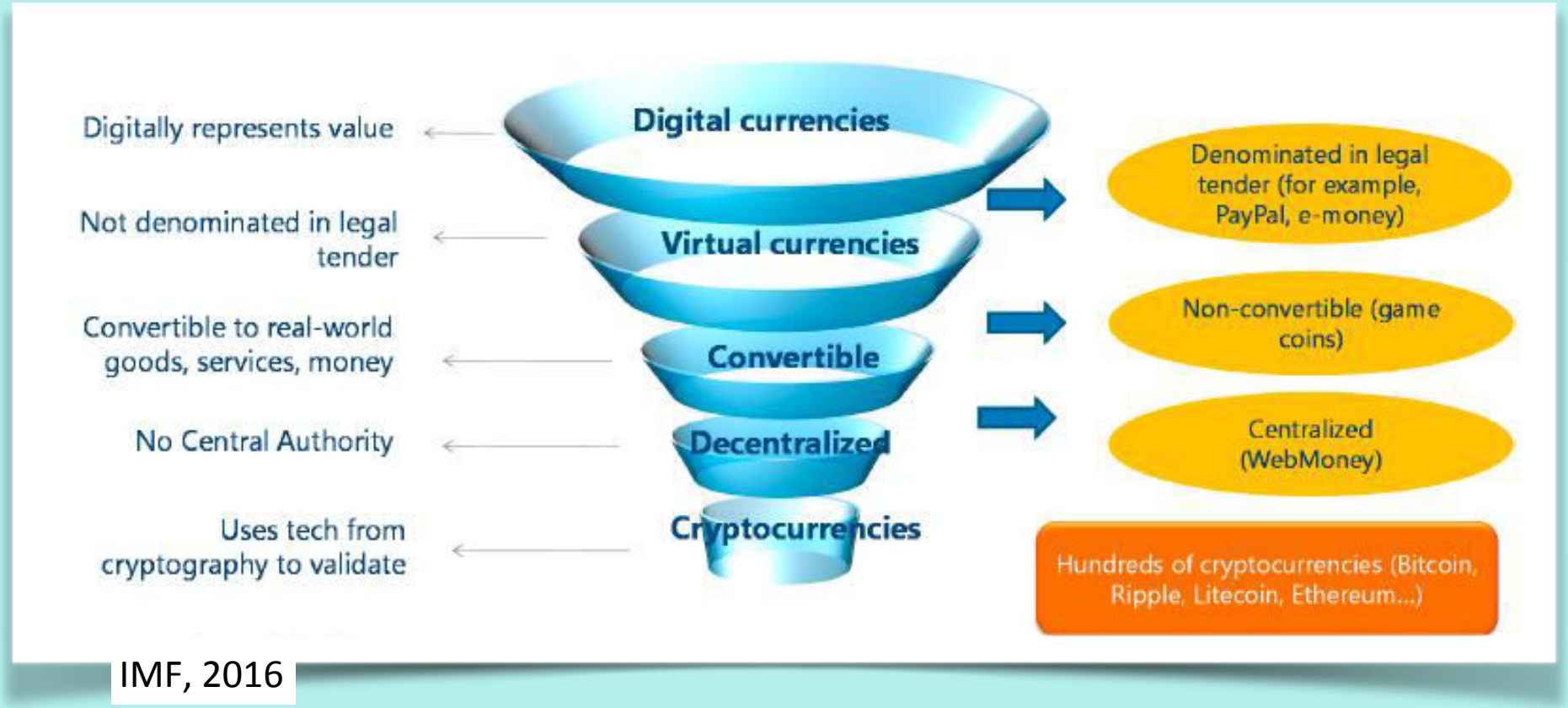
Bitcoins & the Regulatory Landscape

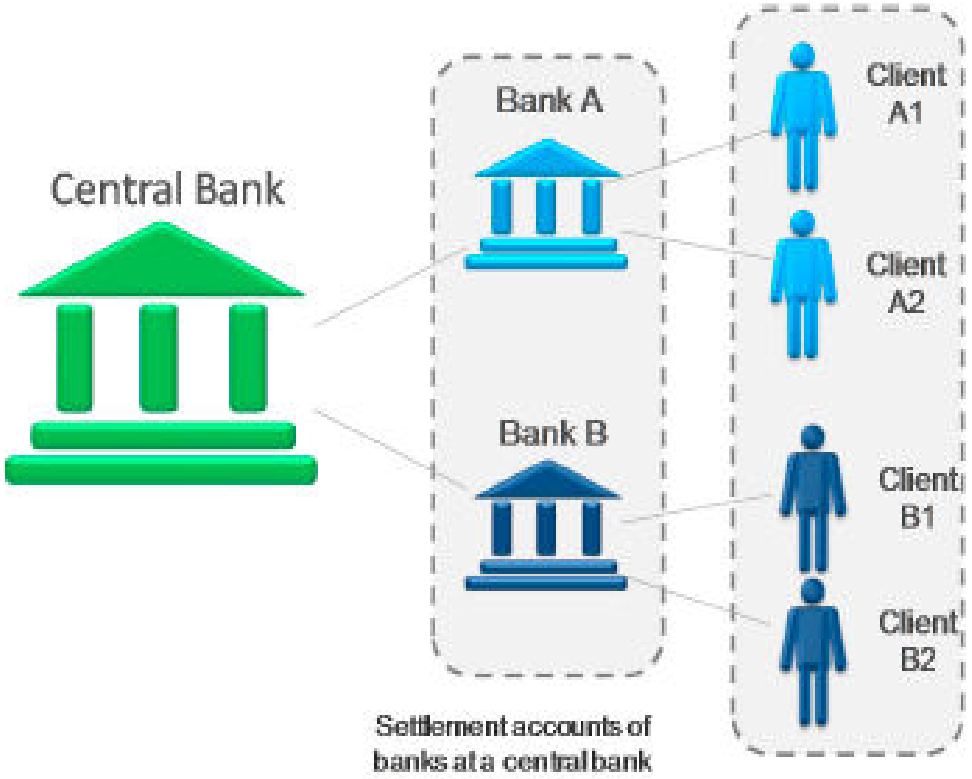
Shikha Mehra

Taxonomy



IMF, 2016

Centralized Payment System

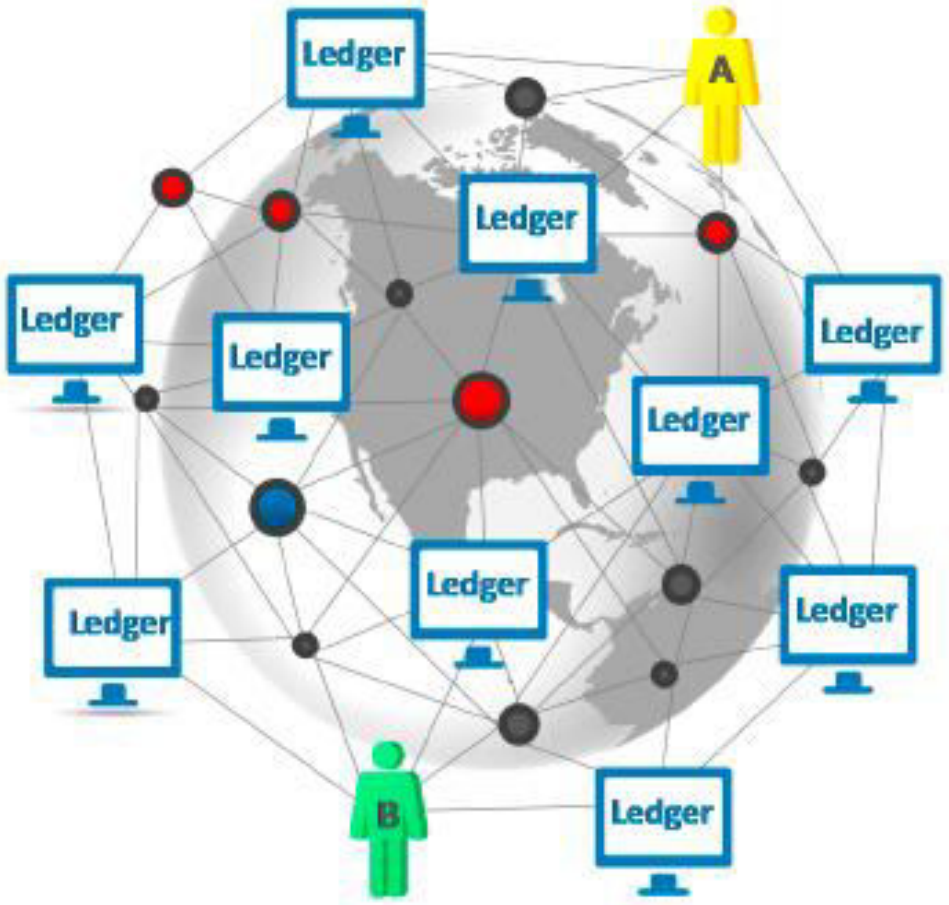


Payment from A1 to B1:

- Money is deducted from A1's account in bank A.
- The central bank moves money from bank A's settlement account to B's.
- The central bank maintains central record (ledger) of interbank transactions, by validating transactions and safeguarding against double-spending and counterfeit.
- Bank B adds money to B1's account.
- Banks A and B maintain the ledger of transactions for their clients A1 and B1 respectively.

IMF, 2016

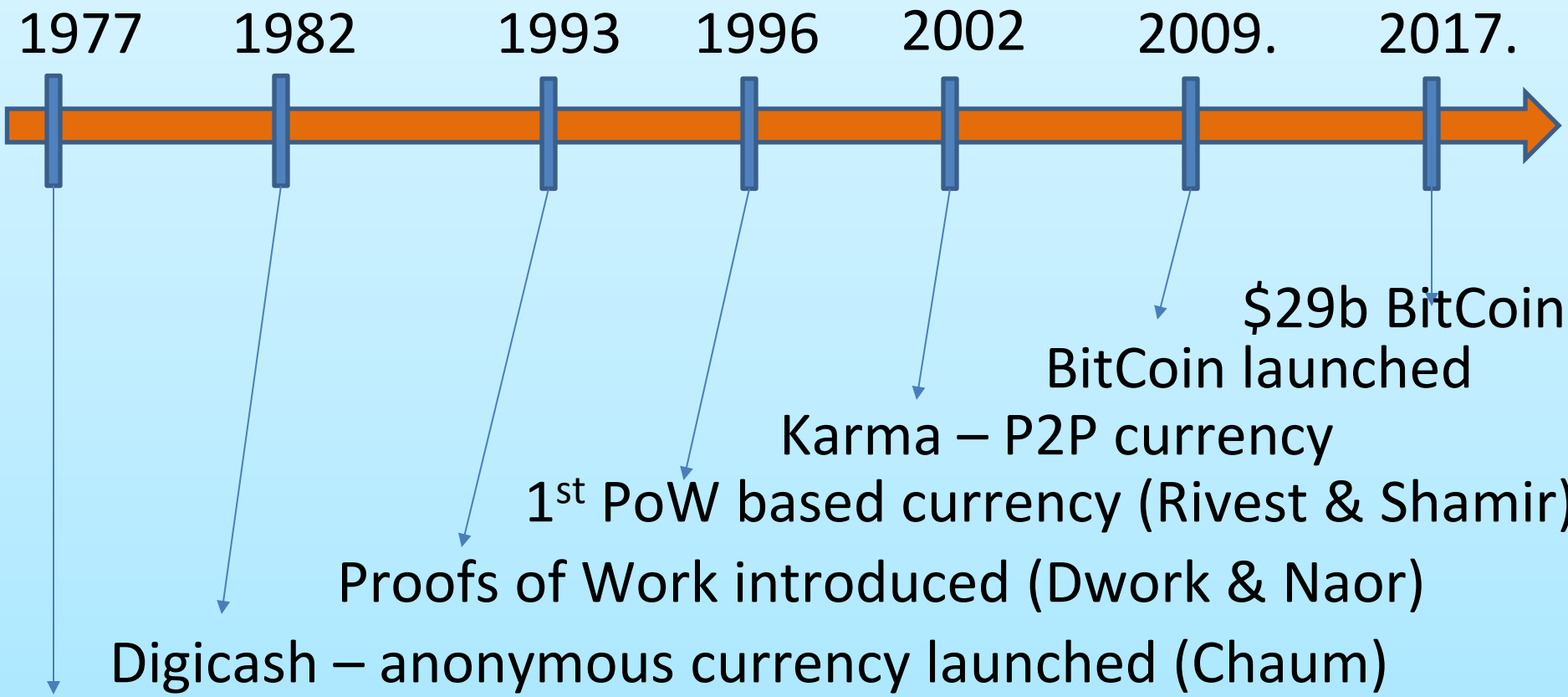
DLT
Technology behind Bitcoin Blockchain;



Payment from A to B:

- Copies of transaction records (ledgers) are kept in multiple computers in the network and visible to anyone.
- The transaction is settled by a multitude of individual nodes (miners), providing computing resources to the network.
- Miners solve a cryptographic puzzle as part of validation process. Miners need to show proof of doing this work to the network (called a "proof-of-work" system), which is costly (computing and energy resources).
- Only the miner who finds the solution faster than any others receives newly minted Bitcoins as reward for their service.
- "Trust" is created by making tampering attempts prohibitively expensive. If a miner wants to record a false transaction, she needs to compete against other miners who are acting honestly (or trying to fake a different transaction).[1]

Technology Time Line

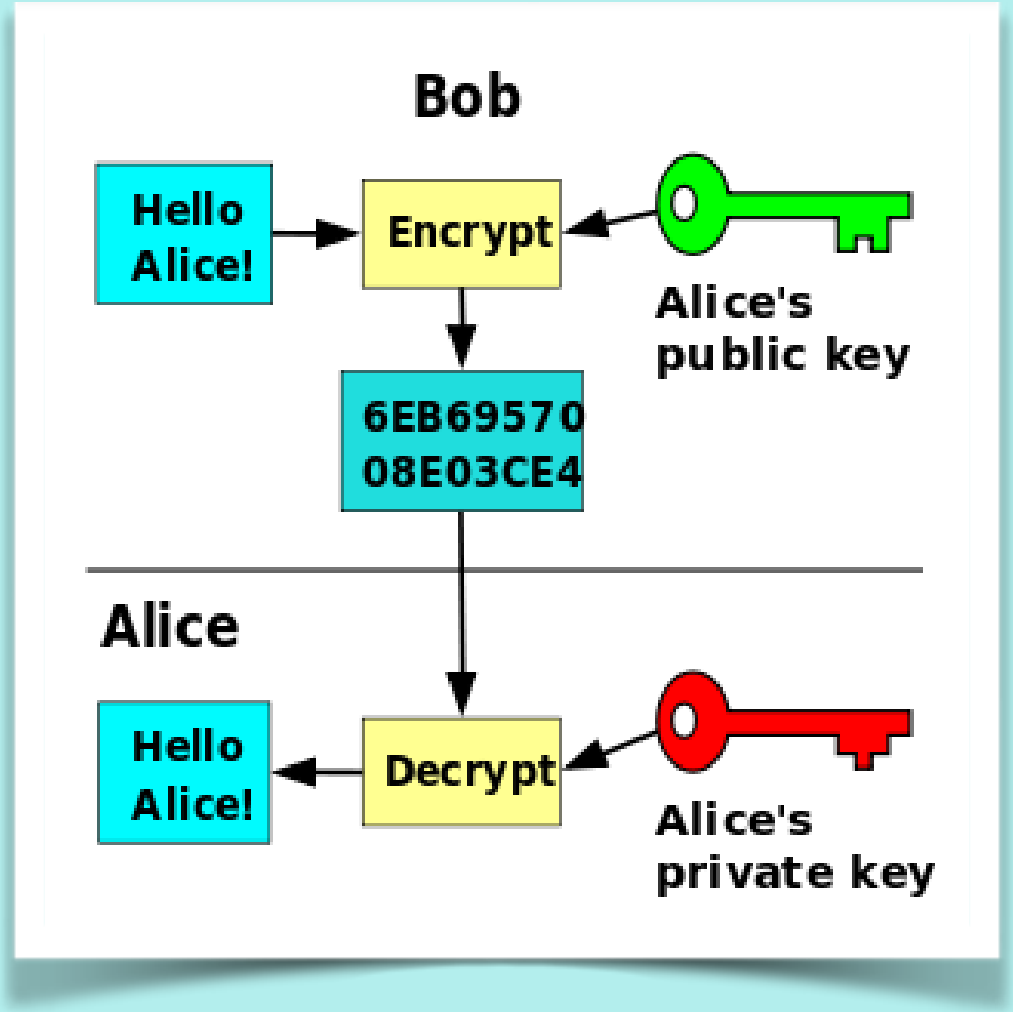


Current mkt. cap of BTC

Increasing DISINTERMEDIATION in the market for goods and services as witnessed in the ever growing peer to peer sharing economy (AirBnB, Uber) has unleashed the demand for disintermediation in the payments system and money transfer markets.

Enabling Technology - RSA

Key generation
Key distribution
Encryption
Decryption



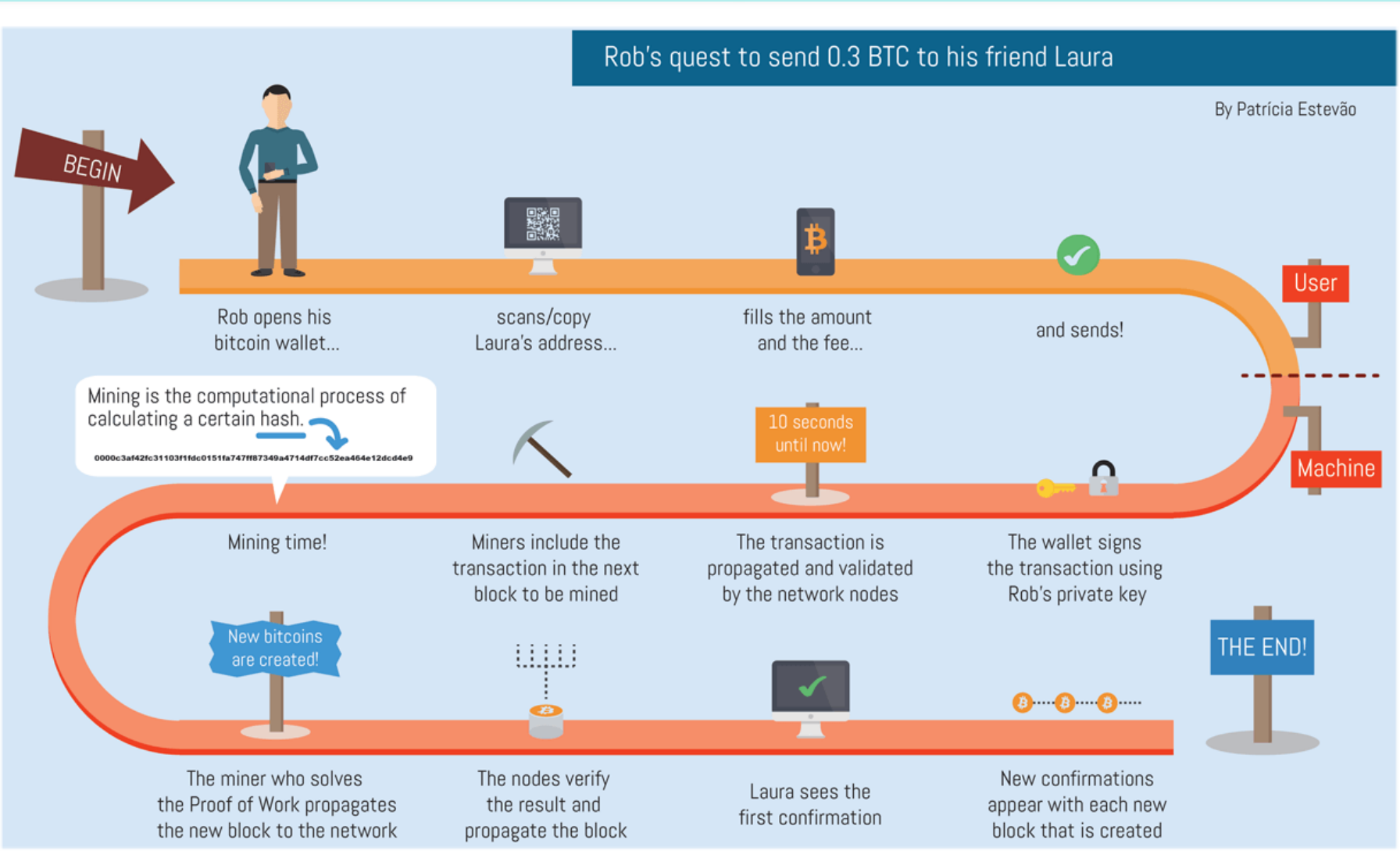
Enabling Technology - Proof of Work

- POW entails huge effort (e.g. for a high end computer it would take 435 years) to find a solution to the puzzle.
  - Nodes/Miners incur Capital costs, electricity costs, cooling costs, space and human resources for purchase and maintenance of computers with immense computational power
- 25 bitcoins per hash/solution generation for POW
- Little effort to verify the solution

Enabling Technology - Proof of Work

- Key problem: how to avoid the risk of collusion between parties to approve a dishonest transaction?
- Only one node should package up transactions for approval by all the others.
- The “Proof of Work” is a math problem that is difficult to execute but easy to verify as done correctly. (This is what’s called “Mining”)
- The first to solve this problem gets to send out the completed block of transactions for review and receives an award of BitCoins for their effort.
- Proof of Work means everyone must race to finish a random number problem. Because the problem is based on random numbers, the winner cannot be predicted so collusion is not possible.

How BitCoin transaction works?



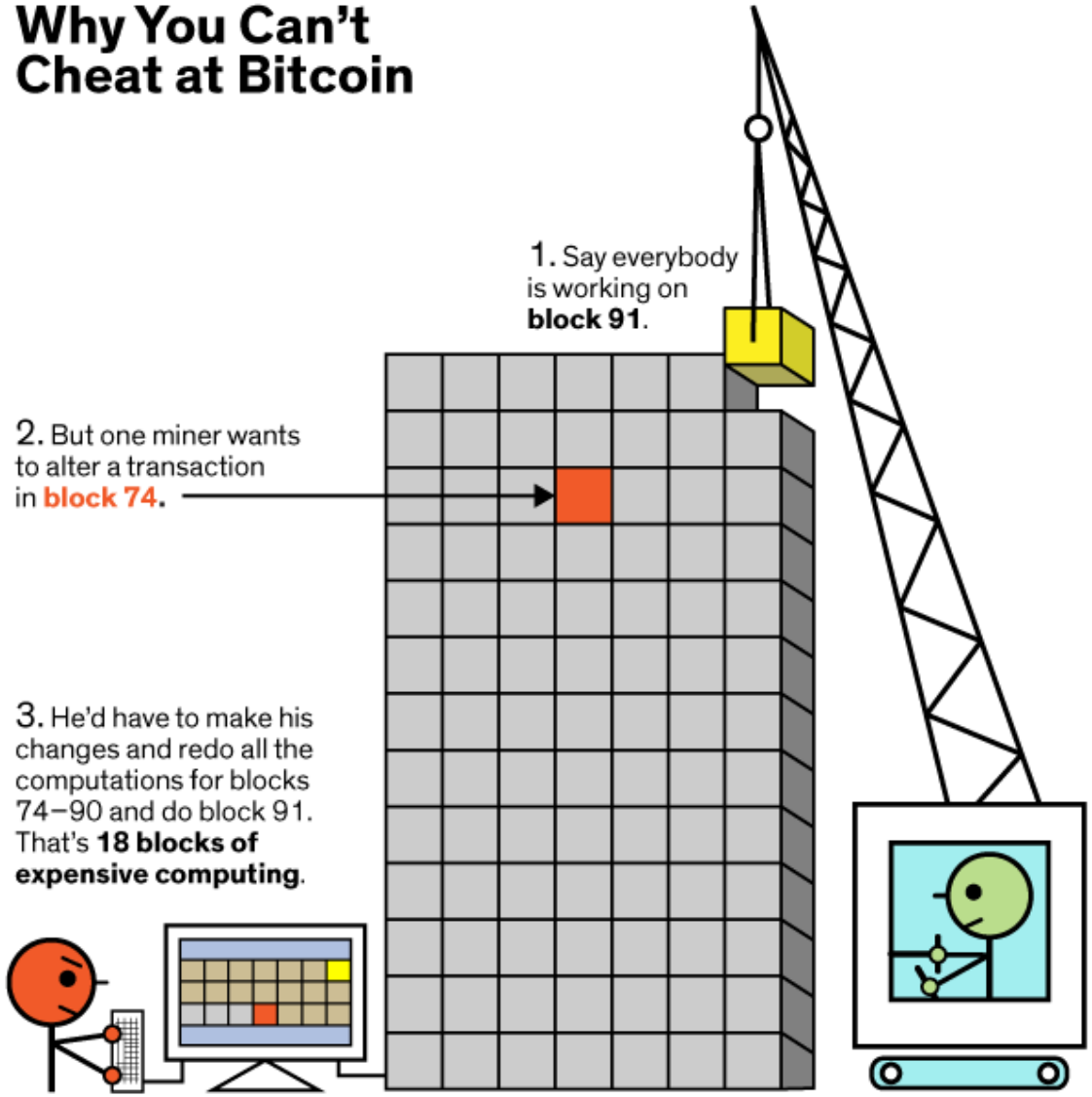
Features of Crypto Currency

- Distributed
- Trustless (requiring crypto proof)
- Consensus
- Security
- Anonymity – pseudo anonymity
- Volatility
- Risk & Vulnerabilities
- Regulatory compliance

Crypto Currency & Security

- Third of bitcoin trading platforms have been hacked (2009-March 2015)
- Bitcoin exchange services pose the weakest link in this Internet-based economy. Many of them are run by programmers rather than experts in the domain of finance and security.
- Bitcoin enthusiasts attribute thefts to ‘centrality’
- Double spending issue in Fiat currency-very rampant (400INR to create 1000INR fake note)

Why You Can't Cheat at Bitcoin

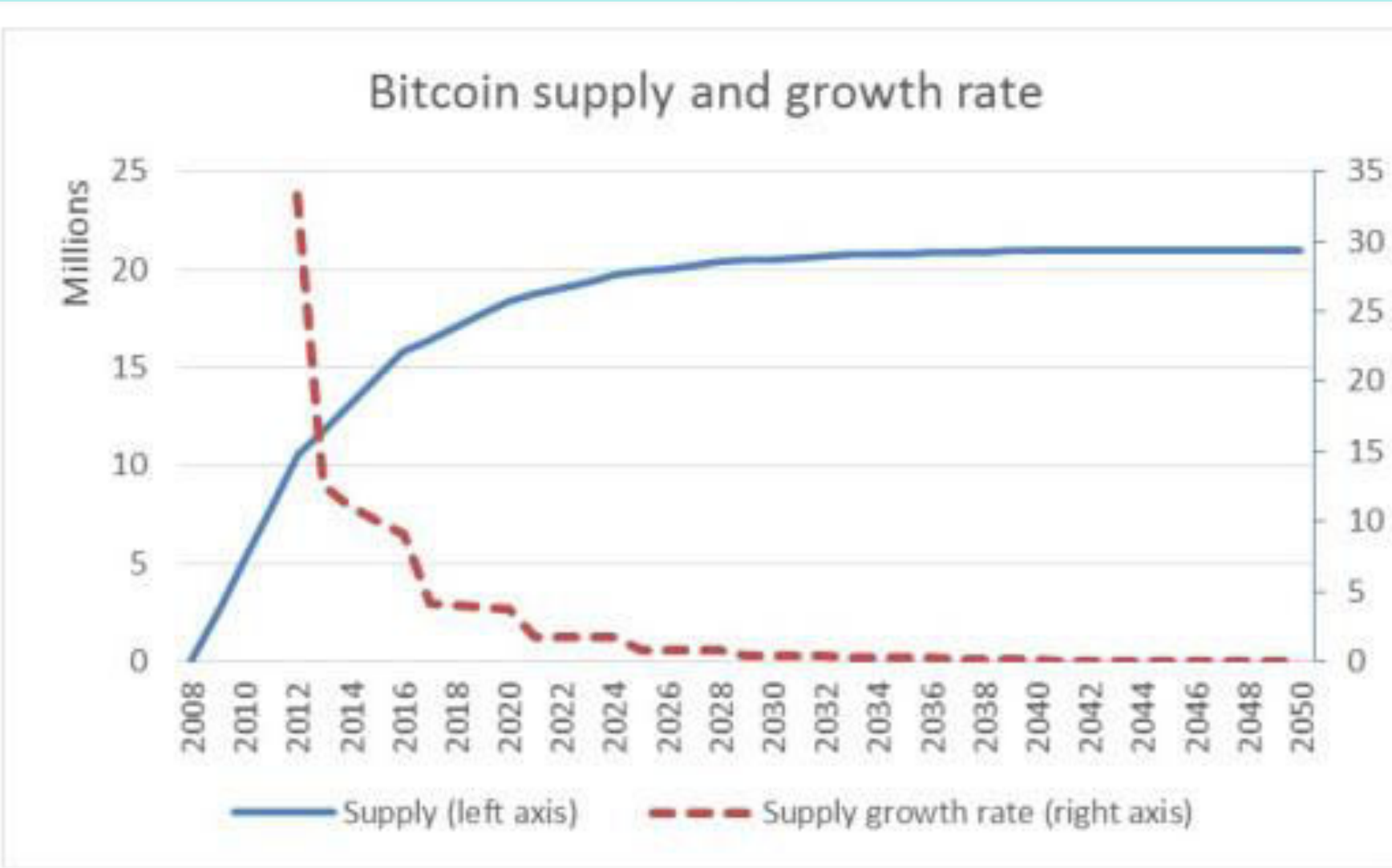


4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.

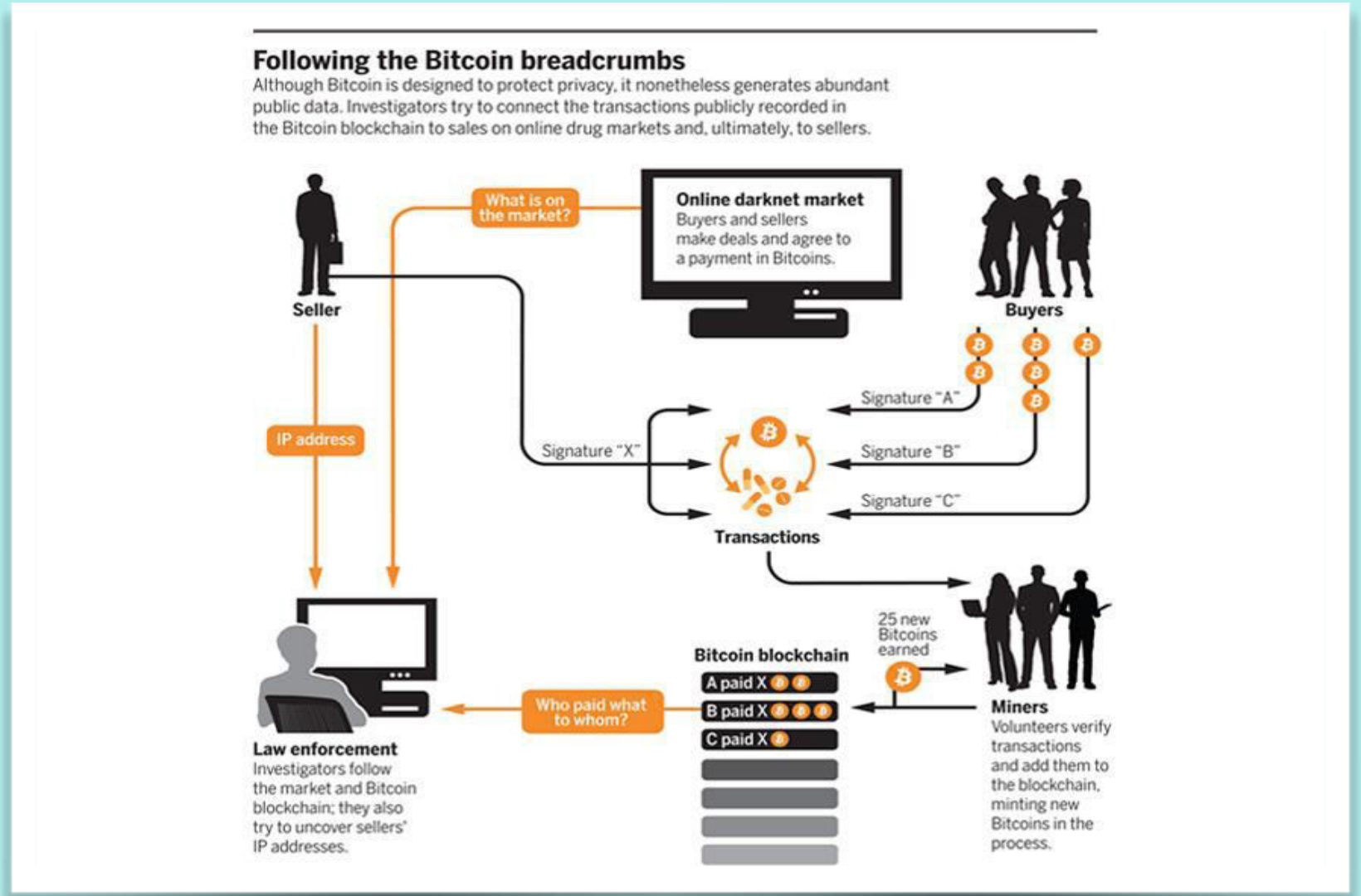
Crypto Currency & Volatility

- Value driven by– market sentiments, principles of demand and supply & network effects, no backing from any source, no intrinsic value, no regulation/no law
  - –Just under $2 billion crash in value over fight of the future of the technology (fork)
  - – CYBER GOLD—safe haven investment
  - –Bad news losing grip over price of Bitcoins
  - –Increasing acceptance all over the world-transactors
  - –Fixed supply and growth rate

Supply of bitcoins



Crypto Currency & Anonymity



Why BitCoin?

- Transactional convenience (demand for faster, cheaper, & irrevocable transaction bolstered by P2P economy)
- Increasing acceptance in commerce (off & online)
- Investment opportunity—outperforming all other indices
- Lack of trust in central banks and governments
- Provides a sense of anonymity

Risks & Vulnerabilities

- Terrorist Financing
- Tax evasion
- Money laundering
- Preventative measures
  - KYC
  - CDD
  - Obligation to report suspicious activity

Regulatory Landscape

- Definitional Challenge- currency, commodity or payment system
- No focal point of regulation because of lack of centrality
- Regulatory responses are being developed at an international level- FATF, UNODC, CPMI,OECD & EBA
- Focus on Interface between VCs & broader economy –the gatekeeper & related consumer protection issues

Varied Responses of Different Countries

- US – VC as ‘property’ for tax purposes and BTC exchanges classified as MSBs/FinCEN
  - IRS issued Subpoenas to CoinDesk
- UK, Canada & Germany – followed the US
- Italy & India – precautionary notes against the use of VC
- China – PBOC bans bitcoin trading and ICOs
- Japan –Legal tender classified as some type of prepaid money system, Japanese can pay power bills with BTCs through CoinCheck

Circumvention of Tax Laws & Capital Flight

- India, China, Greece, Venezuela & Cyprus—lack of trusts in govt.
- VC wallets-Super tax havens
- USA & Australia – BTC as capital asset or property for tax purposes.
- Possible solutions
  - –Taxing each transaction (exchange of value) like STT
  - –Third party information reporting – Form 1099-B revision to capture taxable transactions in Bitcoins

Going Forward

- Inherent strengths will drive mass adoption
- As Blockchain and Cryptocurrencies technology gains prominence, the financial sector can expect higher levels of attrition in its high-level ranks
- Andreesen Horowitz & Union Square Ventures invest $10m in Polychain Capital.
- Regulation needs to be balanced so that innovation is not killed
- compliance and hence legitimacy is key - Brian Armstrong