

Blockchains & Distributed Ledgers

Lecture 10

Petros Wallden



Slide credits: PW, Dimitris Karakostas, Aggelos Kiayias

Blockchains in the Quantum Era

Computational Models and Security

- Security relies on **computational** assumptions
- What is feasible/tractable depends on the computational model
- Quantum Computing is a new computational paradigm that promises great (in some cases exponential) speed-ups
- Need to re-evaluate security through this lense
- See also: **Quantum Cyber Security** course (semester 2)

What Quantum Computing is

Quantum Computer

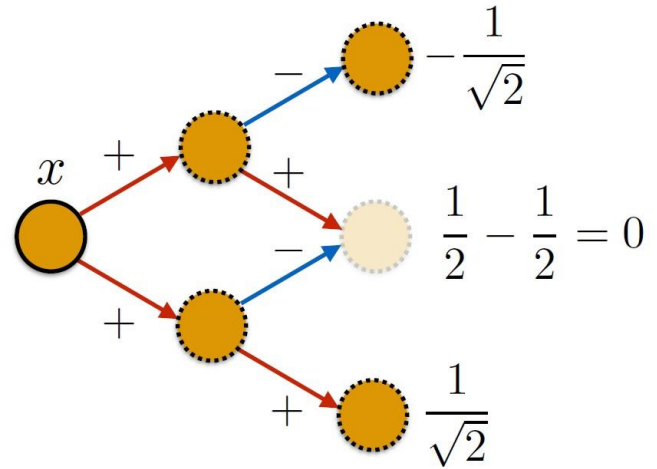
Manipulate in a programmable, fully controllable and flexible way quantum information

- Quantum systems have peculiar properties: from **bits** to **qubits**
- Due to different properties define a different computational model
- What was **hard for classical** computers can be **easy for quantum** (polytime)
- Large-scale (perfect) quantum computers are not yet available, but huge progress
- Quantum hardware being developed based on different physical (quantum) systems
(Superconducting, Ion-traps, Photonic, Neutral atoms, Silicon)

How Quantum Computing works

Quantum computers behave like a probabilistic computer (BPP) but with **complex-valued** probabilities

- Can perform more operations
- Probability is the mod square of the sum of the complex amplitudes

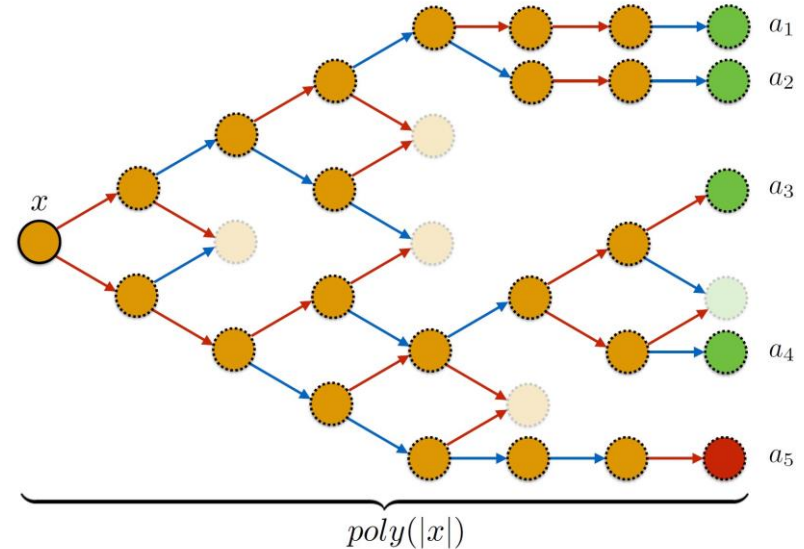


How Quantum Computing works

- For speed-up need many cancellations
- Needs suitable algorithm design

$$|\sum_i a_i|^2 = \sum_i |a_i|^2 + \sum_{i \neq j} a_i^* a_j$$

- **First term:** classical probabilities
- **Second term:** Amplify or cancel probabilities (interference)
- **Classical systems:** random phases (vanishing interference)



Myths and Realities

On the Power of Quantum Computation

Myth 1

Quantum Computers are much faster in performing operations than Classical Computers

Reality

Quantum computers are **not** faster. Speed-up is obtained because quantum theory allows algorithms/operations impossible for classical computers.

Myths and Realities

On the Power of Quantum Computation

Myth 2

Quantum Computers simultaneously perform all branches of a (probabilistic) computation and can use all that information

Reality

QC span the space of possibilities in a peculiar way (behave as complex probabilities). However, at the end of the computation the result is obtained by a **single read-out/measurement** and “unrealised” paths do not contribute.

Myths and Realities

On the Power of Quantum Computation

Myth 3

Quantum Computers give equally impressive computational speed-up to all problems

Reality

Quantum computers can give from exponential speed-up (factoring) to much smaller quadratic speed-up (search). The exact optimal quantum algorithm depends on the problem and is crucial for quantum cryptanalysis.

Myths and Realities

What it takes to be Quantum-Safe

Myth 4

No crypto protocol based on computational assumptions can be secure against quantum attacks. Therefore we can only use information theoretic security

Reality

Quantum computers give speed-ups, but are real devices with well defined limitations. Can base crypto on quantum computational assumptions provided (i) there isn't an efficient quantum algorithm, as for some major cryptosystems (RSA, EC-DSA) and (ii) new security analysis is performed and security parameters are chosen

Myths and Realities

What it takes to be Quantum-Safe

Myth 5

Using problems that are hard for a quantum computer suffices to make a crypto protocol secure against any quantum attack

Reality

This is **necessary but not sufficient** condition. New quantum cryptanalysis, new security definitions and new proof techniques are also needed.

Crypto-relevant Quantum Algorithms

The two main Quantum Algorithms for relevant for Crypto:

- [Shor's Algorithm](#) (factoring and discrete log):

Integer N in time $O((\log N)^3)$. **Exponential speed-up**

- [Grover's Algorithm](#) (unstructured search):

Database with N elements in $O(\sqrt{N})$. **Quadratic speed-up**

Main Issues for Bitcoin and PoW-based Blockchains

- **Signatures:** Elliptic Curve Digital Signature Algorithm (ECDSA), based on EC Discrete Logarithm

Shor's algorithm gives exponential speed-up

Need to revisit/replace signatures used

- **Proof-of-Work:** SHA2 (hash-based) model as random oracle for security

Grover's algorithm gives quadratic speed-up

Need to revisit security/honest majority etc

Signatures

Main potential implications

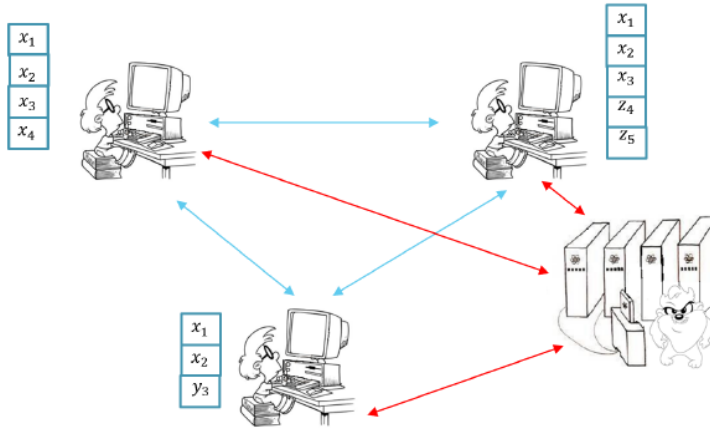
- **Reusing addresses.** Once public key is revealed the quantum attacker can obtain the secret key. If address is used only once (where fresh address is used subsequently) this does not pose a threat.
- **Processed transactions.** Old transactions with several blocks following, transaction is safe (unless out-hashing to double spent – see PoW)
- **Unprocessed transactions.** Transaction broadcasted, but before being included at a block, quantum attacker can use secret key to change the destination to their own and add the compromised block to the blockchain

Signatures

Need to change to signatures that are resistant to quantum attacks!

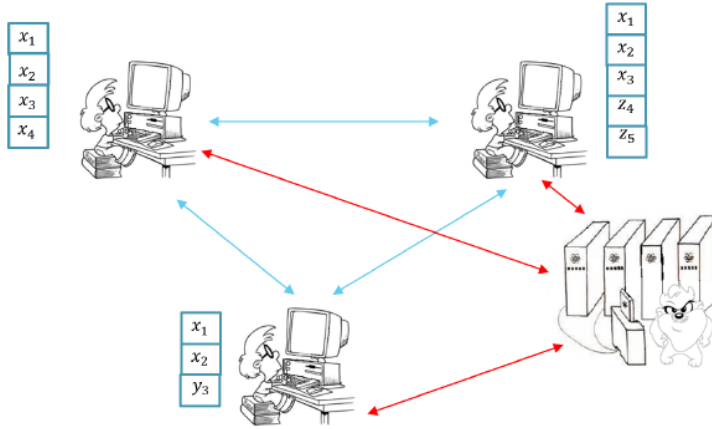
- **NIST post-quantum competition.** Cryptosystems believed to be resilient to quantum attacks have been selected by standardization bodies.
- Post-quantum cryptography: Classical cryptosystems resilient to quantum attacks. See **Quantum Cyber Security** course next term!
- **Lattice-based signatures:** CRYSTALS-Dilithium, FALCON
- **Hash-based signatures:** SPHINCS+

Proof-of-Work



- Single quantum adversary with Q quantum queries
- n honest parties with q classical queries each
- **Quantum Random Oracle:** Access RO in superposition
 - To get speed-up we need to apply sequentially the function
 - Intermediate values are not revealed
 - Decision when to measure is crucial

Proof-of-Work



- **Solving a single PoW Quantumly:**

- After k quantum queries prob of success: $O(k^2p)$, where p classical probability of getting an answer with a single query.
- Cannot get more than one solution (unlike classical)
- Generally best to use queries together $(k_1 + k_2)^2 \geq k_1^2 + k_2^2$

Proof-of-Work

PROBLEM Π_G : CHAIN-OF-POWS

Given: N , $x_0 \in X$, δ and h_0, \dots, h_{N-1} as (quantum) random oracles, where each $h_i : X \times Y \rightarrow X$ is independently sampled.

Goal: Using N total queries find a sequence y_0, \dots, y_{k-1} such that $x_{i+1} := h_i(x_i, y_i)$ and $x_{i+1} \leq D \forall i \in \{0, \dots, k-1\}$ such that the length of the sequence $k \leq N$ is the maximum that can be achieved with success probability at least δ .

Theorem 4.1 (Main Theorem). *For any quantum adversary \mathcal{A} having N quantum queries, the probability that \mathcal{A} solves the CHAIN-OF-POWS problem, by outputting a solution of size at least k is at most:*

$$P(N, k) \leq \exp\left(-2k \cdot \ln\left(\frac{k}{e(N+k)} \cdot \frac{1}{\sqrt{p}}\right)\right) \quad (4.1)$$

where $p := \frac{T}{2^\kappa}$ is the probability of success of a single query to the random oracle.

- Provided $k \gtrsim \sqrt{peN}$ this probability decays exponentially in k .
- If honest parties expect to exceed this, security is maintained.

Proof-of-Work

- **Post-Quantum Honest Majority** condition:

$Q\sqrt{p} \leq f$ with f prob at least one PoW by honest per round

Noting that $f = (nq)p$ we get $\frac{Q}{\sqrt{p}} \leq nq$

Each quantum query worth $1/\sqrt{p}$ classical queries

Note that p is very small

- Number of rounds for **quantum-safe settlement**:

Same as in classical. Prob of failure scales as $\exp(-sf\Omega)$

Proof-of-Work

Subtleties/further research

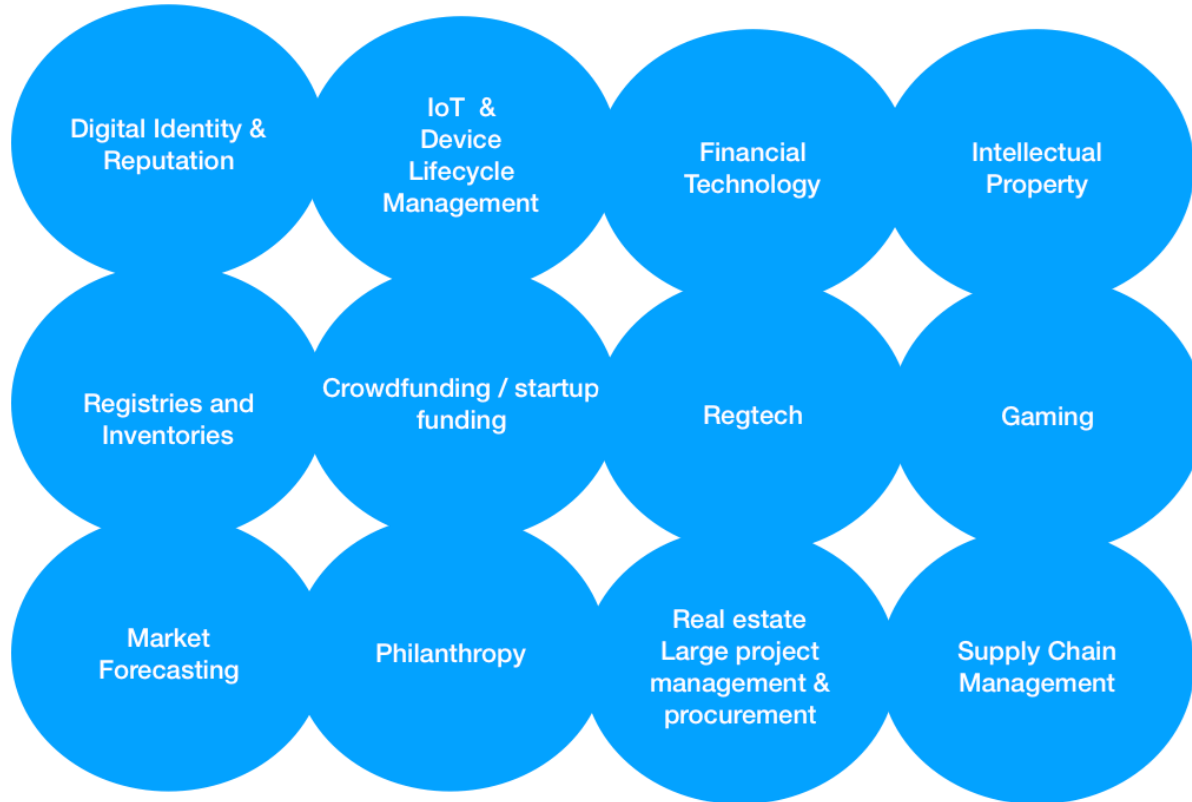
- Grover is NOT parallelizable -> modelling all adversarial queries to a single adversary was not accurate
- ASICS do not have quantum analogue (for now)

Modelling of a single quantum adversary with Q queries comparable to (nq) classical queries was **too pessimistic**

- Should model adversaries with both quantum and classical queries
- **Full analysis:** require treating all parties with quantum capabilities. Harder to prove security; even harder to analyze the incentives and Nash equilibrium.

Applications of Distributed Ledgers

(Possible) Applications of DLT

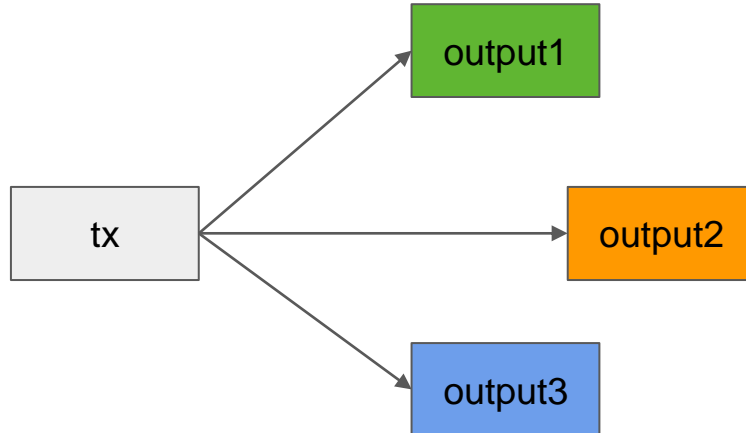


Use an independent DL or piggyback on existing?

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

Piggybacking Example - 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



Piggybacking Example - 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

Piggybacking Example - 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

List of Applications

Digital economy (on a blockchain)

- Use a blockchain to record monetary transactions
- Create new money based on pre-determined algorithm

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 as commodities?
Why would someone sell BTC, if they expect its (USD) price to increase?
- How to accurately value 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

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

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?

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, ...

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)?

Supply chain tracking (on a blockchain)

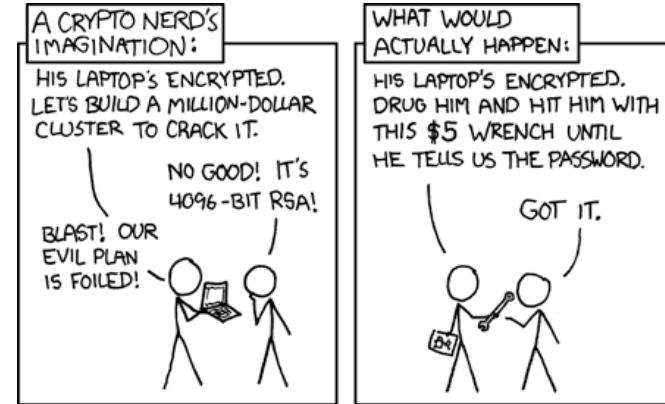
- Real-world products
 - E.g., clothes, shoes, meat, olive oil, even diamonds
- Create a digital fingerprint of the object
- Register the fingerprint on a blockchain
- Record every change in the object's state
 - E.g., creation at source, transportation, selling/buying

Supply chain tracking (on a blockchain)

- 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 to create a fingerprint (unique digital representation) of a physical object?
- How to make sure that people that handle the object actually record its state changes? What if someone bribes someone to insert false data on the chain?



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

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 markets for:
 - Gambling, insurance purposes, ...

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 markets for:
 - Gambling, insurance purposes, ...

Issues

- Trust in the oracle? Can a decentralized oracle for real-world information exist?
- Events may not be well-defined (e.g., is Puerto Rico part of the USA?)

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 gets income for selling their personal data

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 gets 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, resold, offer yield (securities)

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, resold, offer yield (securities)

Issues

- How to guarantee that project will not run away with the funds (i.e., exit scam)?
- What if project tries to scam investors and authorities, e.g., claim a security is utility token?
- Are the promises of the project verified/regulated? Will the project face penalties for lying?

Market Capitalization

Market capitalization (of cryptocurrencies)

- Centralized exchanges are sources of price
 - Price of X: the latest price for which a single X token was sold (in exchange for USD/GBP/Bitcoin/altcoins/...)
- Market cap: <number of coins in circulation> · <price>



<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>



1 BTC



<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1			



1 BTC

Sell 1 BTC for \$1



<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1			



\$1



1 BTC

<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1	\$1	\$1	\$1



\$1



1 BTC



1 ETH

<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1	\$1	\$1	\$1
Ethereum	1			



\$1



1 ETH

Sell 1 ETH
for 1 BTC



1 BTC

<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1	\$1	\$1	\$1
Ethereum	1			



\$1



1 ETH



1 BTC

<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1	\$1	\$1	\$2
Ethereum	1	\$1 (1 ETH=1BTC)	\$1	



\$1



1 BTC

Buy 0.5 ETH
for 1 BTC



1 ETH

<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1	\$1	\$1	\$2
Ethereum	1	\$1	\$1	



\$1



0.5 ETH,
1 BTC



0.5 ETH

<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1	\$1	\$1	\$3
Ethereum	1	\$2 (1ETH=2BTC)	\$2	



\$1

Buy 0.5 BTC for \$1



0.5 ETH,
1 BTC



0.5 ETH

<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1	\$1	\$1	\$3
Ethereum	1	\$2	\$2	



0.5 BTC









0.5 ETH,
0.5 BTC,
\$1



0.5 ETH

<u>Product name</u>	<u>Circulating Tokens</u>	<u>Price</u>	<u>Market Cap</u>	<u>Total MC</u>
Bitcoin	1	\$2	\$2	\$6
Ethereum	1	\$4	\$4	

Cryptos: 21,777 Exchanges: 524 Market Cap: \$825,029,479,545

1	 Bitcoin BTC	\$16,587.72	▲0.07%	▼0.39%	▲0.49%	\$318,646,947,717	\$31,806,610,049 1,917,154 BTC	19,209,806 BTC
2	 Ethereum ETH	\$1,201.47	▲0.26%	▼1.49%	▲0.78%	\$147,028,970,200	\$11,129,826,172 9,258,015 ETH	122,373,866 ETH
3	 Tether USDT	\$0.9996	▲0.00%	▲0.03%	▲1.26%	\$65,917,967,109	\$42,097,899,159 42,115,255,827 USDT	65,944,685,876 USDT
4	 USD Coin USDC	\$1.00	▲0.00%	▲0.02%	▼0.62%	\$44,417,530,170	\$3,698,812,883 3,698,369,386 USDC	44,406,592,473 USDC
5	 BNB BNB	\$267.49	▲0.13%	▼1.44%	▼4.07%	\$42,791,727,100	\$933,939,060 3,489,744 BNB	159,973,721 BNB
6	 Binance USD BUSD	\$1.00	▼0.05%	▼0.05%	▼0.96%	\$23,039,136,412	\$6,672,905,015 6,671,289,989 BUSD	23,037,140,170 BUSD

<https://coinmarketcap.com>

Market capitalization (of cryptocurrencies)

- Centralized exchanges are sources of price
 - Price of X: the latest price for which a single X token was sold (in exchange for USD/GBP/Bitcoin/altcoins/...)
- Market cap: $\langle \text{number of coins in circulation} \rangle \cdot \langle \text{price} \rangle$

Issues

- Market cap may be artificially increased
 - E.g., tokens or dubious “coins” sold for other cryptocurrency
- Question: What is the ratio of *real-world* money to *market cap*? In other words, how much *real-world* money is *actually* in the market?