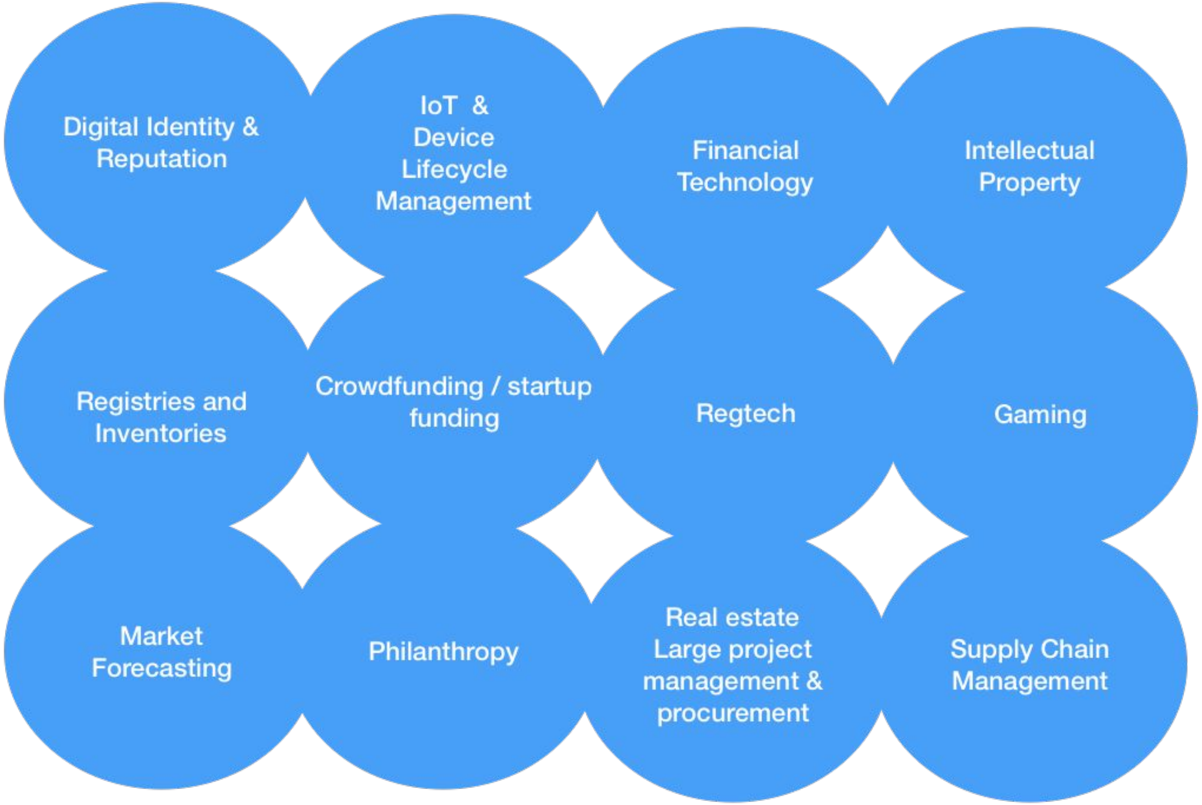
Blockchains & Distributed Ledgers

Lecture 10

Dimitris Karakostas

Slide credits: DK, Aggelos Kiayias

(Possible) Applications of DLT



Digital Identity & Reputation

IoT & Device Lifecycle Management

Financial Technology

Intellectual Property

Registries and Inventories

Crowdfunding / startup funding

Regtech

Gaming

Market Forecasting

Philanthropy

Real estate Large project management & procurement

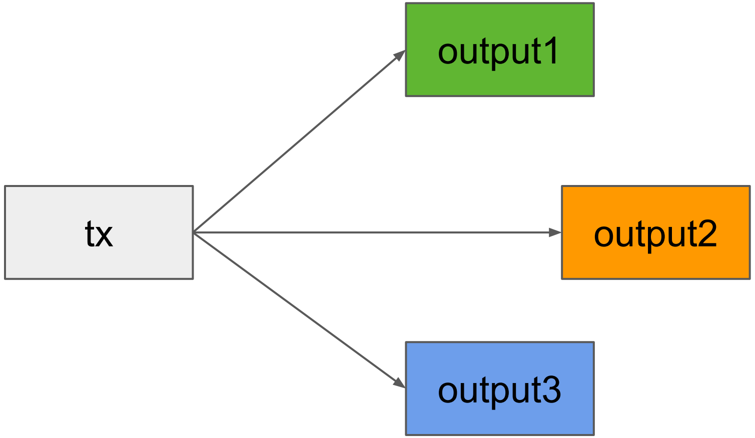
Supply Chain Management

Use an independent DL or piggyback on existing?

Scheme	**Advantage**	**Disadvantage**
Piggybacking	Potential for higher assurance	Need to engineer or program protocol rules into existing ledger
Independent	Ability to customise protocol & enforce individual properties	Might attract a small set of initial nodes and initially be less trustworthy

Coloured Coins

- Even though Bitcoin can be treated as fungible, it is not:
  - the smallest Bitcoin denomination (satoshi) can be tracked following some convention
- “Colouring" outputs so they represent specific assets



Coloured Coins

- Use of the OP_RETURN opcode
  - OP_RETURN signifies that a transaction output is invalid (and unspendable)
  - Can be followed by 80 bytes of data
  - Paying to an OP_RETURN enables storing personal data on the blockchain
- Burn one output to define colouring information for the (rest of the) transaction
- Bitcoin transaction fees still apply
  - transactions have to be formed with OP_RETURN
  - a small amount of storage permitted
- The secret-key of the coloured account controls asset ownership
  - Marker outputs (via OP_RETURN) can be used to further specify quantities transferred etc
  - Accounts should hold a balance to ensure the ability to transfer them onwards

Coloured Coins

- Bitcoin miners do not enforce proper rules of colouring
- Coloured transactions are treated as regular transactions by “colour-blind” miners
- Colouring rules might not be respected by an indifferent or malicious miner
    - Parsing algorithms for colours should take this into account

Applications

Digital economy (on a blockchain)

- Use a blockchain to record monetary transactions
- Create new money based on pre-determined algorithm
- **Issues:**
  - Why would people use on-chain tokens as money instead of commodity? Why would someone give away (spend) a BTC, if they expect its price (in USD) to increase)?
  - How to accurately valuate a blockchain-based economy? (e.g., market capitalization)

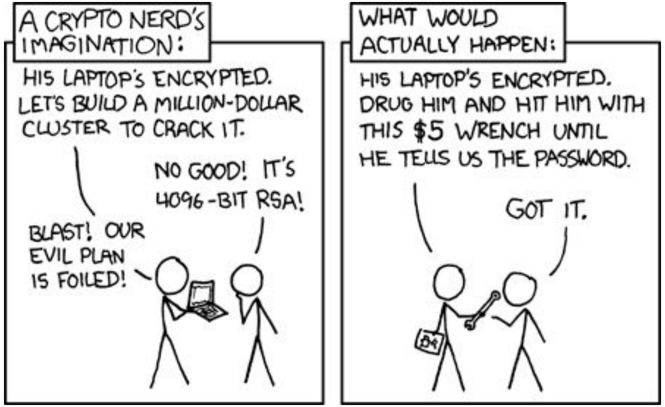
Name registry (on a blockchain)

- Use a blockchain to register names
- Useful in the context of DNS (domain name system) and public-key directories
- Censorship-resistant
- Examples:
  - *Namecoin*: separate blockchain, based on Bitcoin protocol
  - *Blockstack*: piggybacking on the Bitcoin blockchain, as in the case of colored coins
  - *ENS (Ethereum Name Service)*: domain registry implemented as an Ethereum smart contract
- **Issues:**
  - How to connect blockchain-issued names with the rest of the internet?
  - What if some domains *should be* taken down?

Land ownership (on a blockchain)

- Issue a new digital asset linked to land title
- Store information in the digital asset that links to an information resource
    - e.g., insert a URL to real-world registry or an identifier for a torrent file
- Digital asset becomes representation of ownership
    - He who controls the asset can prove or transfer ownership of the linked land
- Same idea can be extended to any real-world asset
- **Issues:**
    - What happens if the information source is no longer available (e.g., the URL breaks)?
    - What if the legal system does not recognize on-chain representation?

Supply chain tracking (on a blockchain)


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

- Real-world products
  - E.g., clothes, shoes, meat, olive oil, even diamonds
- Create a digital fingerprint of the object
- Register the fingerprint on a blockchain
- Record every change in the object's state
  - E.g, creation at source, transportation, selling/buying
- **Issues:**
  - How do you create a fingerprint, i.e., a (unique) digital representation of a physical object?
  - How do you make sure that people that handle the object *actually* record its state changes? What if someone bribes someone to insert false on-chain data?

Philanthropy (on a blockchain)

- An NGO/philanthropic organization creates a smart contract
  - E.g., to collect funds for building a school
- People send funds to the contract
- The contract keeps the funds in escrow:
  - When a proof that the project is complete is provided, the contract releases the funds
  - If a deadline passes, the remaining funds are returned to the participants
- **Issues:**
  - What kind of (secure) proofs of *real-world actions* could be understandable by a smart contract?
  - How can you prevent embezzlement, i.e., a corrupted official publishing incorrect proofs?

Prediction Markets

- A market that enables trading on future events
- Oracles provide real-world information on whether an event occurred
- Example: “10 tornadoes will hit USA in 2020”
  - participants bet in favour or against the event
  - market shares: YES = α, NO = $1-\alpha$; total investment: X; probability of event happening: *p*
  - Expected Profit of YES = $pX - \alpha X$
- Use prediction markes for:
  - Gambling, insurance purposes, ...
- **Issues:**
  - Do you trust the oracle? Can you use a decentralized oracle for *real-world* information?
  - Events may not be well-defined, so whether an event actually occurred can be disputed or depend on oracle (e.g., is Puerto Rico USA?)

Gaming and art collection (on a blockchain)

- In-game currency on a blockchain
  - E.g., Ethereum-based game tokens
- Digital collectibles
  - E.g., trading cards, virtual animans (CryptoKitties), NFTs (Non-Fungible Tokens) of art works
- On-chain games
  - Gambling, strategy games, social network games, ...
- **Issues:**
  - Gaming companies typically want control of in-game economy - why would decentralization benefit them?
  - If some aspects are off-chain (e.g., game graphics or real-world art work), what happens if the company does not support the token system anymore?
  - Why would users pay fees to play, when centralized options are free (or, at worst, pay-to-win)?

IoT and micropayments (on a blockchain)

- IoT devices connected to the internet
  - E.g., smart fridges, sensors
- Utility meters
  - E.g., electricity or water consumption
- User pays in real-time with multiple “micro”-payments to the service provider
- Alternative to subscription model
- Monetization of user data
  - User can get income for selling their personal data
- **Issues:**
  - Blockchains *don’t scale* - fees increase dramatically as usage tends to congestion
  - Blockchains *are not private* - why would you share your daily data with the whole world?
  - Even if you got paid for it, would you want to sell your personal life?

Crowdfunding (on a blockchain)

- A project creates a smart contract that issues tokens
    - Initial Coin Offering (ICO), ERC20 Ethereum tokens
- Users give coins in exchange for tokens
    - Buy tokens with ETH
- Tokens can:
    - Be used in a future platform that the project creates (utility tokens)
    - Be used as investment, be resold, offer yield (securities)
- **Issues:**
    - How can you guarantee that project will not run away with the funds (e.g., exit scam)?
    - What if project tries to scam investors and authorities, e.g., claim a security is a utility token?
    - Are the promises of the project verified/regulated? Will the project face penalties for lying?

Decentralized Finance

Finance

- {creation, management, investment} of **money** and **financial assets**
- Financial assets: non-physical assets whose value is derived by contractual claim
    - Bank deposits, stocks, bonds, loans
- Financial services
    - Lending/borrowing, issuing securities, managing fund
- Financial markets: marketplace for *trading* financial assets

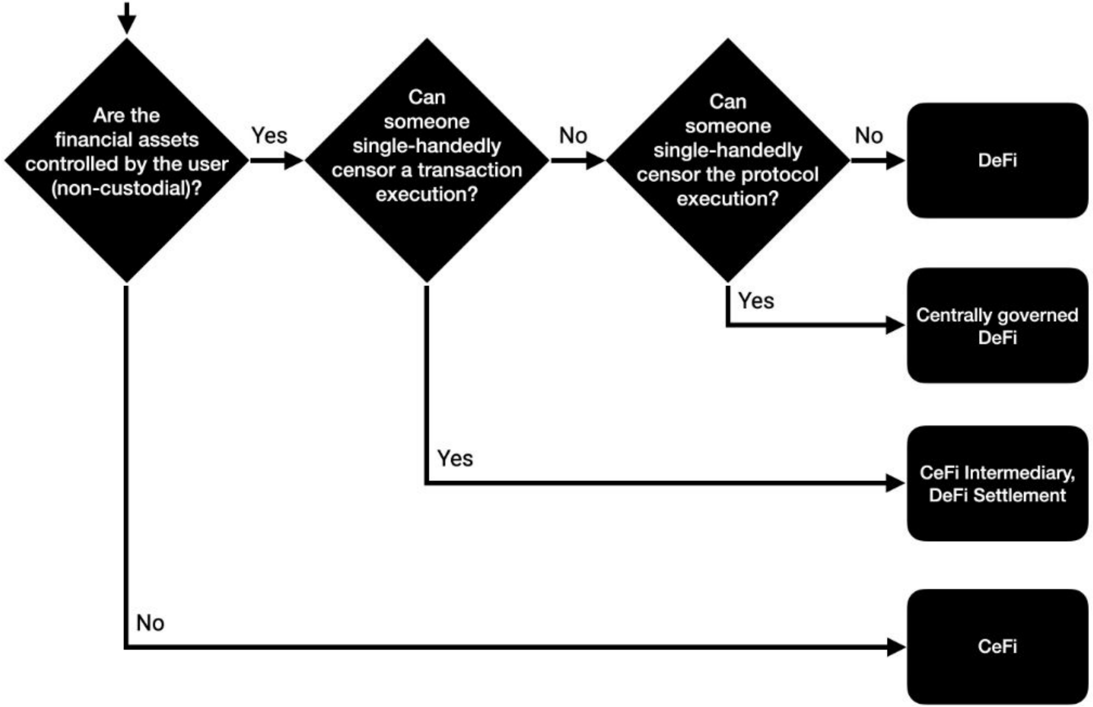
Decentralized Finance (DeFi)

- Financial products and services on decentralized infrastructure
  - Typically Ethereum-based
- Do not rely on centralized intermediaries
  - E.g., exchanges, banks, brokers
- Utilize the security of an underlying blockchain system
- Open to hazards and attacks that stem from public/decentralized nature of blockchains

Securities

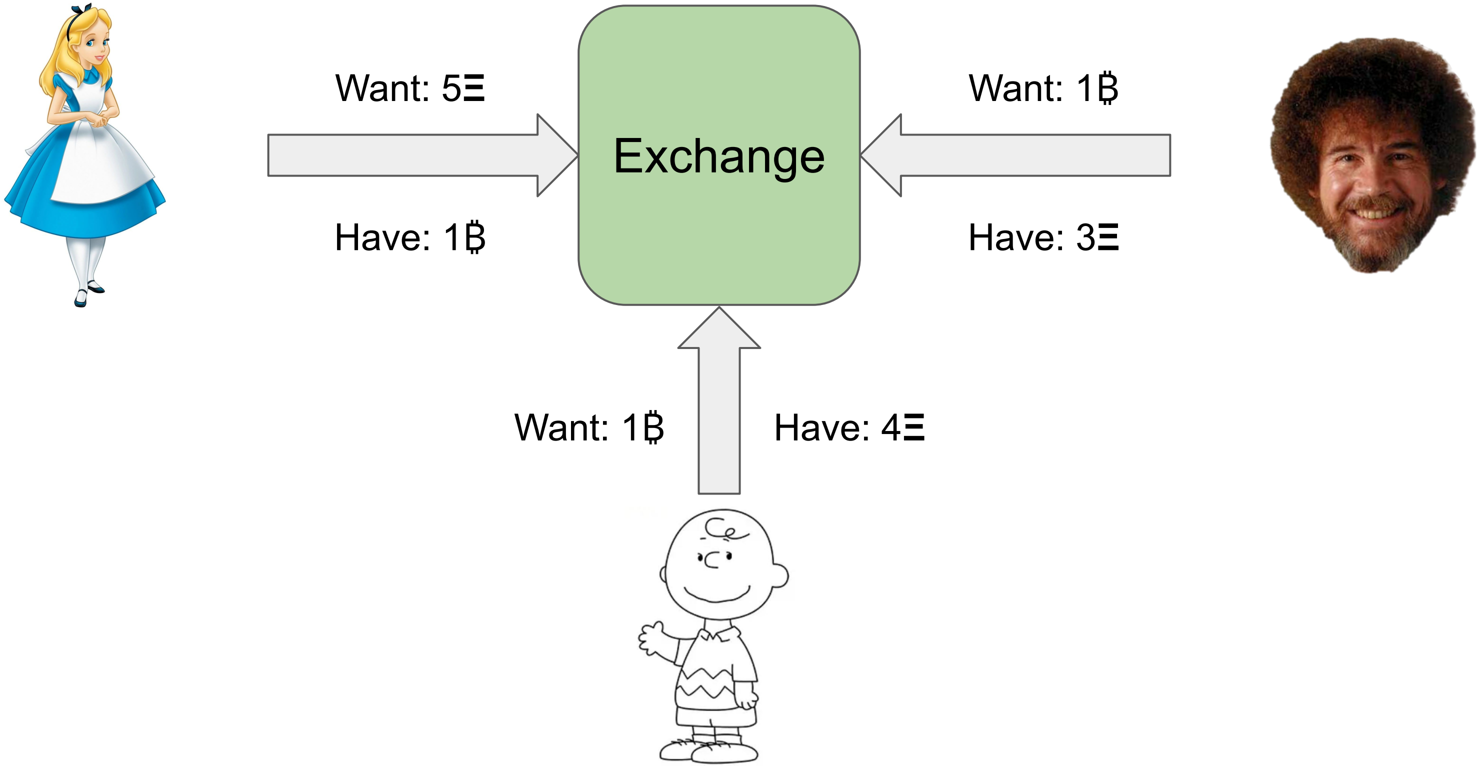
- Security: a fungible, negotiable, financial instrument that has some value
  - a stock (representing ownership of a public company) - **equity security**
  - a bond (representing a creditor relationship with a government) - **debt security**
- In the US (cf. Securities and Exchange Commission (SEC) v. W.J. Howey Co) a security is:
  - a contract, transaction, or scheme whereby a person **invests** his money in a **common enterprise**...
    - *Horizontal commonality*: Investors’ assets are joined and they share the risk and benefits
    - *Vertical commonality*: Investors’ fortunes are linked and dependent upon the efforts of those seeking the investment (**narrow** (investors’ profits rise and fall together with promoter’s) vs. **broad** (investors’ profits depend on promoter’s expertise and performance))
  - … and is led to **expect** profits solely from the efforts of the promoter or a third party

Decentralized Finance (DeFi)


Are the financial assets controlled by the user (non-custodial)?
Yes
Can someone single-handedly censor a transaction execution?
No
Can someone single-handedly censor the protocol execution?
No
DeFi
Yes
Centrally governed DeFi
Yes
CeFi Intermediary, DeFi Settlement
No
CeFi

Source: https://berkeley-defi.github.io/f21

Exchanges/Marketplaces



Want: 5Ξ

Have: 1฿

Exchange

Want: 1฿

Have: 3Ξ

Want: 1฿

Have: 4Ξ

Decentralized Exchanges (DEXs)

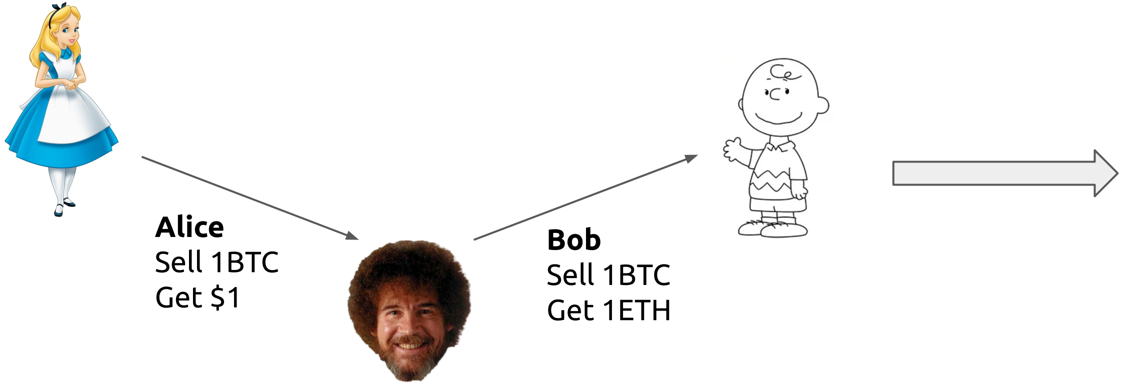
- Completely on-chain
  - Trades between native chain currency (e.g., ETH) and on-chain tokens (e.g., ERC20)
- Censorship resistance
  - Availability depends on underlying blockchain’s safety & liveness
- Differences from centralized (server-based) exchanges
  - (Blockchain) fees for creating orders
  - (Blockchain) fees for cancelled orders
  - Slower matching
  - No KYC and AML provisions

Decentralized Exchanges (DEXs), Attacks

- Front-running
  - Adversary can use gas price to front-run a trading tx
  - Miners choose tx ordering → can front-run plain users
  - Also exists in centralized exchanges (esp. if unregulated)
    - Exchange owner can see all txs, control execution order, and increase/decrease price arbitrarily to “burn” customers (both short and long)
- Insertion (aka sandwitching) attack
  - U creates a “buy” order TX_U, e.g., buy ₿ for Ξ
  - Attacker inserts before TX_U (front-running) a “sell” order and gets x₿ for y_1Ξ, *moving the price*
  - U’s order is executed for the decreased price
  - Attacker inserts a “buy” order after TX_U, which gets back y_2Ξ for x₿
  - Attack profit: $y_2 - y_1$
- Some mining pools offer front-running *as a feature* (e.g., Ethermine)

Market capitalization (of cryptocurrencies)

- Centralized exchanges as source of price
  - Price of BTC: the latest price for which a Bitcoin was sold (in exchange USD/GBP/altcoins/…)
- Market cap: [number of coins in circulation] * [price]
- **Issues:**
  - Market cap does not reflect how much (real) money is *actually* in the market
  - Tokens or dubious “coins” artificially increase market cap

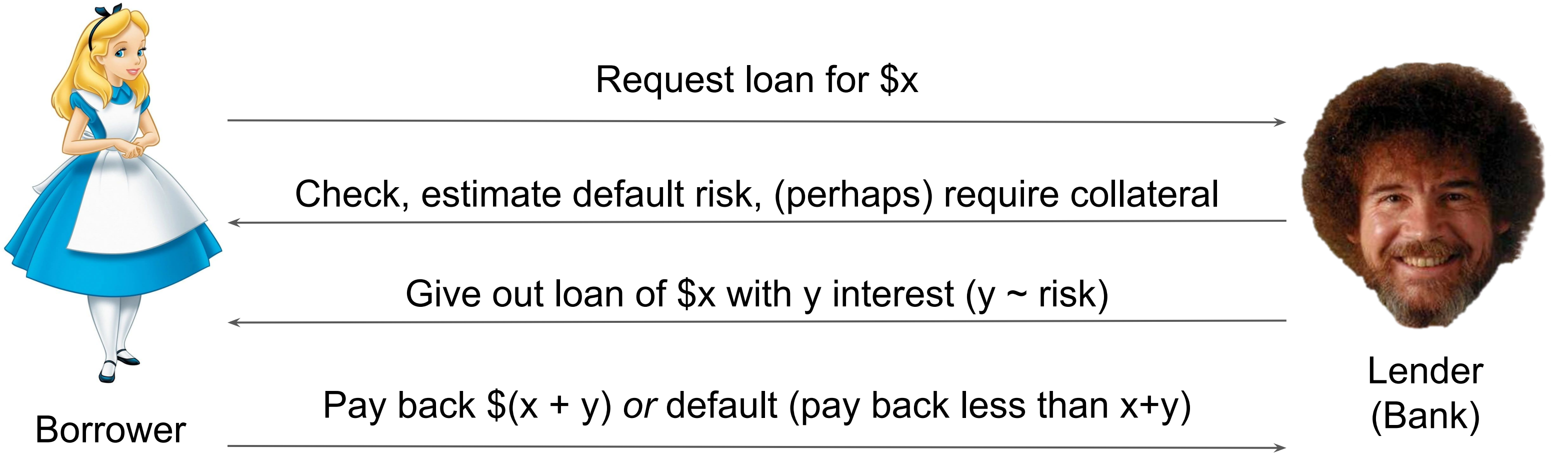


Alice
Sell 1BTC
Get $1

Bob
Sell 1BTC
Get 1ETH

- Alice: $1; Bob: 1ETH; Charlie: 1BTC
- BTC price: $1
  - Market cap: $1
- ETH price: 1BTC
  - Market cap: $1
- “Total market cap”: $2
- *Actual* USD in the market: 1

(Real-world) Loans



Borrower

Request loan for $x

Check, estimate default risk, (perhaps) require collateral

Give out loan of $x with y interest (y ~ risk)

Pay back $(x + y) *or* default (pay back less than x+y)

Lender
(Bank)

Decentralized Loans

- Oracle that reports (real-world) asset prices (e.g., in USD)
  - (semi or completely) centralized
- Lender deposits principal capital to vault (i.e., service’s smart contract)
- Borrower puts collateral to borrow from vault
  - Over-collateralized: value(collateral) (in real prices) > value(loan)
  - If value(collateral) < value(loan), loan automatically liquidated by anyone
    - Liquidator repays debt and gets collateral at a discount
- Borrower returns loan + interest to vault
  - Lender can redeem principal capital + interest

Flash Loans

- A loan that occurs in a **single atomic** transaction
- Lender adds principal capital (“liquidity”) to a smart contract pool
- Within a single transaction:
  - Smart contract pool transfers x assets from the pool to borrower’s account
  - Borrower uses x assets as they want
  - Borrower transfers x assets plus some fee to the pool
  - If any step of the above fails (e.g., borrower cannot repay the pool), tx fails
- No default risk!

Decentralized/Flash Loans, Attacks

- Price oracle manipulation
  - Control collateral requirements
- Risk-free arbitrage
  - DEXs may offer different prices on the same trading pair
  - Use flash loan to: i) buy on one DEX, ii) sell on the other (at higher price), iii) repay loan+fees
- Washtrading
  - Sell and buy the same asset to create misleading activity, e.g., to artificially increase trading volume (and show “demand”)
  - Centralized cryptocurrency exchanges also often perform washtrading
  - Illegal in USA *regulated* markets since 1936

Stablecoins

Fiat-backed stablecoins

- Centralized issuer of “stable price” tokens
- How it works
  - User deposits $1 to service’s bank account
  - Service issues 1 token in exchange
  - *As long as* token in circulation, service keeps $1 in escrow
  - *Whenever* user wants, can redeem 1 token for $1
- Why use such stablecoins instead of USD directly?
  - Exchanges
    - avoid regulation
    - settle inter-exchange transfers faster
  - Users
    - bypass capital controls
    - avoid KYC/AML requirements
    - launder illegal profit

Fiat-backed stablecoins

- If 1-1 promise (silently) breaks
  - Service issues loans (fractional reserve), taking on default risk
  - Service can insert (artificial) liquidity into the market (to pump the price of other assets)
- If regulation tightens
  - The broken 1-1 promise becomes public knowledge
  - Trust in the system decreases, “stable” price no longer stable (reflecting default risk)
  - Liquidity evaporates
- Tether (*by far* the largest “stablecoin”)
  - Opaque (*no audits,* unknown reserves, unknown affiliations, can refuse redemptions at will)
  - Repeatedly misleading behaviour (NYAG, CFTC)
  - *It is known* that Tether does not have $1 for every USDT
  - Circulation: $4B until 2019, $21B end of 2020, $74B in Nov 2021
  - “Daily trading volume” across all exchanges: $87B (>2x Bitcoin’s)
  - Almost every major exchange trades Tether (and is open to Tether collapse risk)

Crypto-backed stablecoins

- (1+x)-1 backing by crypto reserves
- (Centralized) price oracles
- How it works
  - Let: 1 ETH = $1, x = 1
  - Deposit 2 ETH and get 1 stablecoin (over-collateralized)
  - If price(ETH) > $0.5: stablecoin's price unchanged
  - If price(ETH) < $0.5: stablecoin liquidated, investor receives 2 ETH
- Example: Dai

Crypto-backed stablecoins

- Leveraged investment
  1. Buy 1 coin with 2 ETH
  2. Buy 1 ETH with 1 coin
  3. Increased demand for ETH → ETH price ↑
  4. ETH price ↑ (eg. 1 ETH = $2)→sell 0.5 ETH for 1 coin, redeem coin for 2 ETH (profit: 0.5 ETH)
  5. Go to (a) (perpetual motion machine)
- What if ETH price drops?
  1. Stablecoins liquidated for ETH
  2. Investors sell ETH to cut losses → Uncertainty from liquidations, ETH supply ↑ → price ↓
  3. Go to (a) (death spiral)
- Example: March 2020, MakerDAO had to *centrally intervene and inject liquidity* to avoid complete shutdown
  1. What happens if market collapses and external pockets not deep enough?

Algorithmic stablecoins

- (Centralized) price oracle
- Principal idea: *Quantity Theory of Money**
  - MV = PT ([Money supply] * [Velocity] = [weighted Price average] * [sum of all Transactions])
  - If V, T remain the same, P (prices, i.e., inflation) follow M (money supply)
  - By definition true in a snapshot, *cannot* be relied on for predictions
- Two types of assets
  - coins
  - bonds
- How it works
  - price > $1: automatically issue and distribute new coins (assumption: coin supply ↑ → price ↓)
  - price < $1: sell bonds for coins (coin supply ↓ → price ↑)
- Bonds:
  - Buy bond in auction (face value: $1, auction price: y)
  - ~~When~~ If coin price above $1 again, redeem bond to receive new coins (profit = 1 - y)

* Irving Fisher. “The Purchasing Power of Money” (1911)

Algorithmic stablecoins

- All such project have quickly collapsed
  - Nubits (*“World's Best Stable Digital Currencies”*): $0.12
  - Basis (*“an Algorithmic Stablecoin Pegged to 1 USD”*): $0.04
- Why fail?
  - price ↑ → bond-holders and investors receive newly issued coins
  - price ↓ → investors can only buy bonds and *have faith* that price ↑ again
  - if price does not go up quickly
    - lost profit (opportunity cost) ↑
    - if lost profit > bond profit, no reason to remain invested

References

- Philip Daian et al. “Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability” 2020
- Eskandari S., Moosavi S., Clark J. “SoK: Transparent Dishonesty: Front-Running Attacks on Blockchain” 2019
- Qin, K., Zhou, L., Livshits, B. and Gervais, A. “Attacking the defi ecosystem with flash loans for fun and profit” 2021
- Douglas Arner, Raphael Auer and Jon Frost. “Stablecoins: risks, potential and regulation” 2020
- Golumbia, David. “The politics of Bitcoin: software as right-wing extremism” 2016
- David Graeber. “Debt: The first 5000 years” 2012
- Robert Skidelsky. “Money and Government: A Challenge to Mainstream Economics” 2018