Integrity Perils of Blockchain and Cryptocurrencies

ADB Headquarters, kHub

28 May 2019 | 10:00-11:00am

John Versantvoort
Head, Office of Anticorruption and Integrity

ASIAN DEVELOPMENT BANK

Thomas Abell
Chief, SDCC Digital Technology for Development

What are Blockchains and Cryptocurrencies?

ASIAN DEVELOPMENT BANK

Cryptocurrency

Electronic money protected through cryptographic mechanisms instead of a central repository.

Blockchain

Immutable digital ledger systems implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority.

Example Blockchain/Cryptocurrency Ecosystem

ADB ASIAN DEVELOPMENT BANK

Satoshi Nakumoto
2008 - 2010

Bitcoin Whitepaper
31Oct2008

Hal Finney - PoW
Wei Dei - B Money
Nick Szabo - Bit Gold

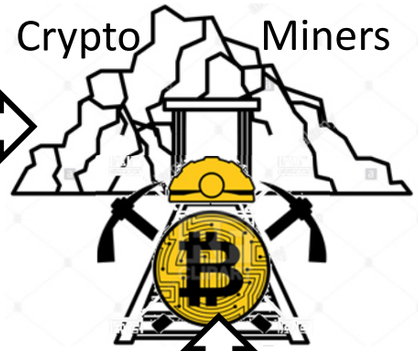
Bitcoin Core
Codebase
network/wallet
12Jan09

Bitcoin Core
Satoshi Nakumoto
Gavin Andresen
Wladimir van der Laan

Bitcoin Core

Open source codebase

Crypto Miners



Blockchain

Master list of all transactions

Private Key

Digital Wallet

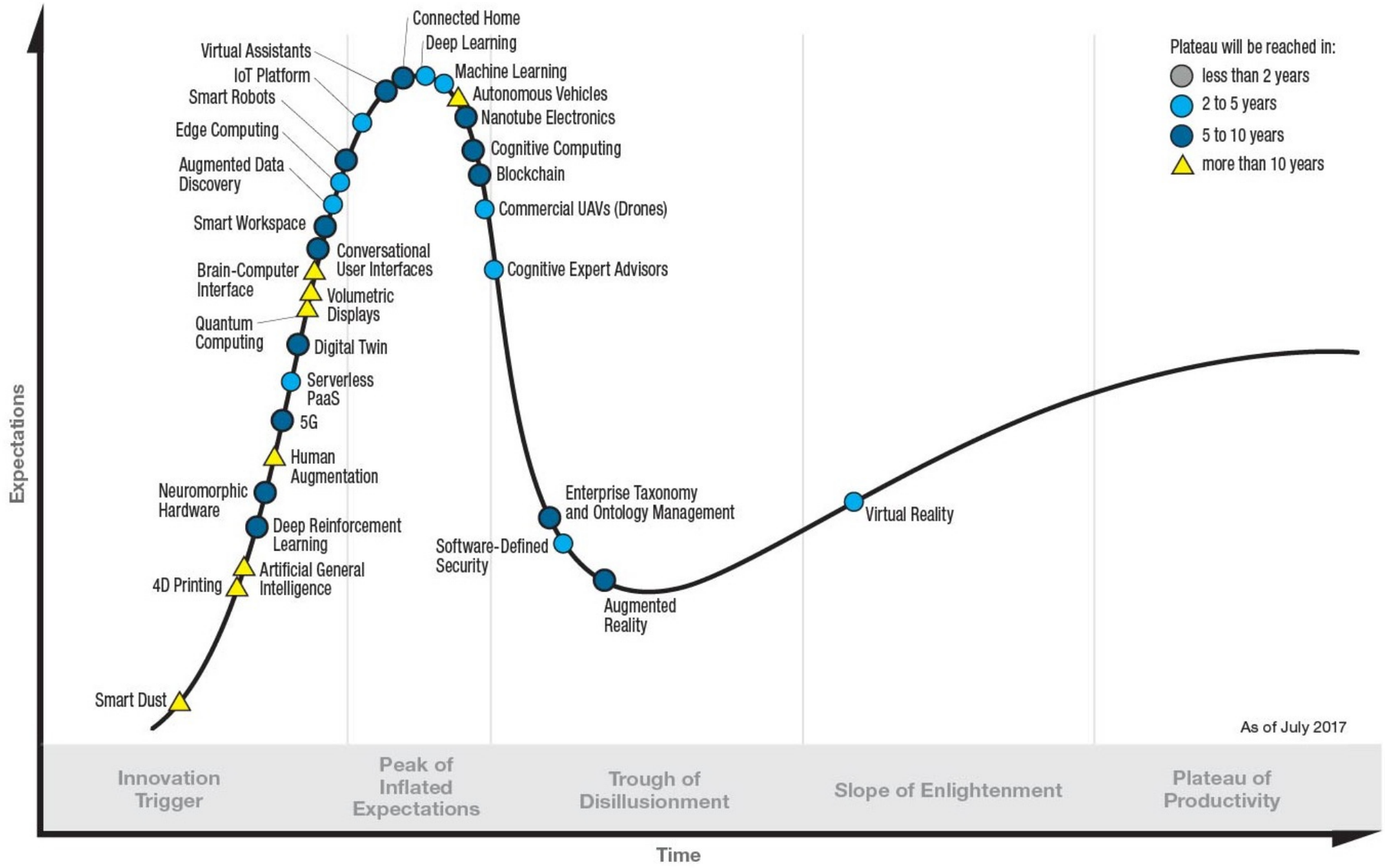
Cryptoexchange

Binance, BitMEX, Bitfinex, etc.

Crypto Capital (Panama)

Hype Cycles: Standard Gartner Hype Cycle

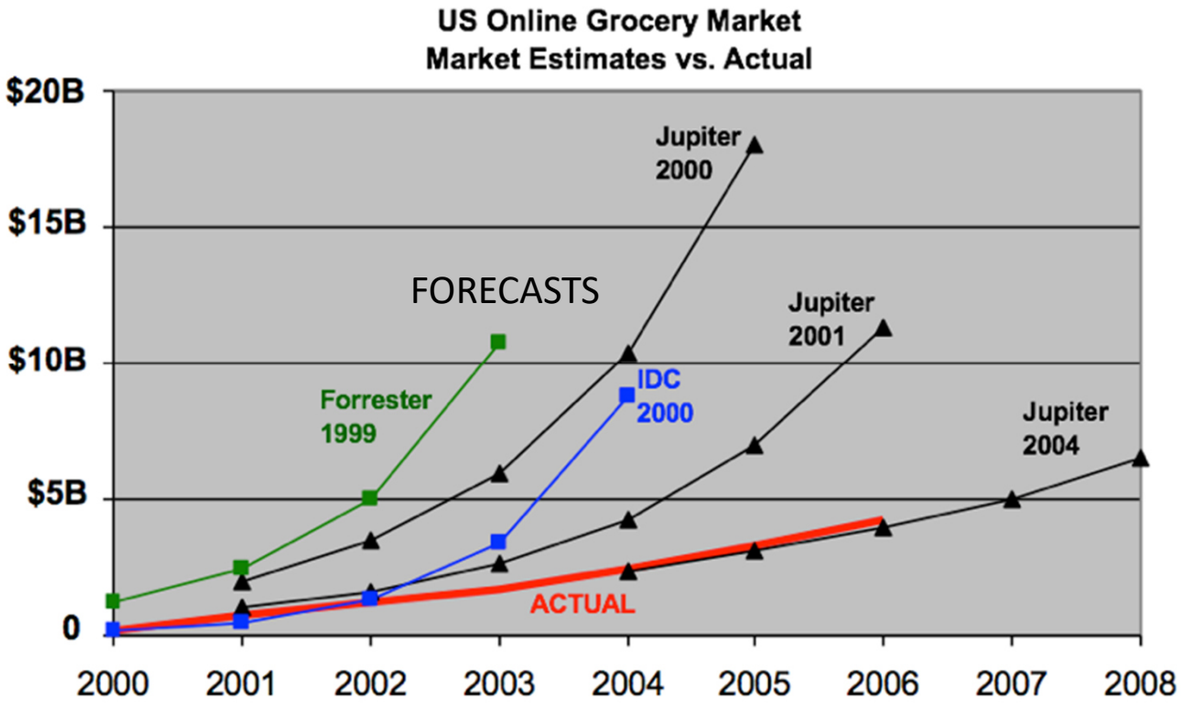
ASIAN DEVELOPMENT BANK



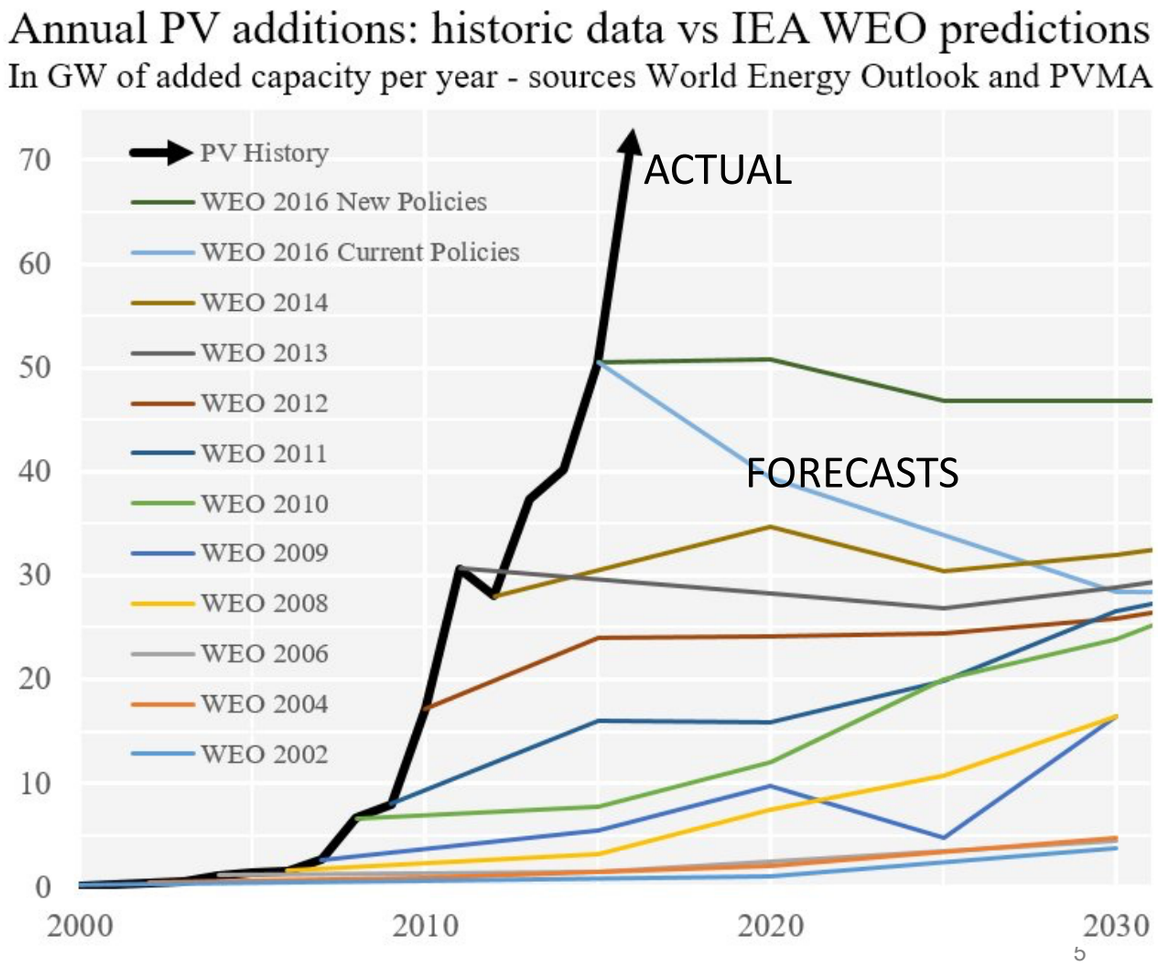
Hype Cycles: Hype and Anti-Hype

ADB ASIAN DEVELOPMENT BANK

Typical Hype: US Online Grocery Market



Anti-Hype: Global Solar Power Market



What's really behind the hype?

ADB ASIAN DEVELOPMENT BANK

- Anonymous Digital Currency
  - Enables anonymous digital transactions globally outside of government regulations
- Avoiding Regulatory Limitations
  - Cryptocurrencies have enabled many different opportunities to avoid government regulations (cross-border money transfers, unregulated exchanges, "darkweb" market places, etc.)
- Digital Wealth Creation
  - Following Bitcoin, hundreds of new digital currencies have launched Initial Coin Offerings (ICO's), creating $200B+ in wealth globally

Anonymous digital payments represent the main value of cryptocurrencies

- Digital payments are currently a core foundation of the global economy
- All governments manage and regulate digital payments, but none of them have created an anonymous digital payment option, due to the obvious need to limit corruption
- One of the main reasons for the continued popularity of cash as a payment mechanism is anonymity
- Cash is highly regulated and is difficult to use for large or cross-border transactions
- There is a tremendous demand for anonymous digital payments, and cryptocurrencies are the only major solution available

ADB ASIAN DEVELOPMENT BANK

Avoiding regulation is a fundamental driver of the use of cryptocurrencies

- Buying/selling illegal goods
  - Silk Road
  - Silk Road 2.0
  - Agora
  - Evolution
  - Black Bank
  - OpenBazaar
  - Alphabay
  - Nucleus
  - Outlaw
  - Hansa
  - Dream Market
- International money transfer
- No process/rules for seizing crypto-assets in legal cases
- Unregulated and anonymous trading on cryptoexchanges
- Money laundering

ADB ASIAN DEVELOPMENT BANK

Critiques of Cryptocurrencies

- Nov, 2017, Joe Stiglitz, Nobel Economist: “One of the main functions of government is to create currency, and Bitcoin is successful only because of its potential for circumvention and lack of oversight, so it seems to me it aught to be outlawed.
  It doesn’t serve any useful social function.”

- May, 2018, CGAP (World Bank) CEO: ”Blockchain is a solution looking for a problem.”

- April, 2019, China National Development Reform Commission, the country’s powerful economic planner, listed crypto-mining among a plethora of industries it intends to eliminate because they “seriously wasted resources” or polluted the environment.

https://www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd
https://dailyfintech.com/2019/04/29/will-bitcoin-go-from-crypto-winter-to-china-crisis/

Cryptocurrency “aught to be outlawed. It doesn’t serve any useful social function.”

https://www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd

Additional Problems with Cryptocurrencies

- Mining consumes 54TWh of power annually, 3x the level of Ireland, producing 30-50M tons of CO2 annually
- Cryptocurrencies are not secure and are open to fraud:
  - Cryptocurrency Thefts, Scams, and Fraud Could Tally More Than $1.2 Billion in First Quarter 2019
  - Cross Border Payments represent 66% of US Cryptocurrency Exchanges as of Jan 2019
- Exchange Thefts since Jan 2018
  - Cryptopia, CoinBene, DragonEx, Bithumb, Coinbin
- Exit Scams since Jan 2018
  - Coinbin, QuadrigaCX ($120M, largest exchange in Canada)
- Dependency on unrecoverable key (~20% of bitcoins are lost)
- Eventually vulnerable to quantum computing (Shur's algorithm 1994)

https://cncf.com.au/carbon-calculator/
https://dailyfintech.com/2019/04/29/will-bitcoin-go-from-crypto-winter-to-china-crisis/
CipherTrace Cryptocurrency Intelligence April 2019

ADB ASIAN DEVELOPMENT BANK

But isn’t Blockchain different from Cryptocurrency?

- Blockchains and public Distributed Public Ledger Systems (DLT) are supported by cryptocurrencies
- Private Ledger Systems are basically open source databases with restricted access
  - Completely dependent on a host organization for operating the system, and can be shut down at any time.
  - Open source code for these ledger systems have limited advantages over other encrypted database technologies
- Public Blockchain/DLT solutions are not more secure than other systems
- Blockchain solutions for consumer applications like ID and supply chain are fundamentally limited in that there is no backup option if the end user loses their key
- Not GDPR Compliant: no ability to remove data

ADB ASIAN DEVELOPMENT BANK

What about Smart Contracts on the Blockchain?

- This is the key innovation of Etherium, enabling the running of code via their blockchain system
- Etherium retains the issues of other blockchain technologies
  - Excessive use of electricity and carbon emissions for mining
  - Anonymity and regulatory avoidance
  - Relying on a single crypto key as only method of identity with no backup
  - GDPR non-compliance due to inability to delete records
  - Unproven opensource code with poor record of security
  - DAO example
- Ultimately, any contracting system should be built upon a legal framework
  - Smart contracts based on private ledger systems may prove valuable, but should have legal and regulatory support
  - When smart contracts are separated from public blockchains and cryptocurrencies, many of the attractive features are lost

ADB ASIAN DEVELOPMENT BANK

Who Benefits from Blockchain/Cryptocurrencies?

- Tech startups
  - Can download open source Bitcoin code and create a new cryptosolution for free
- Miners
  - Cryptomining operations generate ~$10B/year in revenue due to cheap electricity, plus mining has created Bitmain, leading manufacturer of cryptomining rigs
  - PRC has outlawed cryptoexchanges and looks poised to outlaw mining
- Social network
  - Concept of social network-based ”stable coin” will enable building a global payment platform largely outside of current financial system and government regulations, but it will have few attributes of current cryptocurrencies.
- IT Industry
  - Selling cloud platforms, development resources, consulting
- Corruption:
  - Offshoring wealth, buying/selling illegal goods, bribery, …

ADB ASIAN DEVELOPMENT BANK

Central Bank Digital Currency vs. Cryptocurrency

- Role of Central Banks
  - Responsible for issuing currency and managing liquidity
  - Most money issued by central banks is already digital
    - Banks can borrow short-term funds from central banks for liquidity needs
  - Central banks operate some of the most efficient payment networks (ACH) globally
- Central Bank Cryptocurrency
  - There is very little incentive for central banks to issue true cryptocurrency due to the corruption risks
  - Central banks would be unlikely to facilitate unlimited use of anonymous digital currency
- Potential Innovation in Central Bank Digital Currency
  - Stiglitz, "The Theory of Credit and Macro-economic Stability", Nov 2016
  - Transformative approach, recommending central banks more directly controlling the credit cycle via digital currency rather than relying on short term borrowing rates.

https://www.nber.org/papers/w22837

Where are the potential benefits from a development perspective?

- Open Source Software
  - Bitcoin is a great experiment in the widespread use of open source software
- Regulatory Pressure
  - Crypto solutions can put pressure on regulators and banking sector to innovate
- Distributed Networks
  - There is long-term potential for truly distributed networks

ADB ASIAN DEVELOPMENT BANK

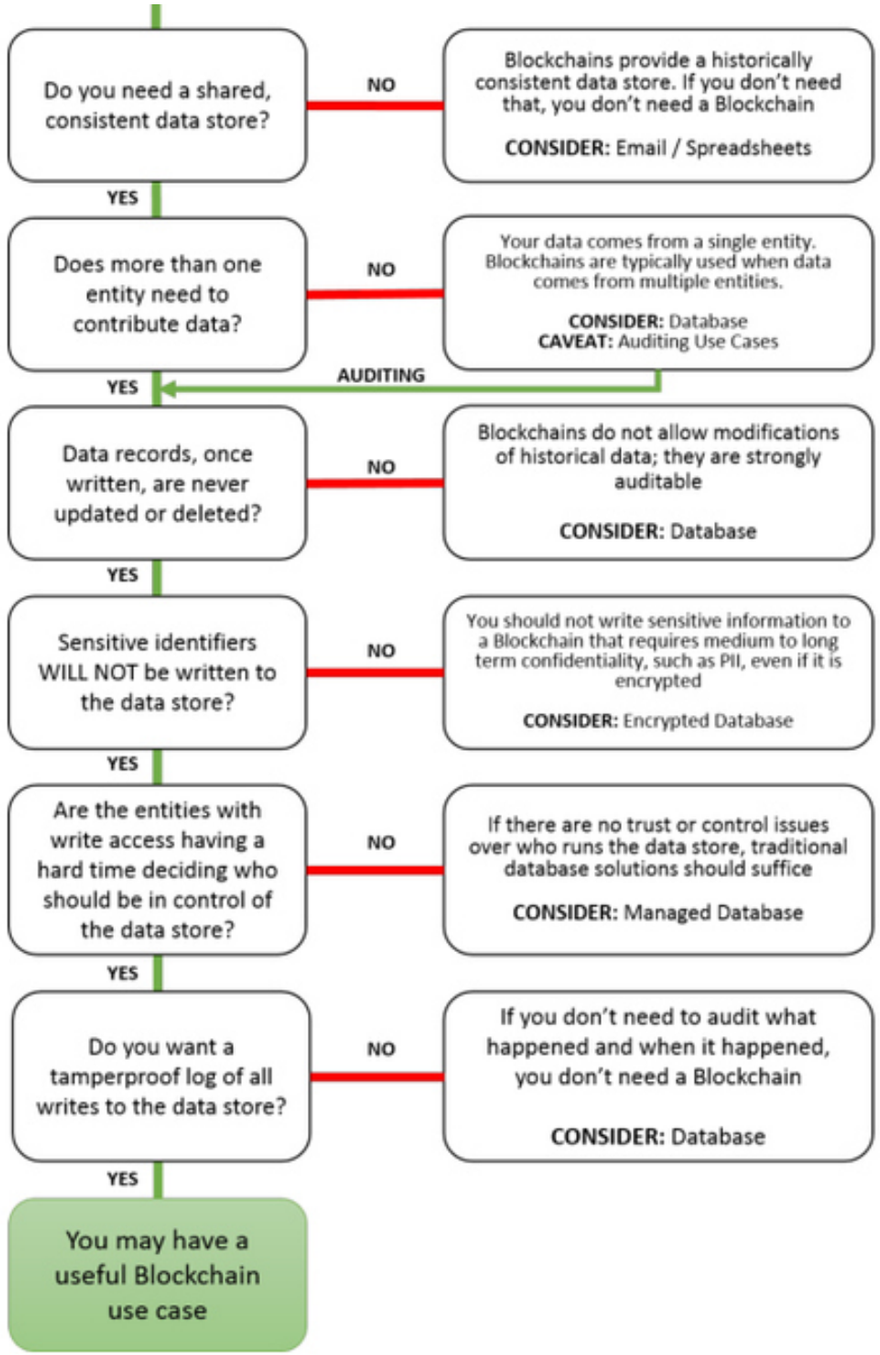
Considerations for ADB Programs

- Consider opportunities relative to the hype cycles in technology
  - Who is really benefiting, and how does it align with ADB's mission
- Be careful to balance the optimism against the corruption and integrity risks
- Consider avoiding solutions on public networks (Bitcoin, Etherium, Monero, etc.)
  - Power consumption alone makes these unsustainable
- If someone recommends a Blockchain/DLT technology, check to see if it can be accomplished with a distributed database

Do you need a Blockchain?

USA National Institutes of Science and Technology (NIST)

Convenient flowchart on logic around using a blockchain versus other IT solutions (Jan 2018).



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Draft NIST Interagency Report (NISTIR) 8202: Blockchain Technology Overview

ADB ASIAN DEVELOPMENT BANK

Thank You

Q&A

Two additional perspectives on blockchain by Nicholas Weaver of US Berkeley
https://www.vox.com/conversations/2018/4/11/17206018/bitcoin-blockchain-cryptocurrency-weaver

https://www.youtube.com/watch?v=xCHab0dNnj4