IMAS Lunchtime Talk Series
Blockchain, Smart Contracts & ICO

17 May 2018

Claudia Marcusson
Practice Head, Investment Risk & Operations

stradegi

Agenda

- Blockchain
  - Definition & characteristics
  - Blockchain in action
  - When Blockchain makes sense
  - Benefits
- Smart Contracts
  - Definition
  - Smart Contracts in action
  - Misconceptions & Limitations
- Applications & challenges
- ICO
  - Definition
  - Statistics
  - Benefits
  - Risks & Regulation
  - Outlook

Blockchain(s)

Bitcoin explained so easy

Definition & characteristics

A type of distributed ledger, comprised of unchangeable, digitally recorded data in packages, called blocks.

DECENTRALISED
shared across organisations, owned equally by all and dominated by no-one;
No 3rd party or one entity can take control, reverse transactions or cease assets

DISTRIBUTED
multi-locational data structure;
any user can keep own copy of the whole Blockchain with all historical transaction;
Peer-to-Peer network (illustration)

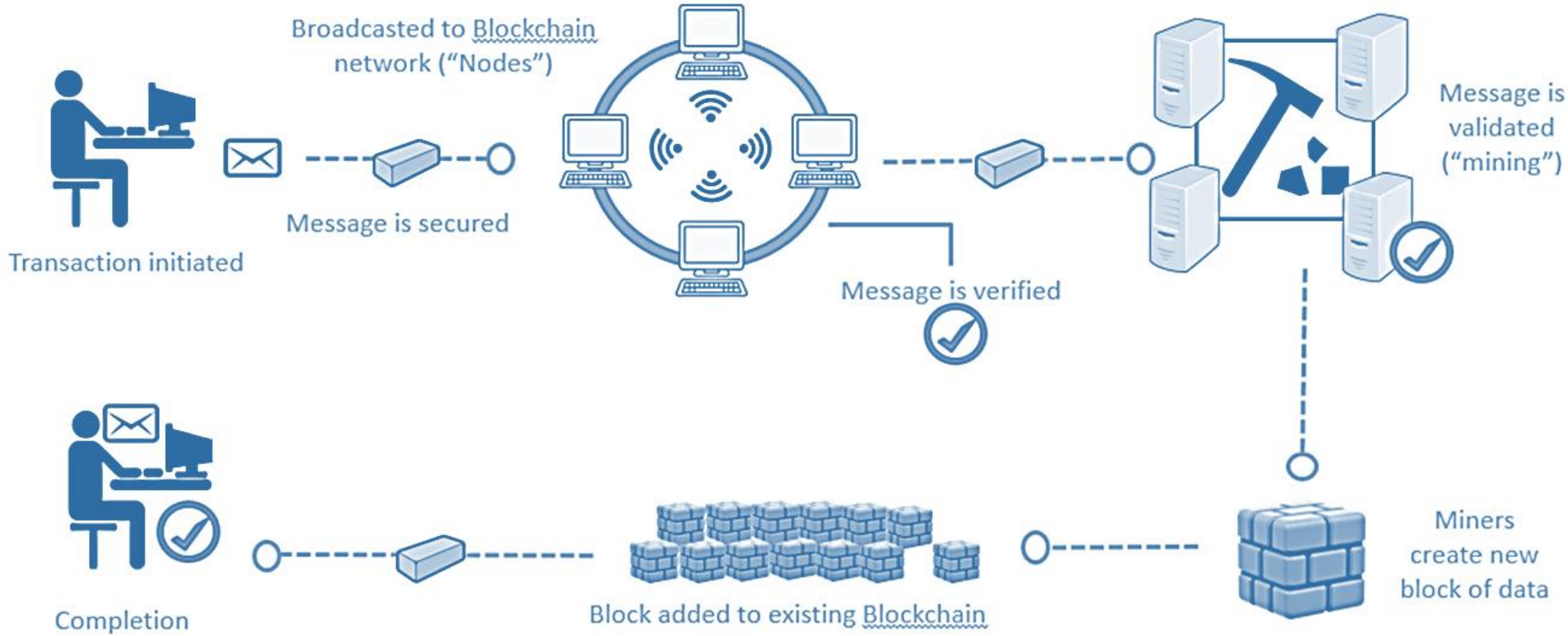
LEDGER
like a "giant excel spreadsheet"
shared openly on the internet;
that can only be added to, nothing can be deleted once written;
Blockchains are immutable

RECORDING TRANSACTIONS
timestamped data entries ("any piece of information")
identified by digital unique 'fingerprint' (hash), captured in a block and linked to each other in a chronological chain

VERIFIED
all members of the Blockchain ("nodes") check that transaction is valid and in the right order of the Blockchain and pass the data to anyone else in the network who does not know yet

CONSENSUS OF USERS
consensus model, where majority of Blockchain members confirm to add new data block to the ledger;
each member updates own copy of Blockchain by adding new block

How does a Blockchain transaction work



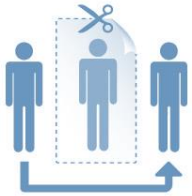
When Blockchain makes sense

☑ multiple parties share the same data,

☑ multiple parties have to update data,

☑ requirement for verification (records need to be validated),

☑ intermediaries add cost and complexity,



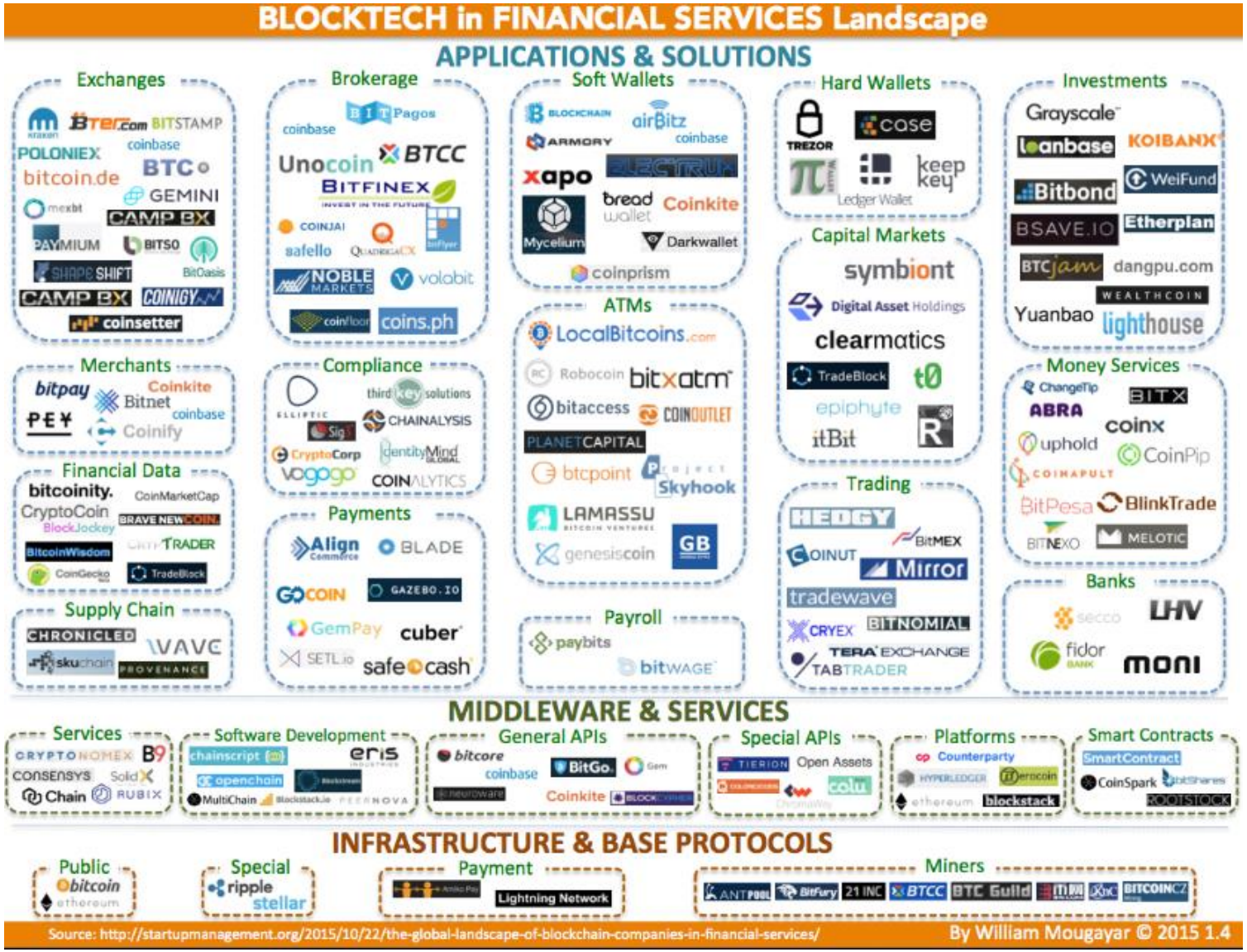
☑ interactions are time sensitive (reducing delay has business benefit),

☑ transactions created by different participants depend on each other.

Benefits of Blockchain technology

- **Cost reduction** due to absence of intermediary, sharing ledger between parties and lower transaction costs
- **Efficiency** due to time savings e.g. more rapid settlement process for any transaction, funding and verification
- **Immutable/permanent transactions** and **real-time audit**
- **Security** due to de-centralized structure and encryption (public + private key); almost impossible to hack or manipulate
- **Enable revenue growth** e.g. attract new business through higher-quality service

Blockchain landscape



Smart Contracts

Connecting Blockchain to the real world

1996 Nick Szabo First Smart Contract: "a set of promises, specified in digital form, including protocols within which the parties perform on these promises"

'self-executing' computable agreements that are immutable and verified by consensus when its own conditions are met

Scaling trust where people can connect 'anonymously'

Contract which both humans and machines can read

Great Grandfather of Smart Contracts

> if money received = $2.50
> & the button pressed is "Diet Coke"
> then release Diet Coke

Smart Contract in action

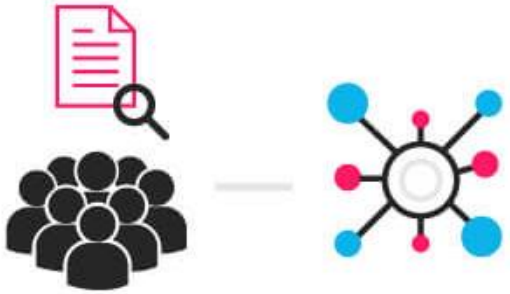
1

Contract is written as code into Blockchain; involved parties/ individuals are anonymous

2

Triggering event (e.g. expiration date and strike price) is hit and the contract gets initiated to execute itself according to the coded terms

3



Regulators can use the Blockchain to understand activity in the market while maintaining privacy of individual's positions

Source: http://blockgeeks.com

Coding legal language


```
pragma solidity ^0.4.20;

contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) public {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) public {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

Benefits of Smart Contracts

- **Autonomy:** no need to rely on broker, lawyer or intermediaries to confirm; no manipulation by a third party, since execution is managed automatically by network
- **Trust:** documents are encrypted on a shared ledger
- **Backup:** documents are duplicated many times over
- **Safety:** cryptography and several securities layers keep documents safe
- **Speed:** software code automates paperwork which is manually processed
- **Savings:** no presence of an intermediary like a notary to witness the transaction
- **Accuracy:** avoids errors that come from manually filling out heaps of forms

Misconceptions

Smart contracts are self-executing bits of code

Like with a vending machine, you need to initiate a smart contract by paying it to run simultaneously on all nodes participating in validating the blockchain (e.g. 14k nodes for Ethereum)

Smart contracts can make payments in normal currencies

In general, smart contracts can only make payments in cryptocurrencies not in fiat currency

Smart contracts to automate processes

No smart contract needed for basic business logic (e.g. make payment based on a share price on a particular date)

Smart contracts communicate directly with the outside world

Because of efficiency and security, data aimed at changing the state of a contract need to be pushed onto the blockchain (via “oracles”).

Smart contracts to make payments

APIs cannot handle large request by all nodes to transfer fiat money into a bank account. Instead a trusted financial services provider could monitor the blockchain’s state and making transfers that mirror on-chain transactions.

Limitations

Not everything can be coded

Some legal phrases demand degree of subjectivity or judgement on a case-by-case basis or capture a non-exhaustive list of circumstances e.g. force majeure, best efforts.

Some transactions require contracts in writing

E.g. transfer of land, original deeds

Coping with events that occur outside the code

After coding, smart contracts are irrevocable. How to avoid that performance of contract is illegal or contrary to business common sense? (e.g. unwinding because of misrepresentation, mistake, duress, change of laws, data bugs)

Privacy issues

Most smart contracts cannot process encrypted data on-chain (only mask the contents, but not keep them completely private). Reliable privacy can only be achieved by off chain computation along with compliance.

No jurisprudence yet

Legally binding and enforceable?; identification of defendant?; applicable governing law and jurisdiction?; dispute resolution & arbitration?; etc.

Applications & Challenges

Broad applications

- **Payments and Remittance Service:** transactions directly between two parties with reduced risk, lower transaction costs and improved speed, efficiency and transparency
- **Trading assets digitally & Transfer of financial instruments:** cut out intermediator (e.g. brokers or clearinghouses)
- **Identity management and data verification:** e.g. Know Your Customer (KYC) and Anti-Money Laundery (AML) registries where individual's or entity's identity is stored in the Blockchain, ensuring secure and rapid ID authentication
- **Regulatory Reporting:** delivering a fully transparent, accessible database for governing bodies
- **Clearing & Settlement:** entire lifecycle of a trade (including execution, clearing and settlement), lowering post-trade latency and reducing counterparty exposures (instant settlement)
- **Reconciliation & Claims Management:** manual reconciliation becomes redundant because synchronized ledger of transactions distributed across network of users

Existing applications

Payments & Remittance

TOAST ABRA coins.ph

Send Money. Save Money. Earn Time.

Health Care Data Storage

BITHEALTH DNA.Bits

Identity management/ data verification

Blocknotary BLOCKSCORE CHAINALYSIS

Clearing and Settlement

clearmatics Lykke

A Blockchain-Enabled Global Marketplace

Trading Platform

DXmarkets WAVE t0 tZERO

Investment Management

funderbeam

Loan provider/ P2P Lending

SALT

Consumer

SHIPCHAIN INS

THE GROCERY INDUSTRY, REINVENTED

Insurance

SingaporeLife Lemonade fizzy Powered by AXA

Smart Home and Internet of Things (IoT)

CHIMERA IOT

Smart Contracts

r3 Attores

Smart Contracts as a Service

Mastering potential challenges

New Technology

Regulation

Legal Enforcement

Cost

Integration concerns

Cultural adoption

ICO

What is in the name?

ICO: Initial Coin Offering
ICS: Initial Coin Sale

versus

ITO: Initial Token Offering
TGE: Token Generation Event

Tokens are crowdfunding units, sold by a project to early supporters to develop products, support expansion and/or accumulate tokens for other goals.

Tokens represent rights, which can largely differ:

- Right to receive service in the future
- Access to the platform/eco-system; transaction fee
- Participation in loyalty programs
- Right for dividends or other underlying assets

Tokens are sold for fiat currency (mainly USD) or liquid cryptocurrencies (e.g. BTC, ETH, XRP, LTC, etc.)

ICO highlights

Year	Raised (m USD)
2014	16
2015	6
2016	90
2017	6,128
2018 (ytd)	4,520

Largest ICO:
Telegram
USD 1.7bn

Average ICO size:
USD 16m

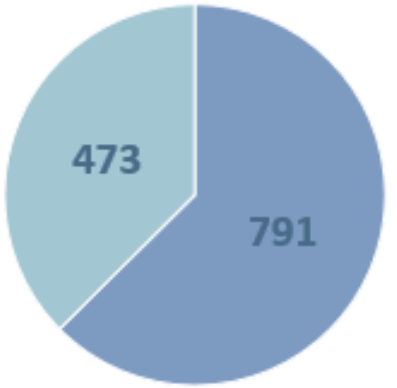
Top countries by number of ICOs	
#1 USA	446
#2 Russia	246
#3 UK	241
#4 Singapore	234
#5 Switzerland	151

+1,565
crypto-currencies

First ICO:
2013

+35,160%
Ripple's cryptocurrency price growth over 2017

Number of ICO*

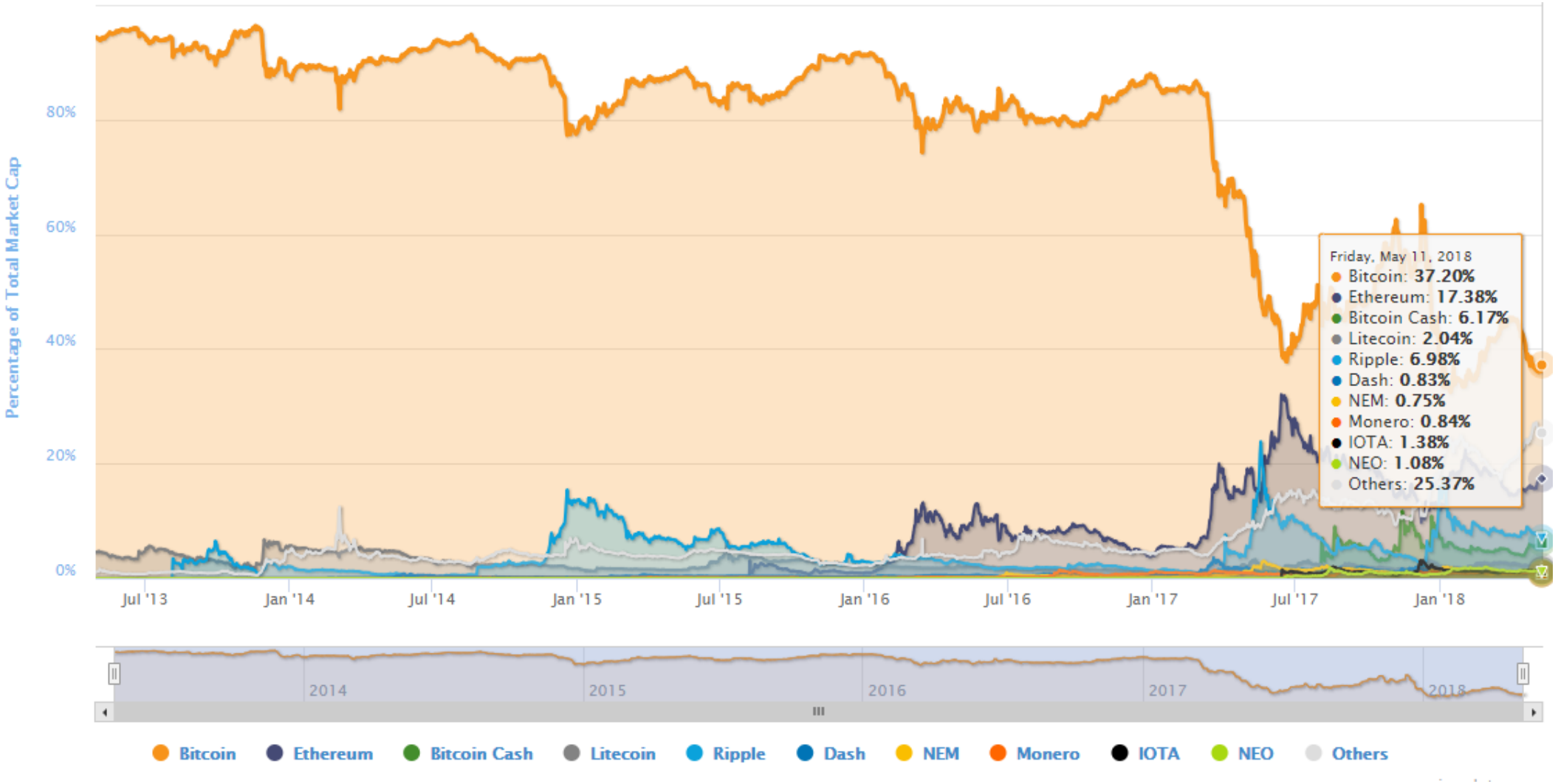


Upcoming (incl. pre-ICO)

Ongoing (incl. pre-ICO)

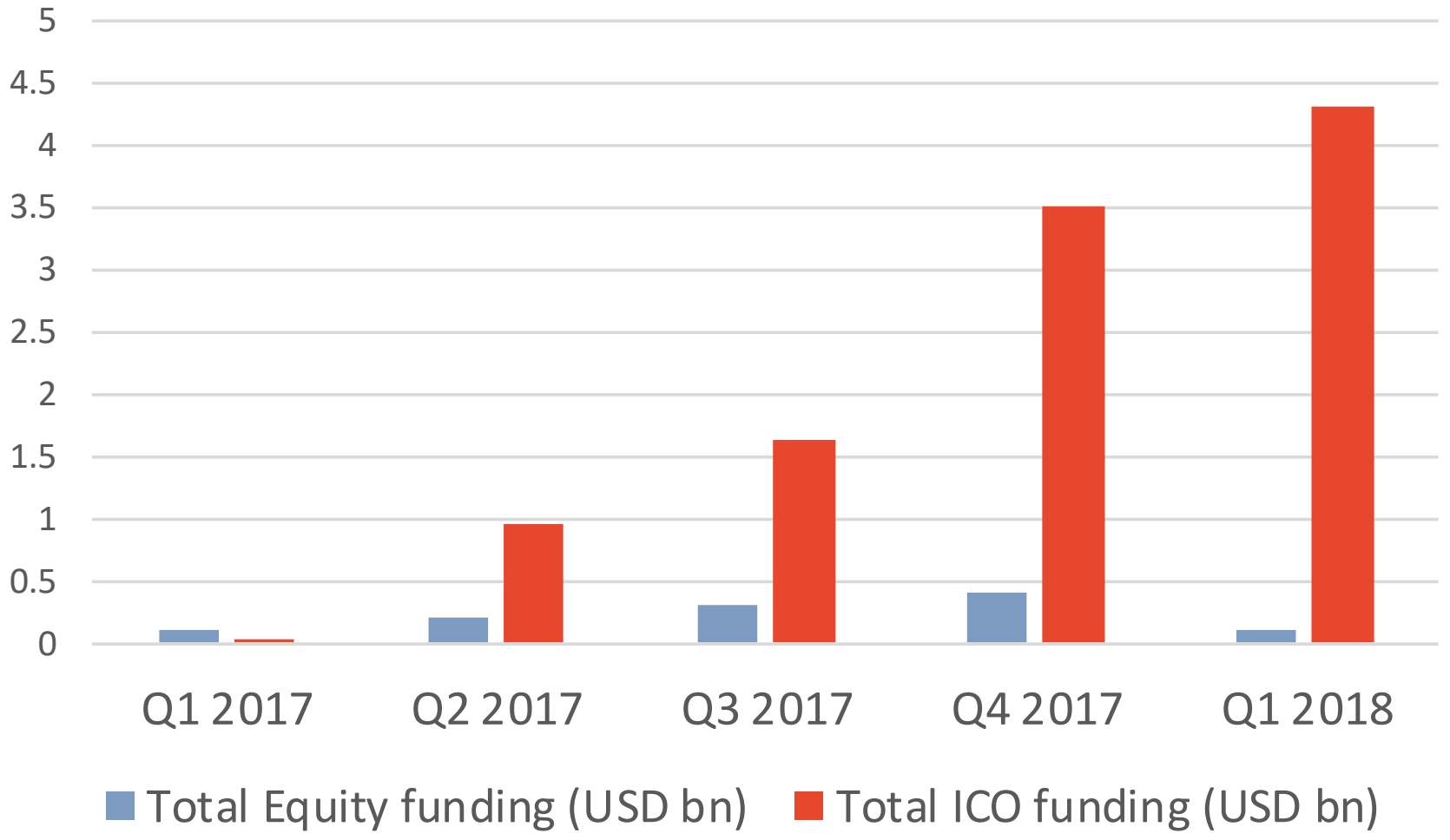
Source: www.icodata.io, www.icobench.com
*as of 11 May 2018, varies per ICO ranking platform

Bitcoin market cap #1



Source: www.coinmarketcap.com

Fundraising 2.0: Equity versus ICO



Source: CB Insights, TokenData, KPMG

Benefits for token purchaser 1/2

Democratization of access
Everyone can participate (at least where not prohibited)
Not limited by geography

Opportunity to invest accumulated cryptocurrency
Divest from main cryptocurrencies; Spending cryptocurrency instead of withdraw into fiat (loosing value)

Opportunity to trade tokens immediately
Unlike VC investments, new token can usually be traded almost immediately on a crypto-exchange (no vesting period)

Involvement
Investor can be part of a community and first users

Early access to token
Potential for capital growth

Benefits for token purchaser 2/2

Diversification of assets
No link to macro economics, fiats, stock markets, etc.

Low interest rates in traditional asset classes
Large amounts of liquidity of (S)HNWI, family offices
Most token purchasers still come from China, Korea, Japan, US

Crypto-community passion for modern technologies and applications
Support of initiatives that are disrupting existing rules and standards

"Gaming" (win big or loose all) and a new innovative & trendy way
to deploy capital

Other benefits

For founders & entrepreneurs

- Efficient fundraising: fast, low-cost, convenient, less documentation, etc.
- Relevant Investors from community (first users/advocates)
- Branding & marketing due to community building
- "Skin in the game" with early adopters
- Share both risks and benefits of efforts with purchasers
- Angel/VC/corp. funding is much more intrusive on founder's vision

For cryptocurrency community

- Internet revolution: new companies and their tokens/coins will help building a new decentralized web, independent from any central entity
- Finance revolution: Blockchain is assumed at cutting edge of Fintech, the technology and business model being proposed will benefit the whole community
- Education and time to mature: more competition makes competitors better and stronger; Blockchain projects getting mature and prepared for real competition with traditional enterprises

Source: www.techinasia.com, bbfund, IT SG

ICO services - a stand alone industry

Strategy & Advisory

Acceleration Services
ICO Strategy & Planning
Influencers & outreach
Token Economics
Whitepaper Assistance

Sales & Marketing

Bounties Management
Customized Sales Portal
Marketing
Online Community Building
Order Book Building
Press/Public Relations
Translation Services

Client Servicing

Partnership Relations
Pre-sales on-boarding
Tokenholder relations

Control & Audit

KYC/AML Process
Post-Sales Audits
Technical Audits
Underwriting

Technology Services

Blockchain as-a-Service
Secure (multi-signature) Wallet Services
Penetration Testing/Cyber Security

Operational Services

Custodial/Escrow Service
Exchanges Listings
Investment Services
Reporting & Analysis
Token Issuance
Token Distribution
Treasury Management

ICO services - examples

Source: www.techinasia.com, bbfund, IT SG

Fundraising via ICO takes time

Source: www.techinasia.com, bbfund, IT SG

Not yet mature industry

Source: www.techinasia.com, bbfund, IT SG

Big money comes with big risks

Regulatory & legal risks

- ICO Tax Risk
- Changing regulations
- Legal basis for ICO documents
- Connection between token holders and issuer
- Intellectual property

Investment/contribution financial risks

- No real financial planning and economics behind
- No previous traction of metrics (often no MVP)
- Post-ICO slowdown (no real value creation/no media coverage)

Token risks

- Lost or stolen tokens
- Hacked wallets
- Challenge of smart contracts

Business ICO risks

- Market demand and macroeconomics
- Traditional players offerings
- New competitors
- Technological shifts
- Regulatory challenges (licenses for business)
- For security tokens: Voting? Control? Participation?
- Multiple Blockchains' interoperability

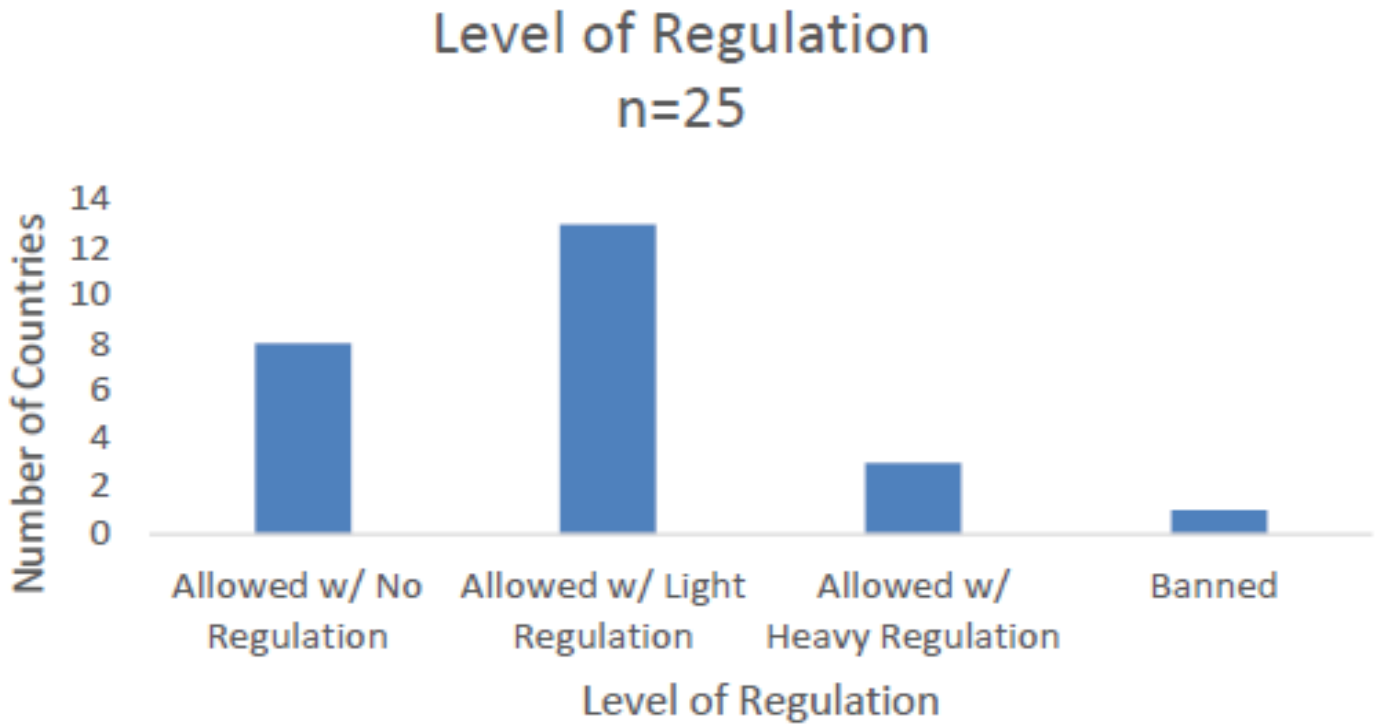
ICO founders risks

- Usually no real world business experience
- Motivation after big ICO?
- Control over funds?
- Salaries?
- Financial statements?

Source: www.techinasia.com, bbfund, IT SG

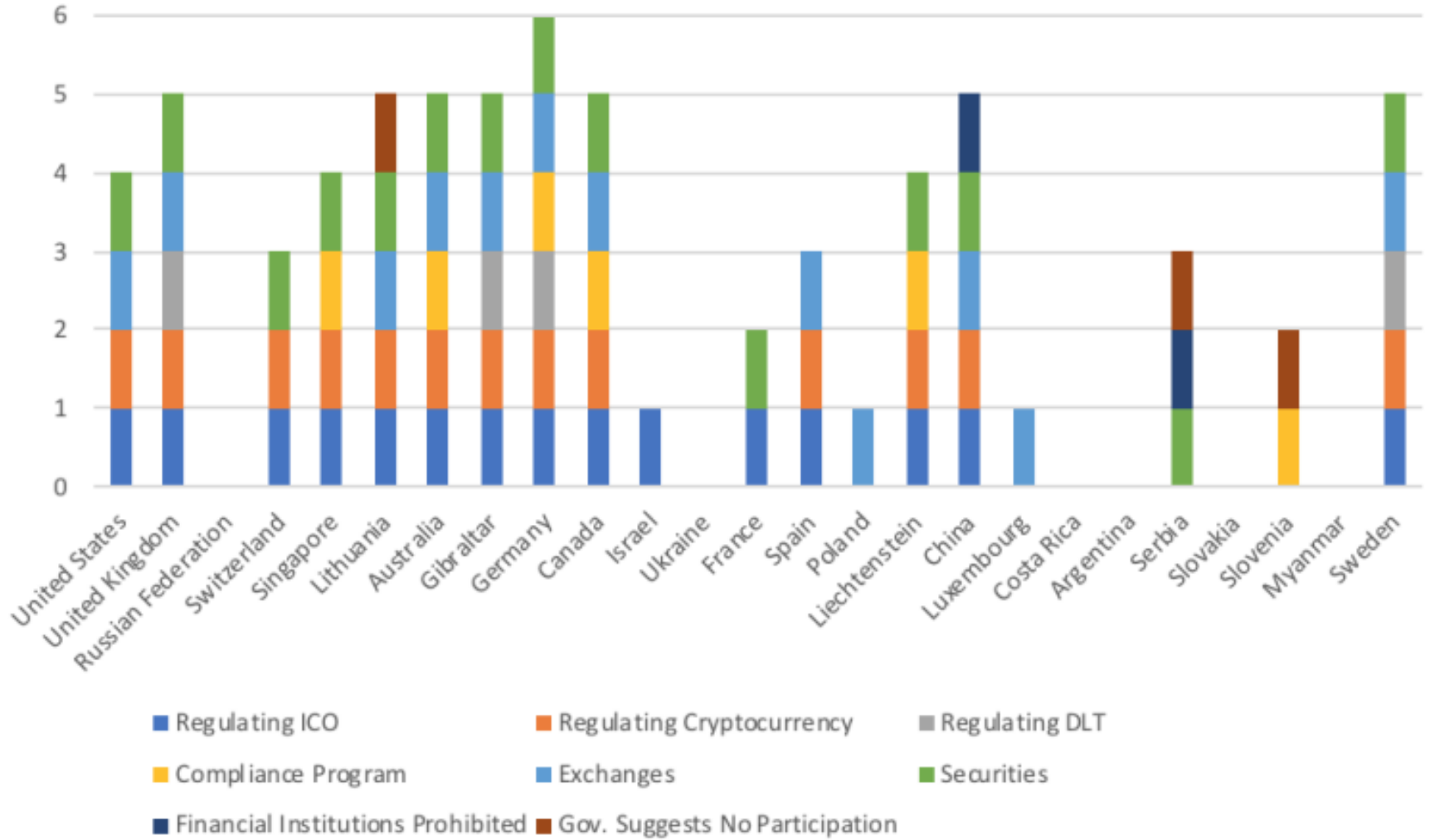
Regulations

Most governments use existing laws to regulate crypto



Source: Wulf A. Kaal in https://ssrn.com/abstract=3117224

What regulations address



Source: Wulf A. Kaal in https://ssrn.com/abstract=3117224

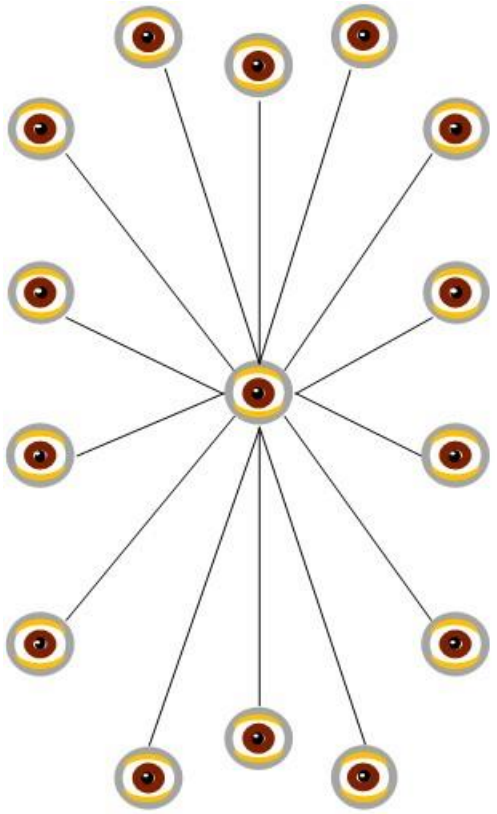
Outlook

- More traditional VC, family offices and other investors purchasing tokens
- Crypto as potential new asset class (CFD/Futures/ETF)
- ICO as project finance for established businesses (Kodak)
- Standardisation on regulation and requirements
  - KYC, AML, Data Protection, security vs. utility token, etc.
- Participation of more mature businesses
  - Minimum Viable Product (MVP) as standard
  - Proven track record of business and team
  - ICO services are too expensive for non-serious businesses
  - Risks to high for non-sustainable businesses
- Prices of tokens will become more stable (based on economic factors not hype)
- Government could take over (“Fedcoin”)
- Social networks to issue tokens (Telegram “Grams”)
- Unlimited options to pay and collaterize; buying crypto becomes more mainstream

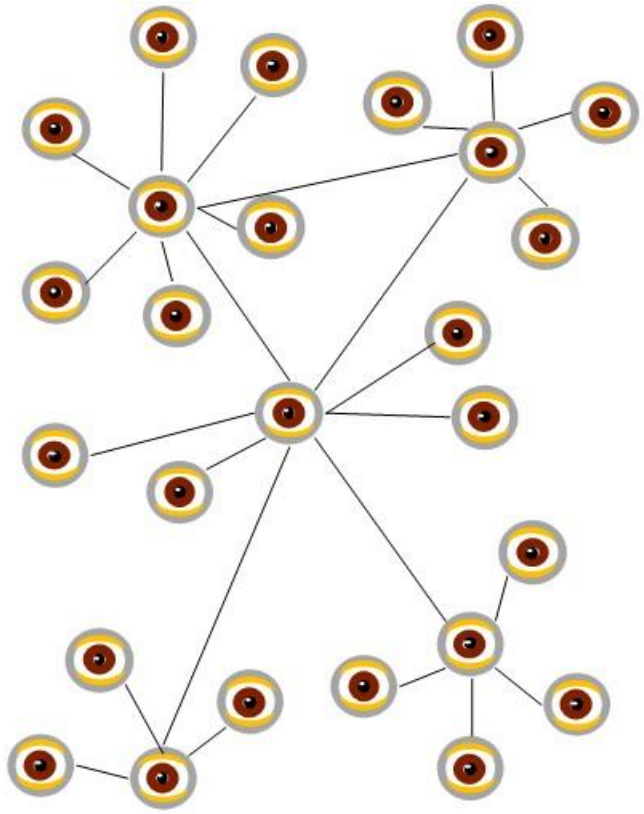
Thank You
Contact Details:
info@stradegi.com
claudia.marcusson@stradegi.com

Follow us on:

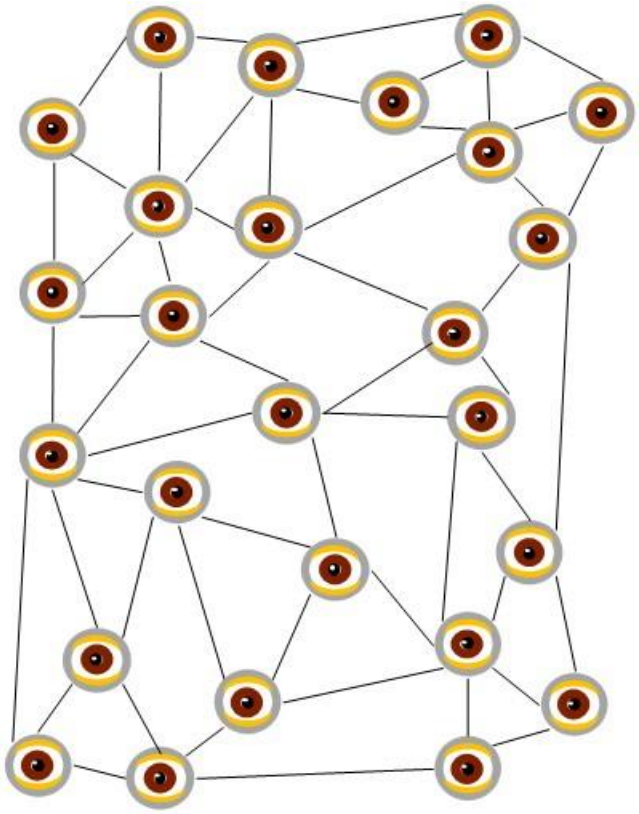
Appendix: Illustration of Different Network Models



Centralised Network



Decentralised Network



Distributed Network