Cryptocurrencies and Regulations (US only)

Blockchains and their Applications
Computer Science 4995-013 Fall 2019
Columbia University
Alex Biliris, Eran Tromer

The case for regulation

Initially

Bitcoin seen as a digital untraceable currency that can facilitate criminal activities

- kidnapping, extorsion, child exploitation
- sales of all sort of illegal stuff and services
- tax evasion
- bypassing capital controls

Case study – Silk Road

February 2011 to October 2013

- largest online market for illegal stuff
- ran as a Tor hidden web server (.onion) – dark web
- Tor browser provides for anonymous web accesses
- payments in Bitcoin, held in escrow while goods shipped

Ross Ulbricht (“Dread Pirate Roberts”)

- arrested in 2013 for operating the website
- convicted in February 2015, currently serving 2x life sentence
- the site generated sales of $1.2 billion according the complaint

Governments reactions

lessons

- real global businesses can be supported with crypto
- Bitcoin is not a toy for crypto scientists

reaction

- ignore it and see what happens
- fight it, somehow make it illegal
- disconnect it from fiat currency financial institutions
- embrace it cautiously, mitigate risk
- embrace it enthusiastically

Additional risks

besides risks to individuals or a single group of people

systemic risk to the local or global financial system

- may lead to cascade collapse of an entire economy
- bank runs (1929-1939, 2007-2008)
- this is unlike the .com bubble collapse (2001)

case in point: (currency/population)

- CAD/37 million, GBP/67m, USD/329m
- RMB/1.4 billion
- Libra/2.4 billion potential users!

Keeping track of coins: wallets and custody

Self-custody wallets

coins are recorded on the blockchain

wallets used to store/use secret keys

- paper wallet
- hardware wallets (Ledger, Trezor, etc.)
- client-side interfaces (MEW, Metamask, etc.)
- 233 wallets available (as of 10/2019) source: cryptocompare.com

pro: you (and only you) own/control your keys

- offline and secure

con: wallet/keys lost => coins lost

- need wallet software to track your keys + nice UI

Custodial exchanges

Coinbase, Gemini, Binance, …

- you get an account with user/password to login
- link your bank account for fiat transfers in and out
- they hold your coins and keys for you
- all assets are commingled on the blockchain
- your transaction is not visible on the blockchain
- they keep track and promise to pay you back later, on demand

It looks like a bank

- pro: familiar convenient model
  - account recovery
  - easy to get in and out of fiat and swap between crypto
  - lower to even zero transaction fees
    - bundling transactions before pushing them onto the blockchain
      - after matching internal orders
- con: risks similar to banks (e.g., bank runs)
    - compromised sites (MtGox, Bitstamp, Mintpal), $2B in hacks
    - no direct access to your coins
    - no anonymity

Regulations

Anti Money-Laundering (AML)

goal is to detect

- moving large amounts of money from one place/business to another (potentially crossing borders) for the whole purpose of “legitimizing” dirty money (money obtained illegally)

Know Your Customer (KYC)

- On-boarding process
  - identify and authenticate the new client
  - evaluate risk of client
  - a client maybe a
    - single individual
    - corporation (small or large, domestic or international)
    - subsidiary of another corporation
- On going process
  - watch for anomalous behavior

Mandatory reporting

Financial institutions operating in the US must

- report currency transactions over $10K
- watch for and report schemes that try to avoid the above reporting (e.g., transfer $5K ten times)

Bitcoin (the currency) is not excluded from this reporting

New York's BitLicense

Would need a BitLicense to conduct any of the following (effective Aug 2015):

1. Virtual currency transmission
2. Storing, holding, or maintaining custody or control of virtual currency on behalf of others
3. Buying and selling virtual currency as a customer business
4. Performing exchange services as a customer business
5. Controlling, administering, or issuing a virtual currency.

Would not need a BitLicense

consumers to purchase goods/services

merchants to sell goods/services

to develop software dealing with CC

a bank already doing business in NY (no but)

a startup that meets some of the reqs (2-year conditional BitLicense)

Applying for BitLicense

provide full and complete information on

- all business owners (high bar, includes fingerprints)
- finance and insurance
- business plan
- working software ready for testing

pay an application fee ($5,000)

renew annually submitting any major change (including major software updates)

licenses are subject to revocation

maintaining BitLicense

designate a compliant officer

provide updated information το NYDFS

- periodic financial statements
- changes to important operating policies
- revised business plan and major software changes

maintain a financial reserve (as set by NYDFS)

follow rules on

- KYC, AML, custody, cybersecurity, recordkeeping

too much hassle?

Bitfinex (see Tether) found these rules invasive

- decided not to apply, not serve NY residents (2015)

NYAG filed an injunction against Bitfinex for

- serving NY residents from ‘17 to early ‘19
- using Tether reserves to cover its own $850m loss
- Bitfinex challenged the NYAG’s authority to investigating them, they lost in court (Aug ‘19)

maybe, not that much

DFS has approved over 20 CC business

the latest most interesting, from most recent (Sep ‘19) to older:

- Paxos Trust (itBit) to offer Paxos Gold, the first gold-backed CC pegged to gold
  - align with BUSD, and PAX pegged to USD awarded earlier
- Coinsourse, kiosks across NY for US cash <-> Bitcoin
- Bitpay and Square, card, wallet, and payment services
- Gemini/Coinbase to offer Zcash trading and custody

Financing and monetization

equity vs. utility coins

coin as a security, it must follow the rules of selling securities

1. on public, open regulated exchanges

   significant requirements on all sorts of financial reporting, risk disclosures, etc

2. privately to accredited investors only

3. regulation A+ crowdfunding providing exceptions for unaccredited investor participation

coin as a utility coin, a way to pay a fee to some kind of service (not an investment)

the goal is to bring the coin at the hands of users, validators/miners, investors as early as possible

Initial Coin Offering (ICO)

ICOs want to be utility tokens [circa 2017]

- have a white paper describing the project
- finance it via a coin offering (ICO)
- very little more than ideas without real business models, no prototypes to test tech and demand
- some (many) outright scams

Hinman test

William Hinman, director at SEC, made some remarks with hints on what coins are not securities

Bitcoin and Ethereum are not equities

- they are sufficiently decentralized
- there is no issuer
- no one can act on insider information (no information asymmetry)

Hester Peirce, SEC Commissioner, differentiates tokens by their use

- as an investment (equities)
- means to operate a functioning network (not securities)

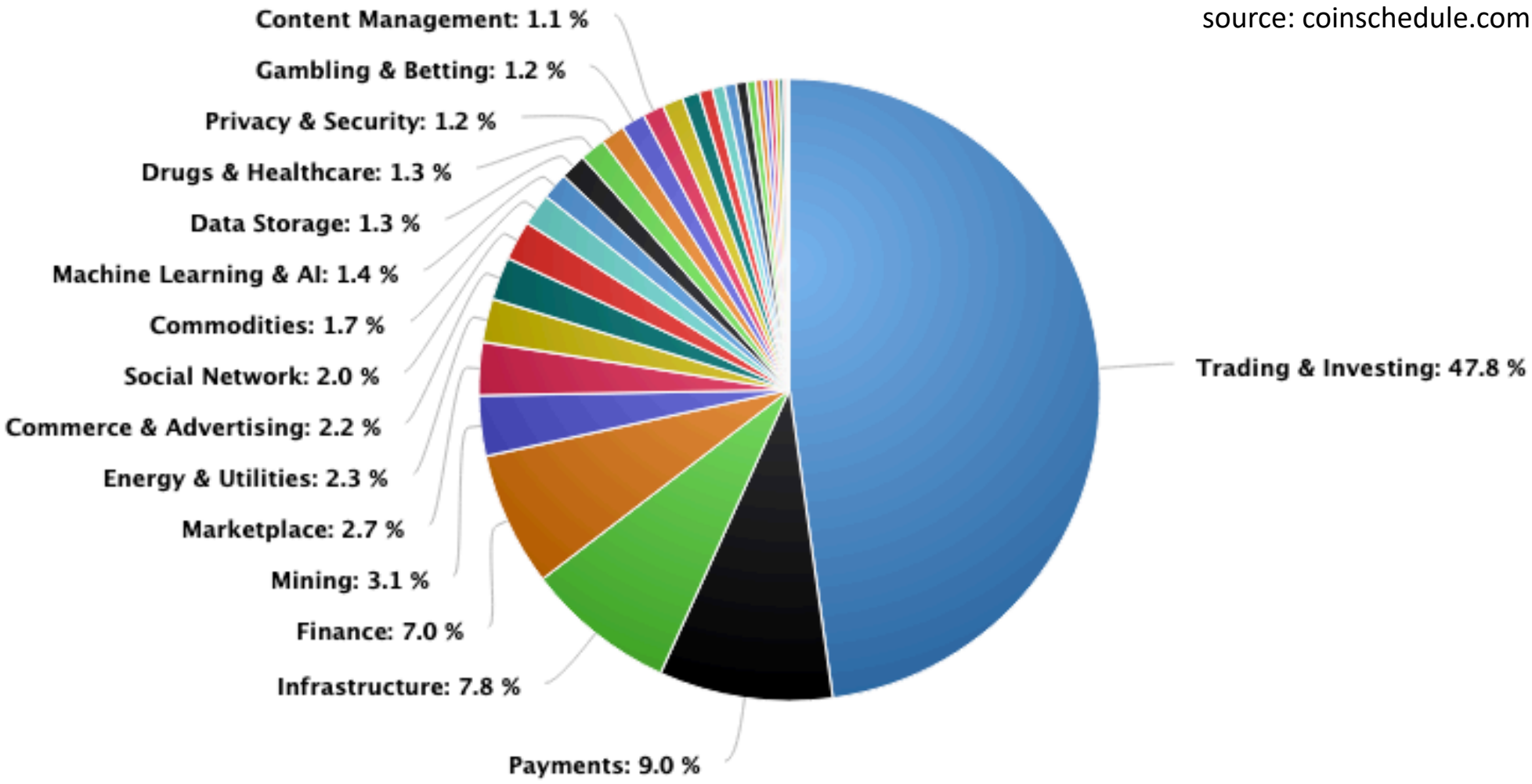
ICOs ↘ IEOs ↗

Initial Exchange Offerings similar to ICOs but

- tokens are sold to investors through a crypto exchange
  - not directly by the startup
- investors must already hold the exchange's token
  - KYC/AML is taken care of
- crypto exchange
  - plays the role of an investment bank
  - takes a cut between 2% to 5% of the sums raised
- +/-
  - - frauds are waiting to happen and people will get burned
  - + exchanges risk their reputational damage if they list bad projects

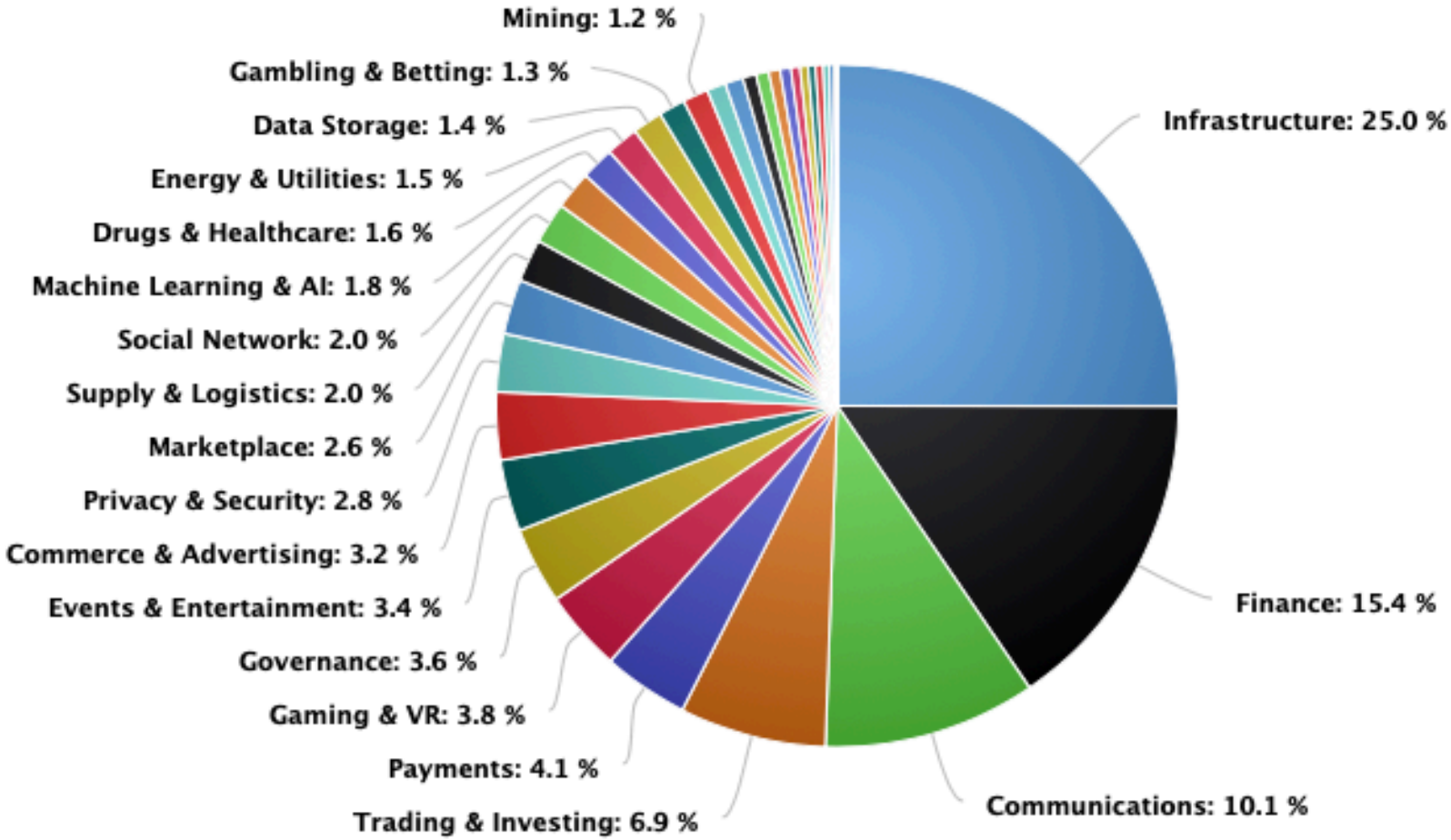
Categories by amount raised ‘19

$3.1 billion raised in ’19 - mid Oct
[Bitfinex (Tether) $1B, Kinesis (KAU,KAG) $193M]
source: coinschedule.com



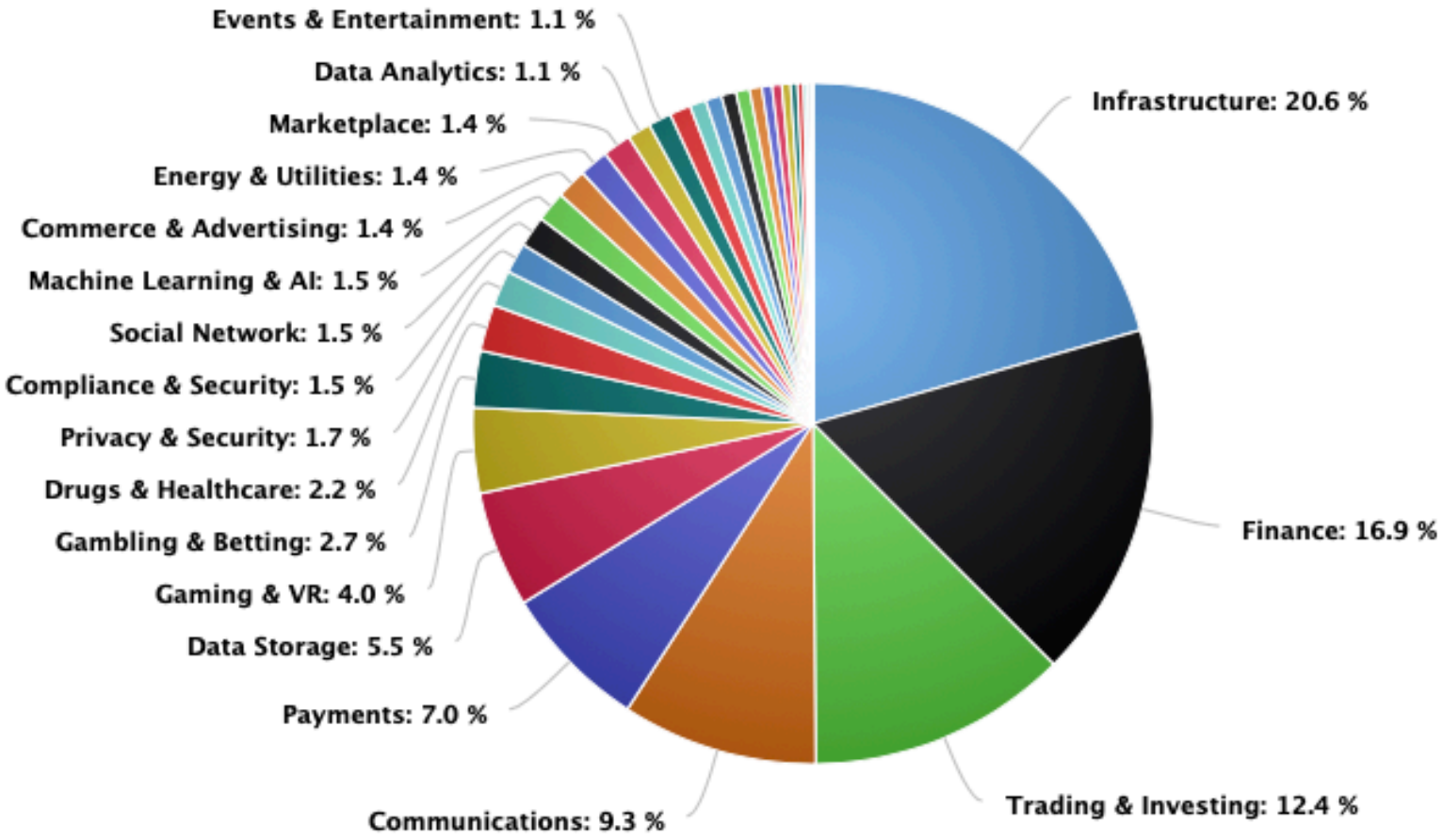
Categories by amount raised ‘18

$21 billion raised in ’18
[EOS $4B, Telegram (GRAM) $1.7B]
source: coinschedule.com



Categories by amount raised ‘17

$6.5 billion in ’17
[Hdac $258M, Filecoin $257M]
source: coinschedule.com



Tax treatment of virtual currencies

IRS treats CC as property

receiving CC as payment of goods/services must be reported as income expressed in US dollars

- this $ amount becomes the cost basis of the CC used
  - to compute the P/L when is sold or
  - as payment for goods/services

buy a $50 ticket using BTC

- sell BTC to buy $50
  - remember BTC cost basic and compute/report P/L
- get the ticket

CCs as currencies

problematic due to reporting requirements of everyday Tx of ordinary people, and

- no threshold for reportable currency transactions
- volatility (- stable coins)

IRS has sent notices to taxpayers in summer ‘19

- to educate them on how CCs are taxed
- then warning letters to CC account owners
- then a another round of letters listing specific amounts owned

latest IRS guidance [Oct ’19]

- fair market value and cost basis
  - actual amount spent to acquire the cc
  - the quoted price on the exchange
  - mark value as reported on an index
- first-in-first-out or specific coin identification
- hard fork & airdrops create an income event
  - when the taxpayer has “dominion and control over the cryptocurrency so that [he/she] can transfer, sell, exchange, or otherwise dispose of the cryptocurrency.”
  - not when a user exercises this control over a new coin