Era of Elusiveness in Security and Privacy

Shin'ichiro Matsuo
Georgetown University

Keynote at ISPEC 2018, Tokyo

GEORGETOWN UNIVERSITY

About Me

@Shanematsuo

- Research Professor at Georgetown University
  - Director of Blockchain Technology and Ecosystem Design (B-TED) research center
- Director’s Liaison for Financial Cryptography at MIT Media Lab

- Co-Founder of Bsafe.network (Blockchain Research)
- Program committee and editor: Scaling Bitcoin, IEEE, ACM conferences, Ledger Journal and more…
  - Program co-chair of Scaling Bitcoin 2018
- Standardization at ISO TC307 (Blockchain and DLT)
- Ph.D. from Tokyo Institute of Technology

About Me

@Shanematsuo

I have no Bitcoin and any cryptocurrencies

I have no position on the exchange rate to FIAT currency.

Talk Plan

Why do we need security and privacy model?

The impact on Bitcoin and Blockchain to our research

The way forward to deal with elusive security and privacy

WHY SECURITY AND PRIVACY MODEL ARE NEEDED

Security model

- Abstract Entity (Alice, Bob, Eve, …)
- Security goal and definition
- Adversarial capability

Why we need model

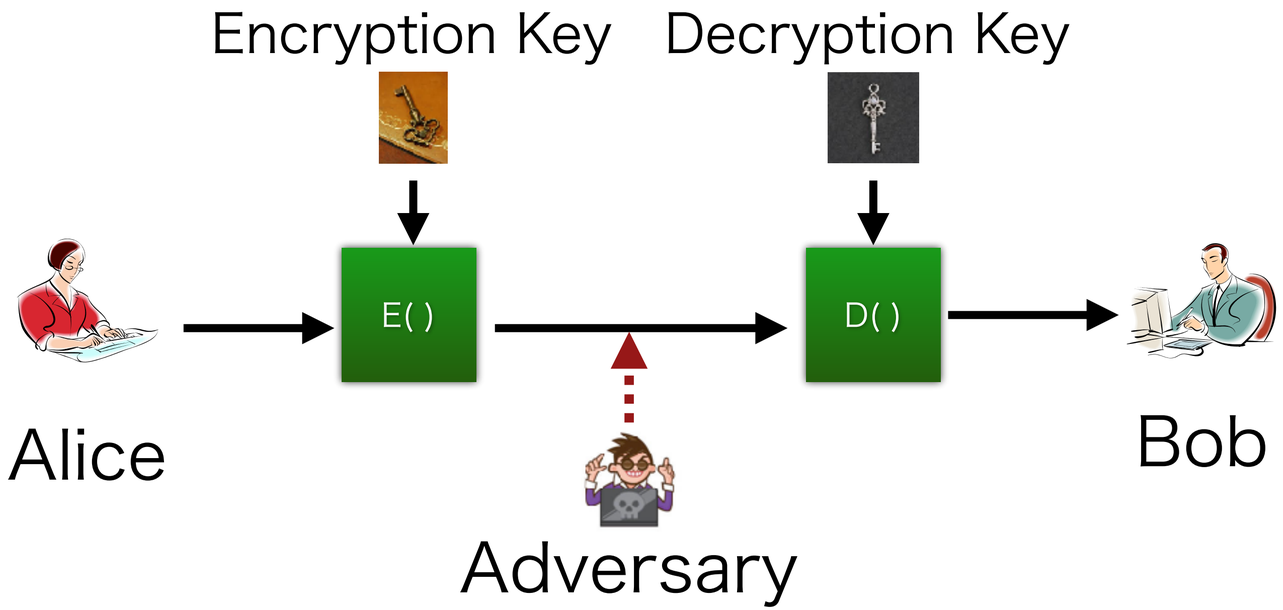
- Capturing entire states w.r.t. security and privacy is hard.
- Model is need for mathematical discussions
  - Understand problem
  - Design solution
  - Evaluation and proof

Assumption helps us

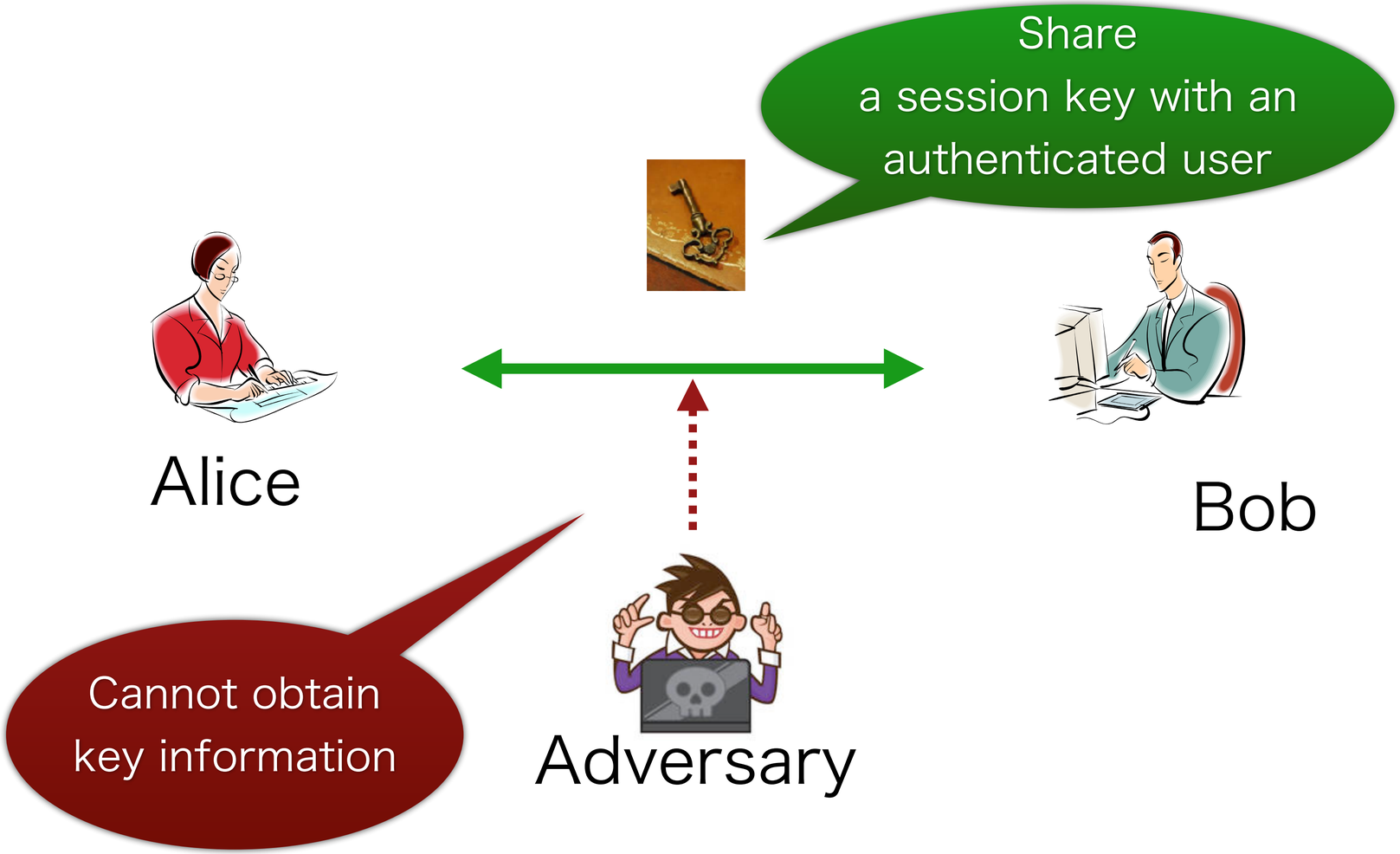
- We can concentrate on essential problem with let solutions to other problems “assumptions”
- We can forget real-life bothering phenomenon
- Examples
  - Mathematical assumptions: DH, DDH, Factoring, …
  - Engineering assumptions: Secure coding, key management
  - Operational assumptions: key management, audit, …

Security model of cryptographic primitive

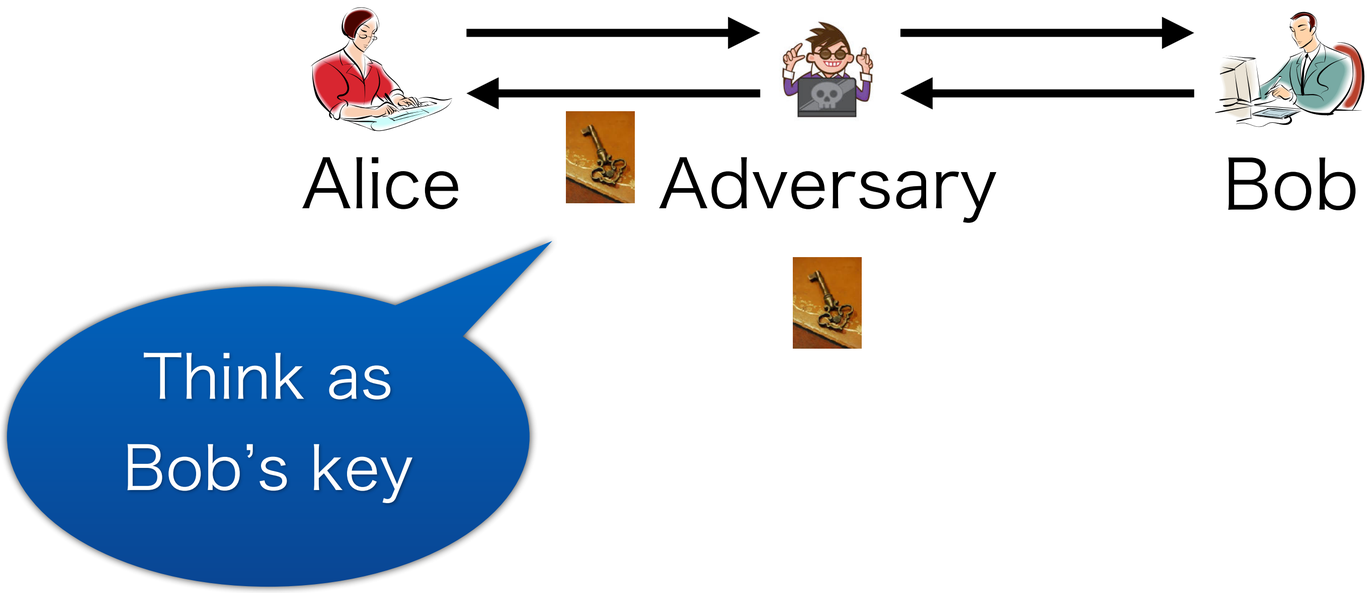
Operational environment is simple.



Secure Channel (Authenticated Key Exchange)



Man-in-the-Middle Attack



Dolev-Yao Model

- Cryptography is treated as ideal operation.
  - Only a party who has a decryption key obtains plaintext.
  - The other party obtains nothing.
  - Same treatment for digital signature and others
- An adversary can control communication channel.
  - Eavesdrop, stop, and send any message.

We were happy.

Two contexts of elusiveness

- Assumption
- New factors caused by applications

Model makes security layers of cryptographic application

Operation	Key Management, Audit, Backup	ISO/IEC 27000
Implementation	Program Code, Script, Secure Hardware	ISO/IEC 15408
Application Protocol	Business process	ISO/IEC 29128
Fundamental Protocol	P2P, Consensus, Merkle Tree	ISO/IEC 29128
Cryptography	ECDSA, SHA-2, RIPEMD160	NIST,ISO

The case of SSL/TLS

Many attacks/vulnerabilities are found during this 6 years.

Heartbleed, Poodle, FREAK, DROWN, CCS Injection

Problems

No security proof

No procedure for verification of technology.

No experts on the verification of cryptographic protocols

Insufficient quality assurance of program code

Heartbleed bug

- Bugs in OpenSSL related to Heatbeat extension
- Insufficient check of data size
- An adversary can obtain the contents of data in the server
- This attack is independent from the strength of underlying cryptographic primitives, too.

Pitfall between specification and implementation

In the case of Heartbleed

- The description in RFC document does not describe the details of implementation
- Treatment of data length (ex. the case of size = 0)
- No instruction is provided for developers

How can we evaluate the security of Crypto Protocol?

Formal Verification

- Formal method
- Find the existence of insecure state
- Automated verification
- Tool-aided

Mathematical Proof

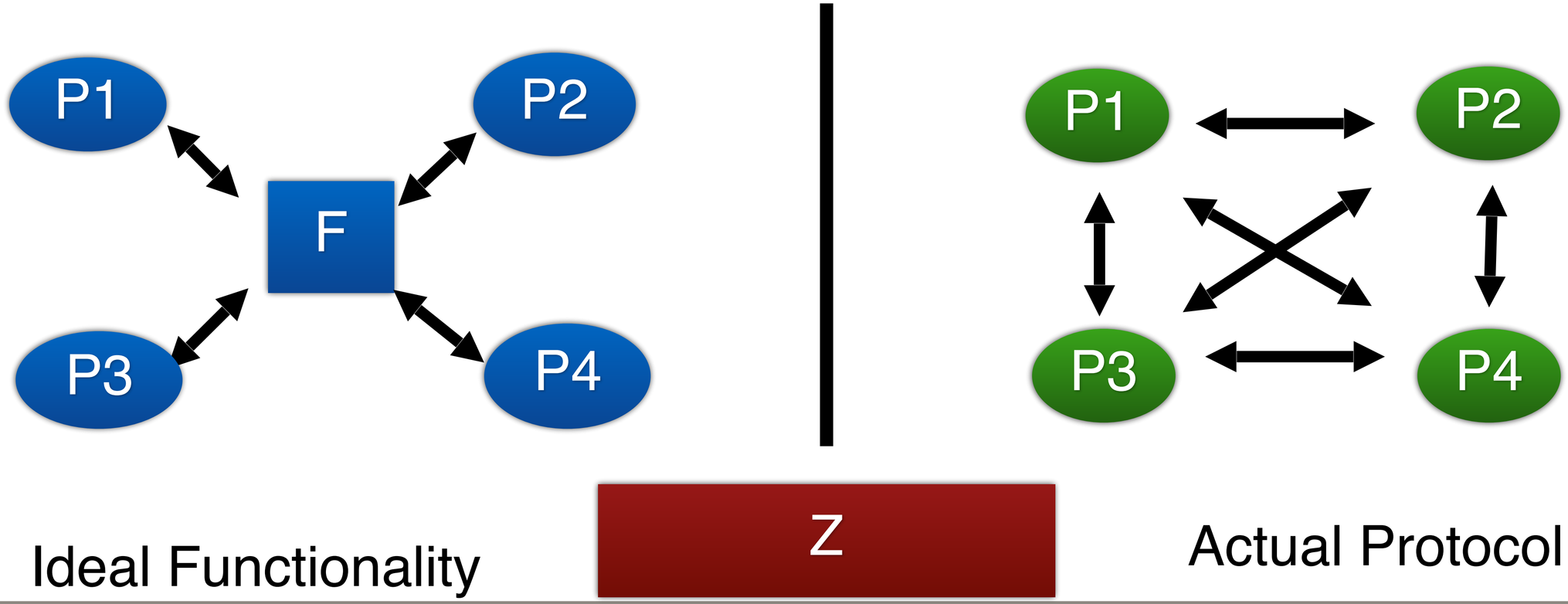
- Rigorous proof
- Estimate probability of attack
- Same as cryptographic Primitive

Formal Verification

- Cryptographic algorithm is idealized.
- Explore the existence of state against the security property.
- Dolev-Yao Model.
  - Omit the possibility of successful attack on underlying cryptographic algorithm.

Mathematical Proof: Universal Composability

- Define the ideal functionality, then prove that the actual protocol is indistinguishable against the ideal functionality.



Assumption of secure multi-party computation

Secret sharing schemes can tolerate an adversary controlling up to *t* parties out of *n* total parties, where *t* varies based on the scheme, the adversary can be passive or active, and different assumptions are made on the power of the adversary. The Shamir secret sharing scheme is secure against a passive adversary when

$$t < \frac{n}{2}$$

and an active adversary when

$$t < \frac{n}{3}$$

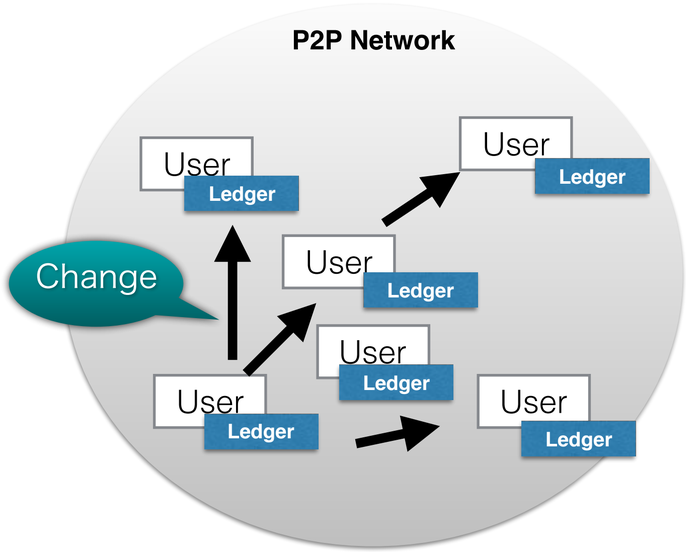
while achieving information-theoretic security, meaning that even if the a
in

How can we make such assumption happen?

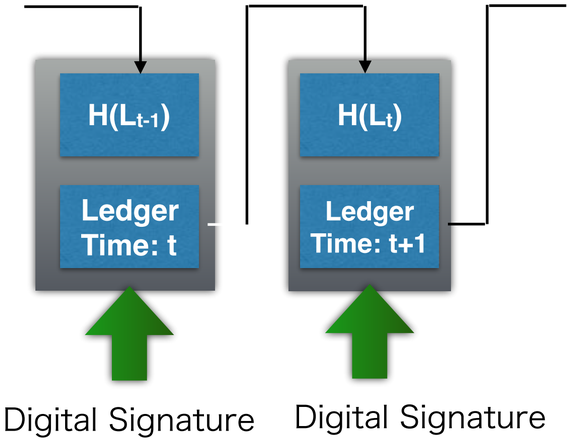
WHAT BITCOIN BROUGHT TO SECURITY RESEARCH

Blockchain

- Fundamental techniques to realize “Public Ledger” using P2P network and chained digital signature
- Used in digital currencies like Bitcoin

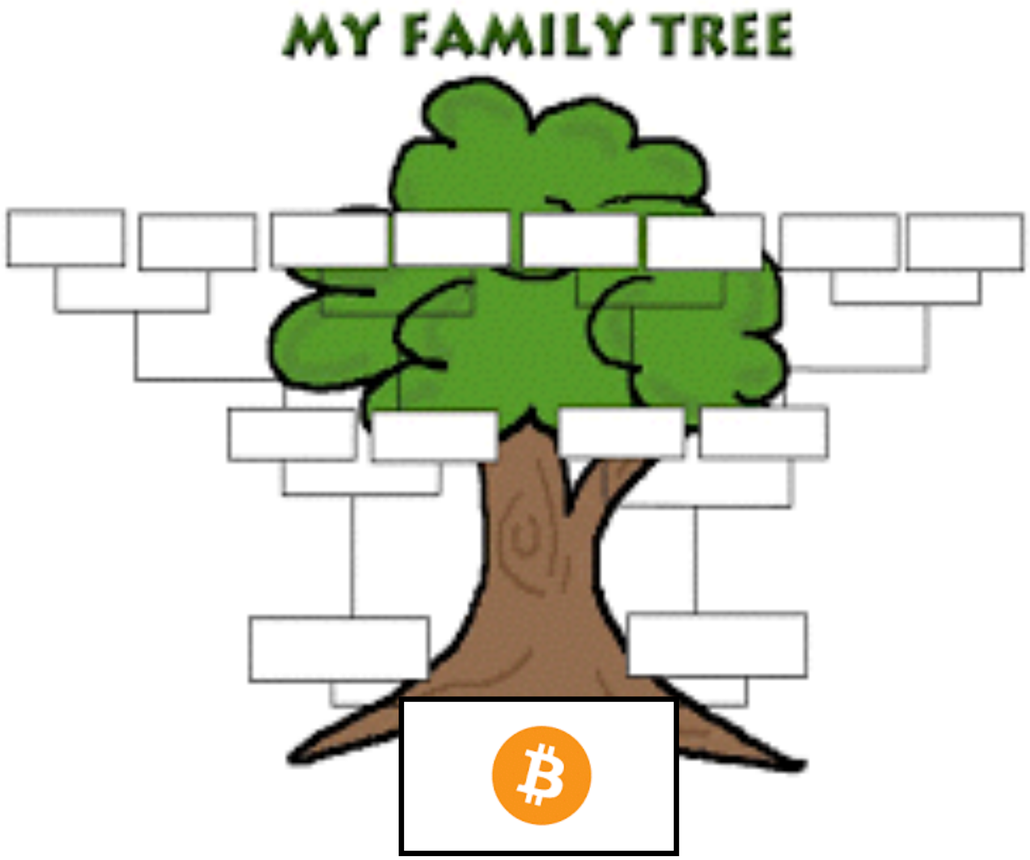


Each node update its distributed ledger

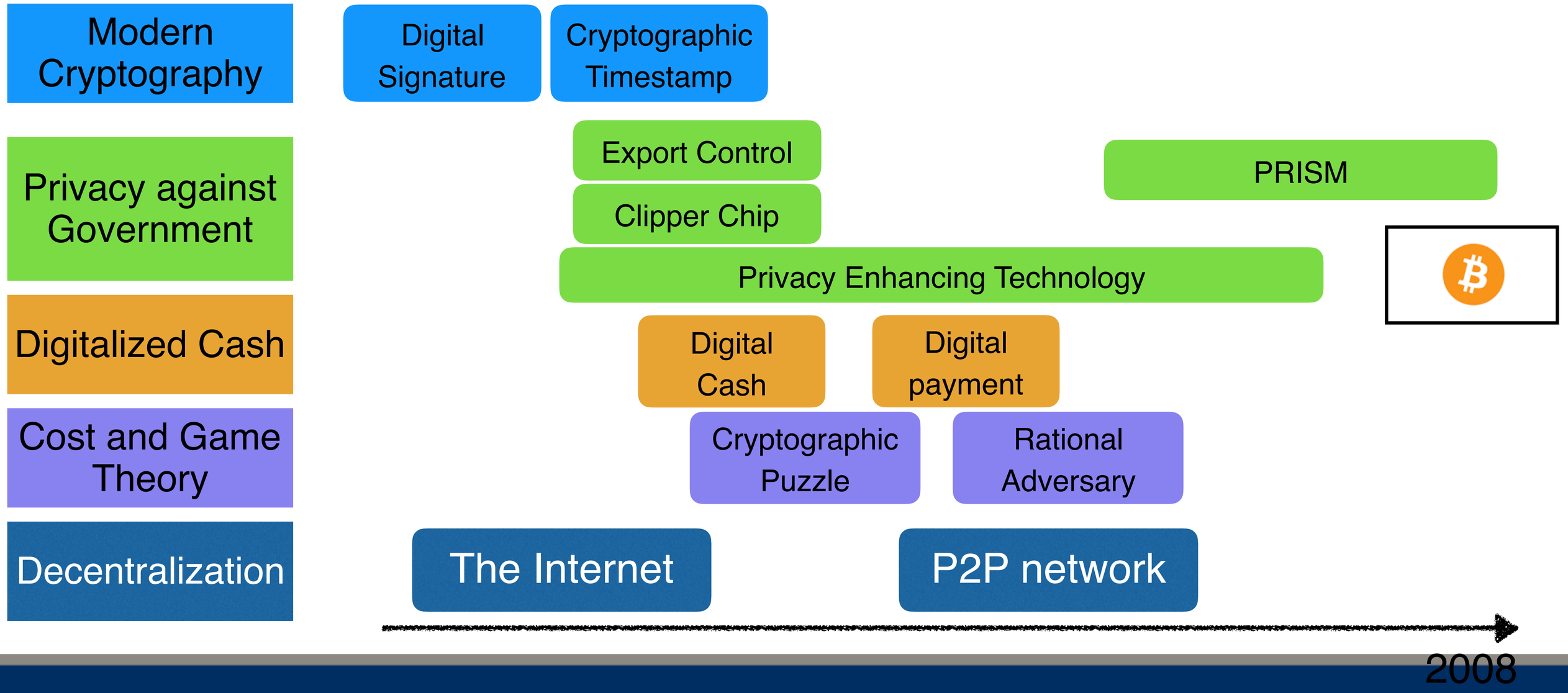


How Did Bitcoin/Blockchain Born?

Entirely new invention?



Chronology Before Bitcoin



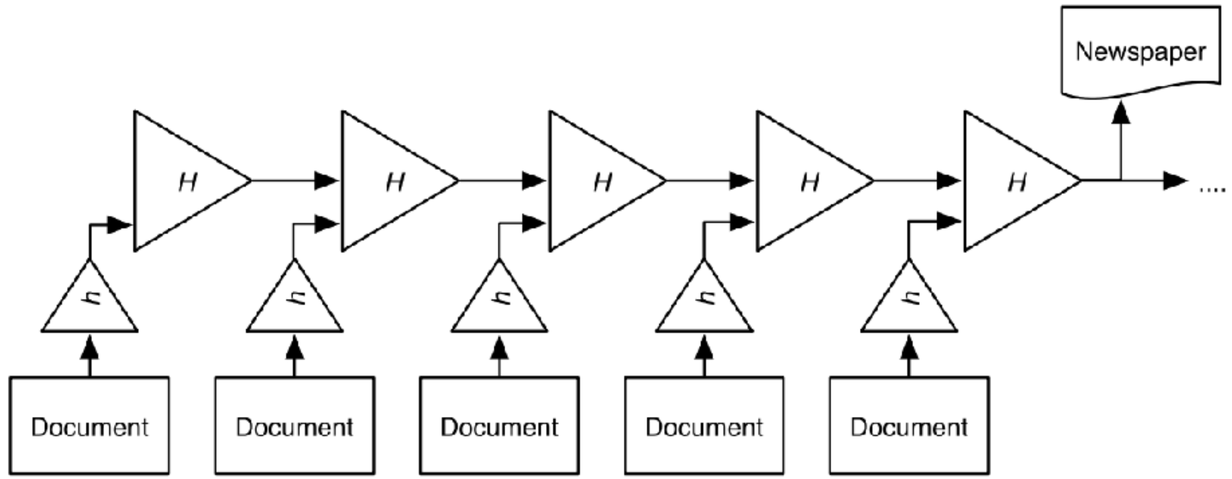
Where the Data Structure of Blockchain Came From… (1990)

How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

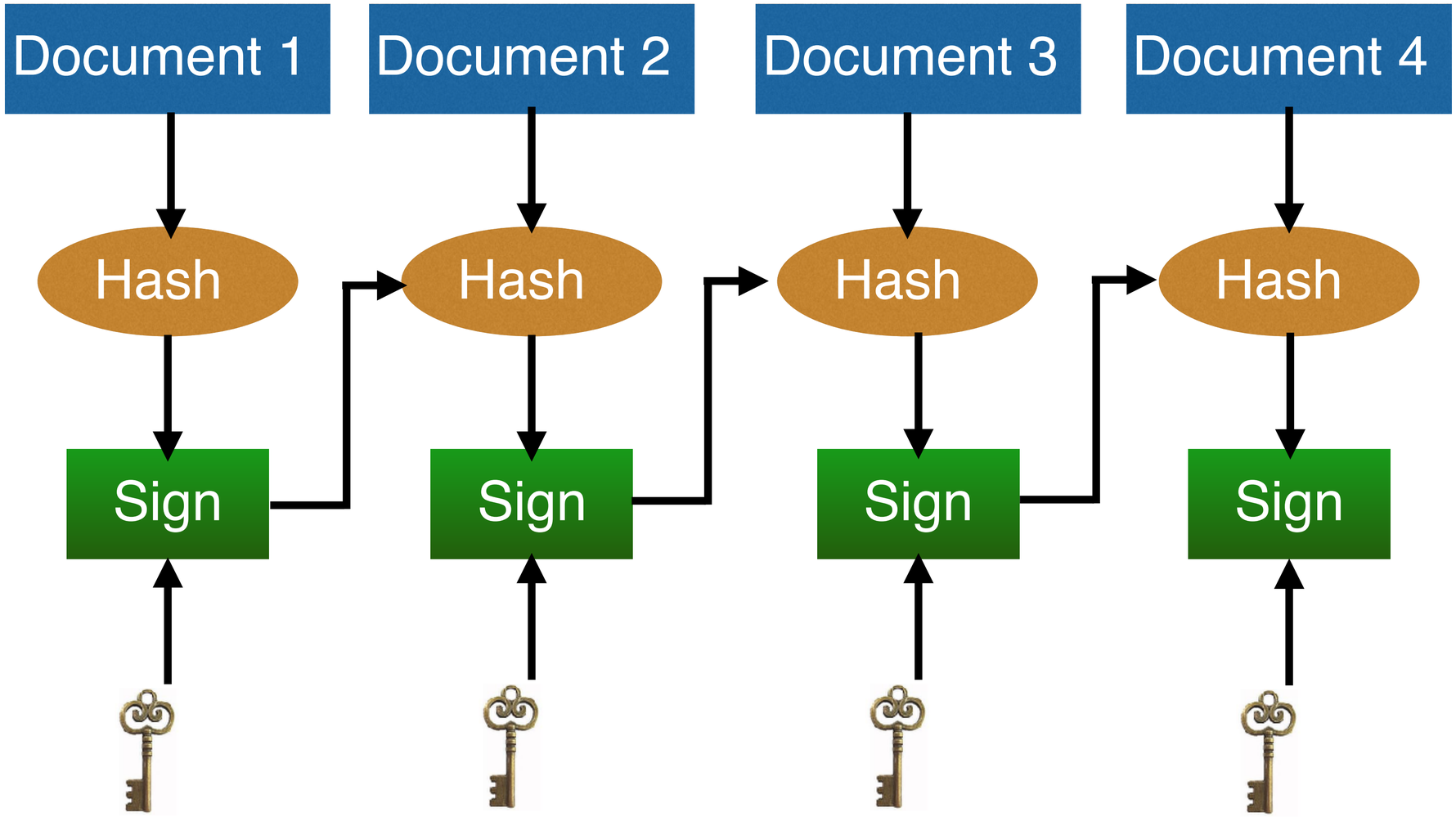
W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910



But needs centralized server(s)

Hysteresis Signature was Invented in Japan (2002)



Waseda Univ., Yokohama National Univ., Tokyo Denki Univ. and Hitachi Ltd.

Needs centralized server(s)

Privacy against Government

Export control of cryptography (-2000)

Clipper Chip by NSA (1993-1996): A encryption/ decryption chip
- US Government can decrypt.

PRISM: Surveillance by NSA

Financial Cryptography Conference

Usually is held in Caribbean Islands

1st conference (1997) was held in Anguilla.

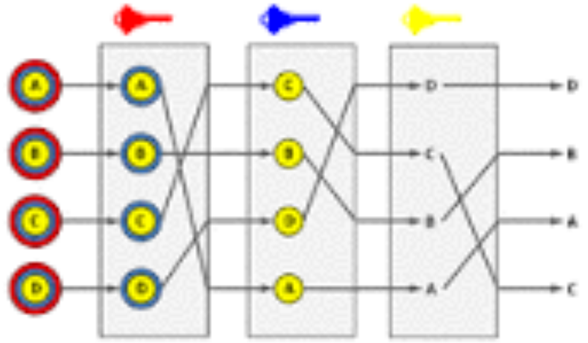
Free from export control of cryptography

Tax Haven

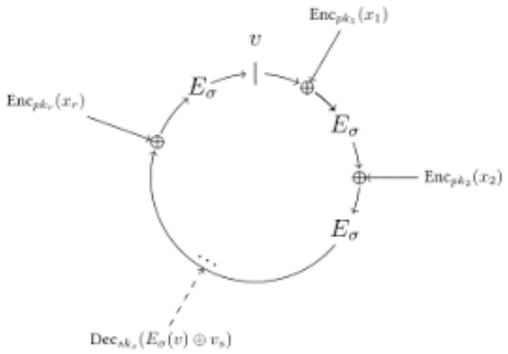
Initiated by Cypherpunk

Privacy Enhancing Technologies

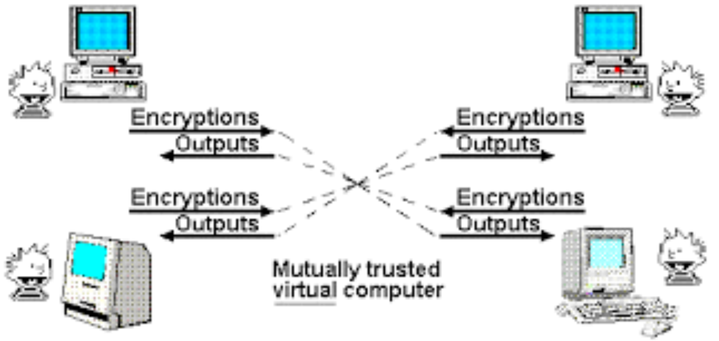
Blind Signature



Mix-Net/Tor



Group Signature/Ring Signature



Multi Party Computation

History of Research on Digitalized Cash (90s)

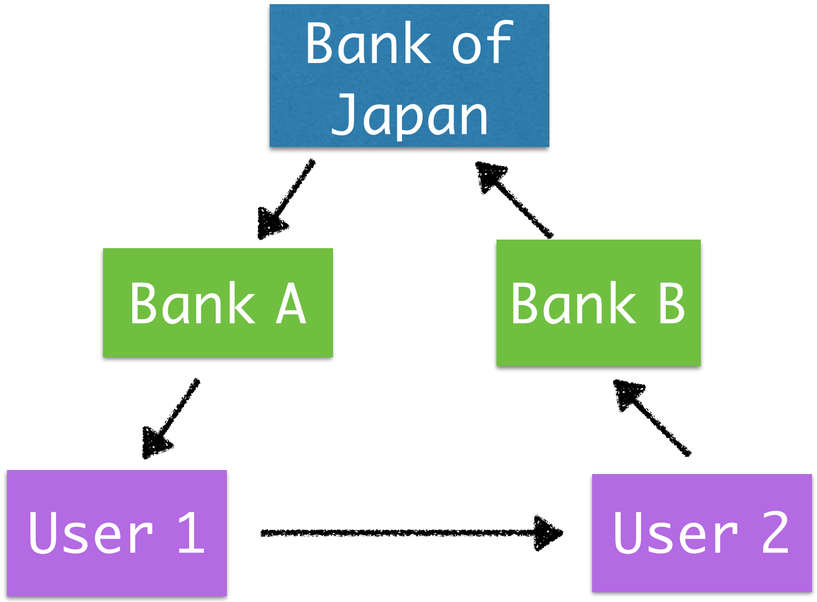
David Chaum

Stephan Brands

Visa Cash

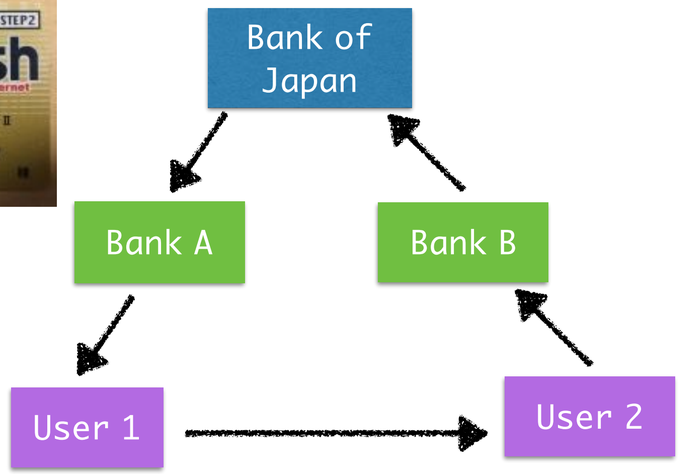
MONDEX

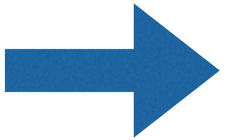
Internet Cash by Bank of Japan and NTT (1997-2000)

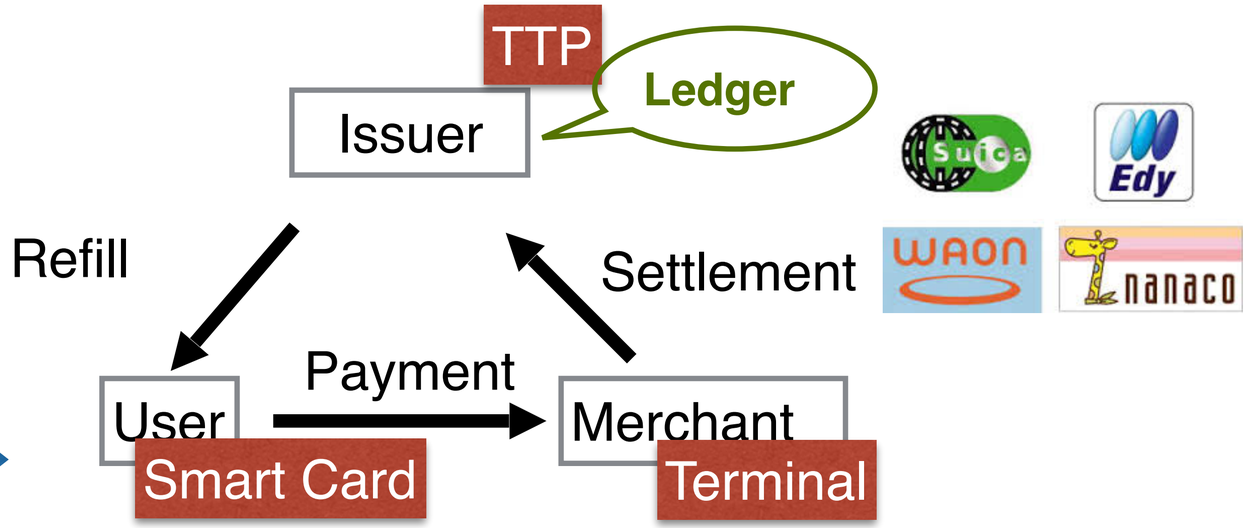


- Implement “Cash” issued by the “Bank of Japan”
- Transferable thorough e-mail attachment
- Multi-currency

Ideal Digitalized Cash vs. Practical Digital Payment







Anonymous
Offline payment
Transferable
Open-loop
Heavy cryptography

Transaction Identified
Online payment
Non-Transferable
Closed-loop
Lighter Processing

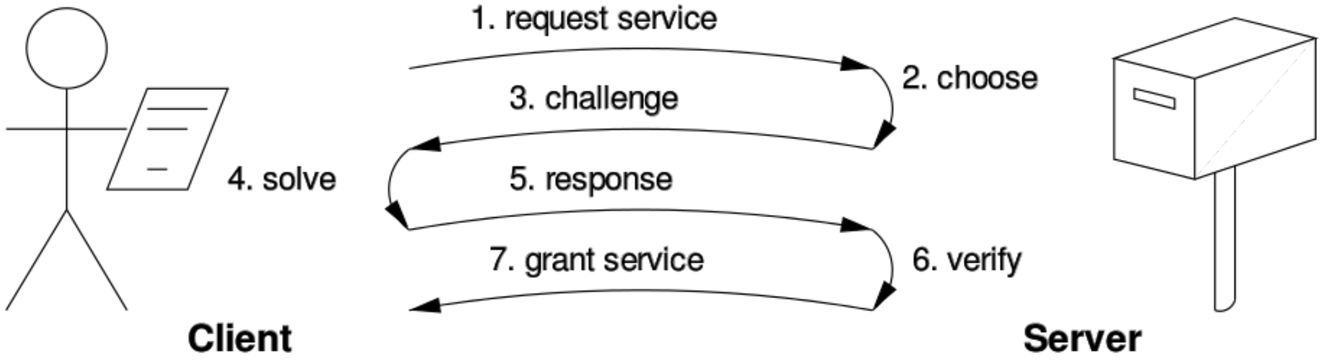
Add Cost to Attack: Cryptographic Puzzle

Originally, was proposed to prevent Denial of Services (DoS) and spam mails (1993).

This idea is utilized in Proof of Work of Bitcoin.

Game theoretical nature in Bitcoin:

- **Cost to attack vs. cost for future reward**



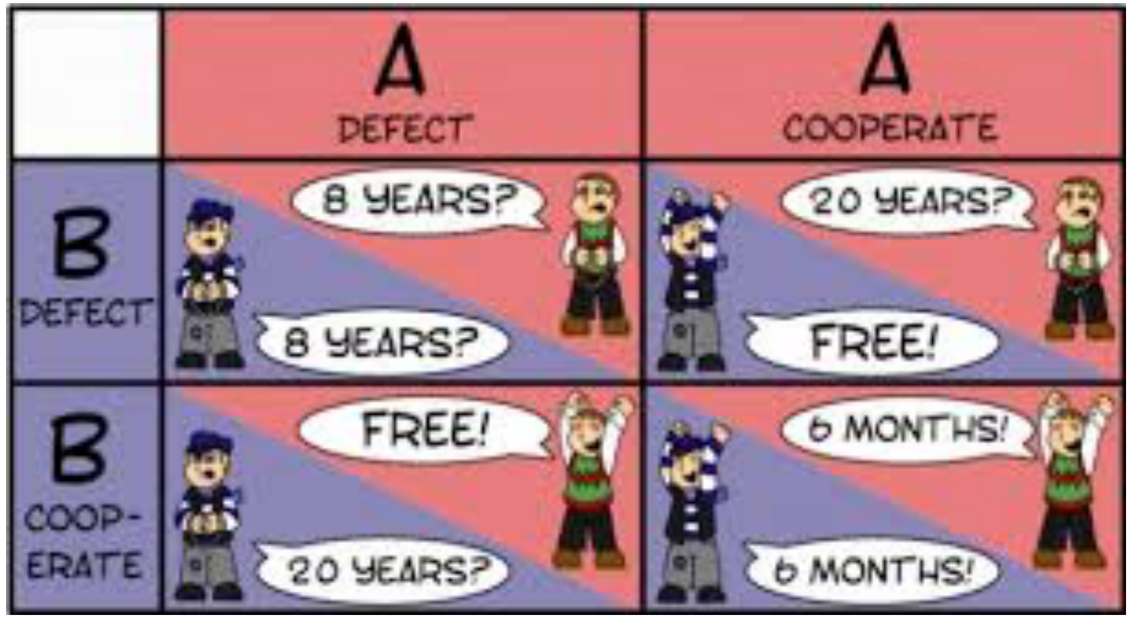
Cryptography and Game Theory (2002-)

Sealed-bid Auction

Vickrey Auction and (M+1) - price auction

Dynamic Programming and combinatorial auction

A class of Pareto Optimal



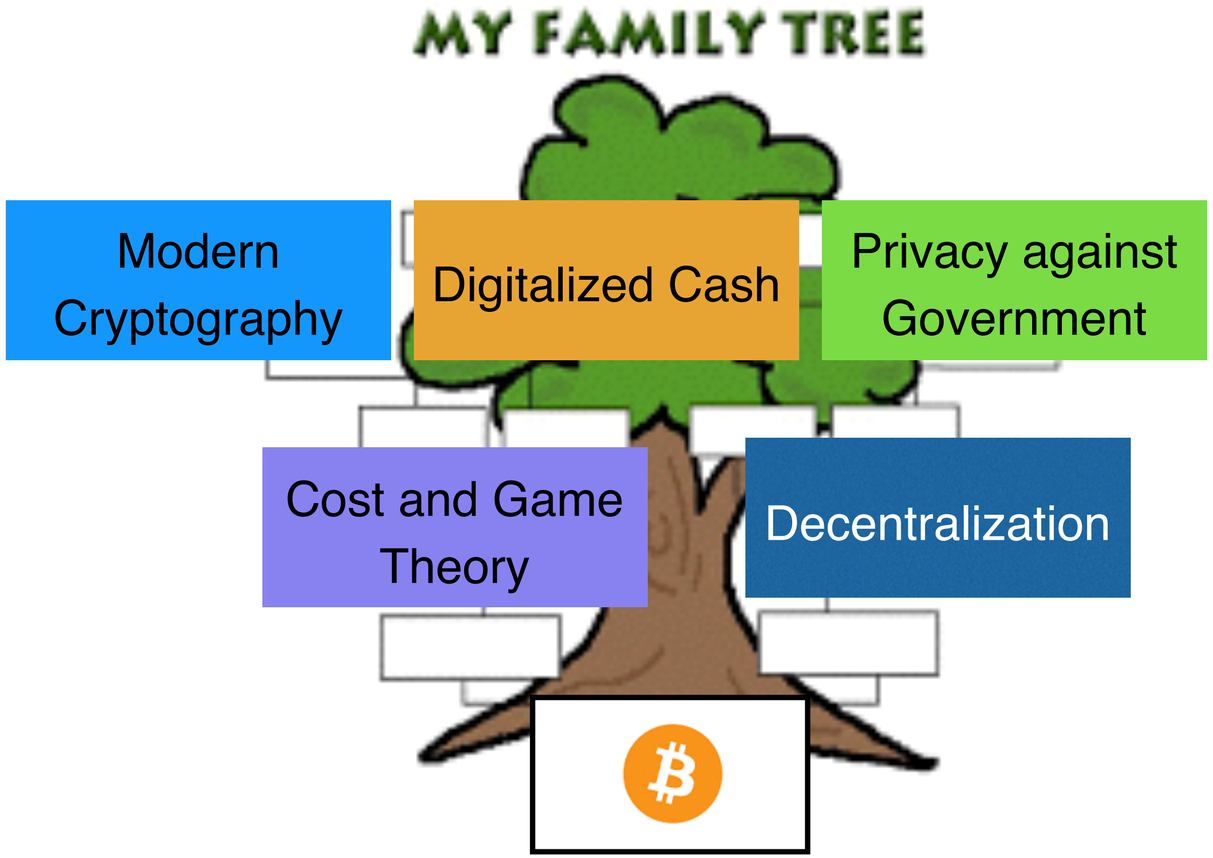
Decentralized Communication: The Internet and P2P

Resilient against fault and malicious activities

No one need to and can govern entire system.

Sharing small trust and responsibility to maintain the system

Bitcoin: Perfect Mix of Past Movements!



Mixing merits of past history of technology development.

Inheritance in Technology Development

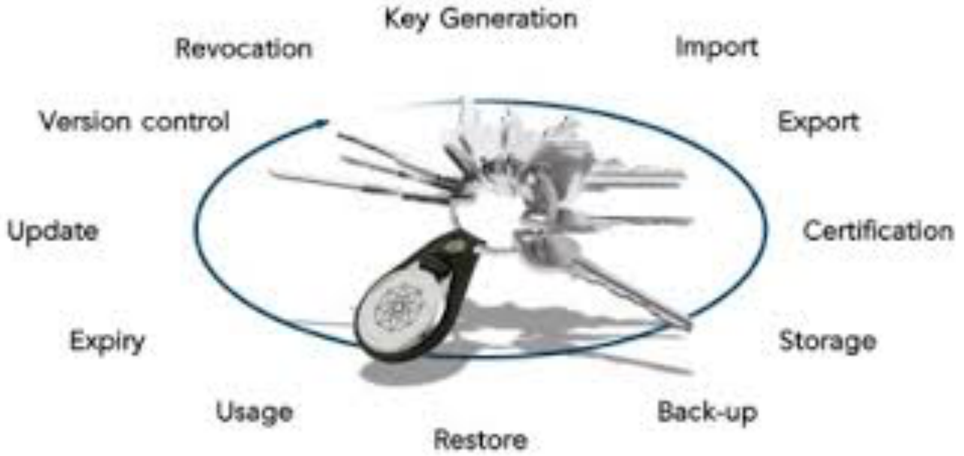
Merits of technologies

Defects of technologies

Operation of Cryptography

Key management:

Cryptography is a tool to transform the problems of confidentiality, authenticity and integrity to key management.



All nodes have responsibility:

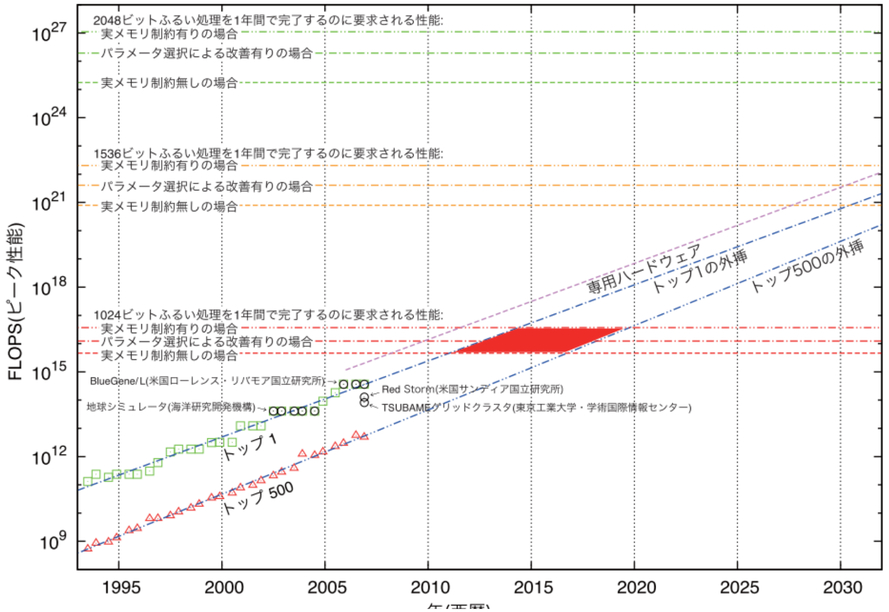
Securely manage the key

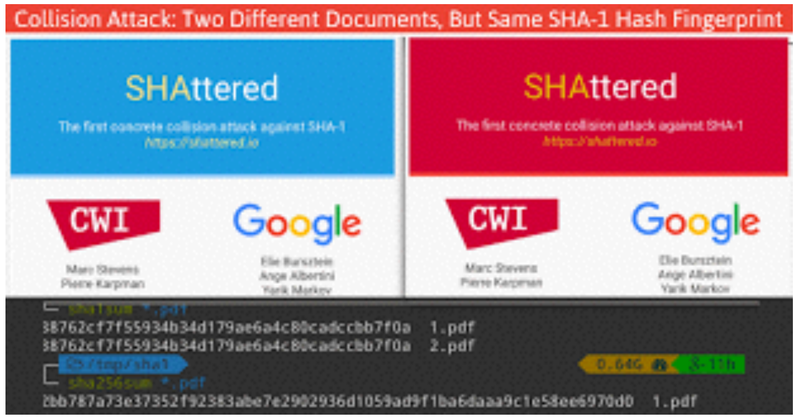
Security against cyber attack

Secure design of a system based on cryptography

Compromise of Cryptography

- Increase of computational power of adversary
  - Need to extend key length
- Finding vulenrbiility of cryptographic algorithm
  - Case of SHA1
- Need transition of underlying cryptography
  - Long-term Signature (ETSI standard)





Several huge incidents

Mt. Gox

The DAO Attack

Coincheck

Selfish Mining

Monacoin

Zaif

Zaif

What is “the Cryptocurrency Exchange?”

No uniformed definitions and models

Revisit what Satoshi proposed

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.

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.

Mind the gap between Payment and Settlement!

Satoshi's border

Without Trusted Party
(nearly equal to
"decentralization")
Prevent double spending

With trusted party

Other functionalities of
currency

Payment system

Settlement system

More applications

Cryptocurrency Exchange

Gaps between Satoshi's paper and real

- There is no exchange to Fiat Currency in the ecosystem
  - Everything is closed inside Bitcoin ecosystem
- All participant has equal computational power
- Lack of consideration of Governance

The case of “the DAO”

Lose 150M Dollars by this attack.

Caused by vulnerability of the code

The way of workaround is still not decided.

Problems

Vulnerability handling

Procedure for work around

Over-investment to uncertified technology and codes

Intersection of technology and financial incentive

Governance and regulation issues

- **Bitcoin = New economical nation**
  - Mathematics of Bitcoin = (economical) Constitution of the nation
  - Current chaos of governance: Lack of procedure of amendment of constitution
  - Branching of Bitcoin: independence with new constitution
- **How do we think the new economical nation?**
  - Decentralized Virtual Currency (for greater innovation) vs. stable virtual currency

Source of technology related immaturity

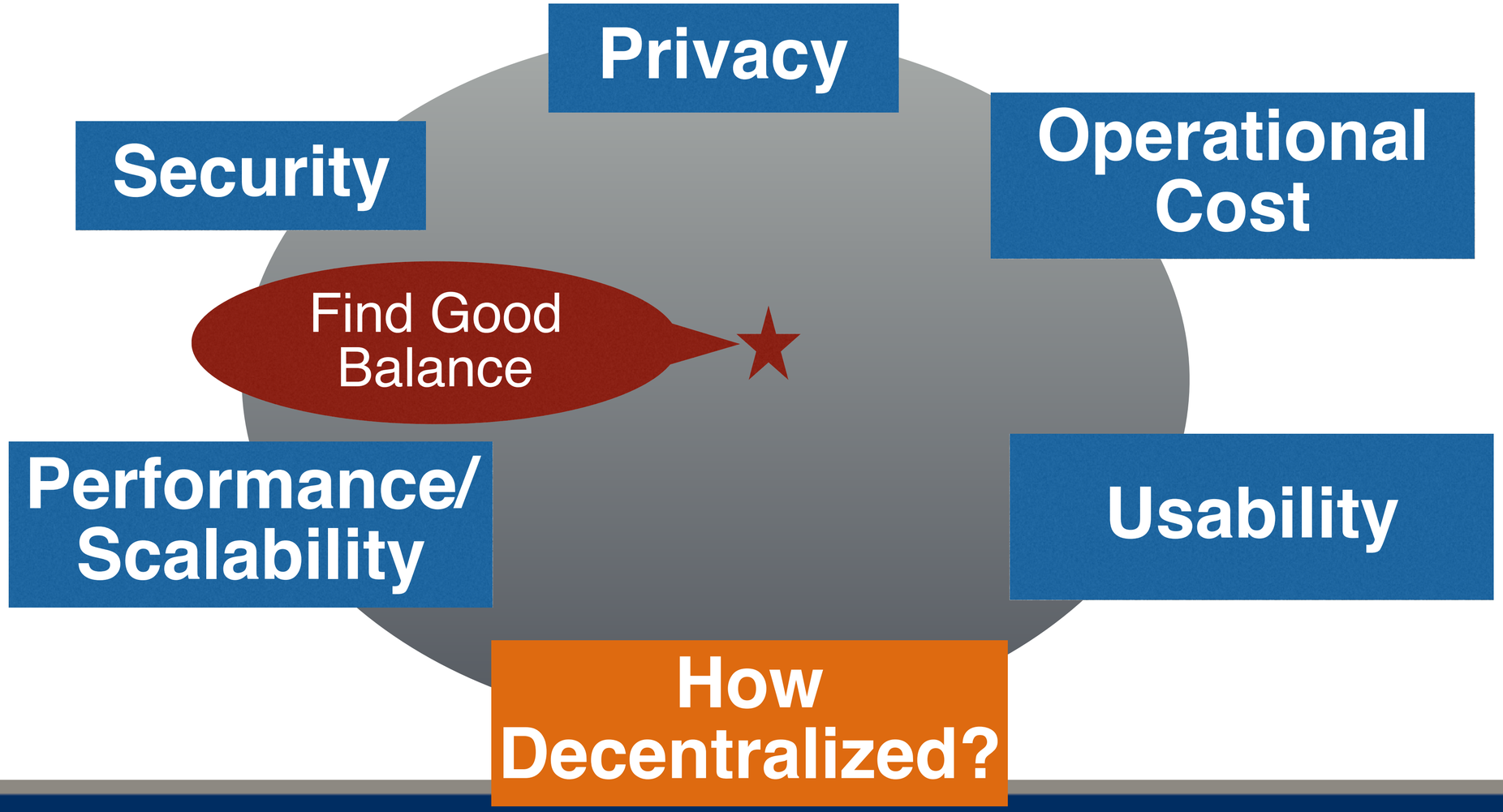
Unproven technology
- Security
- Scalability
- Trust model

Community Risk and Quality assurance
- Need healthy community and ecosystem

Lack of evaluation criteria toward technological due-diligence
- Standardization

Gap between
- What original Satoshi paper proposes and
- Expectation to Blockchain technology and its application

Trade-offs in Bitcoin and Blockchain Technology



Technology Issues of Current Blockchain

Cryptography and Cryptographic Operation

Secure System Design and Operation

Trade-off between Performance/Scalability and "De-centralization"

Finality and Immutability

+ Need healthy community and ecosystem by designing better incentive/economic model

Can we create a model for such cryptographic applications?

Provable Secure Blockchain with Proof of Stake [KKRDO16]

Prove Two Requirements of Blockchain

Persistence and Liveliness [GKL15]: Robustness of the Blockchain

Propose Provable Secure Protocol

Use Multi-Party Coin Flipping for leader election to produce randomness

Many Assumptions

Highly Synchronous
Majority of Selected Stakeholder is available
The Stakeholders do not remain offline for a long time

Number of nodes matters

- Source of security $t < \frac{n}{2}$
- Realized by incentive design: rewarded coin and game theory
- Source of redundancy and performance trade-off

Operation is one of the sources of security

- Bug in Bitcoin software (before 0.16.2): CVE-2018-17144 (September 19, 2018)
  - Shutdown
  - Lead to issue over 21,000,000 BTC! Needs update at all node.
- An issue in migration process
  - Needs over 51% equivalent good miners to avoid 0-day
  - Can we assume it?

Warren Togami liked

Matt Corallo @TheBlueMatt · 1h

This is what happens when people fetishise "decentralization" without considering what it's even there for. At this point, upgrade your own node -> problem solved for you. Who cares about Bob's long-forgotten Raspberry Pi node?

> **Luke Dashjr** @LukeDashjr
> Ugh, 87% of the #Bitcoin network is *still* vulnerable to CVE-2018-17144. Every day this goes on, we are trusting miner(s) and lose credibility with the decentralised network claim. 😐
>
> Show this thread

7 5 42

Trust model

- Application specific trust model depends on
  - Stakeholders
  - Goals of stake holders
  - Which stakeholder is trustable
- Need to consider flexibility of trust model

THE WAY FORWARD

Game theory/ incentives / regulation

The Security of Bitcoin/ Cryptocurrency/Public Blockchain relies not only on technology but also on incentive design.

Some flaws in the current design of Bitcoin ecosystem are the cause of debates and chaos.

Regulation: Recent hot topic

Needs for multi-disciplinary research

Games in blockchain ecosystem

Reconsider Blockchain as a “Slow-network”

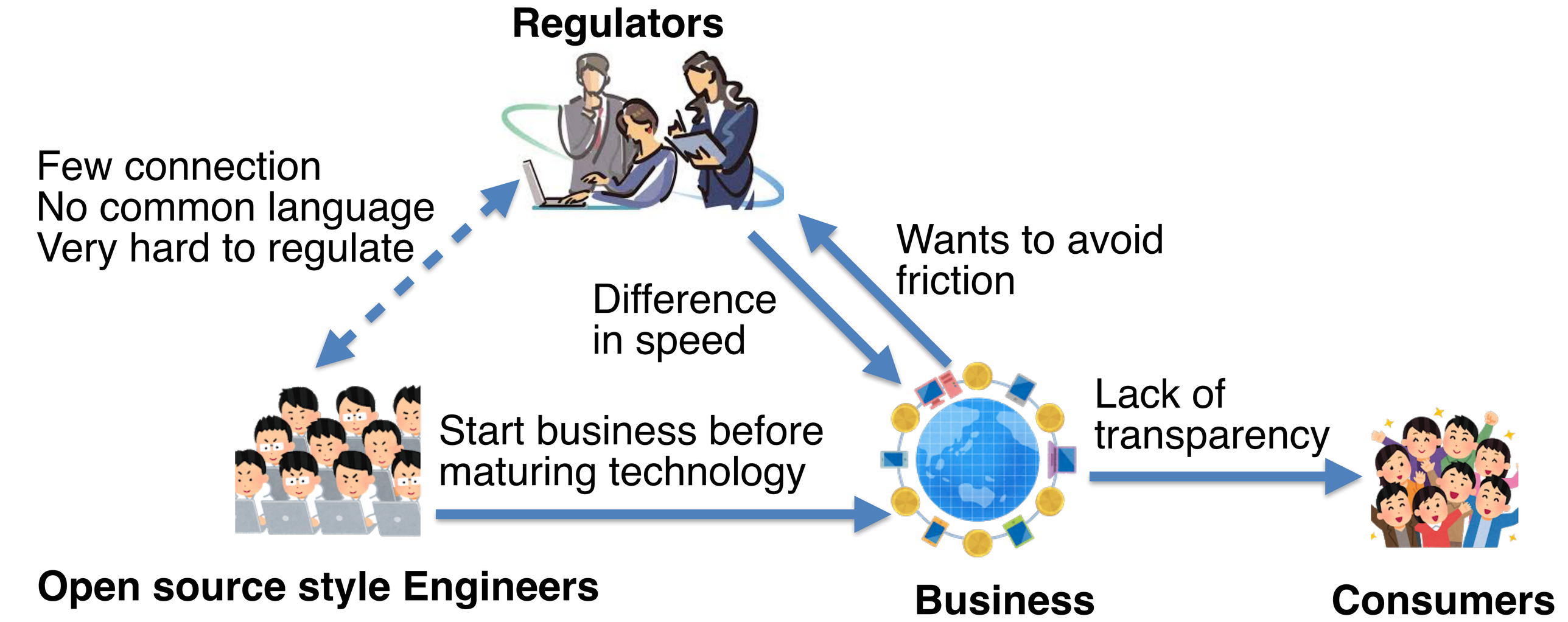
The Internet is called as “Stupid-network”.

End to End Principle
Let the ends do it
Let the user decide
Too redundant but produces permission-less innovation

Blockchain is a “slow network”

10 minutes block interval : for security and from DNS and the Internet limitation
Let collaboration of over 51% nodes do it
Too redundant but eliminate tampering and produces permission-less innovation

Relationship among Stakeholders and Problems



Better Conversation to Grass-root and Agile-Innovation Friendly Governance

Need to have better incentive designs among stakeholders

- Common place
- Common Language
- Harmonized incentive

Standard in the next era:

Criteria to have common understandings

- Lessons from the Internet: ISOC, IETF, ICANN, etc.
- ISO Standardization: Technical reports on Security for Digital Asset Custodians

Internet Society

IETF

ICANN

NSFNet for the Internet

ARPANET

CSNet

Research Networks (NSFNET)
Non-Profit

Externalizing Costs
Commercial ISPs
Making $$$

1969

1981

1985

CIX Association
1991

April 30th 1995

1977

1995

Berkeley Software Distribution (BSD)

NSFNET T3 Network 1992

BSafe.network: Plays the same role as NSFNet and BSD

- **A neutral, stable and sustainable research test network for Blockchain technology by international universities.**
- **Founded by me and Pindar Wong in March 2016. Each university becomes a blockchain node.**
- **Research on Blockchain and its applications**
  - **Not limited to Security. All aspects will be researched.**

- Neutral platform
- de-anchored trust of Blockchain network
- More nodes (with Neutrality)
- Testbed for academic research

65

Why is university the good place?

The place for experiments

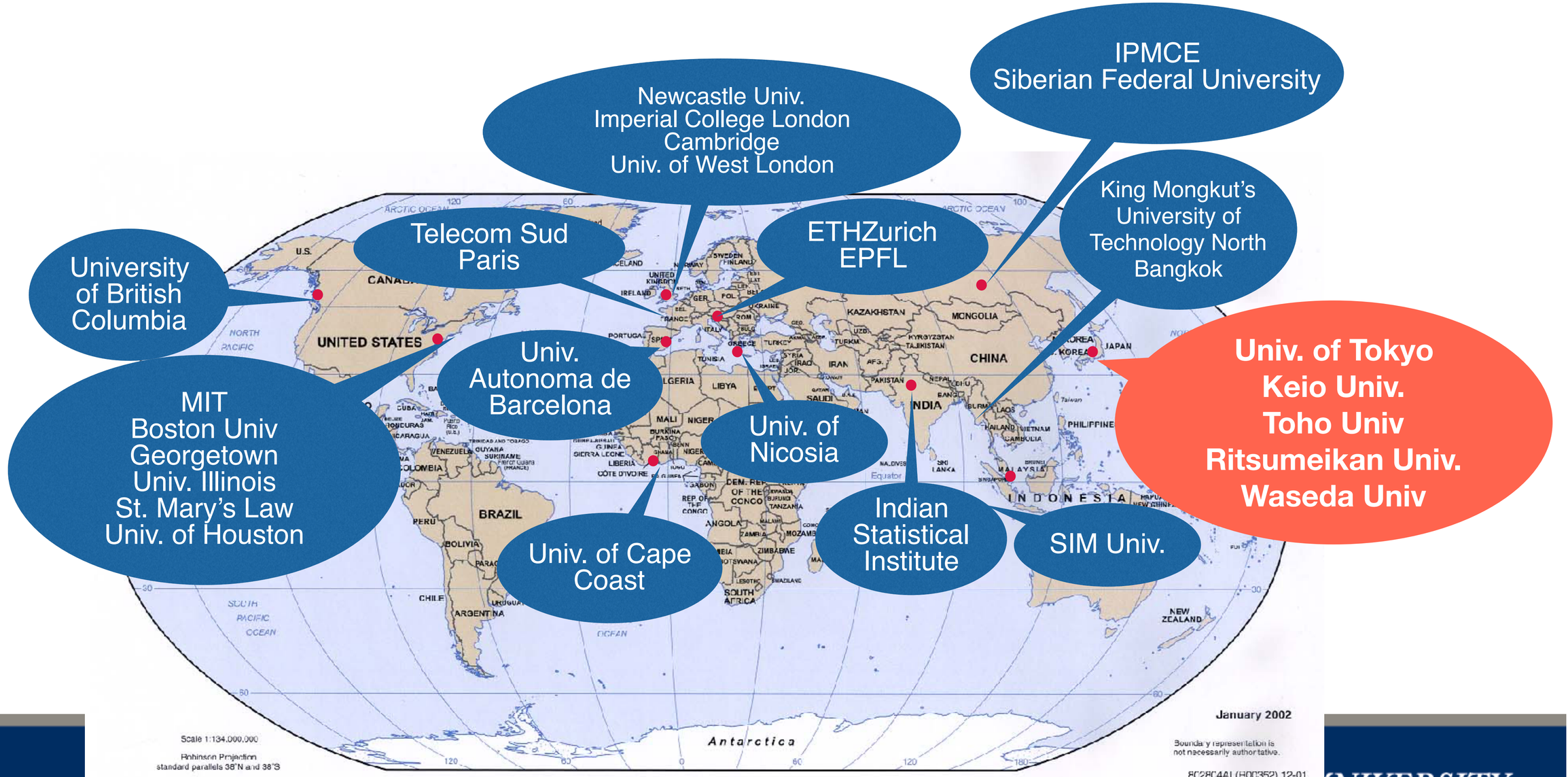
The place of neutrality

The place of diversity

The place of international collaboration

The number of university: > 15K, scalable!

28 International Universities Already Join and We Add More…



Scaling Bitcoin 2018 Tokyo

- A Series of workshops to enhance bitcoin technology
- The place where good new technological advances are presented
  - 2015 Montreal: Lightning
  - 2015 Hong Kong: Segregated Witness
  - 2016 Milan: TumbleBit, MimbleWimble
  - 2017 Stanford: FlyClient, etc
- Scalability, privacy, game-theory, …
- Will be held **in Tokyo** October 6 and 7
- An associated event: Bitcoin Edge Dev++

Theme of this year: Kaizen

改善

- A Japanese word registered in Oxford dictionary. and US version of Wikipedia. It represents Japanese culture on precision engineering.
- Let us “Kaizen” Bitcoin and Blockchain technology!

Definition of *kaizen* in English:

kaizen

NOUN

[mass noun]

A Japanese business philosophy of continuous improvement of working practices, personal efficiency, etc.

+ Example sentences

Origin

Japanese, literally ‘improvement’.

Pronunciation

kaizen /kʌɪˈzɛn/

Cryptographic protocols become assets

Top 100 Cryptocurrencies By Market Capitalization

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$115,491,556,027	$6,681.98	$4,212,082,918	17,284,037 BTC	-0.29%	
2	Ethereum	$24,858,593,288	$243.37	$1,660,372,286	102,141,198 ETH	0.96%	
3	XRP	$22,491,151,240	$0.564976	$1,155,154,088	39,809,069,106 XRP *	1.51%	
4	Bitcoin Cash	$8,437,464,829	$485.90	$387,348,508	17,364,450 BCH	0.81%	
5	EOS	$5,384,195,486	$5.94	$654,713,161	906,245,118 EOS *	-0.46%	
6	Stellar	$5,287,800,077	$0.281424	$299,768,394	18,789,416,663 XLM *	18.27%	
7	Litecoin	$3,557,301,622	$60.89	$305,952,911	58,422,231 LTC	0.60%	
8	Tether	$2,802,278,852	$0.998524	$2,766,905,441	2,806,421,736 USDT *	0.00%	
9	Cardano	$2,325,313,887	$0.089687	$145,207,143	25,927,070,538 ADA *	8.55%	
10	Monero	$1,986,556,816	$120.90	$48,992,051	16,431,240 XMR	-0.97%	

115B USD!

https://coinmarketcap.com

Cryptography and security research are forced to deal with elusiveness. Let us start multi-disciplinary research to secure future ecosystem.

Thank you!

GEORGETOWN UNIVERSITY