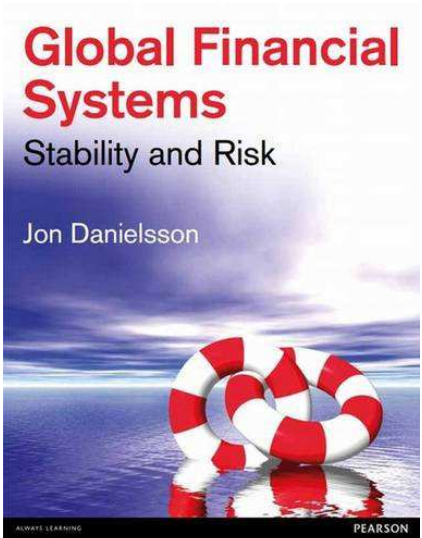
Global Financial Systems
Chapter 20
Digital Currencies

Jon Danielsson London School of Economics

To accompany
Global Financial Systems: Stability and Risk
www.globalfinancialsystems.org/
Published by Pearson 2013

Version 13.0, August 2026

Book and slides



- Updated versions of the slides can be downloaded from the book web page `www.globalfinancialsystems.org`

Digital currencies

Traditional currency

- Traditional money lives in *accounts* — ledgers at banks and payment systems
- Take a card payment of $20 — the money moves through a chain of accounts
  1. your account at your bank
  2. the card network routes the instruction
  3. to the merchant's bank
  4. to the merchant's account
- Nothing physically moves — each institution debits and credits its own ledger
- Every step needs verification, clearing and settlement — fees, delay and counterparty risk

What is a token?

- A token is a *digital claim* — akin to a casino chip
- It represents some asset — suppose it is fiat money, say \$20
- Change the owner of the token — I give it to you — and the claim to the \$20 moves with it
- A direct transfer from owner A to owner B, in one step
- No clearing or reconciliation — settlement is the transfer itself, faster and cheaper

Blockchains and permissions

- A token can sit on a *blockchain* — a shared ledger where validation is spread across participants rather than run by one operator
- But a blockchain is *not necessary* — any trustworthy database will do, and is usually faster and cheaper
- Blockchains differ by *who is allowed to write to them*
  - *Permissionless* — anyone can validate, as in Bitcoin
  - *Permissioned* — only approved parties can, as for a central bank or a consortium
- CBDCs typically use a permissioned ledger, or none at all, while stablecoins mostly sit on public chains
- How a blockchain actually works — hashes, blocks and mining — is in the appendix

Two families of digital money

- Cryptocurrencies keep the public chain and its consensus process — no issuer, no backing, volatile — we set them aside
- Digital currencies keep the token and add an *issuer*
  - *Private* — stablecoins, issued by firms and pegged to fiat (next section)
  - *Public* — central bank digital currencies, the fiat itself (later)

What is a stablecoin?

- *Private money in token form*, designed to trade at *par* with a reference fiat currency — usually the US dollar
- Issued by *private firms* — Circle (USDC), Tether (USDT) — not central banks
- Usually *fully backed* by liquid assets — cash, bank deposits and short-dated Treasuries — though reserve quality and disclosure differ by issuer
- Early *algorithmic* designs held the peg without reserves — TerraUSD collapsed in May 2022, taking some $40bn of the wider Terra ecosystem with it
- On-chain, 24/7 and low-cost (next slide)

What does on-chain mean?

- A transfer is *on-chain* when it is recorded and settled directly on a *public blockchain*
- The token moves on the ledger, peer-to-peer and visible to all — no bank in the middle
- The contrast is *off-chain* — value moving through traditional accounts and settled later
- So on-chain transfers are near-instant, 24/7 and borderless — though moving in and out of fiat is neither
- Stablecoins ride on a few public chains — in mid-2026 Ethereum (≈49%), Tron (≈29%), Solana (≈5%)

How the industry is organised

Issuers Circle, Tether — mint the tokens and promise one-to-one convertibility with the dollar

- To *mint* is to create a new token — a dollar comes in, goes into the reserves, and a token goes onto the chain
- Redemption is the reverse — the issuer pays out the dollar and *burns* (destroys) the token

Primary participants redeem directly with the issuer at, or near, par — wholesale only, Tether's published minimum is around $100,000

Secondary markets exchanges, brokers, OTC desks and market makers — from licensed venues to informal money changers, open 24/7

End users trade through the intermediaries above, or directly on-chain

What stablecoins are used for

Crypto trading in and out of crypto without converting to fiat — much the largest use

Cash layer settlement and collateral for tokenised assets and DeFi

Idle balances on-chain cash management

Cross-border transfers individuals and smaller businesses, at a fraction of the fees on the old rails

Currency escape a dollar substitute where local money is weak, and a way around capital controls — still very small

- Everyday domestic payments remain limited
- Overwhelmingly USD-denominated, whatever the use

Stablecoins and dollarisation

- Citizens of weak-currency countries have always *dollarised* — holding dollars for savings and daily transactions
- The traditional routes all have problems
  - Paper dollars are bulky and hard to secure
  - Domestic dollar deposits can be confiscated or controlled
  - Foreign bank accounts are hard to access
- Stablecoins ease all three — cheap to acquire, easy to store and quick to transfer, and harder for a government to reach
- So adoption is fastest where currencies are weakest — Turkish stablecoin purchases have run at 4.3% of GDP and gross stablecoin flows in Latin America at 7.7% of GDP
- Argentina, Nigeria and Lebanon show the same pattern

Stablecoins are not the root of the problem — they are a response to the problems of the local currency

Market scale

- About *$300 billion* outstanding in 2026 — Tether (USDT) ≈$180bn, USD Coin (USDC) ≈$73bn, the rest in smaller coins
- The top two issuers are about 85% of the market
- Still *small* beside traditional money — the US monetary base ≈$5.5 trillion, M1 ≈$19.8 trillion

Non-USD stablecoins

- Stablecoins can be issued in any currency, but are *overwhelmingly USD* — almost all of the ≈$300bn
- Euro coins are only ≈€700 million, while yen, Singapore-dollar and sterling coins are emerging but tiny
- Why so small? Little cross-border or crypto-trading demand, and weak network effects
- A variant — a coin in a currency pegged to the dollar, such as the UAE dirham, gives dollar exposure outside US banks

Regulation

US — GENIUS Act (2025) banks and approved non-banks may issue stablecoins, backed 1:1 by permitted reserves — cash, deposits, short Treasury bills, repo and government money funds — with monthly disclosure, and issuers may not pay interest

US — Clarity Act before Congress in 2026 — would allow narrower activity-linked rewards, which issuers want and banks resist

EU — MiCA euro stablecoin reserves must be low-risk and liquid — stablecoin rules applied from June 2024, the rest from December 2024

Rest Singapore has a framework (2023), China bans them, most others still mixed

Stablecoin issues

Danielsson and Macrae (2026)

modelsandrisk.org/appendix/stablecoins

The concern is runs

- Stablecoins are still small, so both the advantages and the threats are mostly hypothetical
- But network effects can scale a payment instrument quickly — an order-of-magnitude increase within a few years is entirely possible
- *Much of what follows is conditional* — if and when stablecoins become large enough to matter
- In stress, money-like assets are judged by a single criterion — can they be converted into fiat *at par, quickly and in size*?
- Monetary sovereignty, disintermediation and bond-market spillovers emerge gradually and can be handled by ordinary regulation
- A run can only be addressed *before* the crisis emerges

Par is manufactured, not inevitable

- The one-to-one peg is neither guaranteed nor self-executing — it is produced continuously
- Arbitrage along the industry chain holds the price at par — the issuer, the primary participants and the secondary markets
- The coins trade 24/7 while the reserves trade in business hours
- In stress, liquidity providers step back, spreads widen and prices reflect fire-sale values and rumour

Three failure modes

Asset reserves are worth less than liabilities

Plumbing conversion fails even though reserves are fine — outages, banking hours, disrupted rails, compliance freezes

Belief everyone runs because everyone expects everyone else to run Diamond and Dybvig (1983)

- The modes interact — banking rails down over a weekend can trigger a belief run, and fire sales can turn a solvent issuer into an insolvent one

Even a stablecoin backed by perfectly safe assets can run

Why stablecoins are run-optimised

- Stablecoins are not designed to run — they are designed to reduce frictions, and that facilitates runs
- Transfers settle in near real-time, markets never close and holders can reallocate globally
- The fastest leg is on-chain — stablecoin-to-stablecoin flight is close to instantaneous, so stress migrates between issuers before it touches the banking system
- Reserves sit in Treasuries, so heavy redemptions transmit stress to the Treasury market
- Cross-border by default — stress is not confined within the domestic perimeter
- Private circuit breakers — freezes, gates, throttles — create the incentive to *run before the gate*

The features that make money usable also make it runnable

The anatomy of a run

- The speed and form of exit depend on *who* is running
  - Retail is slowest — identity checks and banking rails
  - Institutions move faster, through OTC desks and direct redemption
  - On-chain algorithmic systems are the fastest of all
- Early on, the run is coin-to-coin — risk is redistributed across issuers without touching system-wide liquidity
- Prices slip first in secondary markets, visible on-chain outflows follow, then liquidity providers widen spreads or step away
- Damage escalates only when secondary markets go illiquid and redemptions force reserve sales into already stressed markets
- The run begins where friction is lowest — on-chain — and becomes politically visible only later, in bank money

Old fragilities, new speed

- The fragilities are not new — Bagehot (1873) identified them
- What is new is the speed, the cross-border reach, the obscurity and the compression of coordination time
- And the loss of the *public circuit breakers* that contain banking crises — business hours, deposit insurance, the lender of last resort, suspension of convertibility
- Stablecoins have only private controls, built for compliance (next slide)
- Stablecoins can also accelerate bank runs — in a general banking panic, a coin fully backed by Treasuries is an attractive destination for fleeing deposits
- Had stablecoins existed in the autumn of 2008, that crisis would probably have been faster, more severe and harder to manage

Gates and circuit breakers

- In principle, stablecoin runs can be controlled the way bank runs are — freezes, blacklists, throttles and gates
- But gates are unpopular — an issuer that imposes them loses business to those that do not, so nobody adopts them voluntarily
- Only a *binding mandate on all operators* can make them a credible defence
- Even then, the threat of a gate creates the incentive to exit *before* it is imposed
- So the rules, the plans and the operations must be in place *long before* problems emerge — and used quickly and decisively when they do

At scale — the Treasury market

- Reserves already hold some $150 billion of short-dated Treasuries and repo — small beside a $28 trillion market, but concentrated in a few custodians and dealers
- If stablecoins grow, their reserves become *large holders of government bonds*
- A run then forces reserve sales into a falling market — pro-cyclical, as money market funds showed in 2008 and 2020
- A stablecoin crisis becomes a *contagion vector* — coins in several currencies, or a coin run coinciding with a run on a country
- And a vehicle for flight from one currency and its bond market into another — disrupting foreign exchange and government bond markets in both countries

The backstop question

- Bank deposits have deposit insurance and a lender of last resort — stablecoins have neither, at least not explicitly
- History is full of backstops that were unthinkable until they were not — Bagehot after Overend Gurney, the Federal Reserve after 1907, the FDIC after the Depression
- Once an asset is widely held it becomes a *middle-class good* the state is expected to guarantee Chwieroth and Walter (2019)
- If stablecoins become enmeshed in day-to-day transactions, they become, like banks, too big to fail
- We have already seen it — when SVB failed in March 2023, USDC de-pegged over Circle's $3.3 billion deposit, and par returned only when the authorities guaranteed all SVB deposits

The view from the US Treasury

"The dollar now has an internet-native payment rail that is fast, frictionless, and free of middlemen. This groundbreaking technology will buttress the dollar's status as the global reserve currency, expand access to the dollar economy for billions across the globe, and lead to a surge in demand for US Treasuries, which back stablecoins. ... The signing of this bill marks a seminal moment for digital assets and dollar supremacy."

Scott Bessent, US Treasury Secretary,
on the signing of the GENIUS Act, July 2025

Stablecoins and the dollar

- Stablecoins are overwhelmingly dollar instruments — the dollar is the reserve currency, the settlement currency for cross-border commerce, the most trusted foreign currency and crypto's unit of account
- The US gains three ways
  - *Fiscal* — reserves held in Treasuries channel overseas savings into US debt
  - *Privatised seigniorage* — issuers capture the yield on the reserves, paying US taxes and wages
  - *Geopolitical* — the world becomes more dependent on US-controlled infrastructure
- Even offshore issuers depend on US banks, custodians and the OFAC compliance perimeter — Tether is based in El Salvador, but its viability is decided in the US

"The dollar is our currency, but it's your problem" — Connally, 1971

The exorbitant obligation

- The benefits accrue to the US now — the one genuine cost, the latent backstop, is contingent
- If a major issuer broke its peg, countries that dollarised through it would face losses the US has *no mechanism* to address — swap lines reach sovereigns, not retail token holders
- A crisis in a dollar instrument brings a demand for the US to respond — refusing could look like default on the obligations of the reserve-currency issuer, threatening that very status
- In a banking panic, flight into Treasury-backed coins makes stablecoins a *crisis amplifier* — testing whether the crisis-response framework still works

Four kinds of country

The US the main beneficiary — gains now, a latent backstop obligation later

Hubs Singapore, Hong Kong, the UAE, the UK — capture the exchanges, custody and licensing with little dollarisation risk — the on-chain eurodollar market

Most countries credible money and sound payments, so little to gain or fear — *benign neglect* is appropriate

Weak-currency countries the fastest adoption and the most to lose — dollarisation is the *symptom*, the currency is the problem

Weak-currency countries

- In a confidence shock, stablecoins become the natural conduit for *currency flight* — around the clock, offshore and often outside capital controls
- Faster outflows, sharper exchange-rate pressure, more strain on reserves
- Outside help is slower than the crisis — Fed swap lines reach only a narrow, discretionary set of central banks
- Dollar clearing runs through CHIPS, a private system of about 40 banks — a country facing a run has no leverage over it, and issuers freeze wallets when law enforcement asks, most consequentially the US
- The authorities cannot control informal networks — if they cannot see the activity, they cannot stop it

The countries with the most to lose are those where adoption is fastest

What should the authorities do?

- Prohibition is tempting but unlikely to work — driving activity underground ends monitoring altogether
- Most countries should monitor stablecoins without granting them the status or protection of banks
- Weak-currency countries can only reduce the *demand* — credible local money and payments that work, with PIX and UPI the template
- All countries should decide in advance what to do when a coin too politically embedded to fail, fails
- For most countries, *CBDCs* and a legal framework for tokenised transactions answer the challenge (next section) — perhaps crypto's lasting legacy

Where stablecoins leave policy

- Stablecoins exist because of demand for stable, accessible, liquid money — and the features that make money attractive also make it runnable
- The fragilities are a century and a half old — stablecoins accelerate and amplify them
- The benefits accrue largely to the United States, while some of the costs fall on countries that cannot provide the backstops a crisis requires
- Who stands behind a stablecoin when everyone tries to exit at once?

Exorbitant privilege comes with exorbitant obligations

What is a CBDC?

- A CBDC is the national currency issued digitally by the central bank — as tokens or as accounts
- A digital form of cash — a direct claim on the central bank, like a banknote
- Unlike bank deposits, which are claims on a commercial bank
- And unlike stablecoins, which are private tokens promising to track fiat — a CBDC *is* the fiat
- It runs in parallel with cash and deposits, not replacing them
- Retail (for everyone) or wholesale (financial institutions only) — discussed below

Why issue a CBDC?

- A common motivation is competition from private payment systems
- Especially foreign systems threatening monetary sovereignty
  - Above all *dollar stablecoins* (previous section)
  - Also big-tech wallets and foreign payment systems — Alipay, WeChat Pay, Apple Pay
- The second driver is the *tokenisation* of assets and wholesale settlement (next slide)
- Governments face a dilemma — CBDCs risk disrupting banking but inaction cedes control

Tokenised assets and the wholesale demand

- Finance is being *tokenised* — bonds, money market funds and deposits are moving onto ledgers
- A tokenised asset needs a *cash leg on the same ledger*, so that asset and payment settle together, instantly — atomic delivery versus payment
- That removes the principal risk the old clearing chain carries (first section), though legal, liquidity and operational risks remain
- The candidates for the cash leg are stablecoins, tokenised bank deposits or *tokenised central bank money* — a wholesale CBDC
- Central banks want settlement to stay in *central bank money*, as it does today — hence the wholesale push
- Retail demand is weak, but the wholesale demand is real (below)

The obvious implementation — the direct model

- The central bank issues tokens on its own fiat, on a ledger it controls — possibly a blockchain, but none is needed
- No mining and no consensus problem — trust comes from the central bank
- People swap their old-school fiat for tokens and transact by swapping tokens on the central bank ledger
- In effect, everyone banks at the central bank
- So the central bank must run retail services for millions — onboarding, identity checks, fraud, support — which central banks are not built for
- And it is very disruptive — replacing big parts of the financial system's infrastructure (below)

What the direct model would mean

- Every transaction is visible to the central bank — it can monitor and control them (next slide)
- Private financial institutions are much diminished — more power to the government (below)
- Monetary policy gains new tools — vary the number of tokens directly, pay interest on them, even at negative rates, and make transfers straight to citizens
- Tempting for the state, worrying for everyone else

The privacy paradox

- Cash is the most private payment instrument there is — its digital replacement is the least
- Tokens on a central bank ledger are traceable by default — salary, rent, donations and the pub bill, one record
- Democratic societies demand privacy from state surveillance — in China, the visibility is the attraction (below)
- Anonymity collides with anti-money-laundering rules, so most designs sacrifice privacy for compliance
- The attempted fixes — offline payments (the digital euro), transaction limits, tiered anonymity, zero-knowledge proofs
- In the US, the House bill banning a retail CBDC is called the Anti-CBDC Surveillance State Act

Banking sector disruption

- A bank deposit is a claim on a bank — a CBDC is a claim on the state, so free of credit risk
- In calm times deposits might drift to the CBDC — in a panic they would flood to it, accelerating the run (recall the stablecoin discussion)
- Deposit insurance exists precisely to stop that — an unlimited CBDC would blunt it
- Banks create most of the money supply through lending — if the deposits leave, who lends? Does the central bank become the retail lender?
- This is why CBDC designs carry *holding limits*, and why nearly everyone has retreated to *intermediated* models (next slides)

Hybrid model — intermediated retail CBDC

- The CBDC remains a direct claim on the central bank, but private banks face the clients
- The central bank issues and settles — the banks do the retail work it cannot (as above)
- Clients hold and transact in central bank money by proxy, through their bank
- This is the digital euro's design (below)
- A close cousin is the *synthetic CBDC* — private e-money fully backed by reserves at the central bank, not itself a central bank liability — in effect a regulated stablecoin
- Substantial new infrastructure, so slow to implement

Wholesale CBDC

- Restricted to financial institutions — the public never touches it
- Banks already hold digital central bank money — *reserves* — so a wholesale CBDC is simply reserves in token form
- The point is the tokenised world discussed above — a cash leg on the ledger, settling asset and payment together, atomically
- And cross-border — tokenised settlement between currencies, as in mBridge (below)
- Banks remain customer-facing, on existing infrastructure — far cheaper and less risky than any retail model

The strategic split

- The major monetary areas have chosen opposite answers
- In 2025 the US barred federal agencies from pursuing a retail CBDC by executive order, and a statutory ban has passed the House
- It chose *private dollar stablecoins* as the internet dollar — the GENIUS Act
- Europe and China have gone the *public* route (next slides)
- The open question is *public or private* — and whose currency it carries

The digital euro

- The flagship advanced-economy project — driven by *strategic autonomy*, not user demand
- About two-thirds of euro-area card payments run on Visa and Mastercard, and dollar stablecoins add a new dependence
- Intermediated design — banks and payment firms distribute it, with *holding limits* to protect bank deposits — the ECB has tested figures up to €3,000, with the banks pushing for far less
- Offline payments for cash-like privacy
- Council and Parliament backing in 2025–26, a pilot planned for 2027 and possible issuance in 2029
- Banks worry about deposit flight, and privacy scepticism runs deep

China — the e-CNY

- The largest CBDC pilot — around 225 million personal wallets and some 17 trillion yuan (about $2.3 trillion) in cumulative transactions by late 2025
- That sounds large but is tiny — Alipay and WeChat Pay process a similar amount in a couple of weeks, and reining in that duopoly was part of the motive
- Fully centralised and two-tier — the PBoC issues, the banks distribute — and from 2026 balances in bank wallets pay *interest* and count as bank deposits, no longer just digital cash
- Every transaction is visible to the central bank — surveillance the authorities consider an advantage — and programmability allows expiry dates and directed spending
- Now pushing the e-CNY abroad — an operations centre in Shanghai and the mBridge cross-border platform — part of the longer game of renminbi *internationalisation* and sanctions resilience

The rest of the world

- Most central banks are exploring a CBDC — 85 of the 93 in the latest BIS survey — but few have launched
- India pilots the digital rupee, but UPI already delivers instant, cheap payments — the CBDC adds little
- Brazil's Drex is a wholesale tokenisation platform rather than digital cash — and PIX already covers retail
- Canada has scaled back, Sweden has paused for a legal review and the UK is still in design — none has committed to issue
- The pattern — where domestic payments already work, retail CBDC demand is hard to find

Adoption reality check (2026)

- Every live retail CBDC has minimal uptake
  - Nigeria's eNaira — under 2% of the population
  - Bahamas Sand Dollar and Jamaica Jam-Dex — under 1%
  - The Eastern Caribbean's DCash pilot ended in 2024, pending a successor
- The large pilots have not found organic demand either (previous slides)
- Wholesale is where the momentum is — Project mBridge (the BIS exited in 2024) and the bank-to-bank Project Agorá

Why retail CBDCs struggle

- For the user there is no problem to solve — cards, apps and instant payments already work, and network effects protect them
- The benefits accrue to the state, the risks to the user — privacy above all
- Banks quietly resist — disintermediation with no upside for them
- So there is no constituency — the public does not ask for it, the banks do not want it and many politicians oppose it
- Wholesale is different — there the users are institutions with a real settlement problem
- None of this bears on a CBDC issued to preserve access to public money rather than to win users

"A solution in search of a problem"
Christopher Waller, US Federal Reserve, 2021

Appendix — how a blockchain works


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.
E-mail: SCOTTADAMS@AOL.COM
© 1995 United Feature Syndicate, Inc.(NYC)

Trusting data

- Double entry bookkeeping solved the problem of trusting accounting books
- Records today are almost always kept in databases (ledgers)
  - accounting data, identity management, land registers, asset ownership,...
- That can be updated maliciously or by mistake without anybody knowing — data is *mutable*
- What prevents that — creating trust — are institutions
  - legal system (police, courts), banks, government
- We trust institutions because if they cheat or make too many mistakes they would forgo future profits/benefits

$$\text{profit from cheating} < \text{NPV future profits}$$

Blockchain — Classical (cryptocurrency) sense

- A new type of database (ledger)
- Designed so information cannot be changed without it being evident — data is *tamper-evident*
- The entire transaction history can be validated by any full node
- All data is public — complete transparency
- Consensus comes from the protocol rules and the validators who follow them
- Publicly auditable — everybody can see the blockchain
- Held in many copies — nobody can quietly change records
- Decentralised
- Integrity rests on cryptography and incentives rather than on institutions

Trust model

- Public: it is assumed that the controllers of a majority of the hashing power (or of the stake) have a strong enough incentive to keep an accurate record and so can be relied on as accurate by all others
- Permissioned: it is assumed that the permissioned entities have a strong enough incentive to keep an accurate record and so can be relied on as accurate by all others
- Consensus comes by *proof of work* or *proof of stake* (next slide)

Proof of work versus proof of stake

- *Proof of work* — miners compete to solve a hard puzzle (the nonce), and the winner adds the block
  - Security comes from the cost of computing power — energy-intensive
  - Bitcoin still uses it
- *Proof of stake* — validators post ("stake") their own coins for the right to add blocks
  - Cheat and part of the stake is destroyed ("slashing") — security from money at risk, not electricity
  - Ethereum switched in 2022, cutting its energy use by over 99%
- Both make rewriting past blocks costly enough to deter it

Digital fingerprint — Hash

- Fixed-length summary of data, whatever the size of the data
- A tiny change to the data gives a completely different hash
- Finding two inputs with the same hash is designed to be computationally infeasible

Data	Hash(Data)
J	c3e0836d
K	b5874a6f
London School of Economics	42765779
London School o*t* Economics	ab4ed6fe

- When done with R function

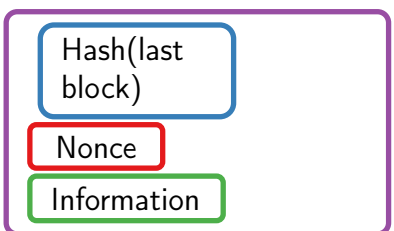
```
digest("London School ot Economics",algo="xxhash32")
[1] "ab4ed6fe"
```

Nonce

- A number used once in a cryptographic protocol
- In proof of work it is a field in the block header that miners vary
- They try values until the hash of the header falls below the target

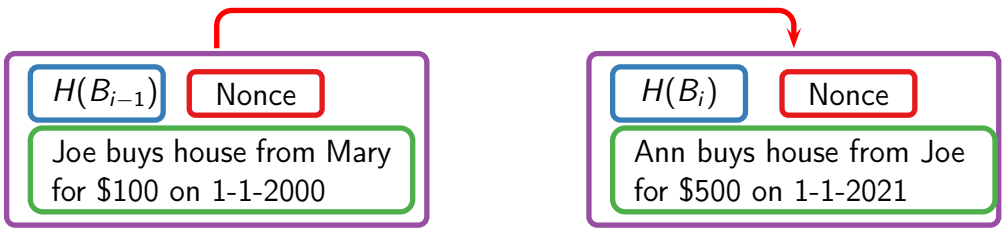
Block

- Information, e.g.
  - ownership of house, art, money, ...
  - record of transaction, house sold by person A to person B
  - the contents and movements of a shipping container
  - steps in procurement process



Blockchain — Blocks linked in sequence

- Maybe record of a sale of a house



Updating information

- By default, blockchain is publicly visible
- A new block batches the pending transactions
- Its header carries the hash of the previous block's header
- Changing an old block breaks every later hash, so the change is visible
- Rewriting history also means outrunning the consensus rules

Trust — Who can add to chain?

- Originally a cryptocurrency *miner*; now often a *staking validator*
- The cost of (maliciously) updating *past blocks* higher than profit from doing so
- That is a *public permissionless* blockchain (ledger)
- Alternative is *permissioned*

Public and permission-less blockchains

- Open to the public, and anyone meeting the protocol's requirements can take part in validation
- Full nodes keep a copy of the ledger — most users do not
- Use a distributed consensus mechanism to reach a decision about the eventual state of the ledger
- The majority of cryptocurrencies fall under this category

Private and/or permissioned blockchains

- Private means not publicly visible
- Permissioned means some entity decides what can be added
  - bank, consortium, firm, government, ...
- Then the blockchain is essentially a database with special features (like preventing updates of past records, but have to trust the stewards of the blockchain)
- Examples: JPM Coin (now Kinexys); Facebook's Libra/Diem, since abandoned

Are blockchains a good idea?

- Answer depends very much on whom you ask
- Some say they will revolutionise the world
- Others that blockchains are a fad that will go away
- Much depends on cryptocurrencies
- Blockchains (without cryptocurrencies) may be a useful database technology
- Not efficient compared to existing database technology
- Making it easier to resolve disputes by increasing the amount of information that both parties agree
- Important for accountants and IT people
- But not revolutionary

Bibliography I

Bagehot, W. 1873. *Lombard Street.* London: H.S. King.

Chwieroth, Jeff, and Andrew Walter. 2019. *The Wealth Effect: How the Great Expectations of the Middle Class Have Changed the Politics of Banking Crises.* Cambridge, UK: Cambridge University Press.

Diamond, D.W., and P. Dybvig. 1983. "Bank Runs, Deposit Insurance, and Liquidity." *Journal of Political Economy* 91:401–419.