BLOCKCHAIN AND ITS IMPLICATIONS

NEIL KANE

MEMBER, BURGESS INSTITUTE FOR ENTREPRENEURSHIP & INNOVATION AT MICHIGAN STATE UNIVERSITY

STATE ASSOCIATION OF ACCOUNTANTS, AUDITORS, AND BUSINESS ADMINISTRATORS (SAAABA) MEETING

JUNE 17, 2020

SPEAKER

- Mechanical engineer, MBA
- Sales at IBM
- Business development at Microsoft
- EIR many times. Founder many times.
- Advisor to several tech transfer offices
- Co-director of “Illinois Technology Enterprise Center” at Argonne National Lab
- Member of Illinois Governor’s Innovation Council
- Named a Technology Pioneer by the World Economic Forum
- Twice testified in Congress on technology commercialization
- Director of Undergraduate Entrepreneurship at Michigan State University
  - Top 25 program in 2 ½ years.
  - Top 20 program in 3 ½ years.
- Co-author of *The Innovator’s Secret Formula*
- Mentor in The Mentor Project

OBJECTIVES

Give you a basic understanding of blockchain…

And its implications

WHAT IS BLOCKCHAIN?

Blockchain is a technology that enables value to be transferred using only software. (BDO)

It's a protocol that allows entities to store and share transactional information in a controlled and systematic way. (Deloitte)

It's a distributed, immutable ledger

Immutable: Information cannot be altered—only appended

Distributed: No central authority is in "control". Everyone has a copy of the ledger.

It ensures trust, but not accuracy (NDK)

MY WORDS

Blockchain allows two anonymous parties to participate in commerce without any counterparty risk.

In other words, it removes trust from being a risk.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

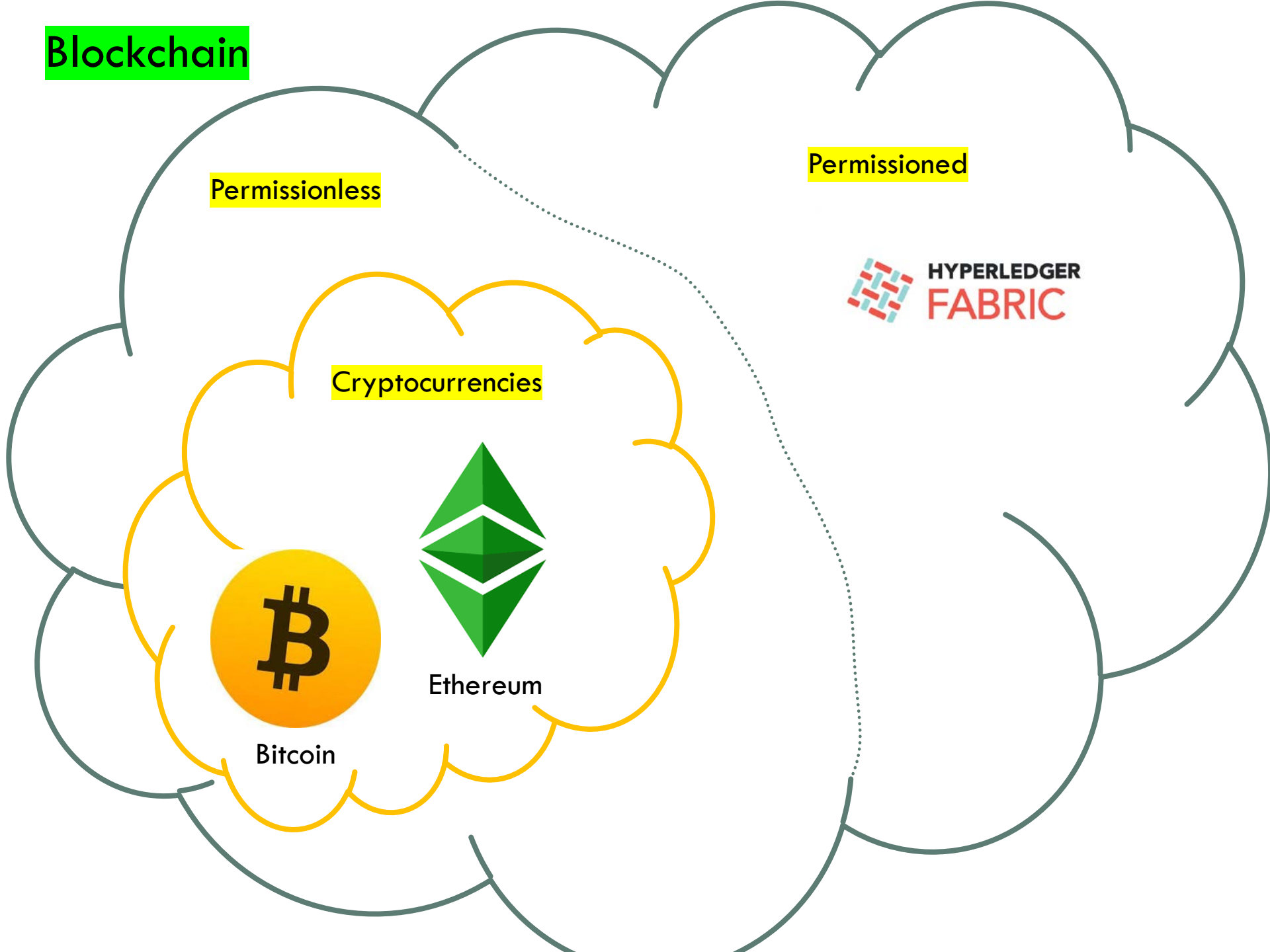
October 31, 2008

Grounding

Bitcoin is a specific version of blockchain

Blockchain and cryptocurrencies are two different things

Digital currencies and crypto-currencies are not the same


Blockchain
Permissionless
Permissioned
HYPERLEDGER
FABRIC
Cryptocurrencies
Ethereum
Bitcoin

GOLDMAN SACHS ON BITCOIN

- Cryptocurrencies are not an asset class
  - Do Not Generate Cash Flow Like Bonds
  - Do Not Generate any Earnings Through Exposure to Global Economic Growth
  - Do Not Provide Consistent Diversification Benefits Given Their Unstable Correlations
  - Do Not Dampen Volatility Given Historical Volatility of 76%
  - On March 12, 2020, the price of Bitcoin fell 37% in one day
  - Do Not Show Evidence of Hedging Inflation

- We believe that a security whose appreciation is primarily dependent on whether someone else is willing to pay a higher price for it is not a suitable investment for our clients.
- We also believe that while hedge funds may find trading cryptocurrencies appealing because of their high volatility, that allure does not constitute a viable investment rationale.

https://resources.goldman.com/content/dam/pwm/direct-links/isg-calls/client_call_materials_27May20.pdf?sa=n&rd=n

WHAT IS A BLOCKCHAIN

{ Shared, peer-to-peer, disintermediation }

No single ownership, Multiple contributors, No third party

A distributed ledger that allows digital assets to be transacted in a real time, immutable manner

something represented in a digital form that has an intrinsic or acquired value (e.g., land, house, currency, vote, goods, certificates, identity, rewards etc.)

Transparent, Secure, Irreversible

Low Friction
Near real time settlement of recorded transactions

Cryptography (Public & Private Keys)

Verifiable record of every transaction

Types of use cases

Record Keeping
- Automated, high fidelity, and low-cost mechanisms for record keeping

Smart Contracts
- Protocol is programmable to trigger transfer of value and information under certain conditions

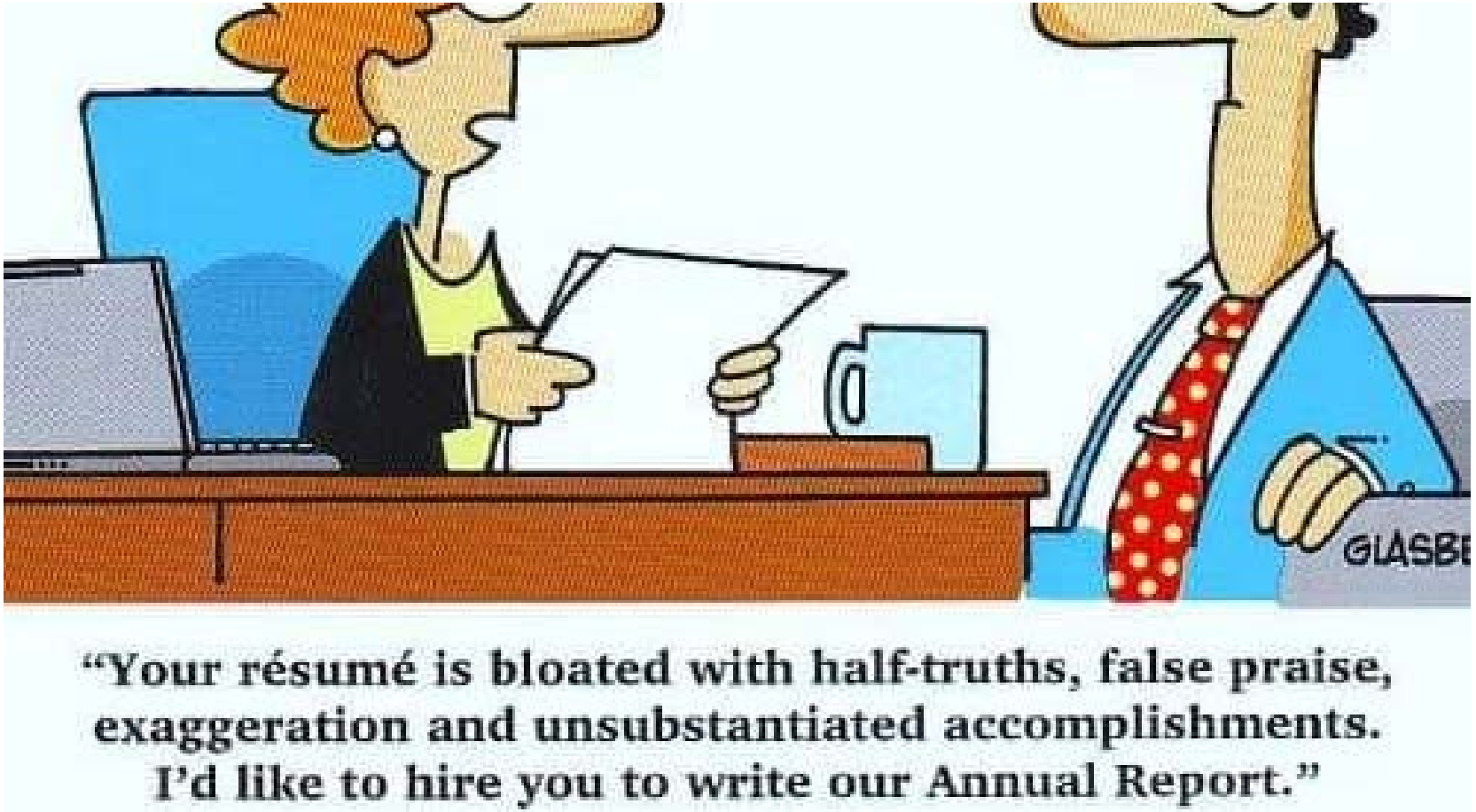
Transfer of Value
- Secure, near-real time, low cost transfer of value without intermediary

Types of blockchains

Enterprise Friendliness →

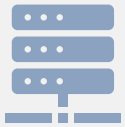
	"Open"	*"Federated"*	*"Closed"*
	Public Blockchain	***Permissioned Blockchain***	**Private Blockchain**
Access	Open read and write	Permissioned write and/or read	Centralized to one entity
Speed	Slower	Faster	Fastest
Security	Open network	Approved participants	One participant
Identity	Anonymous or pseudonymous	Known identities	Known identity
Asset	Native assets	Any asset	Determined by platform chosen
	✓ Bitcoin, Ethereum	✓ Many implementation examples	Do you really need blockchain?

Attendance check



WHAT MAKES IT POSSIBLE?

Cryptography

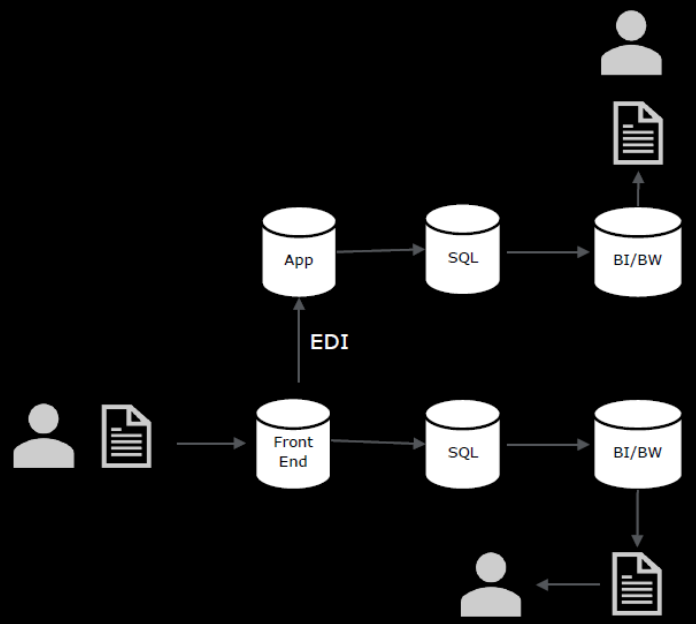


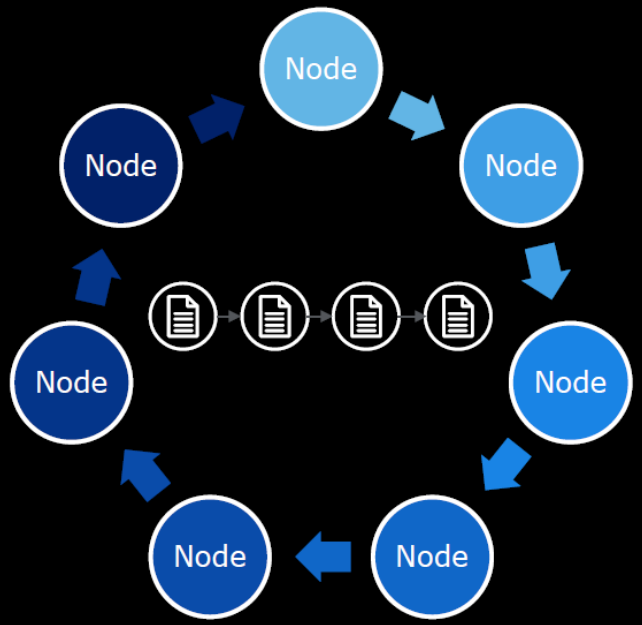
Lots and lots (and lots and lots) of computing power

Some amazing computer science

Blockchain | Why is it revolutionary?

Traditional	Blockchain
MULTIPLE SOURCES OF THE TRUTH	SINGLE SOURCE OF THE TRUTH





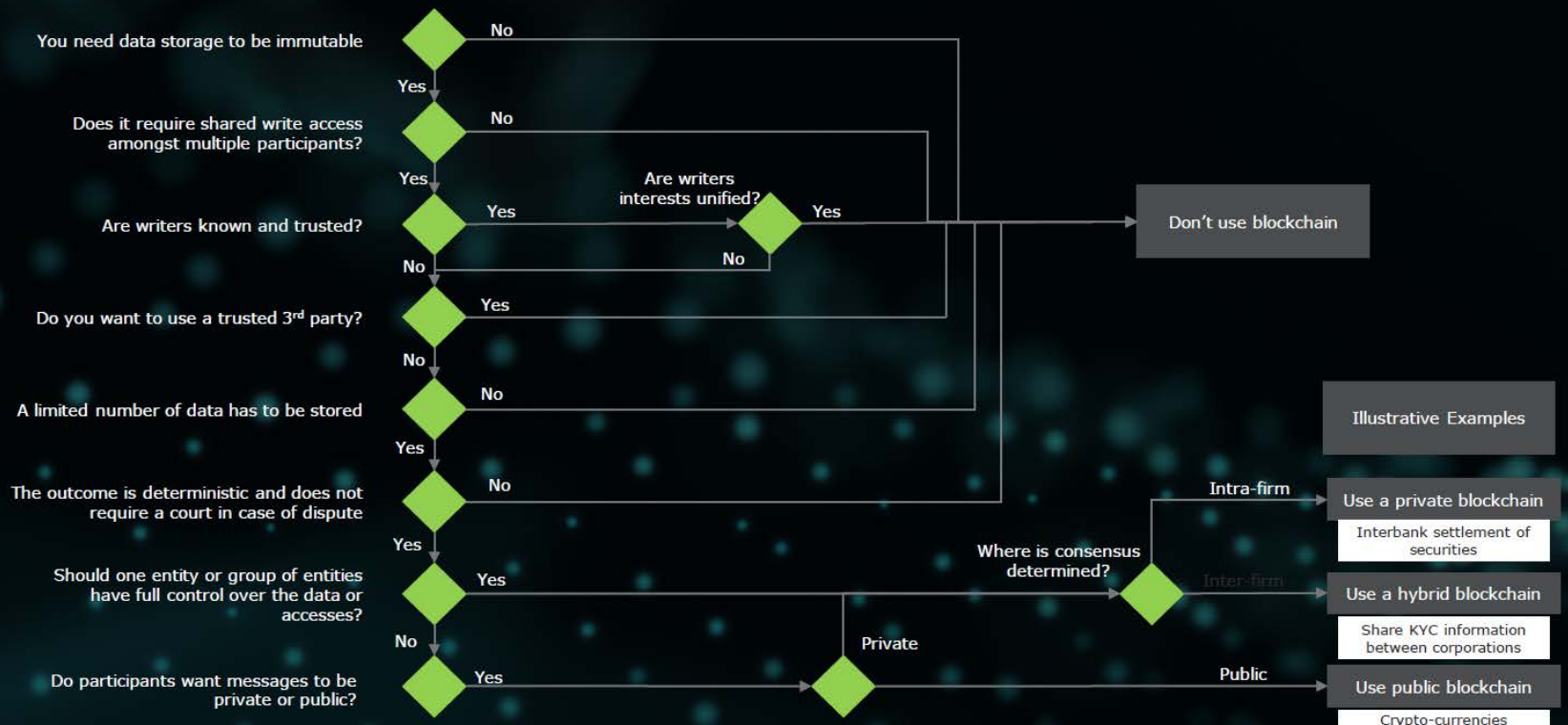
When is blockchain the right fit?

There are a handful of requirements that, when met in part or in full, should indicate whether blockchain will sufficiently address a client's needs

Shared Data	**Structured repository** of information
Multiple Writers	**More than one entity** generating the transactions that modify the database
Absence of Trust	Level of ***mistrust*** **between the entities** writing to the database (*e.g.*, one user will not accept the "truth" as reported by another user)
Opportunity for Disintermediation	**Lack of trusted intermediary** or central gatekeeper to verify transactions
Transaction Interaction	Interaction or **dependency between the transactions created by different entities**

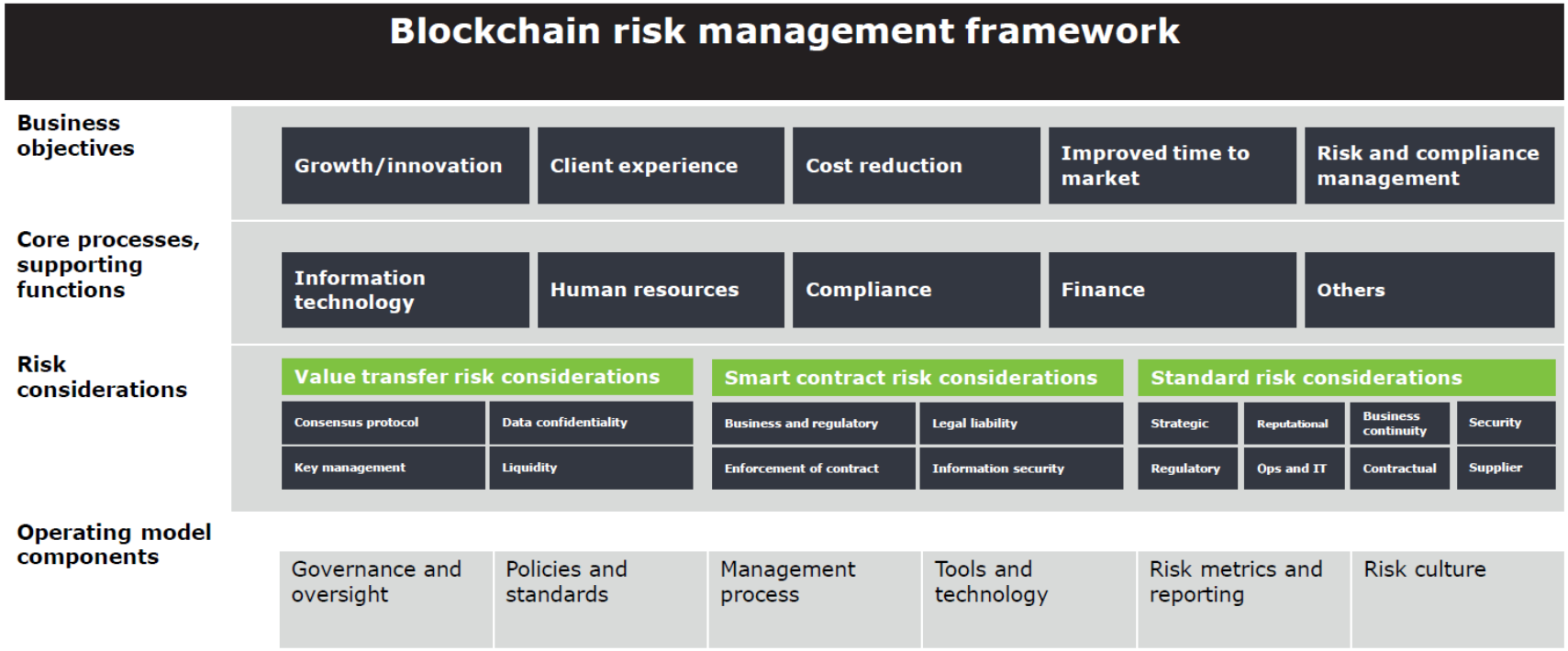
Do you need a Blockchain?

Blockchain is a good solution only when specific requirements are united

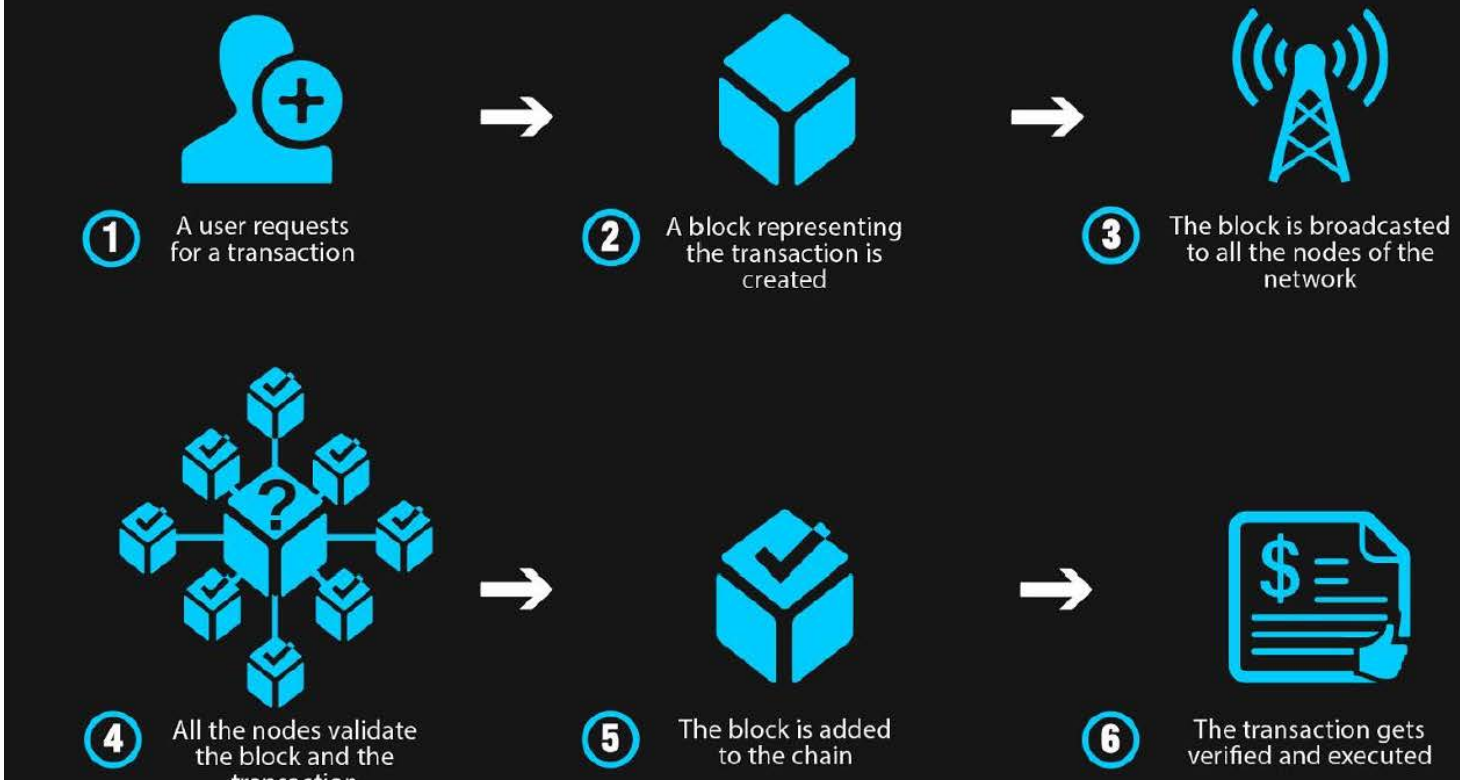


BLOCKCHAIN RISK MANAGEMENT

Technology continues to be a key enabler of growth for financial institutions. The blockchain risk management framework may be used to advise entities on blockchain use case-specific risk management topics, ranging from strategy, implementation, market, entity specific, and technology considerations.



How Does a Blockchain Work: A Step-by-Step View



Remarkable Benefits of Blockchain Technology

Faster Settlement
Way faster than the manual process of validation

Immutable
The transactions cannot be undone if they are already on the blockchain

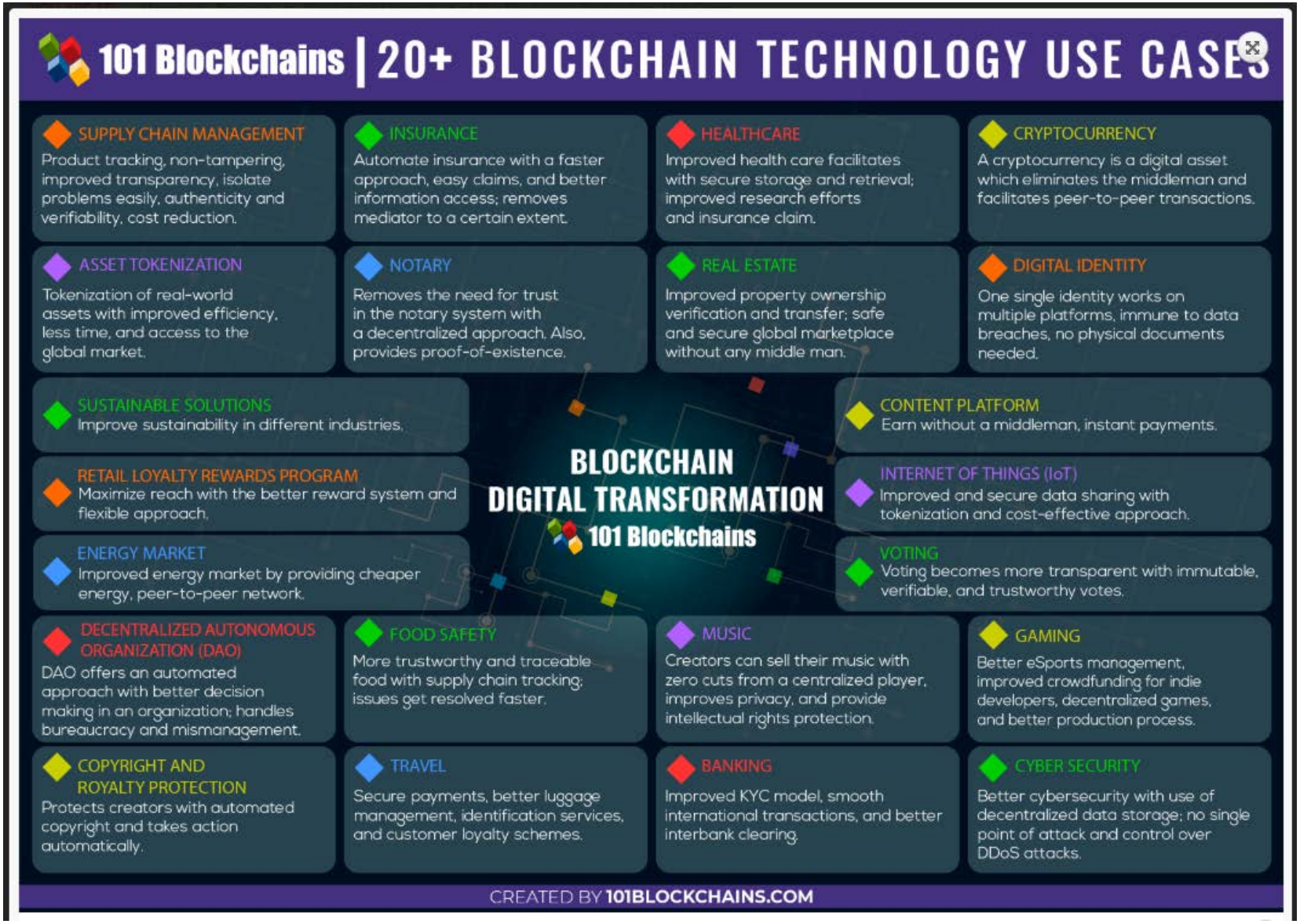
Increase Network Capacity
Much more capable than the traditional network

Shared and Distributed
Blockchain technology offers a shared and distributed ledger that is open for all users

More Secured
Much safer than the traditional methods

Decentralized
Not dependable on server based technology and no one has authority over the system

101 Blockchains
Created by 101blockchains.com


101 Blockchains | 20+ BLOCKCHAIN TECHNOLOGY USE CASES
SUPPLY CHAIN MANAGEMENT
Product tracking, non-tampering, improved transparency, isolate problems easily, authenticity and verifiability, cost reduction.
INSURANCE
Automate insurance with a faster approach, easy claims, and better information access; removes mediator to a certain extent.
HEALTHCARE
Improved health care facilitates with secure storage and retrieval; improved research efforts and insurance claim.
CRYPTOCURRENCY
A cryptocurrency is a digital asset which eliminates the middleman and facilitates peer-to-peer transactions.
ASSET TOKENIZATION
Tokenization of real-world assets with improved efficiency, less time, and access to the global market.
NOTARY
Removes the need for trust in the notary system with a decentralized approach. Also, provides proof-of-existence.
REAL ESTATE
Improved property ownership verification and transfer; safe and secure global marketplace without any middle man.
DIGITAL IDENTITY
One single identity works on multiple platforms, immune to data breaches, no physical documents needed.
SUSTAINABLE SOLUTIONS
Improve sustainability in different industries.
RETAIL LOYALTY REWARDS PROGRAM
Maximize reach with the better reward system and flexible approach.
ENERGY MARKET
Improved energy market by providing cheaper energy, peer-to-peer network.
BLOCKCHAIN
DIGITAL TRANSFORMATION
101 Blockchains
CONTENT PLATFORM
Earn without a middleman, instant payments.
INTERNET OF THINGS (IoT)
Improved and secure data sharing with tokenization and cost-effective approach.
VOTING
Voting becomes more transparent with immutable, verifiable, and trustworthy votes.
DECENTRALIZED AUTONOMOUS ORGANIZATION (DAO)
DAO offers an automated approach with better decision making in an organization; handles bureaucracy and mismanagement.
FOOD SAFETY
More trustworthy and traceable food with supply chain tracking; issues get resolved faster.
MUSIC
Creators can sell their music with zero cuts from a centralized player, improves privacy, and provide intellectual rights protection.
GAMING
Better eSports management, improved crowdfunding for indie developers, decentralized games, and better production process.
COPYRIGHT AND ROYALTY PROTECTION
Protects creators with automated copyright and takes action automatically.
TRAVEL
Secure payments, better luggage management, identification services, and customer loyalty schemes.
BANKING
Improved KYC model, smooth international transactions, and better interbank clearing.
CYBER SECURITY
Better cybersecurity with use of decentralized data storage; no single point of attack and control over DDoS attacks.
CREATED BY 101BLOCKCHAINS.COM

FURTHER CONSIDERATIONS

Anonymity

Business value

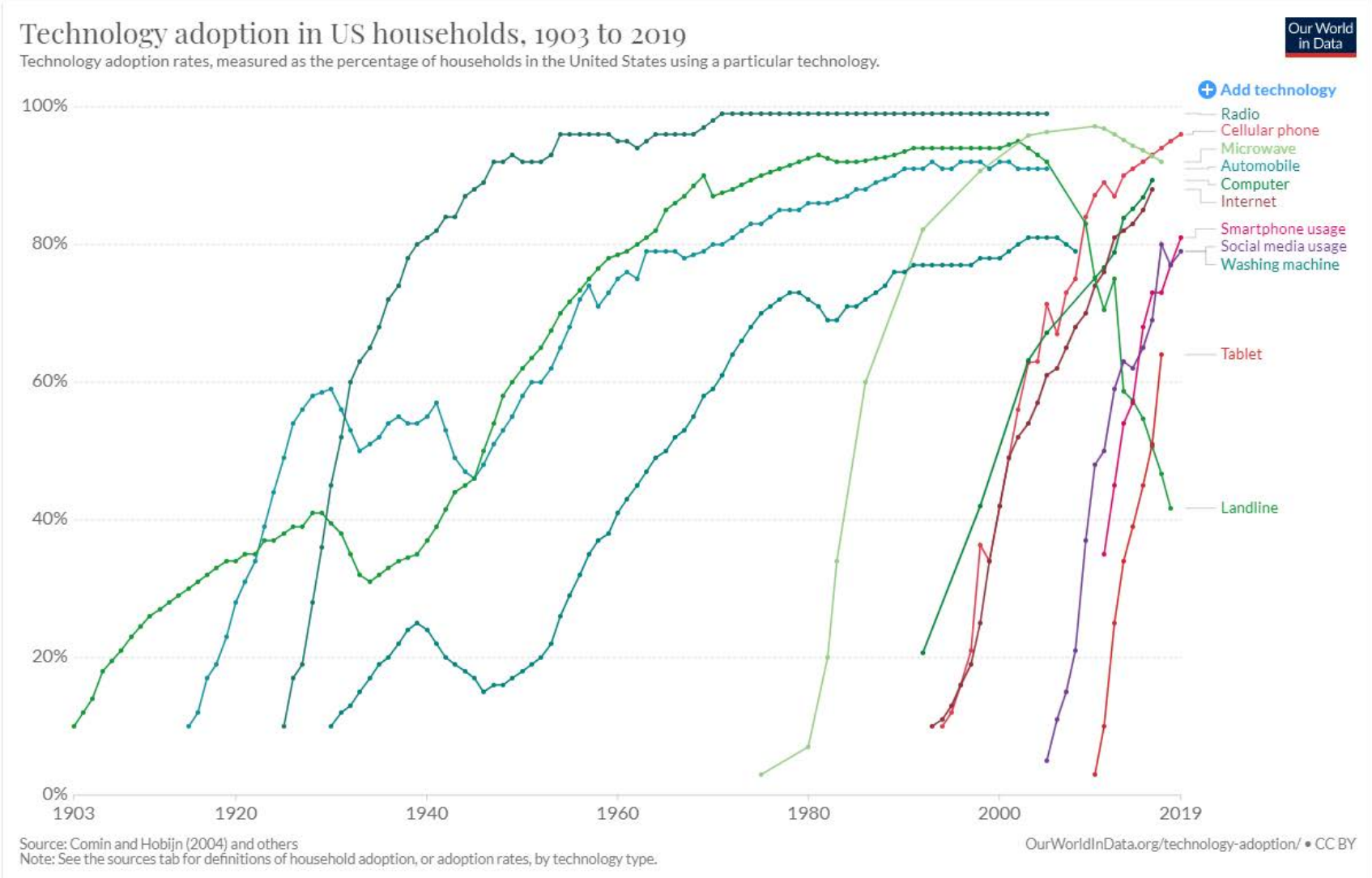
Most of the time blockchain is not the right solution

ATTENDANCE CHECK

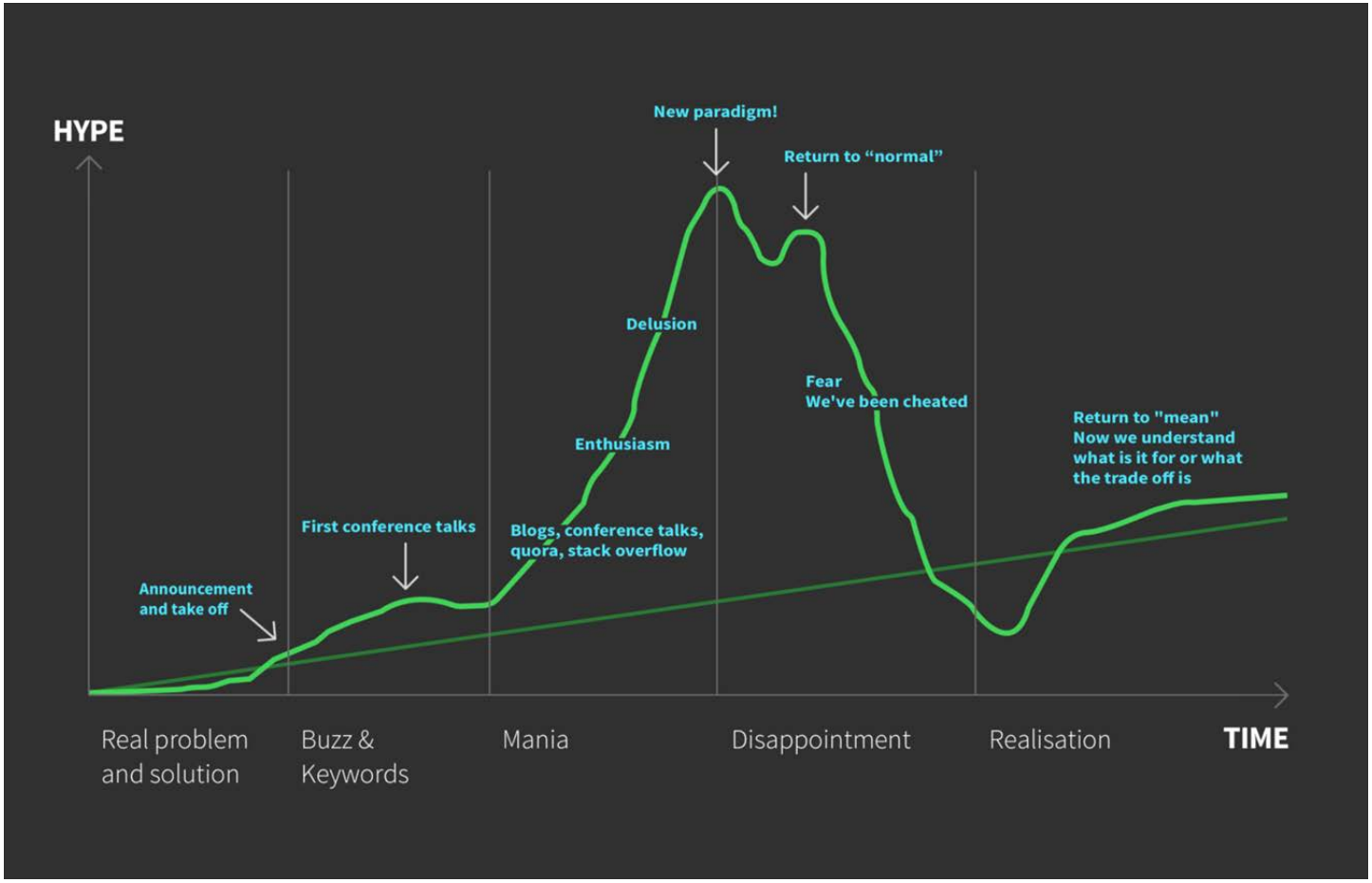
What do you a call
a 90-year-old accountant?

Someone at the end
of their useful life


MOTOROLA


Technology adoption in US households, 1903 to 2019
Technology adoption rates, measured as the percentage of households in the United States using a particular technology.
Our World in Data
Add technology
Radio
Cellular phone
Microwave
Automobile
Computer
Internet
Smartphone usage
Social media usage
Washing machine
Tablet
Landline
100%
80%
60%
40%
20%
0%
1903
1920
1940
1960
1980
2000
2019
Source: Comin and Hobijn (2004) and others
Note: See the sources tab for definitions of household adoption, or adoption rates, by technology type.
OurWorldInData.org/technology-adoption/ • CC BY

The Hype Cycle



https://blog.daftcode.pl/hype-driven-development-3469fc2e9b22

https://markets.bitcoin.com/crypto/BTC as of 6/10/2020

ATTENDANCE CHECK

To Executive Staff and direct reports

From Bill Gates

Date May 26, 1995

The Internet Tidal Wave

Our vision for the last 20 years can be summarized in a succinct way We saw that exponential improvements in computer capabilities would make great software quite valuable Our response was to build an organization to deliver the best software products In the next 20 years the improvement in computer power will be outpaced by the exponential improvements in communications networks The combination of these elements will have a fundamental impact on work, learning and play Great software products will be crucial to delivering the benefits of these advances. Both the variety and volume of software will increase

Most users of communications have not yet seen the price of communications come down significantly Cable and phone networks are still depreciating networks built with old technology. Universal service monopolies, and other governmental involvement around the world have kept communications costs high Private networks and the Internet which are built using state of the art equipment have been the primary beneficiaries of improved communication technology The PC is just now starting to create additional demand that will drive a new wave of investment. A combination of expanded access to the Internet, ISDN, new broadband networks justified by video based applications and interconnections between each of these will bring low cost communication to most businesses and homes within the next decade.

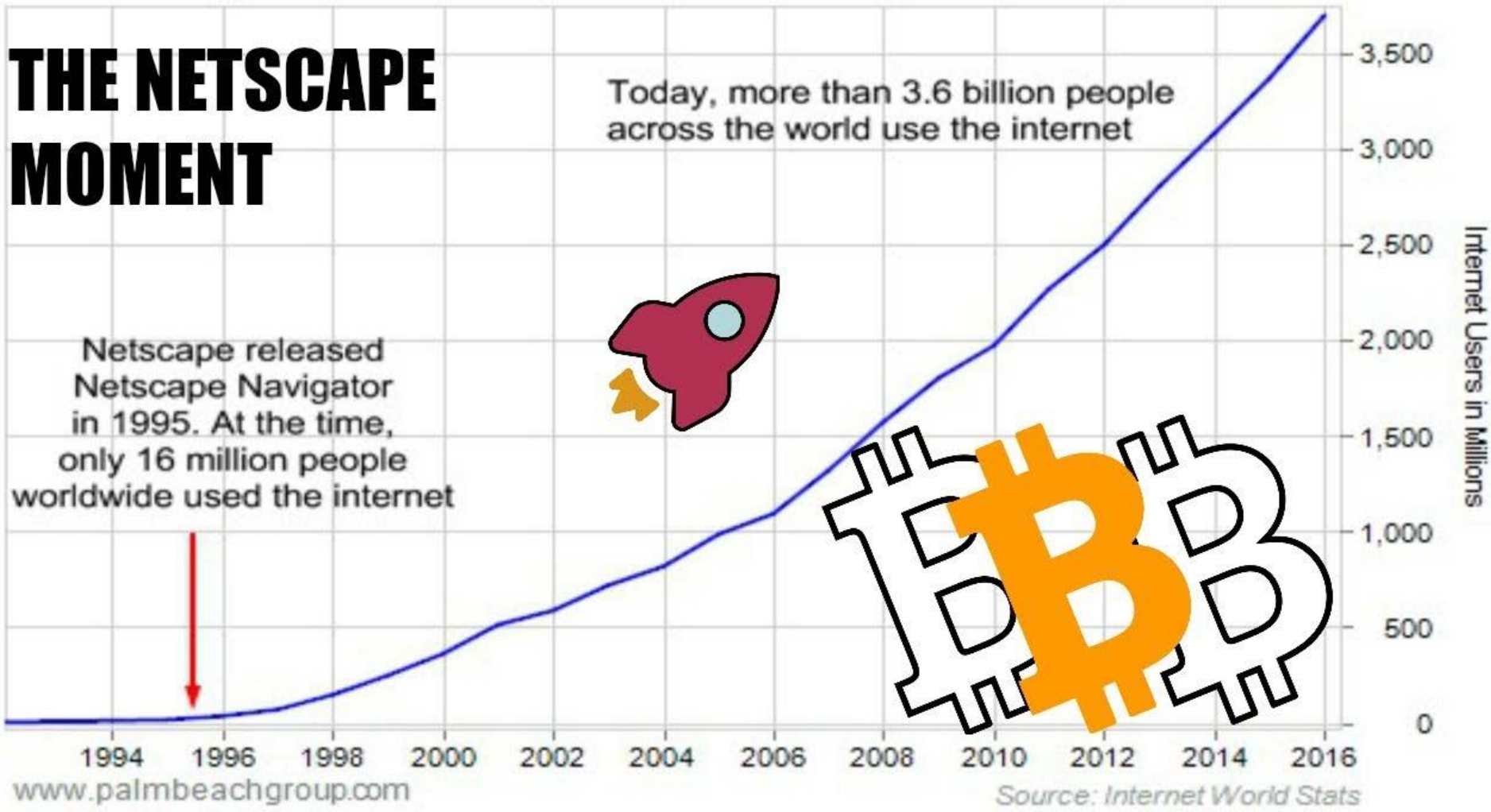
The Internet is at the forefront of all of this and developments on the Internet over the next several years will set the course of our industry for a long time to come. Perhaps you have already seen memos from me or others here about the importance of the Internet. I have gone through several stages of increasing my views of its importance. Now I assign the Internet the highest level of importance. In this memo I want to make clear that our focus on the Internet is critical to every part of our business. The Internet is the most important single development to come along since the IBM PC was introduced in 1981. It is even more important than the arrival of graphical user interface (GUI) The PC analogy is apt for many reasons The PC wasn't perfect. Aspects of the PC were arbitrary or even poor. However a phenomena grew up around the IBM PC that made it a key element of everything that would happen for the next 15 years. Companies that tried to fight the PC standard often had good reasons for doing so but they failed because the phenomena overcame any weaknesses that resisters identified

The Internet Today

The Internet's unique position arises from a number of elements The TCP/IP protocols that define its transport level support distributed computing and scale incredibly well The Internet Engineering Task Force (IETF) has defined an evolutionary path that will avoid it running into future problems even as virtually everyone on the planet connects up The HTTP protocols that define HTML Web browsing are extremely simple and have allowed servers to handle incredible traffic reasonably well All of the predictions about hypertext - made decades ago by pioneers like Ted Nelson - are coming true on the Web Although other protocols on the Internet will continue to be used (FTP, Gopher, IRC, Telnet, SMTP, NNTP), HTML with extensions will be the standard that defines how information will be presented Various extensions to HTML including content enhancements like tables, and functionality enhancements like secure transactions, will be widely adopted in the near future There will also be enhanced 3D presentations providing for virtual reality type shopping and socialization

M 1028049
CONFIDENTIAL

MS98 0112876
CONFIDENTIAL



We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.

Other resources

- An internal auditor's guide to auditing blockchain from Deloitte
  - https://www2.deloitte.com/us/en/pages/risk/articles/internal-auditing-guide-to-blockchain.html
- Bitcoin white paper
  - https://bitcoin.org/bitcoin.pdf
- Many free online courses on edX, Coursera, etc.

Thank you

Neil Kane

neildkane@outlook.com

LinkedIn: www.linkedin.com/in/neilkane

Blog: www.illinoispartners.com/blog

Book: http://innovators-secret-formula.com/


Any
Questions