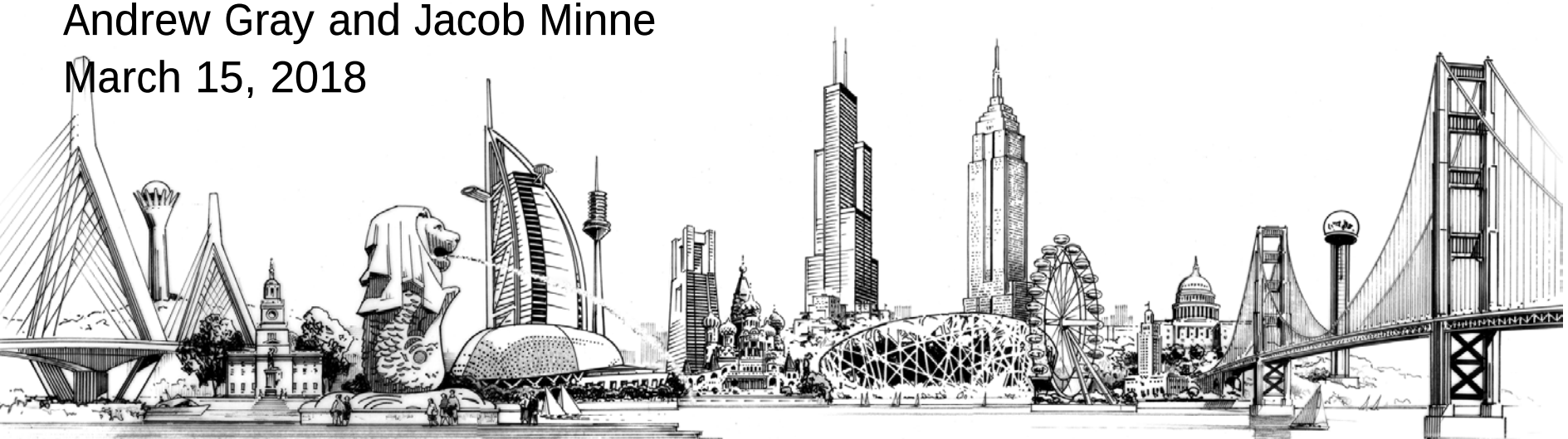
Morgan Lewis

BITCOIN, BLOCKCHAIN, AND CRYPTOCURRENCIES – AN OVERVIEW OF TECHNOLOGY AND LEGAL ISSUES

Andrew Gray and Jacob Minne

March 15, 2018



INTRODUCTION TO BLOCKCHAIN

What is Blockchain?

A consensus between users to create

1. A database,
2. that is distributed (not centralized),
3. whose data elements are immutable (unalterable); and
4. Cryptographically secure

"At its simplest level, a blockchain is nothing much more than a fancy kind of database"

- Blythe Masters, Digital Assets

1- Database

- Many financial assets (stocks, bonds, currency) are now held in electronic digitized form
- These digitized financial assets or transaction data relating to such assets are stored in databases, ledgers or registers
- Financial Services Databases
  - Bank Accounts
  - Trade Registers
  - Cleared Trade Registers
  - Price Quote Data
  - Swap data repositories
  - Transfer Agent – Shareholder/Investor Data

2- Centralized Databases

- Most databases we are familiar with are centralized
  - Banks, Brokers, Exchanges, Dealers, Clearinghouses, and Asset Managers maintain a proprietary ledger of customer accounts and assets
- These Databases are proprietary
- Data is controlled solely by the “owner” of the database
- The centralized database is the sole repository of the data

2- Distributed Databases

- A Blockchain database is not centralized, but rather, distributed
  - A network of users, each of which stores its own copy of the data
  - Every participant in a blockchain has access to a complete copy of the entire database
  - Every participant has the potential to add data to the blockchain database pursuant to a consensus mechanism

3- Immutable

- In a “regular” database, it is possible for the owner of the database to alter, replace, or delete data
- In a blockchain, once data is added to the database through the consensus mechanism, it is permanent, the data element, as a practical matter, cannot be deleted or modified
- Only new data elements can be added to a blockchain
- Most blockchains maintains a permanent record of what data was added, when, and by who

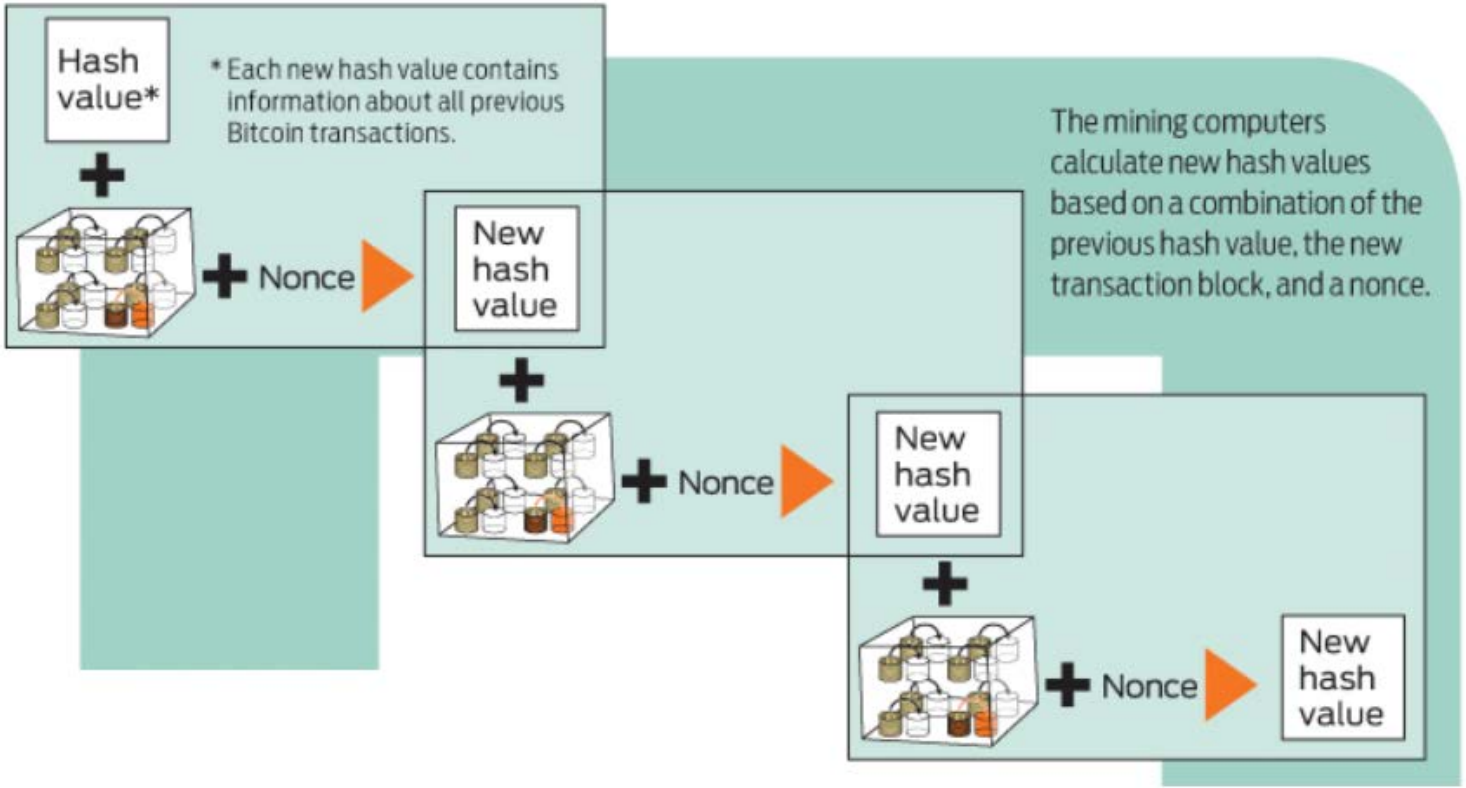
4- Cryptographically secure

- Access to a traditional centralized database maintained by a Bank, Broker, Asset Manager, Exchange, Clearing, etc... (a “Trusted Provider”) is controlled by the owner of the database
- A distributed database needs to be able to have a secure and reliable method for updating the database
- Cryptographic techniques and consensus mechanisms make it possible for participants to verify that every new entry to the blockchain database is valid

Consensus Mechanism

- All blockchains use some type of consensus mechanism to add new blocks to the database
- The consensus mechanism will differ depending on the design of the database, particularly whether it is permissioned, or permissionless
- If permissioned, degree of trust in the participants matters and affects mechanism – “permissioning members”
- If permissionless, no need to trust other participants, rather the blockchain relies on network of participants to confirm transactions using a variety of algorithms to ensure validity of transactions
- “Proof of Work” and other types of consensus mechanisms

Consensus Mechanism - Illustrated



https://spectrum.ieee.org/image/MjA3NDM1OA.jpeg

Public vs. Private Blockchain

- Public vs. Private Blockchain Databases
  - A blockchain may be “public” (non-permissioned)
    - Open to anyone (broad accessibility, no central control)
    - All may participate in approving transactions
  - A blockchain may also be “private” (permissioned)
    - Open only to those who meet the membership criteria of the network
    - Certain members control the confirmation of transactions (“consensus authorities”)

Adding Blocks to the Blockchain

- A transaction on the blockchain is simply the change in the registered owner of an asset.
- For a person A to transfer an asset to person B, it is first necessary to determine that A is the rightful owner of the asset.
- Reference past transactions in the blockchain to find that at some point A obtained the asset and has not yet sold it.
- Once this verification is done, A and B can agree to the transaction.
- A block is created with details of the new contract (A sells asset to B).
- A's agreement to the new contract is finalized by A's digital signature.
- B's agreement to the new contract is finalized by B's digital signature.
- A cryptographic hash is calculated based on: contract details; signatures of A and B; and previous block. The hash is used to link the new block to the last bock in the chain.
- Once the consensus mechanism agrees to the changes, the new block is added to the previous chain of blocks.

ICOs and Smart Contracts

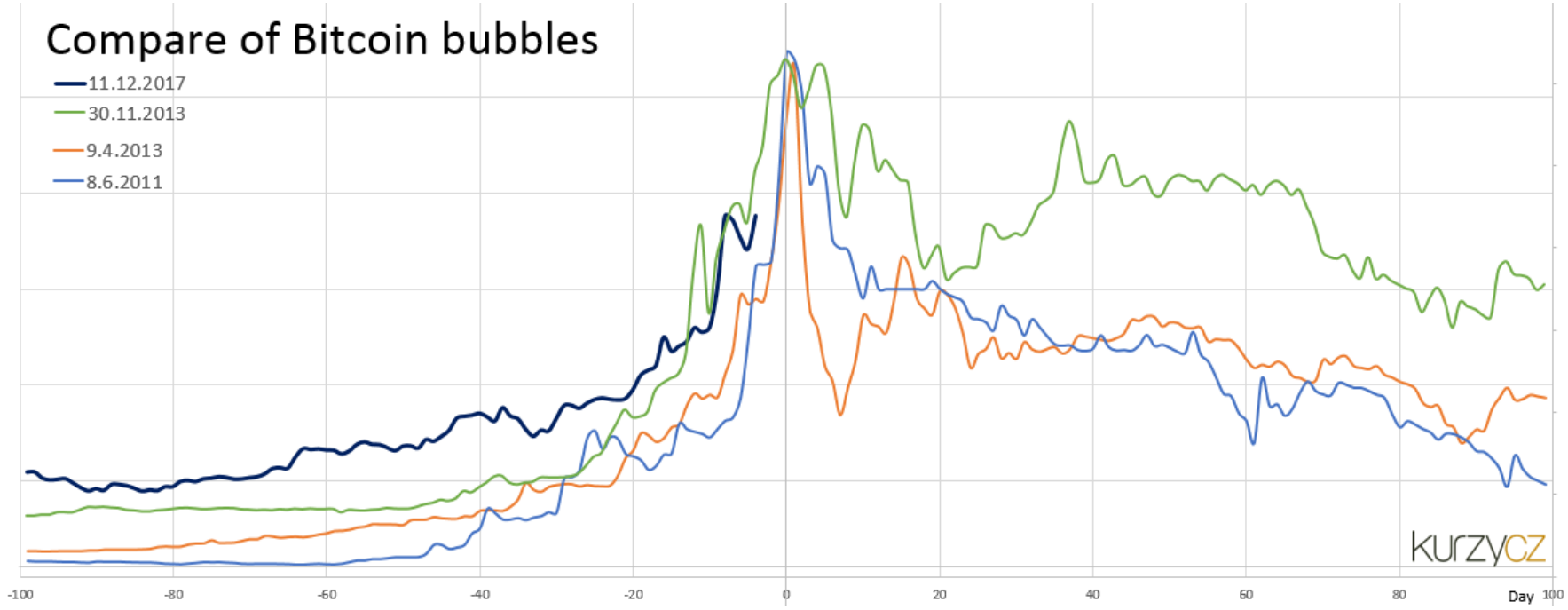
- Using scripts, a cryptocurrency transaction can be turned into a program, and information can be stored on the blockchain.
- Examples
  - Games (“Cryptokitties”)
  - Gambling
  - Data Storage
  - Inventory Tracking
  - Multisignature Wallets
- Users can also use smart contracts to launch “tokens”—these are like a coin-within-a-coin and can be traded with other users on the host blockchain (e.g., Ethereum)

POPULAR CRYPTOCURRENCIES

Bitcoin

- The Original Cryptocurrency, invented by “Satoshi Nakamura”
- First mined January 3, 2009
- Recent market value fluctuating between $8,000 - $12,000; market capital around $150 Billion
- Responsible for 0.24% of global power consumption

Bitcoin – A History in Price



Bitcoin – Recent History

Bitcoin – Comparative Value

Asset	Total Market Value / Capital
Bitcoin	$147 Billion
US M1 Deposits	$3,647 Billion
US M2 Deposits	$13,838 Billion
All Gold Mined	$7,700 Billion
Global Real Estate	$217 Trillion

Ethereum

- Initial Release on July 30, 2015
- Proposed in late 2013 Vitalik Buterin
- First major support for a fully “turing complete” scripting language, allowing complex “smart contracts” and ICOs.
- Recent market value fluctuating between $600 – 1,200; market capital around $75 Billion
- Planned change from a “Proof of Work” to “Proof of Stake” consensus mechanism

Litecoin

- Initial Release on October 7, 2011 by Charlie Lee
- Faster block times and a different algorithm, designed to be more resistant to GPU (and ASIC) mining
- Early Support for Lightning Network
- Recent market value fluctuating between $160 – 220; market capital around $10 Billion

Bitcoin Cash

- Created as a “Hard Fork” from Bitcoin on August 1, 2017 – all Bitcoin holders got Bitcoin Cash
- Goal to allow “on chain” scaling via 8MB or larger blocks to deal with high transaction fees / Limited developer support for Lightning Network or other off-chain scaling solutions
- Bitter community divide
- Recent market value from $900 – 1300; market capital around $17 Billion.

Other Cryptocurrencies

- Monero
- Dash
- Zcash
- Ripple
- Tether
- Bitcoin Gold
- Siacoin

IP ISSUES

Recall Blockchain means:

- a distributed ledger network
- using public-key cryptography to cryptographically sign transactions
- that are stored on a distributed ledger,
- with the ledger consisting of cryptographically linked blocks of transactions.
  - The cryptographically linked blocks of transactions form what is known as “a blockchain.”

Unlikely to be foundational blockchain patent:

- A nine-page white paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System,” describing the concept of a blockchain, was published under the pseudonym Satoshi Nakamoto in 2008 to “The Cryptography Mailing List.”
- Nakamoto did not apply for a patent on the concept of a blockchain described in that paper.
- Someone claiming to be Nakamoto — an Australian CS professor named Craig Wright — has filed 73 blockchain patent applications in the United Kingdom.
  - Why the UK?
  - Why announce these applications rather than wait for them to issue or publish?

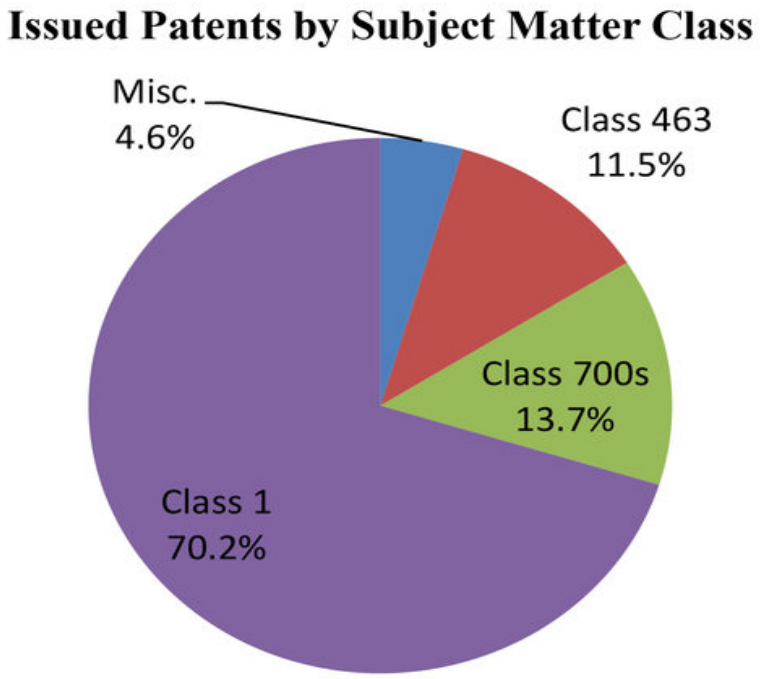
Blockchain Patents???

- Because core blockchain technology is already part of the public domain, only novel and non-obvious variations can be patented.
- Putting aside the questions of patent eligibility and obviousness, patent filings are increasing roughly three-fold each year:
  - 282 issued patents and 1258 published patent applications (blockchain or bitcoin or “distributed ledger”).
- Competition is building for patents that go beyond bitcoin and cover inventions that support a distributed public ledger.

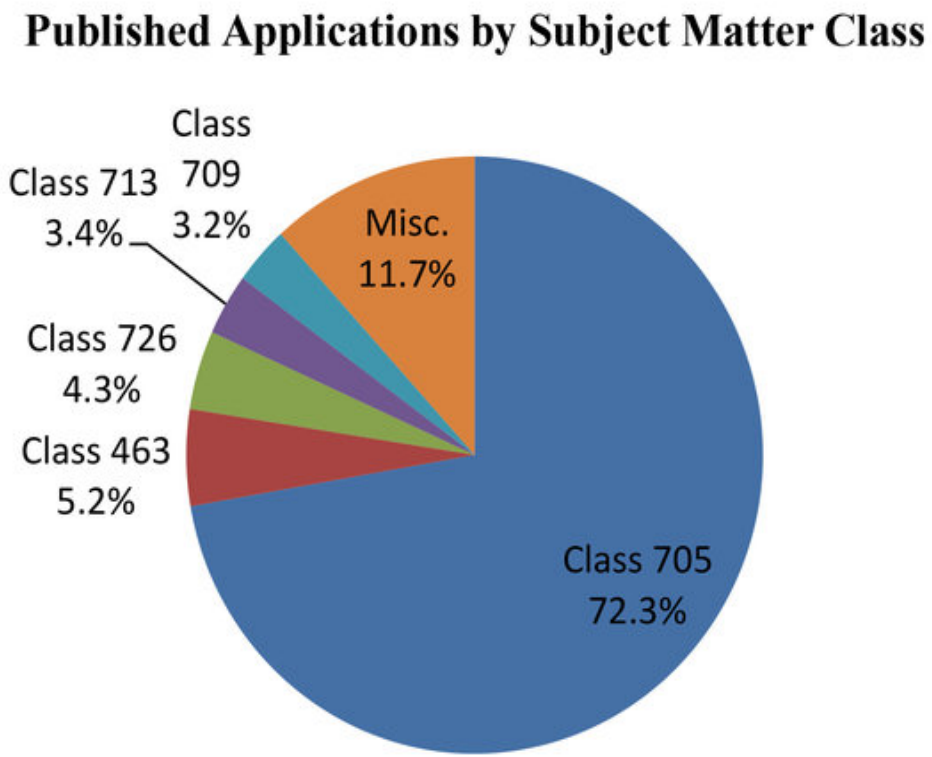
Exemplary Blockchain Patent Titles

- 9,825,931 - System for tracking and validation of an entity in a process data network
- 9,825,765 - Method for distributed trust authentication
- 9,824,540 - Method and system for gaming revenue
- 9,824,408 - Browser payment request API
- 9,824,222 - Method of distributed discovery of vulnerabilities in applications
- 9,824,031 - Efficient clearinghouse transactions with trusted and un-trusted entities
- 9,820,120 - Mobile security technology
- 9,818,116 - Systems and methods for detecting relations between unknown merchants and merchants with a known connection to fraud
- 9,818,109 - User generated autonomous digital token system

Blockchain Patents:



Blockchain Patent Applications



Blockchain Patent Filers

- Financial Institutions
  - Bank of America
  - Goldman Sachs
  - MasterCard
  - Visa
  - Wells Fargo
- Tech Companies
  - Amazon
  - Apple
  - Facebook
  - Dell
  - IBM
- Blockchain-Focused Startups
  - Coinbase
  - Coinlab
  - Chain
  - 21 Inc.

Open Source Blockchain

- Core blockchain technology is unpatented.
- The non-profit Linux Foundation has formed the Hyperledger Project to create an open-source standard for distributed ledgers. The founding members include:
  - technology companies (such as Oracle, Intel and Cisco)
  - integrators (such as IBM and Accenture)
  - financial institutions (such as J.P. Morgan and Wells Fargo)
  - pure-play blockchain companies (such as Ripple and Blockstream).
- Notable blockchain players that have made their software open-source are:
  - Ethereum (smart contracts)
  - block.one (commercial applications)
  - Chain (enterprise-grade blockchain infrastructure)
  - Digital Asset Holdings (financial applications).
- Blockchain Defensive Patent License

REGULATORY CONCERNS – JURISDICTION, DATA PRIVACY AND SECURITY

Blockchain, Jurisdiction, and Personal Data

- Any blockchain system that holds personal data will need to comply with applicable data protection laws.
  - Which data protection laws will apply?
  - Must decentralized blockchain comply with the laws of every territory in relation to personal data it holds?
    - How do you enforce this?
    - Who?
    - Where?

Immutable Transactions and the GDPR

- The EU's General Data Protection Regulation
  - Obligation on data processors to pseudonymize data
  - Right for data subjects to request erasure of their personal data (the 'right to be forgotten').
  - Personal data must be deleted to or corrected if it is incorrect.
  - The person concerned has the right to limit the processing of his/her data.

National Defense Authorization Act- FY 2018

- **SEC. 1646. BRIEFING ON CYBER APPLICATIONS OF BLOCKCHAIN TECHNOLOGY.**
  - (a) BRIEFING REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the heads of such other departments and agencies of the Federal Government as the Secretary considers appropriate, shall provide to the appropriate committees of Congress a **briefing on the cyber applications of blockchain technology**.
  - (b) ELEMENTS.—The briefing under subsection (a) shall include—
  - (1) a description of potential **offensive and defensive cyber applications of blockchain technology** and other distributed database technologies;
  - (2) an assessment of efforts by **foreign powers**, **extremist organizations**, and **criminal networks** to utilize such technologies;
  - (3) an assessment of the use or planned use of such technologies by the Federal Government and critical infrastructure networks; and
  - (4) an assessment of the vulnerabilities of critical infrastructure networks to cyber-attacks.

Enhanced Cybersecurity Features

- Secure transactions
  - Payments
- Tamper-Resistant
  - Preventing data manipulation and fraud
- Encryption
  - Privacy
  - Protecting data
- No single point of failure
  - Decentralized
  - Protect against DDoS attacks
- Authenticating users and devices
- History of transactions

Vulnerabilities

- Access Issues
  - Theft of private keys
- Insider Threat
- System Damage
- Outages

Role of Cybersecurity Program

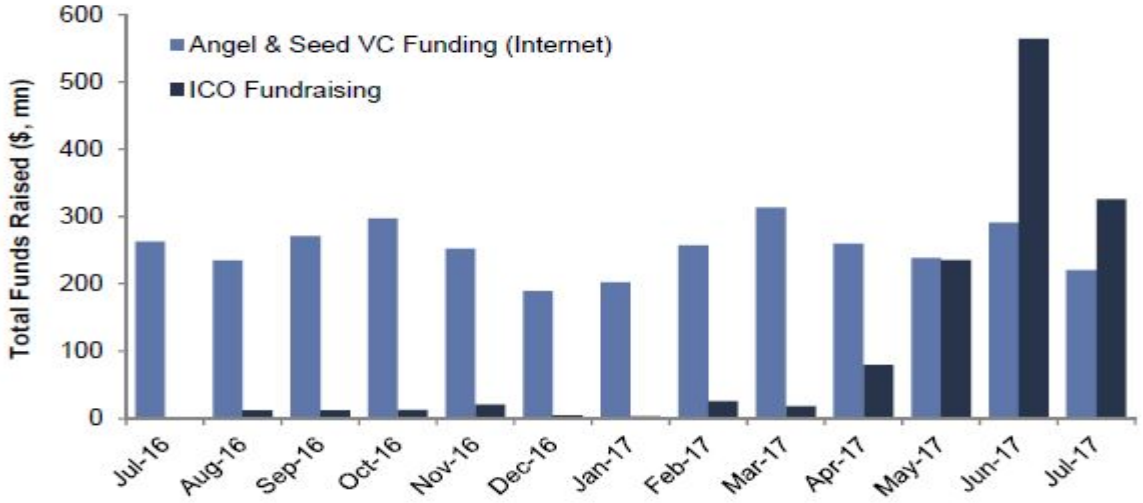
- Cybersecurity Program
  - Risk assessment
  - Tailored approach
  - Controls, policies and procedures
  - Authentication and authorization issues
  - Encryption and security

- Withstanding Regulatory Inquiry
  - Reasonable cybersecurity
  - Examples
    - Data breach encryption safe harbor
    - Third party hosting

REGULATORY CONCERNS – ICOS AND SECURITIES LAWS

ICO's – Why We Care

Exhibit 8: The pace of ICO fundraising has now surpassed Angel & Seed stage Internet VC funding globally
Total Funds Raised by month ($, millions)

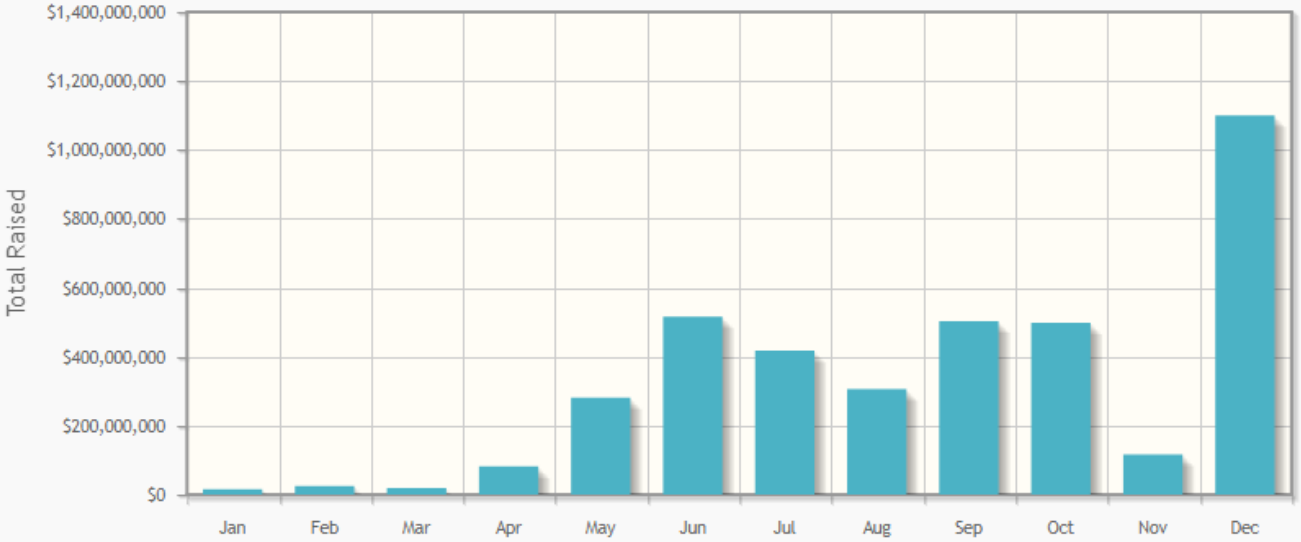


Note: ICO fundraising as of July 18th, 2017, per Coin Schedule. Angel & Seed VC funding data as of July 31st, 2017 and does not include "crowdfunding" rounds.

Source: CoinSchedule, CB Insights, Goldman Sachs Global Investment Research.

ICO's – Why We Care

Cryptocurrency ICO Stats 2017



Totals raised are grouped by the ICO closing date and are valued using BTC exchange rate at that time. Data last updated on 9th March 2018 22:45 UTC

Total: $3,880,018,203

Total Number of ICOs: 210

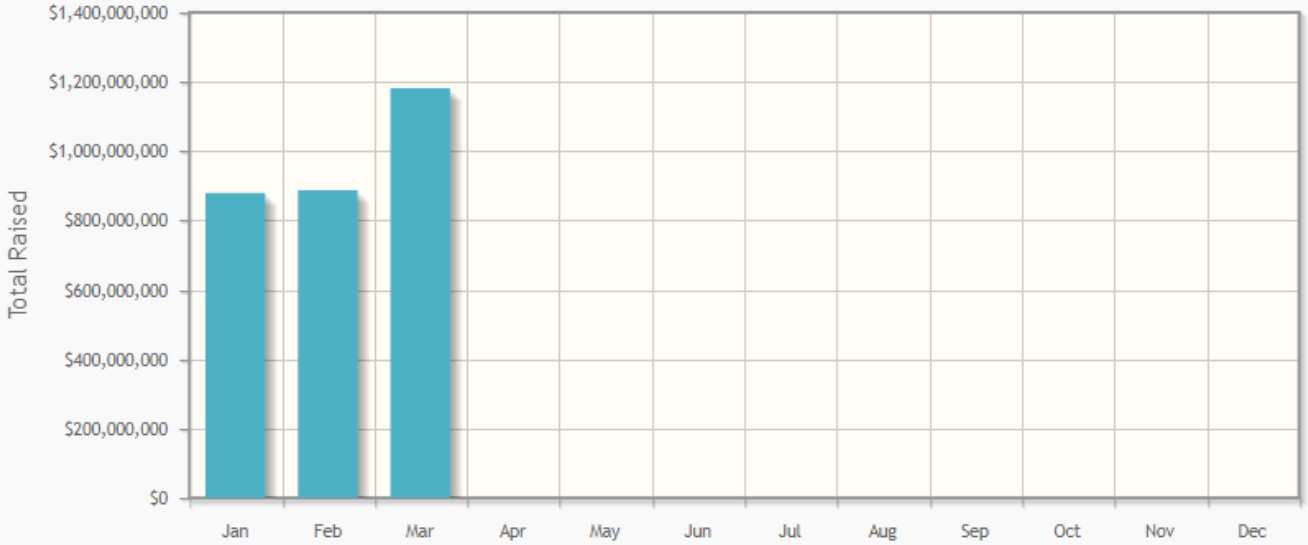
Top Ten ICOs of 2017

Position	Project	Total Raised
1	Hdac	$258,000,000
2	Filecoin	$257,000,000
3	EOS Stage 1	$185,000,000
4	Paragon	$183,157,275
5	Bancor	$153,000,000
6	Status	$90,000,000
7	BANKEX	$70,600,000
8	TenX	$64,000,000
9	Nebulas	$60,000,000
10	MobileGO	$53,069,235

https://www.coinschedule.com/stats.html?year=2017

ICO's – Continuing in 2018

Cryptocurrency ICO Stats 2018



Totals raised are grouped by the ICO closing date and are valued using BTC exchange rate at that time. Data last updated on 9th March 2018 22:45 UTC

Total: $2,947,568,888

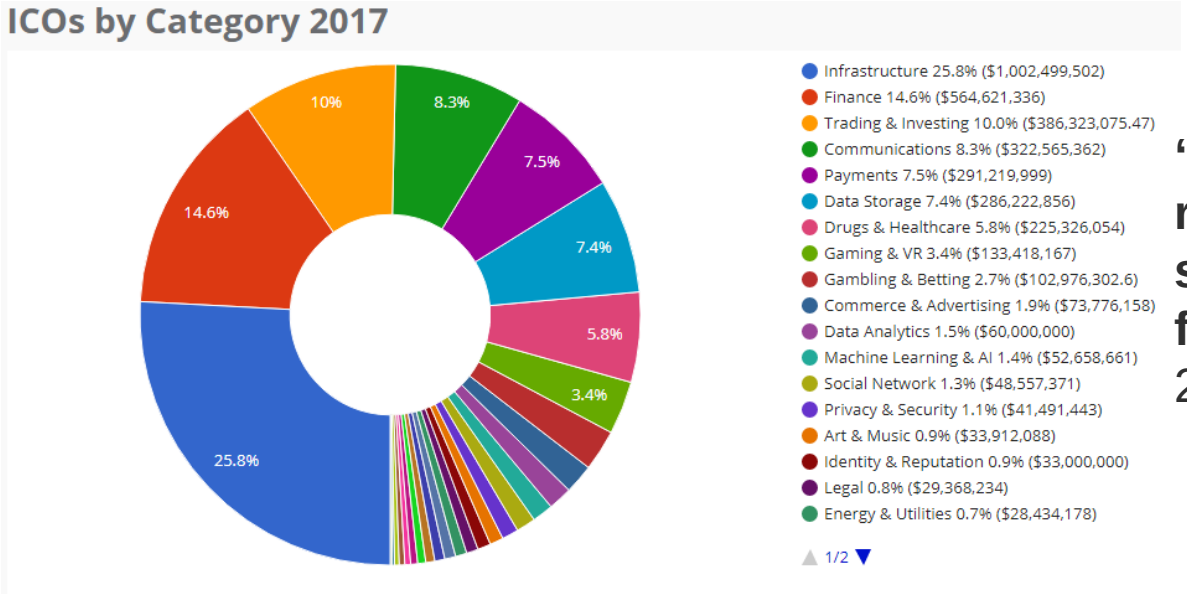
Total Number of ICOs: 78

Top Ten ICOs of 2018

Position	Project	Total Raised
1	Telegram ICO (Pre-sale 1)	$850,000,000
2	Huobi token	$300,000,000
3	Bankera	$150,949,194
4	Envion	$100,000,000
5	Neuromation	$71,669,400
6	Crypterium	$51,656,963
7	SwissBorg	$50,000,000
8	Lendroid	$47,500,000
9	iungo	$45,978,800
10	Fusion	$42,185,216

https://www.coinschedule.com/stats.html?year=2018

ICO's – The #1 Source for Early Stage Financing



"Initial coin offerings have raised $1.2 billion and now surpass early stage VC funding" – MSNBC, August 2017

https://www.coinschedule.com/stats.html?year=2017

Securities Law Issues – ICOs and Cryptocurrency

Are virtual currencies, coins, or tokens “securities”?

According to the SEC, “it depends”:

- “Depending on the facts and circumstances of each individual ICO, the virtual coins or tokens that are offered or sold may be securities. If they are securities, the offer and sale of these virtual coins or tokens in an ICO are subject to the federal securities laws.”

  – *Report of Investigation re: The DAO (July 25, 2017)*

A contrasting view:

- “ICOs represent the most pervasive, open and notorious violation of federal securities laws since the Code of Hammurabi.”

  – *Former SEC Commissioner Joseph Grundfest (quoted in N.Y. Times, Nov. 26, 2017)*

Securities Law Issues – ICOs and Cryptocurrency (cont'd)

When might virtual currency be a security?

- Federal securities laws are designed "to regulate investments, in whatever form they are made and by whatever name they are called." The definition of "security" is broad enough "to encompass ***virtually any instrument that might be sold as an investment***."
  – *SEC v. Edwards*, 540 U.S. 389, 393 (2004); 15 U.S.C. § 77b(a)(1)
- SEC's July 2017 DAO Report confirms the prevailing view that the test of an "investment contract" is central. An "investment contract" is a contract, transaction, arrangement, or scheme (need not be a formal contract) in which:
  1) a person invests money
  2) in a common enterprise
  3) with expectation of profit from the efforts of others

  – *SEC v. W.J. Howey Co.*, 328 U.S. 293, 298-99 (1946)

ICO's – What Do You Get?

- Equity?
- "Utility"?
- A "Donation"?

"With these ICOs, we don't have anything," says Zach Hamilton, a partner at General Crypto, a hedge fund that invests in digital currencies but for now has avoided the coin offerings. Two of the main reasons: The assets "are outright nonexistent or very obscure" and there is a lack of clarity about what a token actually gives him. "They're not a share," he said. "Or, it depends. It could be."

"Coin Offerings Are Hot, but What Are They? Tezos's problems reveal divide on whether ICOs are investments or donations," *WSJ*, Oct. 24, 2017.

SEC – Recent Guidance

- "Investors should understand that **to date no initial coin offerings have been registered with the SEC**. The SEC also has not to date approved for listing and trading any exchange-traded products (such as ETFs) holding cryptocurrencies or other assets related to cryptocurrencies.[2] **If any person today tells you otherwise, be especially wary.**"

SEC – Recent Guidance

- "[C]ertain **market professionals have attempted to highlight utility characteristics of their proposed initial coin offerings** in an effort to claim that their proposed tokens or coins are not securities. **Many of these assertions appear to elevate form over substance.** Merely calling a token a "utility" token or structuring it to provide some utility does not prevent the token from being a security. Tokens and offerings that incorporate features and marketing efforts that emphasize the potential for profits based on the entrepreneurial or managerial efforts of others continue to contain the hallmarks of a security under U.S. law. **On this and other points where the application of expertise and judgment is expected, I believe that gatekeepers and others, including securities lawyers, accountants and consultants, need to focus on their responsibilities.** I urge you to be guided by the principal motivation for our registration, offering process and disclosure requirements: investor protection and, in particular, the protection of our Main Street investors.

https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11

Securities Law Issues – ICOs and Cryptocurrency

Investment contract application to virtual currency

- Most SEC enforcement actions to date have involved virtual currencies used as capital (money) for investments in more traditional forms of securities (shares, notes, or investment contracts issued by Blockchain-related businesses).
- The DAO case: ETH used to buy DAO tokens, which conferred voting and ownership rights and profit interests in projects to be undertaken by The DAO.
  - (i) investment; (ii) common enterprise; (iii) profit expectation
- Use of tokens to purchase goods/services (consumption is not an investment)
- Tokens acquired for speculation (arguably no common enterprise)
- Tokens issued in exchange for seed capital (may be a security)

Consequences of Security Treatment

1. Securities registration requirement

- To be lawfully offered or sold, a security must be registered with the SEC, or qualify for an exemption from registration (under the Securities Act of 1933)
  - Registration is a multi-step, expensive process
  - Common exemptions include sales limited to institutional investors and sales in private offerings to "accredited investors" (special requirements)
- Registration or exemption requirement applies to ***every*** sale, including secondary market resales by initial purchaser
- Securities registration noncompliance gives rise to an onerous ***rescission*** remedy under federal law and the laws of most states

Consequences of Security Treatment (cont'd)

2. **Securities fraud statutes apply**
   - Any material misrepresentation or omission in connection with an offer, sale, or resale may give rise to liability
   - Laws governing initial offerings and some state statutes allow remedies without intentional fraud; due care is only a defense
   - SEC warning re celebrity ICO endorsements (failure to disclose compensation)
   - Several SEC/USAO actions and several putative securities class actions filed within the last few months re particular ICOs
3. **Broker-Dealer Registration Requirements**
   - Anyone in the business of buying or selling securities (a dealer) or effecting securities transactions for others (a broker), unless exempt, must register with the SEC and state securities regulators
4. **Exchange Registration**
   - Any organization or group that "maintains or provides a market place or facilities for bringing together purchasers and sellers of securities" is subject to SEC regulation as a national securities exchange.

Biography

Andrew J. Gray IV
Silicon Valley
T +1.650.843.7575
andrew.gray@morganlewis.com

Serving as the leader of Morgan Lewis's semiconductor practice, Andrew J. Gray IV concentrates his practice on intellectual property (IP) litigation and prosecution and on strategic IP counseling. Andrew advises both established companies and startups on computer and Internet law issues, financing and transactional matters that involve technology firms, and the sale and licensing of technology. He represents clients in patent, trademark, copyright, and trade secret cases before state and federal trial and appellate courts throughout the United States, and before the US International Trade Commission.

Biography

Jacob Minne
Silicon Valley
T +1.650.843.7280
jacob.minne@morganlewis.com

Jacob Minne advises clients on patent, trademark, copyright, and trade secret litigation, as well as related antitrust matters. His litigation experience includes cases for clients in a diverse range of technology fields such as semiconductor chip manufacturing methods, medical devices, and mobile software. He has experience in forums including the US District Court for the Central District of California, the US Court of Appeals for the Federal Circuit, and the US International Trade Commission (USITC).

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington

Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

THANK YOU