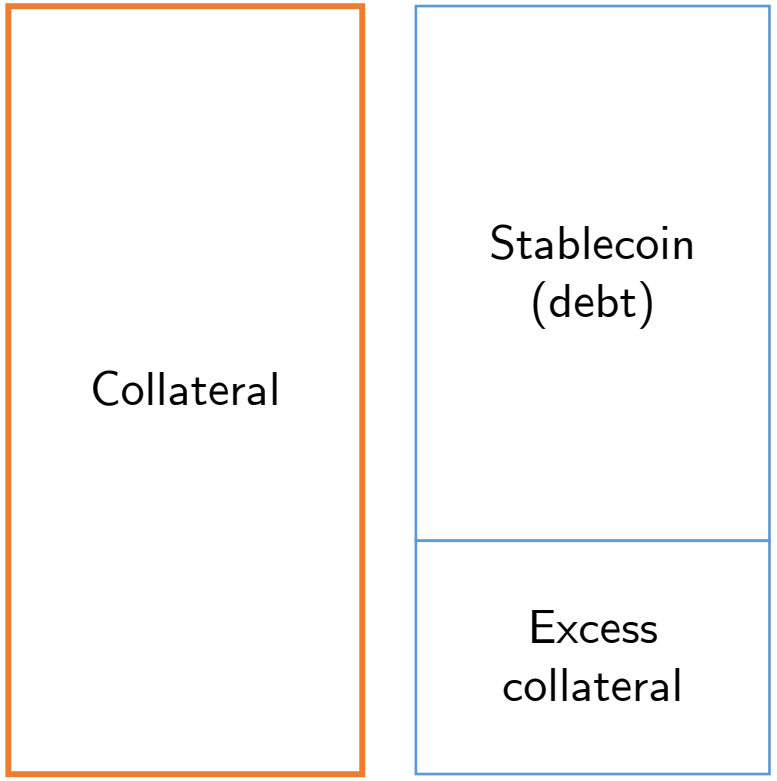
Asymmetric information: adverse selection, moral hazard
Agency cost: conflict of interest

Collateralization / residual risk bearer & skin in the game.

Many DeFi transactions are based on the same principles of security design: overcollateralization.

Examples: stablecoin CDP (DAI), collateralized DeFi loan





If users don't have enough excess collateral, they will be **automatically deleveraged** via liquidation.

Price information to calculate collateral value is not native to blockchain, and thus a **data oracle** is required to import that information for calculation.

MESSARI

Dai Minting and Redemption Example

Users can deposit collateral into vaults to mint/borrow Dai. Their underlying collateral may be redeemed upon paying back their loan plus interest

Minting Process

In this example a user deposits $200 of ether into a vault at a 200% collateralization ratio to maintain a margin of safety in case the collateralization ratio falls below the minimum 150%. The user then borrows $100 of Dai that Maker mints

Redemption Process

In this example a user redeems their $200 of ether from the vault after a 20% price decrease in ETH. They do this by repaying their borrowed Dai plus interest accrued on the loan which in this example is 1%

Data as of: Feb. 25 2021
Source: Messari

Will blockchain transform finance?

CHULALONGKORN BUSINESS SCHOOL
FLAGSHIP FOR LIFE

Blockchain allows permissionless fundraising and self-custody, but are your digital assets really held on-chain via private key wallets?

Do they really exist?

Not your keys,
Not your coins!

MARKETS | FINANCIAL REGULATION

Coinbase Says Users' Crypto Assets Lack Bankruptcy Protections

Cryptocurrency trading firm warns its customers could be viewed as general unsecured creditors

The trading platform Coinbase Global held $256 billion in cash and cryptocurrencies for its customers at the end of the first quarter.

PHOTO: SHANNON STAPLETON/REUTERS

By Paul Kiernan Follow
May 11, 2022 2:35 pm ET

PRINT AA TEXT

Listen to article (4 minutes)

TERRA LUNA

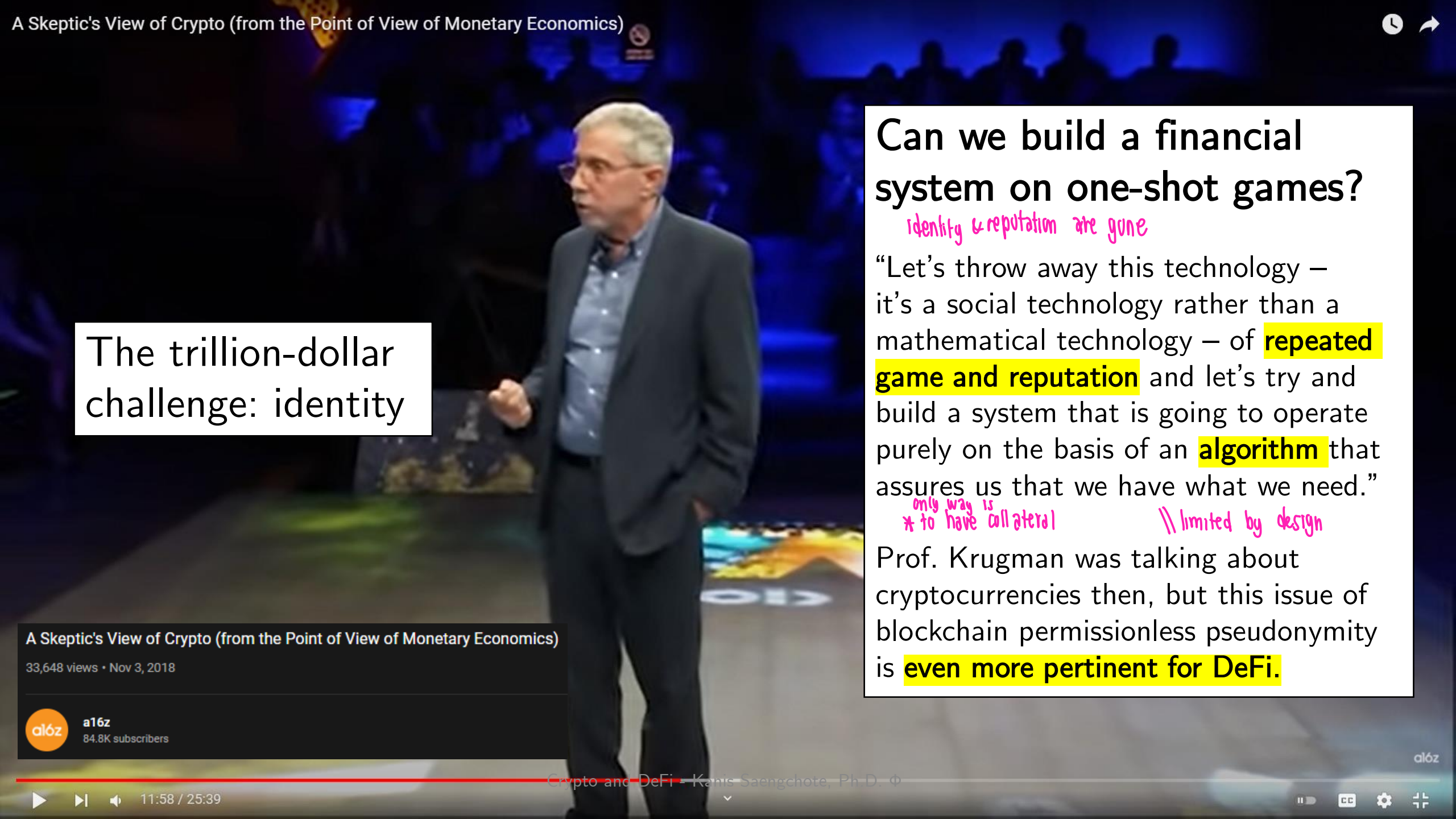
FTX
SALT
FTX

Failures in financial institutions stem from mismatches: revenue / expenses, assets / liabilities

Key takeaway: the best way to understand everything that's going on in DeFi is balance sheet accounting.

$$\textbf{Assets} = \textbf{Liabilities} + \textbf{Equity}$$

And we can more easily trace this relationship among all participants in DeFi.



Can we build a financial system on one-shot games?

identity & reputation are gone

"Let's throw away this technology – it's a social technology rather than a mathematical technology – of **repeated game and reputation** and let's try and build a system that is going to operate purely on the basis of an **algorithm** that assures us that we have what we need."

only way is
* to have collateral

\\ limited by design

Prof. Krugman was talking about cryptocurrencies then, but this issue of blockchain permissionless pseudonymity is **even more pertinent for DeFi.**

Banks and credit institutions are data companies

Ant Group + Add to myFT

Beijing summons Jack Ma over $37bn Ant IPO

Four Chinese regulators call in Ant founder and 2 other executives for questions ahead of Thursday's listing

Jack Ma last month gave a speech in Shanghai criticising regulators in China and abroad © FT montage; Bloomberg

Ryan McMorrow in Beijing and **Henny Sender** in Hong Kong
NOVEMBER 2 2020

71

Alternative lenders have made progress in addressing information asymmetry with detailed borrower-specific data.

"China doesn't have a systemic financial risk [problem], China's finance basically doesn't have risk, the risk is instead from lacking a system," said Mr Ma.

"**Today banks are still operating with a pawnshop mentality, needing collateral and guarantees are just like pawn shops . . . China's financial pawnshop mentality is the most serious**," he added.

"Supervision and regulation are two different issues," said Mr Ma. "Supervision is to watch and pay attention to development, while regulation is to manage when there is a problem. Right now we are strong at regulation but lacking in the ability to supervise."

Conclusion

Banks and credit institutions are data companies that allow wealth to be transferred across **form, space, time and space**.

The ability to increase trust in the presence of **uncertainty and information asymmetry** is the essence of the financial system.

Key takeaways

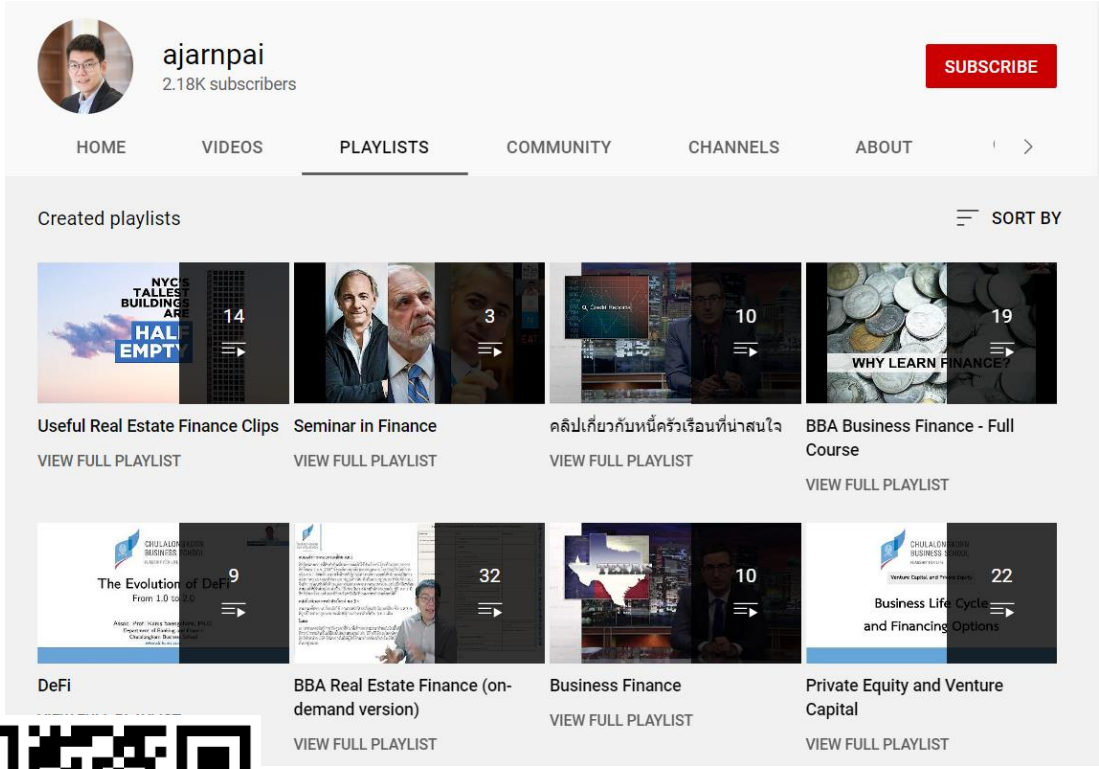
1. **Different forms of money exist**
   Some types of money are nature's gifts (social contract collective belief). Most others are formed as asset-liability relationship (economic contract as creditor)

2. **Pandora's box: permissionless interaction is now possible**
   Smart contract blockchains allow unfettered interactions (asset custody, fundraising, trading), where users are pseudonymous [permissionless] and direction interactions require gas payment [incentive].

3. **Trust is at the heart of financial system**
   Fundraising = a set or promises made in exchange for benefits today. Many aspects of trust cannot be coded on to the blockchain.

Thank you!

For more on DeFi and current issues in finance, please visit my channel ☺



← Please scan here to access channel

For my research, and CV please visit www.dr-kanis.com

Please scan here for downloadable e-book →