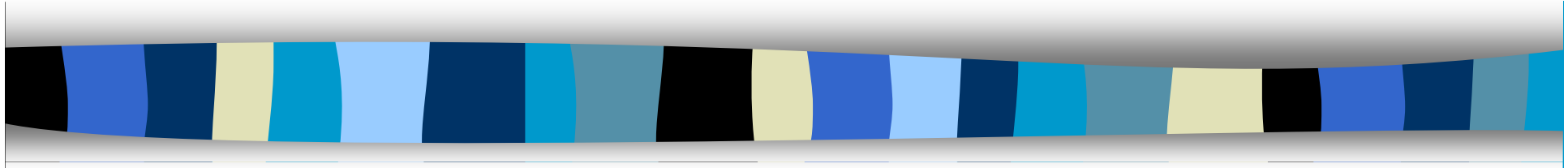


7CCSMDLC: Distributed Ledgers & Cryptocurrencies

Lecture 5: ICOs



Peter McBurney

Professor of Computer Science

Department of Informatics

King's College London

Email: peter.mcburney@kcl.ac.uk

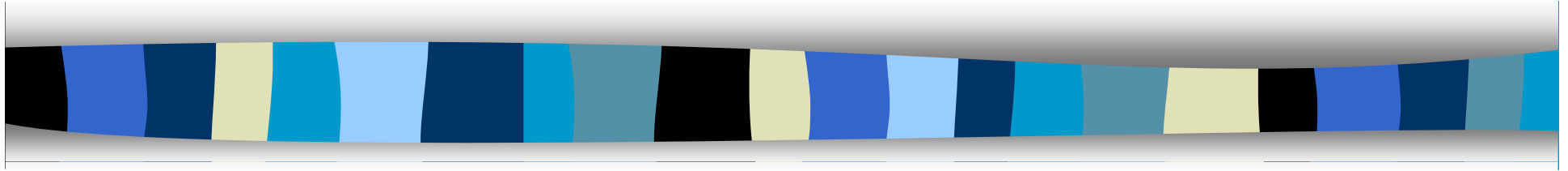
Bush House Central Block North – Office 7.15

2020



Outline

- Raising Funds
- ICOs
- Case Studies



Raising Funds for Start-ups



How is money raised for startups?

- FF&F – Founders, Friends and Family
- Angel investors
- Government grants and loans
- Commercial lenders (eg, banks)
- Venture Capital (VC) firms
- Initial Public Offers (IPO)
 - When the company lists on a stock exchange
 - Shares are now for sale to the public.



Seeking loans or investors

- Issue a Prospectus
 - A document presenting the opportunity, the terms and conditions (T&C) and the risks
 -
- Strict rules in most countries
 - USA: Securities and Exchange Commission (SEC)
 - UK: Financial Conduct Authority (FCA)
 - Prudential Regulation Authority (PRA)
- May also be industry-specific regulators
 - UK: Ofcom – Office for Communications & Postal industries
 - Ofgem – Office for Gas and Electricity Markets
 - Gambling Commission
 - Competition and Markets Authority
 - Food Standards Agency
 - Etc.

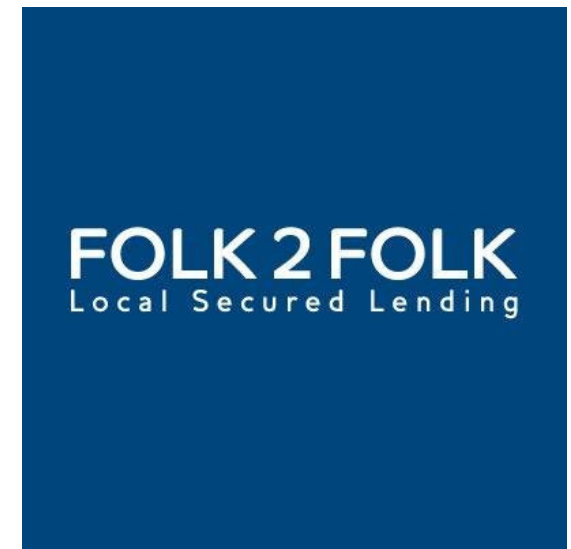


Newer forms of fundraising

- Traditional forms of lending
 - Savers place deposits into banks, building societies, credit unions
 - Banks etc aggregate the savings
 - Then lend larger amounts to borrowers (individuals, companies)
- Crowd Funding
 - Aggregation done via a web-site or a crowd-funding service
 - Large number of investors invest a small amount each
- Peer-to-Peer lending
 - Lenders connect directly to borrowers
 - An intermediary may match borrowers and lenders (and do credit checks)
 - 126 lending platforms listed on
 - www.p2pmoney.co.uk/companies.htm
- ICOs
 - Presale of tokens.

Case Study — P2P lending

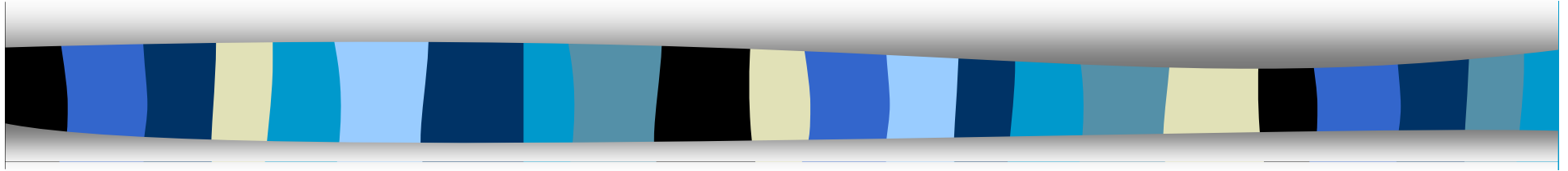
- Folk2Folk
 - P2P lending company in England
 - Established 2013 by Parnalls (Solicitors in Cornwall)
- Lenders – High Net Worth individuals
- Borrowers – companies or NHW individuals
- Loans secured against property or land
- Social base: Local rural communities & market towns
- Cumulative loanbook: £ 200m.



Case Study — Crowd funding



- CrowdCube
 - UK's largest crowd-funding platform
 - First to receive FCA approval (2013)
- Crowd-funded equity raises
 - eg, Chilango in 2015: 1300 investors paid £3.4m total for 8.7% equity
- Also, crowd-funded mini-bonds (ie, loans)
 - eg, Chilango in 2014: 347 lenders lent £2.0m total for 8% pa return
 - eg, Brewd0g in 2015: 815 lenders lent £2.3m total for 6.5% pa return
- Disclosure: Crowdcube is a partner on research project we are doing on voting using distributed ledgers (VOLT) project.



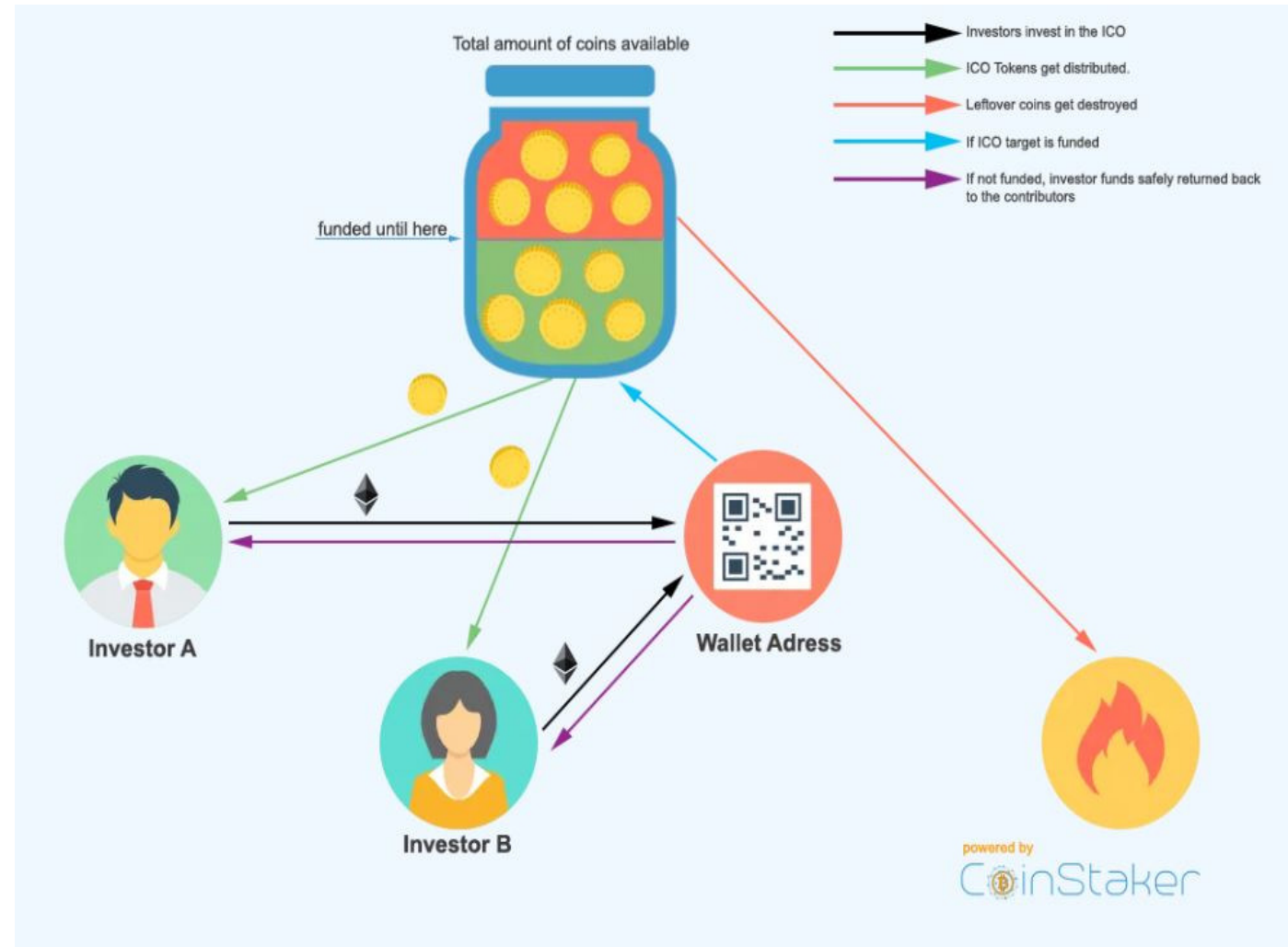
ICOs

What is an ICO

- Consider we plan a start-up airline
 - Our first route: London, UK and Zurich, Switzerland
 - We want to support the Crypto Valley community
 - Pre-sell the frequent flyer miles
- Why invest?
 - Business or utility reason
 - Investment reasons
 - to hold tokens and resell them later
 - Speculation reasons
 - to buy and sell tokens.
- Called an Initial Coin Offering (ICO)
 - Named following “IPO – Initial Public Offering” (of shares in a company)
 - Also called a Token Generation Event (TKE).



Overview of Initial Coin Offerings (ICO)



Source: <https://www.coinstaker.com/initial-coin-offering/>.
Accessed: 12/02/2018



2017 ICO fundraising statistics

Total Raised in 2017: \$4.8 billion in 279 ICOs

Rank	ICO	Amount (USD m)
1	HDAC	258
2	Filecoin	257
3	Tezos	232
4	EOS Stage 1	185
5	Paragon	183
6	Bancor	153
7	Kin Kik	97
8	Status	90
9	BANKEX	71
10	TenX	64

Source: <https://www.coinschedule.com/stats.php>.

Accessed: 2018-02-12



2018 ICO fundraising statistics

Total Raised in 2018: \$ 886 million in 35 ICOs

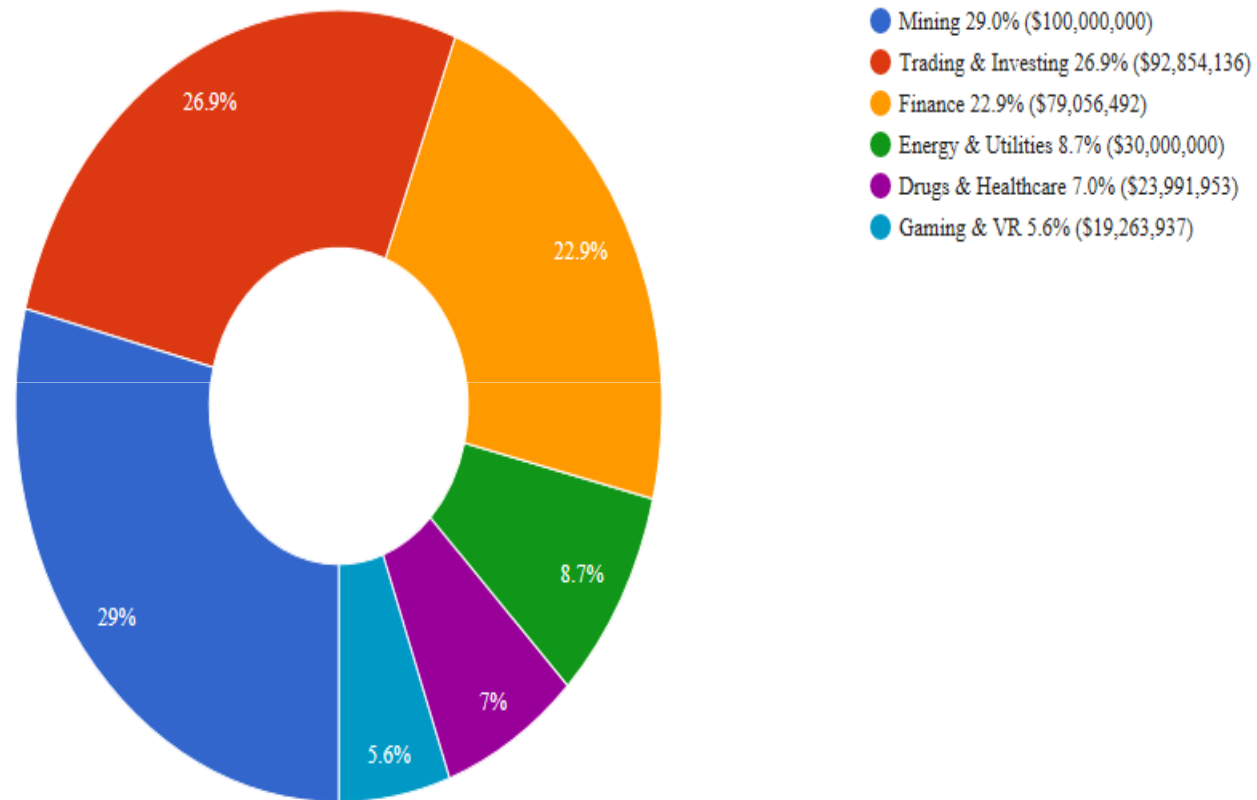
Rank	ICO	Amount (USD m)
1	Envion	100
2	Crypterium	52
3	SwissBorg	50
4	iungo	46
5	Bloom	41
6	Mobius	39
7	Current	36
8	Pundi X	35
9	trade.io	31
10	Jibrel Network	30

Source: <https://www.coinschedule.com/stats.php>.

Accessed: 2018-02-12

Securities tokens or utility coins?

ICOs by Category 2018



Source: <https://www.coinschedule.com/stats.php>.

Accessed: 2018-02-12



Token standards

- ERC20 – The Ethereum standard for tokens
 - ERC = Ethereum Request for Comment
- A protocol for tokens to interact on the Ethereum network
 - So that tokens can easily be sent and be received without developers of new tokens have to re-create interaction code for each new token.
 - So that wallets & exchanges can have a single API for dealing with new tokens.
- Eidoo site lists 459 tokens which are ERC20 compliant:
 - <https://eidoo.io/erc20-tokens-list/>
- ERC223 token standard
 - An update on ERC20
 - Does not permit tokens to be transferred to a smart contract which does not permit tokens to be withdrawn.



Concerns of regulators

- To prevent scams and frauds
- To ensure promoters reveal all they know to investors regarding
 - Past records of promoters
 - True plans & intentions of company
 - Legal & regulatory status
 - Insider deals and connections
 - Risks
- Types of risks
 - Market demand
 - Competitors
 - Regulatory risks
 - Technology developments.



Accredited investors

- Most financial sector regulators are more concerned with risks to ordinary consumers & investors
- Less concerned with risks to
 - High-Net-Worth individuals (people with wealth over, say, US\$100K)
 - Private pools of investment
- Some agencies have a category of Accredited Investors
 - Less regulation & oversight of these investors and the pools they join
 - Hedge funds – pools of accredited investors using high-risk strategies.



Cryptocurrency Hedge Funds

- Pooled investment funds targeting investments in:
 - Cryptocurrencies and alt-coins
 - ICOs
 - Start-up businesses running over blockchains
- Often created by partners & investors in traditional hedge funds
 - Crypto is too volatile for traditional investors
- Examples:
 - Pantera Capital (2013) – first crypto fund for US investors
 - Galaxy Digital Assets Fund
 - Chromatic Capital
 - Polychain Capital.



Checks on investors

- KYC – Know Your Customer regulations
 - Identity
 - Location
 - Wealth & assets
 - Other investments
- AML – Anti-Money Laundering
 - Source(s) of funds
- Money-laundering
 - Proceeds of criminal activity (often in cash)
 - Proceeds of transactions with entities under sanctions
 - eg, Syria, DPRK, Iran (until recently), Rhodesia (1965-1980), South Africa (ca. 1985-1991).



Registration of security

Need to register securities with SEC (unless exempted), providing details on:

- The company's properties and business purpose
- The security being offered
- The company's management
- Financial statements, certified by independent accountants.



Howey Test

- What counts as a “security” under US Securities law
 - ***Securities and Exchange Commission v. W. J. Howey Company***, 328 U.S. 293 (1946)

Under the Howey Test, a transaction is an investment contract for securities if four conditions are satisfied:

- It is an investment of money
 - “Money” may include other forms of near money
- There is an expectation of profits from the investment
- The investment of money is in a common enterprise
 - Pooling of funds into a joint-stock company or similar joint enterprise
- Any profit comes from the efforts of a promoter or third party
 - If profit arises from investor’s own actions, then likely not a security.



For intending ICOs, there are 3 broad choices

- Option 1 (Reg-Heavy)
 - Register tokens as securities with the USA SEC
 - Around USD 500K in legal fees
 - 4-6 months for the process
- Option 2 (Reg-Lite)
 - Gain exemption from the SEC by not selling to US citizens or residents
 - Similarly, not selling to Chinese or South Korean residents
 - Around USD 50-100 K in legal fees, 2-3 months
 - Need to collect KYC and AML information
 - Contrary to Cypher-punk ethos
- Option 3 (No-Reg)
 - Ignore these regulations
 - Risk being prosecuted by regulators and/or sued by investors
 - Employ a good lawyer!



Stages of an ICO

- Private token allocation
 - To friends & employees
- Private token allocation
 - Typically to large investors and crypto-hedge funds
- Public token allocation
 - To anyone (perhaps subject to constraints)
 - eg, Not to citizens or residents of the USA, China or South Korea
 - Money raised on basis of a White Paper and a Prospectus
- Development of Platform
 - And creation of tokens
- Launch of Business
 - And use of the tokens.



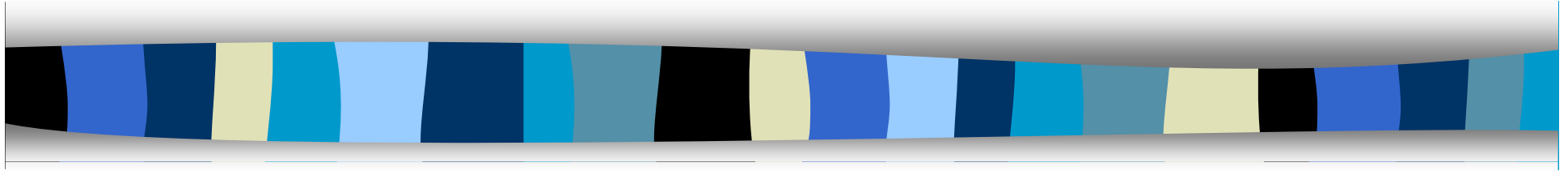
ICOs — A typical organization structure

- A charitable foundation (F) initiates the ICO and receives the funds
 - Has independent board of directors
- A software development firm (D) develops the idea and the white paper
 - When money is raised, some is allocated by F to D to build the platform
- Locations
 - Foundation often registered in regulation-friendly jurisdictions
 - eg, Switzerland, Gibraltar, Singapore.
 - Software company registered elsewhere
 - eg, UK, USA.
 - Employees may be anywhere.
- Potential Governance issues
 - What is relationship between Foundation (F) & S/W company (D)?
 - Place of jurisdiction if disputes?
 - Do token-holders have rights over software?



Token allocation mechanisms

- A variety of allocation mechanisms are used to allocate tokens in the public sale
 - Usually an auction with tokens awarded to highest bidder
- Basic Attention Token (BATCoin) ICO
 - May 2017: \$35 million raised in 30 seconds
 - 130 investors only
 - Top 20 addresses control more than 50% of tokens
- Bancor ICO
 - 12 June 2017
 - \$153 million (in Ether) raised in 3 hours
 - \$51 million more than planned
- Criticisms
 - Favouritism to insiders
 - Speed
 - Not capping total tokens.



Some ICO Case Studies

Ethereum



- Ethereum
 - 2013: White Paper by Vitalik Buterin
 - Proposed to enable full programming capabilities over a blockchain

- ICO in July-August 2014
 - 6th highest ICO at that time
 - \$18.4 million raised
 - Payment in BTC at descending fixed prices
 - 2000 ETH / BTC falling to 1337 ETH / BTC
 - 31.5 K BTC or 60 million ETH

The DAO



- The DAO
 - Decentralized Autonomous Organization
 - Self-running VC fund running over Ethereum
 - Raised \$150 million in 1 month (May 2016) from 11,000 investors
 - Intended that token holders would vote on investment proposals
- June 2016: Code vulnerability exploited
 - \$50 million siphoned off
- Risk to investors
 - Loss of funds due to poorly-designed (or tested) code
- Ethereum nodes voted to hard-fork to restore lost funds
 - 20 July 2016 at block 1,920,000
 - Now 2 branches:
 - Ethereum (the blockchain excludes the exploitation)
 - Ethereum Classic (the exploitation continues).

Tezos

- A decentralized blockchain to facilitate formal verification of code, and smart contracts
 - Initiators and s/w developers: Arthur Breitman & Kathleen Breitman (USA)
 - Tezos Foundation (Switzerland): Johann Gevers
- ICO in July 2017
 - \$232 million raised in ETH and BTC
- Disagreement between the Breitmans and the Foundation
 - Lawyer's letters between the two
 - Delay in development & launch of tokens
 - Who will do the s/w dev?
- Investors disaffected by the delays
 - Risk of class-action suits from investors.





Polkadot

- Goal
 - to link private and public blockchains together
- Promoters
 - Gavin Wood (former CTO, Ethereum)
 - Jutta Steiner (ex-Ethereum)
 - Parity Software
- Parity Software Company (UK)
- Web 3.0 Foundation (Berlin)
- ICO in October 2017
- Raised:
 - Private Sale: \$83 million in Swiss Franks
 - Public Sale: \$140 million in Ether & Bitcoin
- Auction process was a descending-price auction (Dutch Auction).





Polkadot — Issue with multi-sig wallets

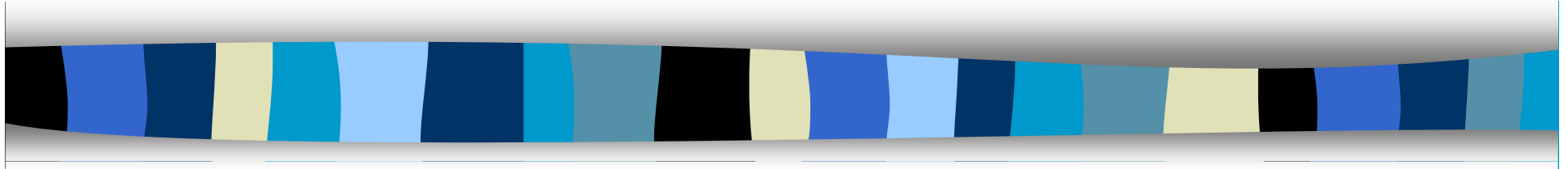
- Funds paid into a multi-sig wallet on Ethereum
- Ethereum multi-sig wallet template put most of the processing (apart from payments out) in a library wallet
 - This was to reduce processing costs
- The library wallet had a vulnerability
 - Someone could call it and initialize it (taking ownership of it)
 - Then could kill it
 - Someone did! (probably accidentally)
- Any multi-sig wallet which used this wallet was no longer accessible
- Some 500K ETH no longer accessible
 - Including \$90m of funds raised for Polkadot.



Risks of an ICO

- Risks of any business investment
 - Investment may fail
 - Market demand may not be present
 - Especially for products seeking to create new market categories
 - Scams & frauds
- Risks of investments in new technologies
 - Technology may move on
 - Shortage of skilled people
 - Competition may arise
 - Network effects & path dependence
- Risks particular to ICOs
 - Tech is new & immature, and not yet well understood
 - Regulatory risks (eg, prosecution by regulators)
 - May be a Ponzi scheme
 - Class-action suits by investors
 - Earlier investors may be sued by later investors.

Thank you!



peter.mcburney@kcl.ac.uk



Exercises

1. What was the vulnerability in the DAO exploitation? Explain how recursive code enabled the vulnerability to be exploited.
2. For each of the Top 10 ICOs in 2017 and 2018, identify the following
 - What was the intended application and technology?
 - What was the state of development at the time the ICO closed?
 - What is the state of development now?
 - How many tokens were there? What the allocation of tokens?
 - What the mechanism for allocating tokens in the public sale?
 - Who is the management team behind the ICO?
 - What is the organizational structure of the proposal?
 - When will the company launch service? When will tokens be issued?