How Formal Methods and Analysis Help Security of Entire Blockchain-Based Systems

Shin'ichiro Matsuo

MEMOCODE/FMCAD 2017 Tutorial

GEORGETOWN UNIVERSITY

Outline of this talk

1. Blockchain technology and Blockchain-based systems
2. Security of Blockchain-based systems
3. How we can apply formal analysis/verification

About me

@Shanematsuo

- Research Professor at Georgetown University
- Director’s Liaison for Financial Cryptography at MIT Media Lab

- Co-Founder of Bsafe.network (Blockchain Research)
- Founder of CELLOS Consortium (Evaluation of Cryptographic Protocols)
- Program committee and editor: Scaling Bitcoin, IEEE, ACM conferences, Ledger Journal and more…
- Ph.D. from Tokyo Institute of Technology

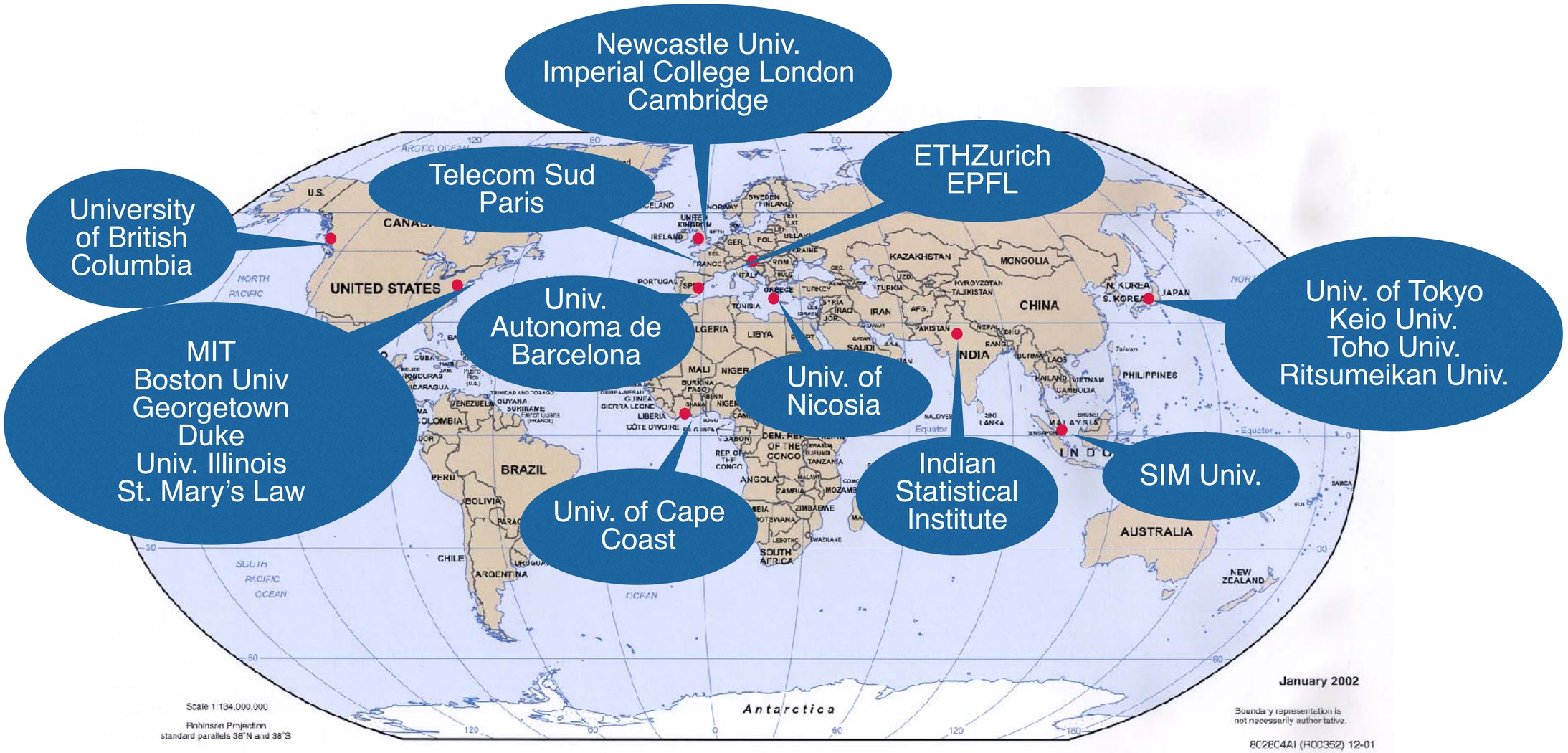
BSafe.network: Plays the same role as NSFNet and BSD

- **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**

4

23 International Universities Already Join and We Add More…



CELLOS: An International Consortium for evaluation of Cryptographic Protocols

CELLOS
Cryptographic protocol Evaluation toward Long-Lived Outstanding Security

- Organize working groups from researchers, protocol designer and vendors.
- Discuss on the evaluation results and their adequacy.

University, Research Institutes, …

Vendors

Check by Expert

Evaluation by Expert

Online Discussions

Evaluation results

Papers

Evaluation method, tools

New Theory Method

Tools

Update evaluation method in evaluation system

Update evaluation results DB

The action example against POODLE

Date/Time (JST)	Action
Oct. 14, 18:39	Find new in the Twitter and reported to the online discussion system. Discussed on the impacts.
Oct. 15, 14:04	Started editing a prompt report
Oct. 15, 14:04	1st draft of the prompt report
Oct. 15, 21:48	2nd draft of the prompt report Add important descriptions on attacking condition and impacts
Oct. 15, 22:20	3rd draft, add product names
Oct. 15, 22:20	Edit both English and Japanese version
Oct. 15, 22:52	Publish the 1st prompt report
Oct. 15, 23:09	Add information on new version of OpenSSL
Oct. 16, 10:07	Correct editorial errors

BLOCKCHAIN TECHNOLOGY AND BLOCKCHAIN-BASED SYSTEM

The Most significant keyword of Blockchain

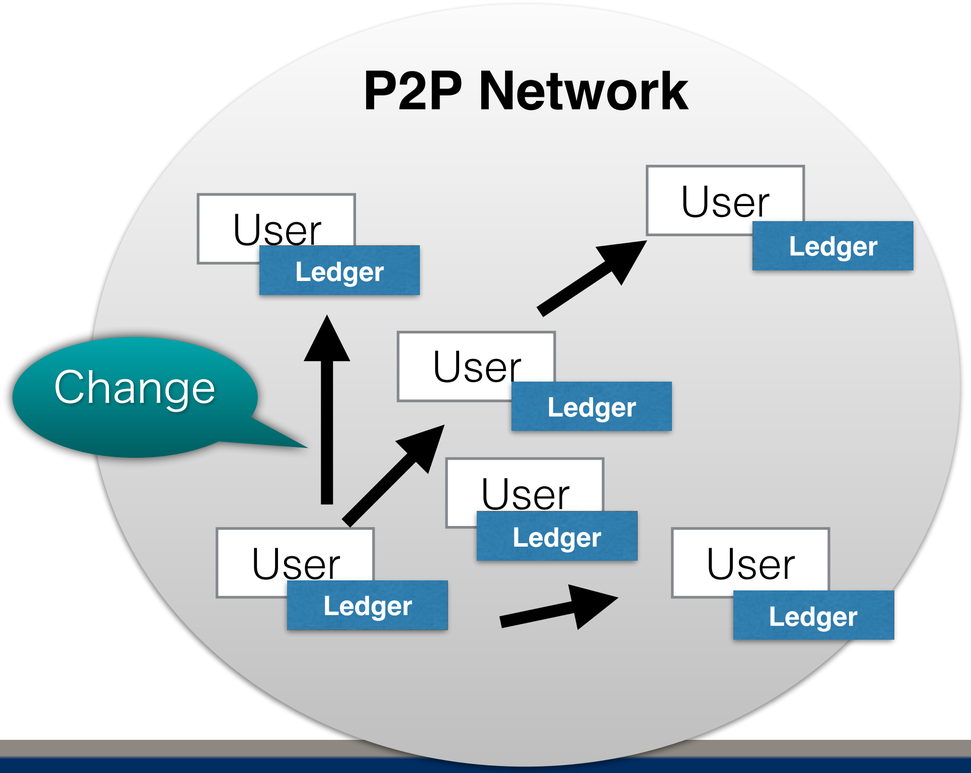
De-centralization

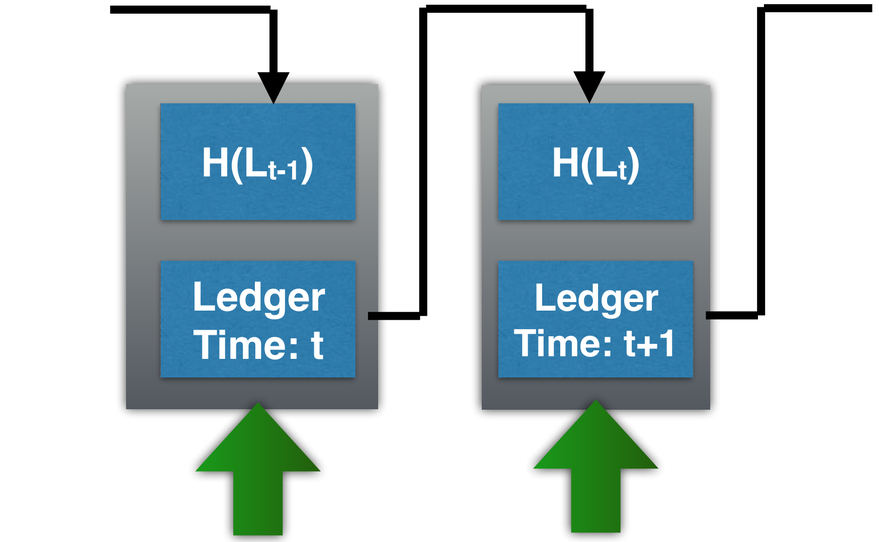
Telephone, postal mail	vs.	The Internet
.Net /C# (Microsoft)	vs.	Java Applet
Proprietary	vs.	Open Source

Blockchain

- Fundamental techniques to realize “Public Ledger” using P2P network and chained digital signature
- Used in digital currencies like Bitcoin
- Anyone can join/leave at any moment

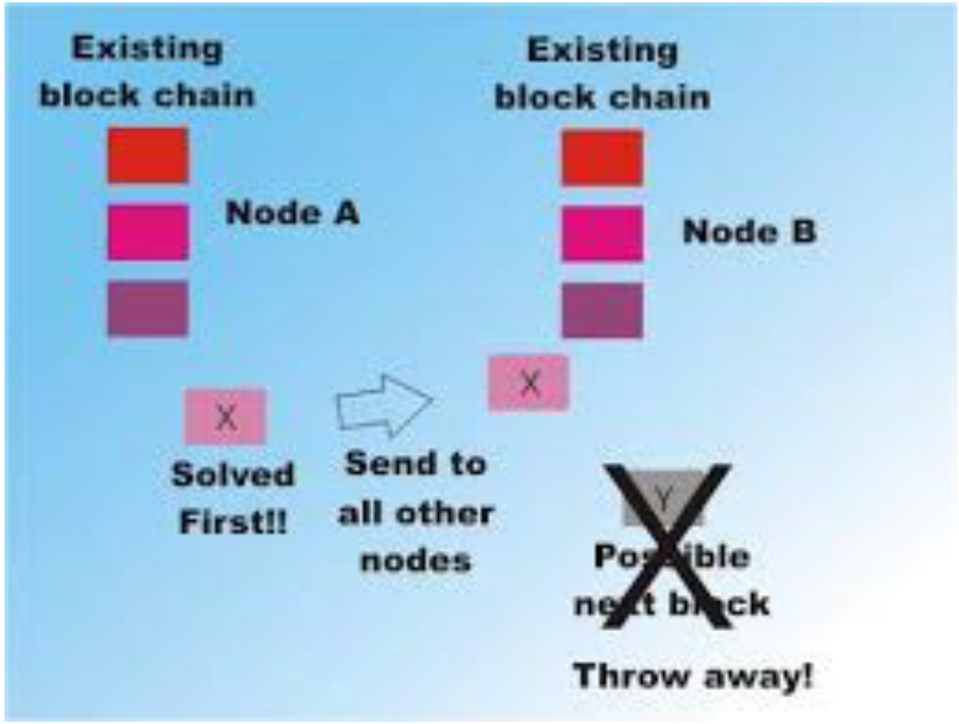
Each node updates its distributed ledger





Proof of Work (PoW)

- A consensus mechanism in Bitcoin Blockchain
- Competition among P2P nodes (miners), which try to solve cryptographic puzzle
  - Finding a data of which hash value fulfills some conditions (difficulty)
- Winner of PoW gains a certain amount of Bitcoin every 10 minutes. (12.5 bitcoin = 5,500 USD)
- Transform power for attacking to power for maintain system



Example of Proof of Work (PoW)

Finding Hash value start with “0000”

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

How Mature?


Experimental
Technically Confirmed
Commercialization
New Applications/ Ecosystem

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

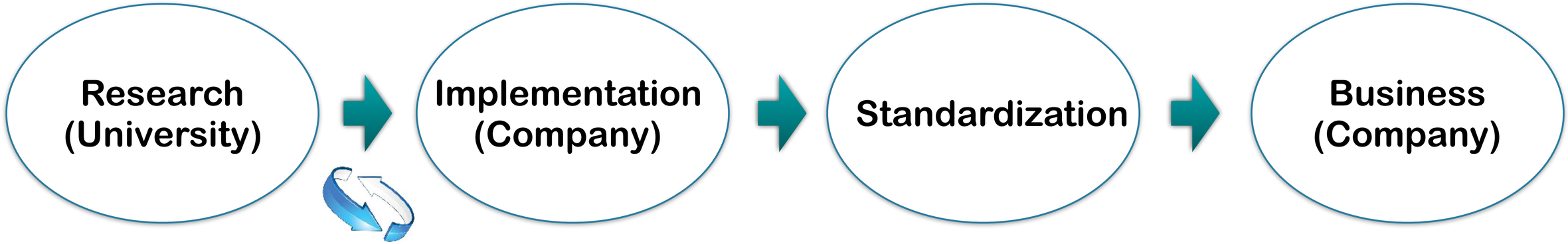
1977 — 1995

Berkeley Software Distribution (BSD)

NSFNET T3 Network 1992

Academic Research is still needed

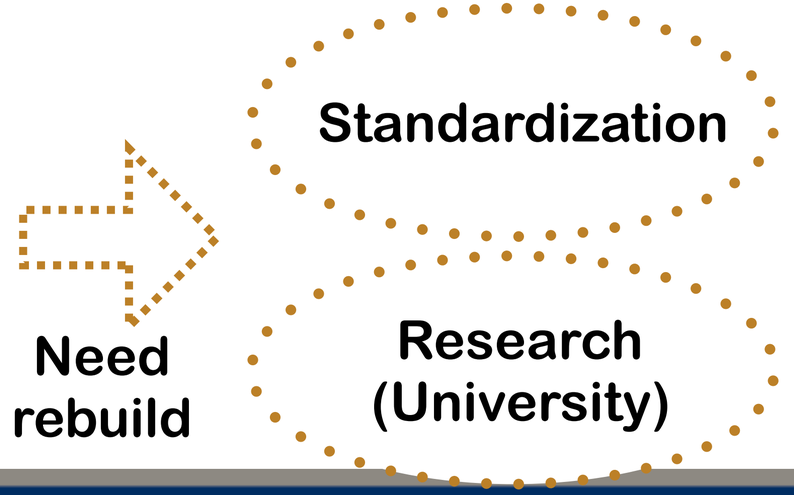
The Case of Internet Technology



"BSD" and open-source facilitated innovation

The Case of Bitcoin and Blockchain

Innovation by iteration

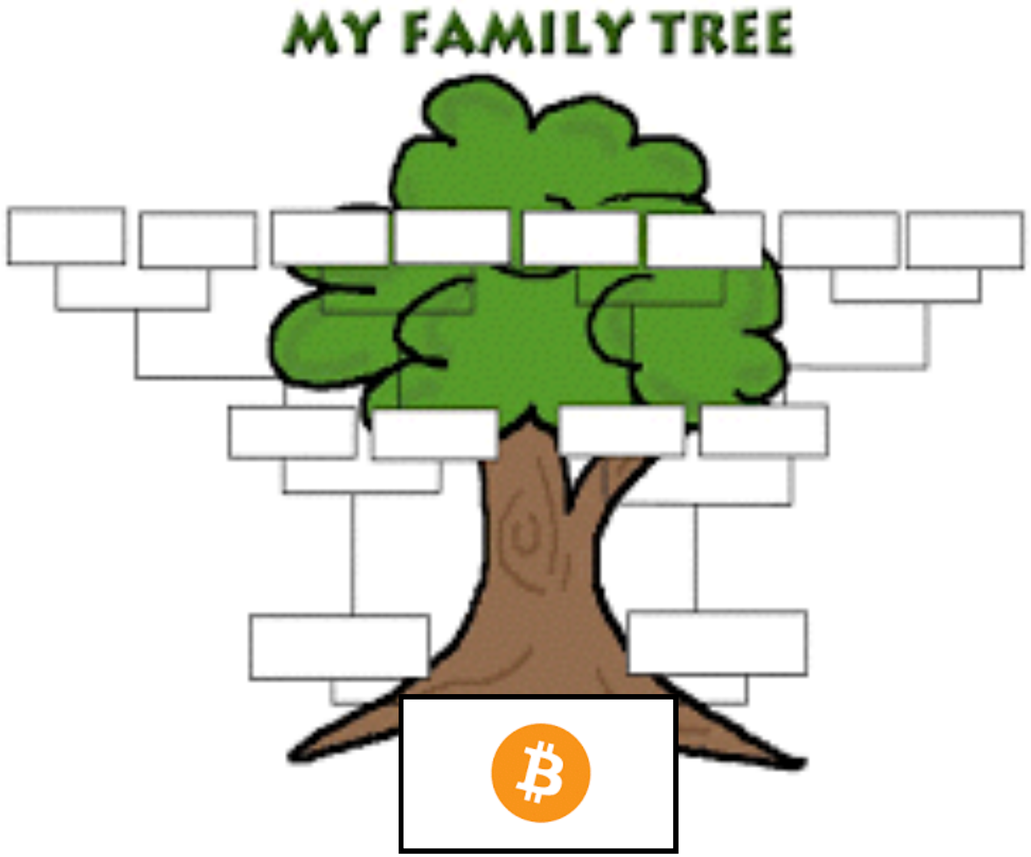


Is Blockchain really secure?

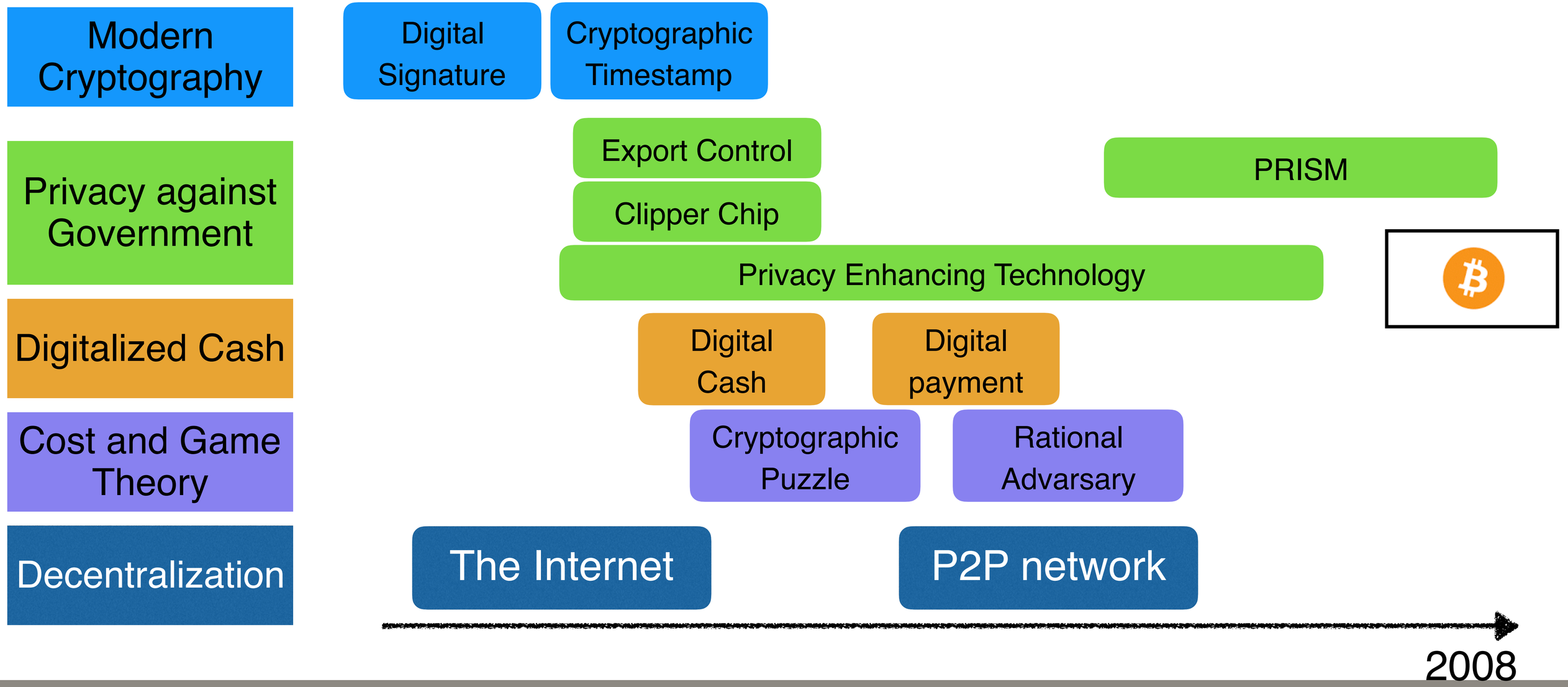
- **Who does verifies/certificates/proofs the security of Blockchain?**
  - **No-one does.**
- **Formal security definitions and fine-grained technical requirements for entire systems?**
  - **No.**
- **Trustless by Cryptography?**
  - **No. Sharing responsibilities by multiple stakeholders, technology and operations.**

How Did Bitcoin/Blockchain Born?

Entirely new invention?



Chronology Before Bitcoin



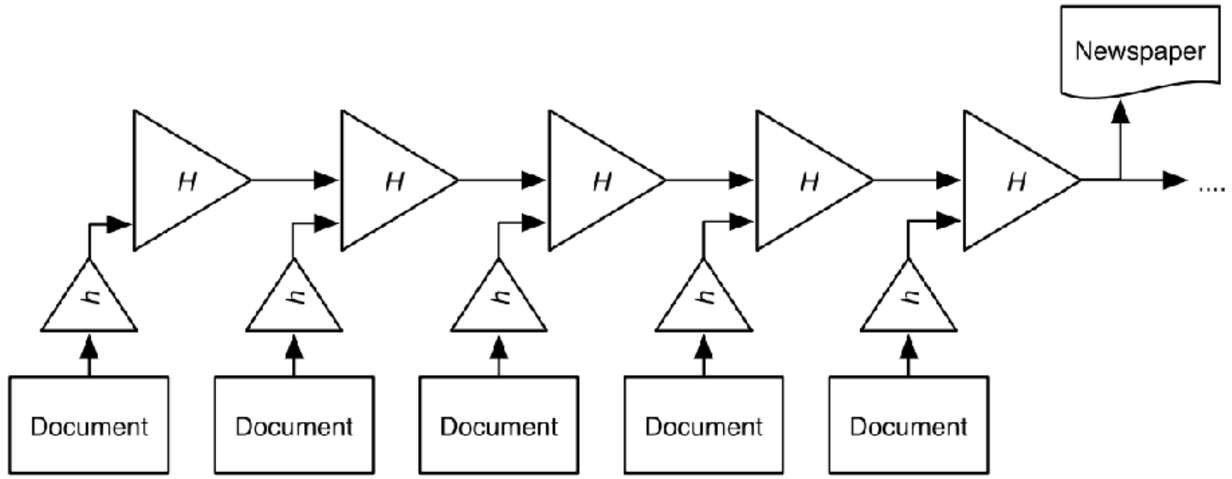
Where the Data Structure of Blockchain Came From… (1990)

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



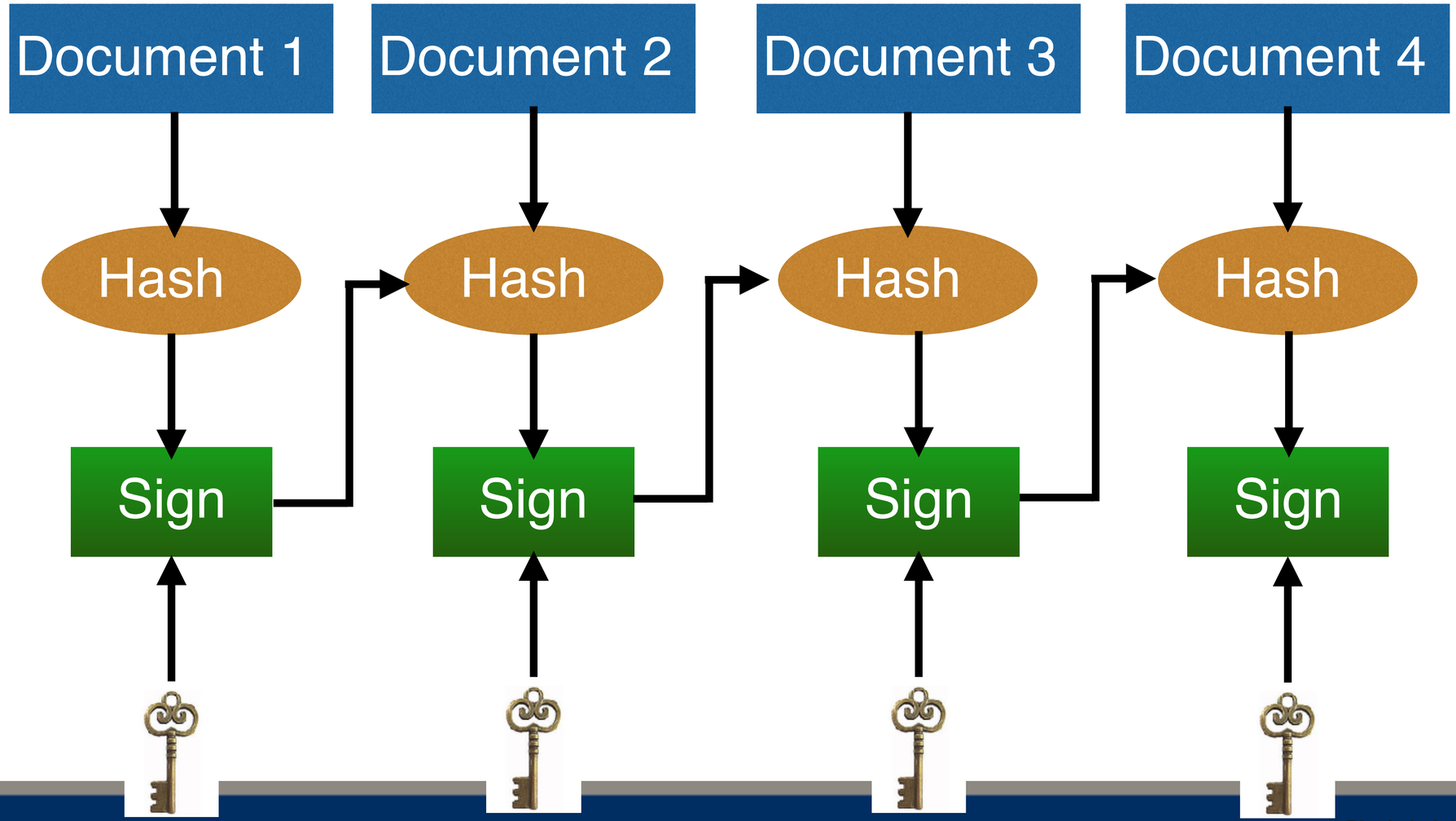
But needs centralized server

Blockchain's today and tomorrow are scholers of yesterday.

]Shin'ichiro Matsuo, Ph..D.

GEORGETOWN UNIVERSITY

Hysteresis Signature was Invented in Japan (2002)



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

Needs centralized server

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.

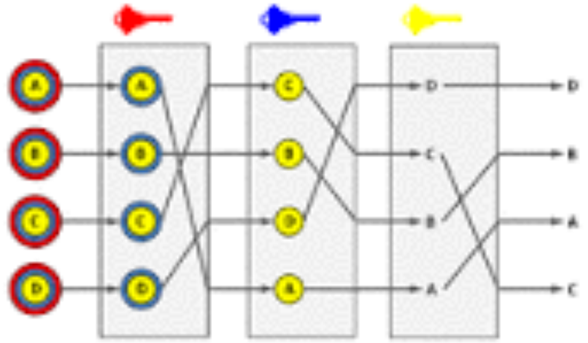
Free from export control of cryptography

Tax Haven

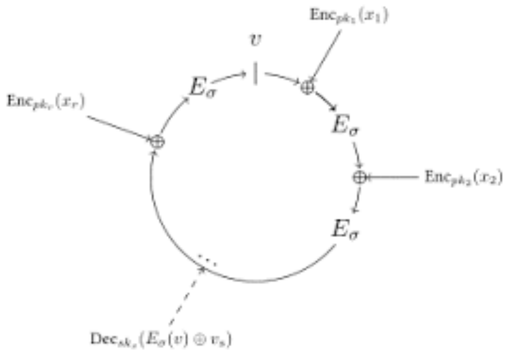
Initiated by Cypherpunk

Privacy Enhancing Technologies

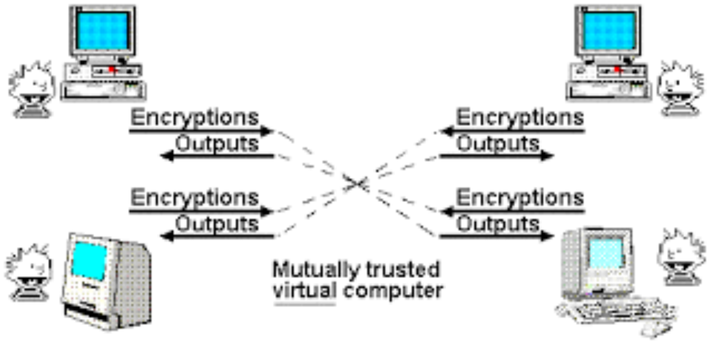
Blind Signature



Mix-Net/Tor



Group Signature/Ring Signature



Multi Party Computation

History of Research on Digitalized Cash (’90s)

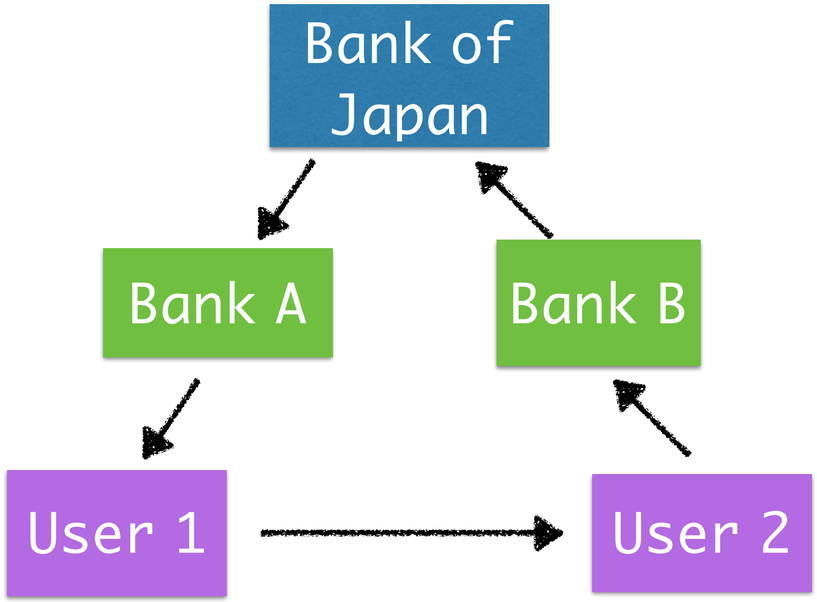
David Chaum

Stephan Brands

Visa Cash

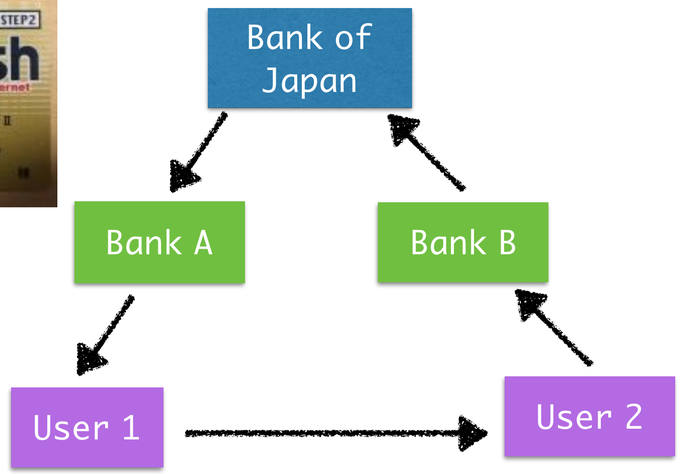
MONDEX

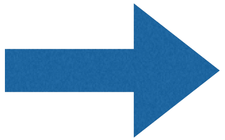
Internet Cash by Bank of Japan and NTT (1997-2000)

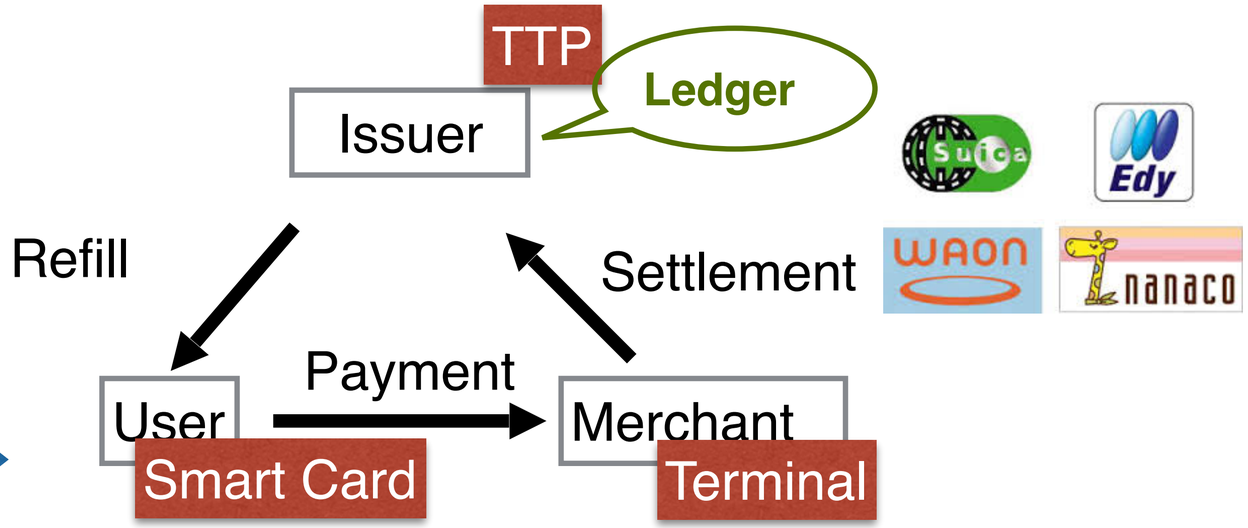


- Implement “Cash” issued by the “Bank of Japan”
- Transferable thorough e-mail attachment
- Multi-currency

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

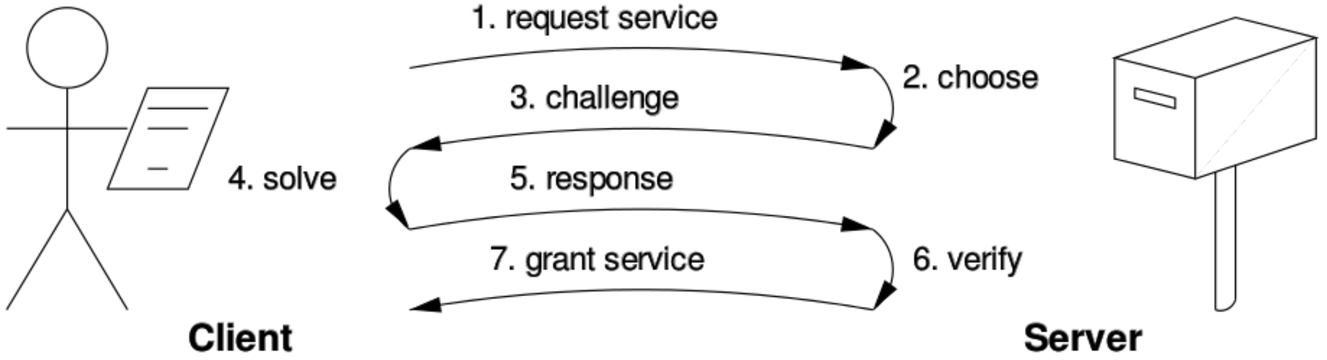
Add Cost to Attack: Cryptographic Puzzle

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.



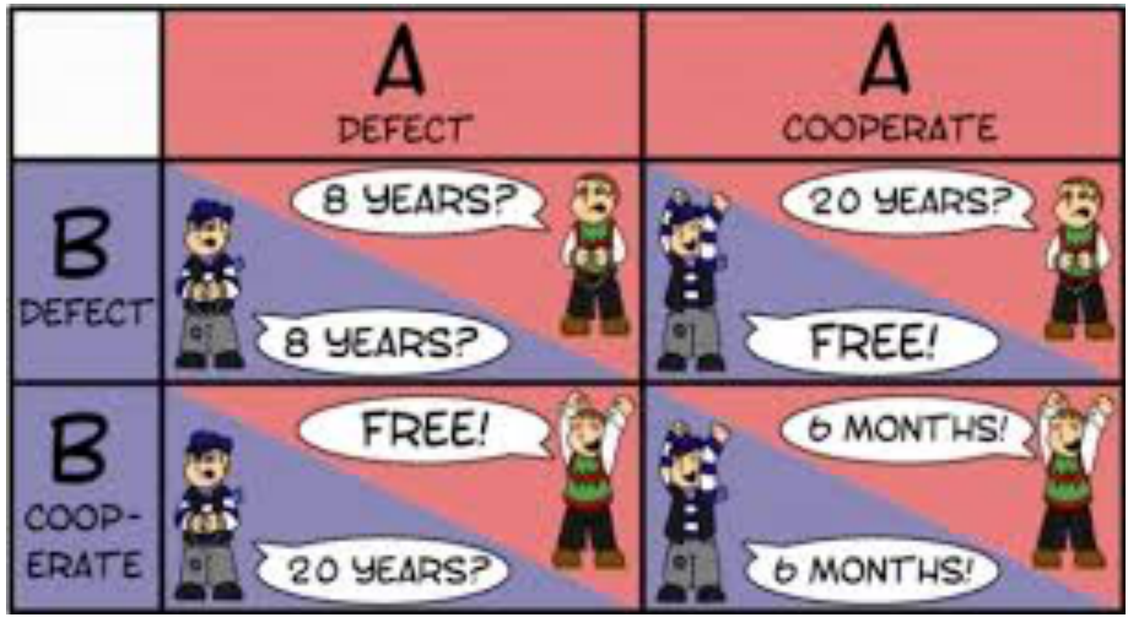
Cryptography and Game Theory (2002-)

Sealed-bid Auction

Vickrey Auction and (M+1) - price auction

Dynamic Programming and combinatorial auction

A class of Pareto Optimal



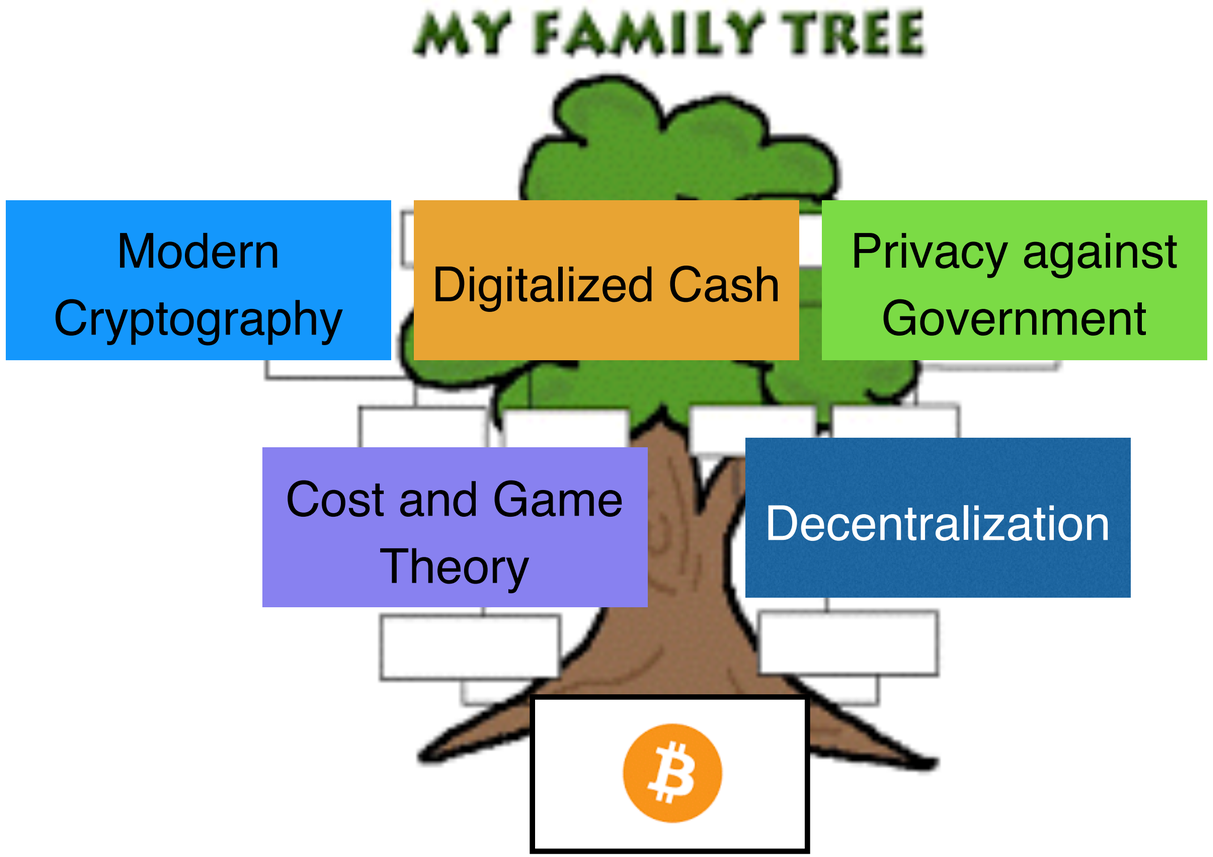
Decentralized Communication: The Internet and P2P

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

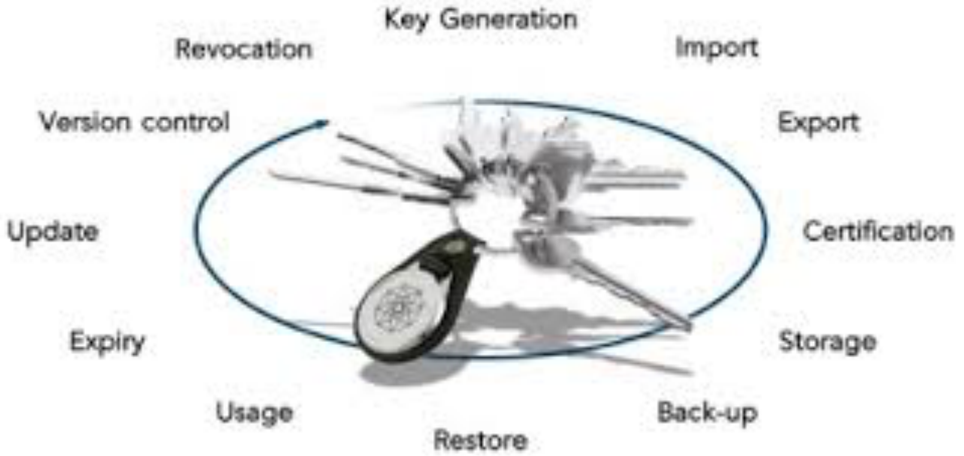
Merits of technologies

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

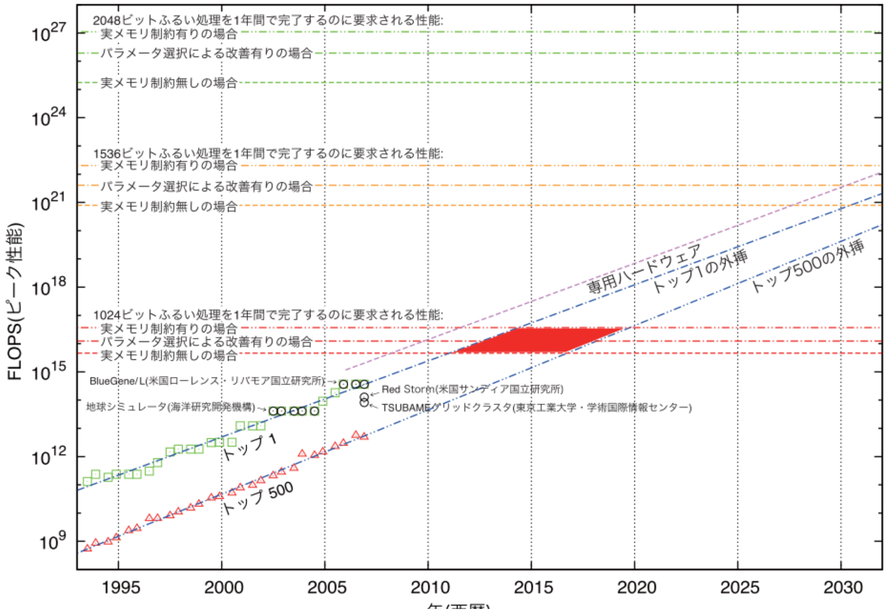
Finding vulenrbiility of cryptographic algorithm

Case of SHA1

Need transition of underlying cryptography

Long-term Signature (ETSI standard)

Impact Analysis [GCR16] by Cas Cremers et al.



Difficulty of Long-term Assurance: Time-stamp Business

Cannot stop even if the business is not profitable

In the case of public blockchain?

Can we maintain enough number of blockchain nodes for a long term?

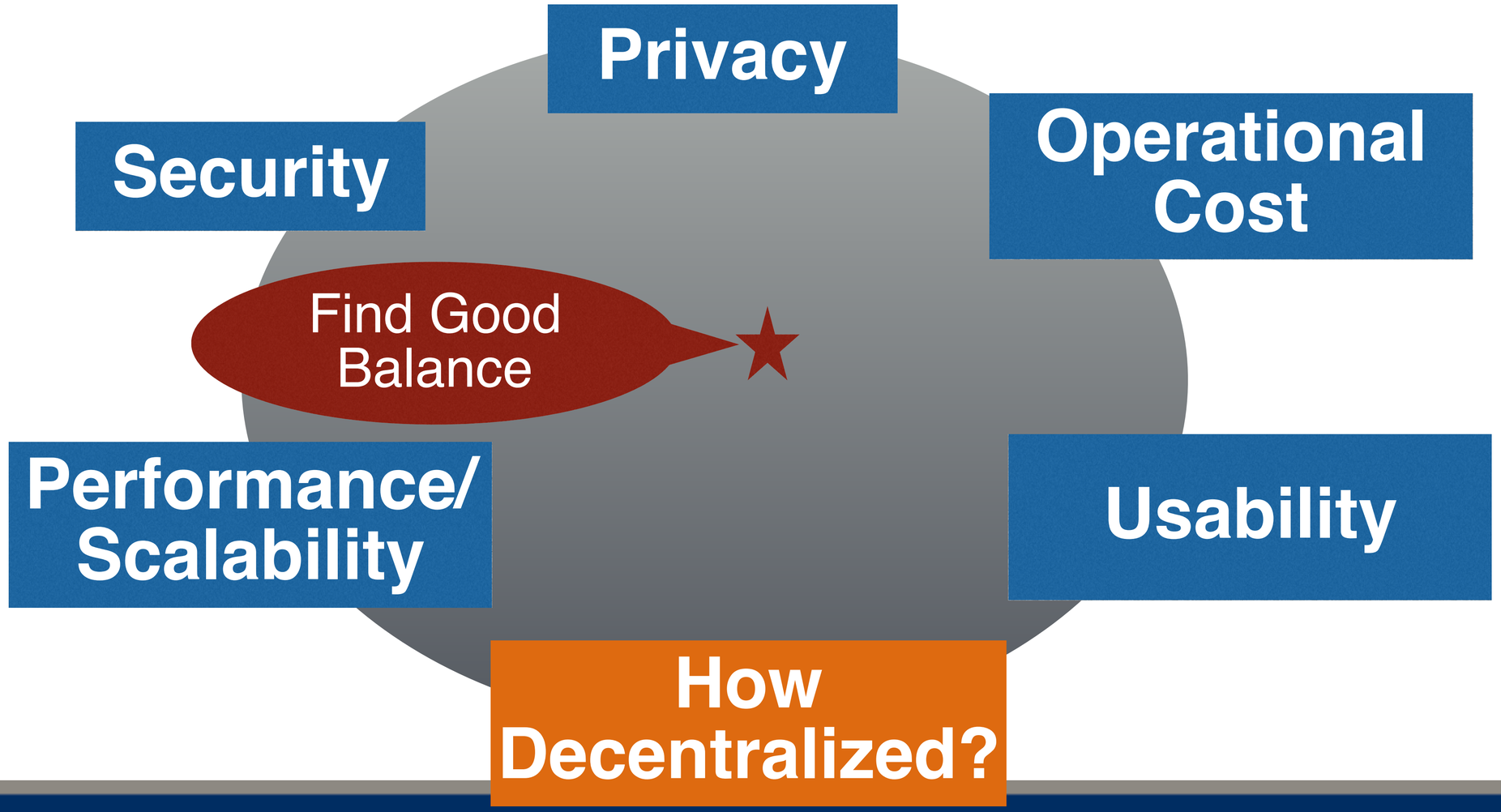
Understanding Redundancy of De-centralization

A mechanism for de-centralization is redundant.

In the Internet, the same packet is resent when the original packet is lost.

In the Blockchain, all nodes should execute chatty protocol and store the same and huge data.

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

Security economics/ game theory/ incentives

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.

Games in blockchain ecosystem

SECURITY OF BLOCKCHAIN BASED SYSTEMS

Background: The case of “the DAO”

Had chance to lose 50M 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

Security definitions of blockchain

Several Proposals on back-bone protocol

Need Consideration for Security of Entire System(?)

Security Definitions for backbone-protocol [GKL15]

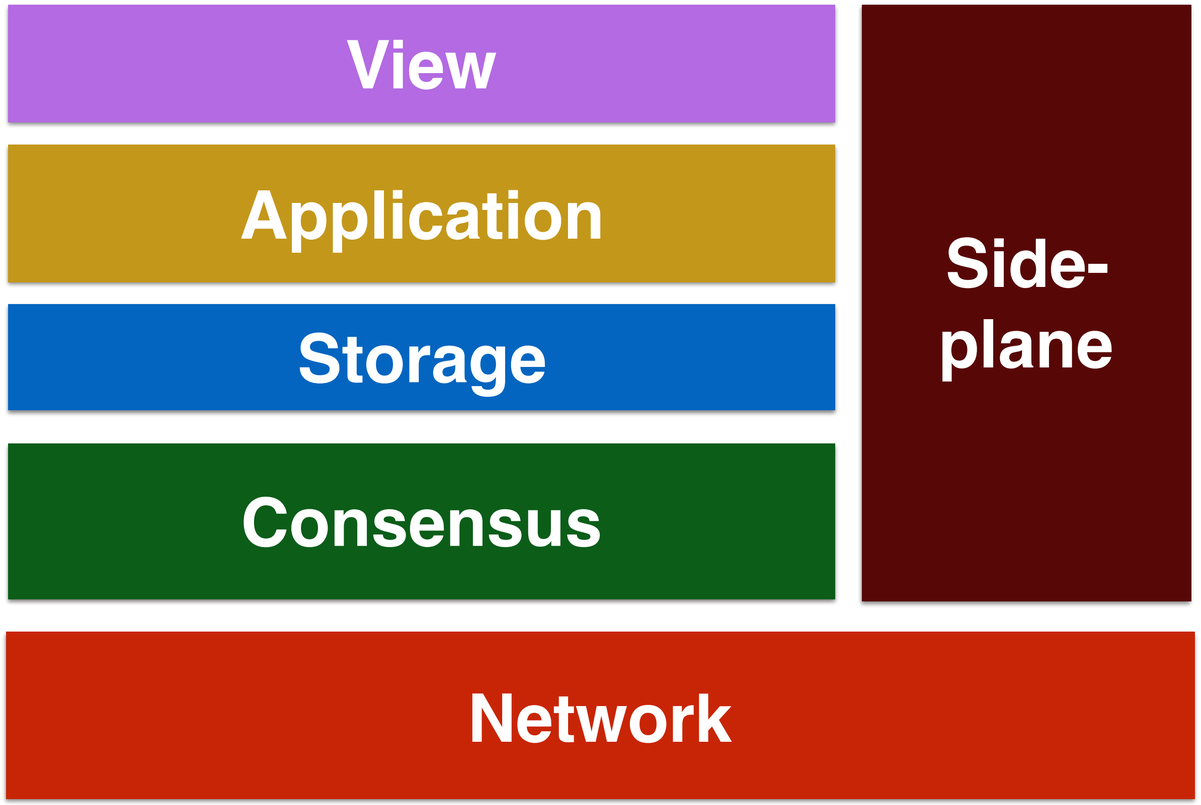
Two definitions
Common Prefix Property
If two players prune a sufficient number of blocks from their chains, they will obtain the same prefix.

Chain Quality
Any large enough chunk of an honest player's chain will contain some block from honest players.

There are results on provable secure protocol but needs assumptions [KKRDO16]

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

Example of Blockchain Technology layers [BitcoinWorkshop2016]



Network: broadcasting transactions and blocks

Consensus: the agreement-reaching engine

Storage: bootstrapping new nodes, storing archival data

Application: transaction graph, scripting language semantics

View: cached summary of the transaction log

Side-plane: off-chain contracts

Layers for security consideration

Operation	Key Management, Audit, Backup	ISO/IEC 27000
Implementation	Program Code, Secure Hardware	ISO/IEC 15408
Application Logic	Scripting Language for Financial Transaction, Contract	Secure coding guides
Application Protocol	Privacy protection, Secure transaction	ISO/IEC 29128
Backbone Protocol	P2P, Consensus, Merkle Tree	ISO/IEC 29128
Cryptography	ECDSA, SHA-2, RIPEMD160	NIST,ISO

Cryptography Layer

Security goals in Blockchain
Realizing authenticity and integrity

Digital Signature: ECDSA
Hash Function: SHA-2, RIPEMD-160
Underlying Mathematics: Secure parameter of elliptic curve

Firm analysis model

Provable Security,
Estimation of security margin

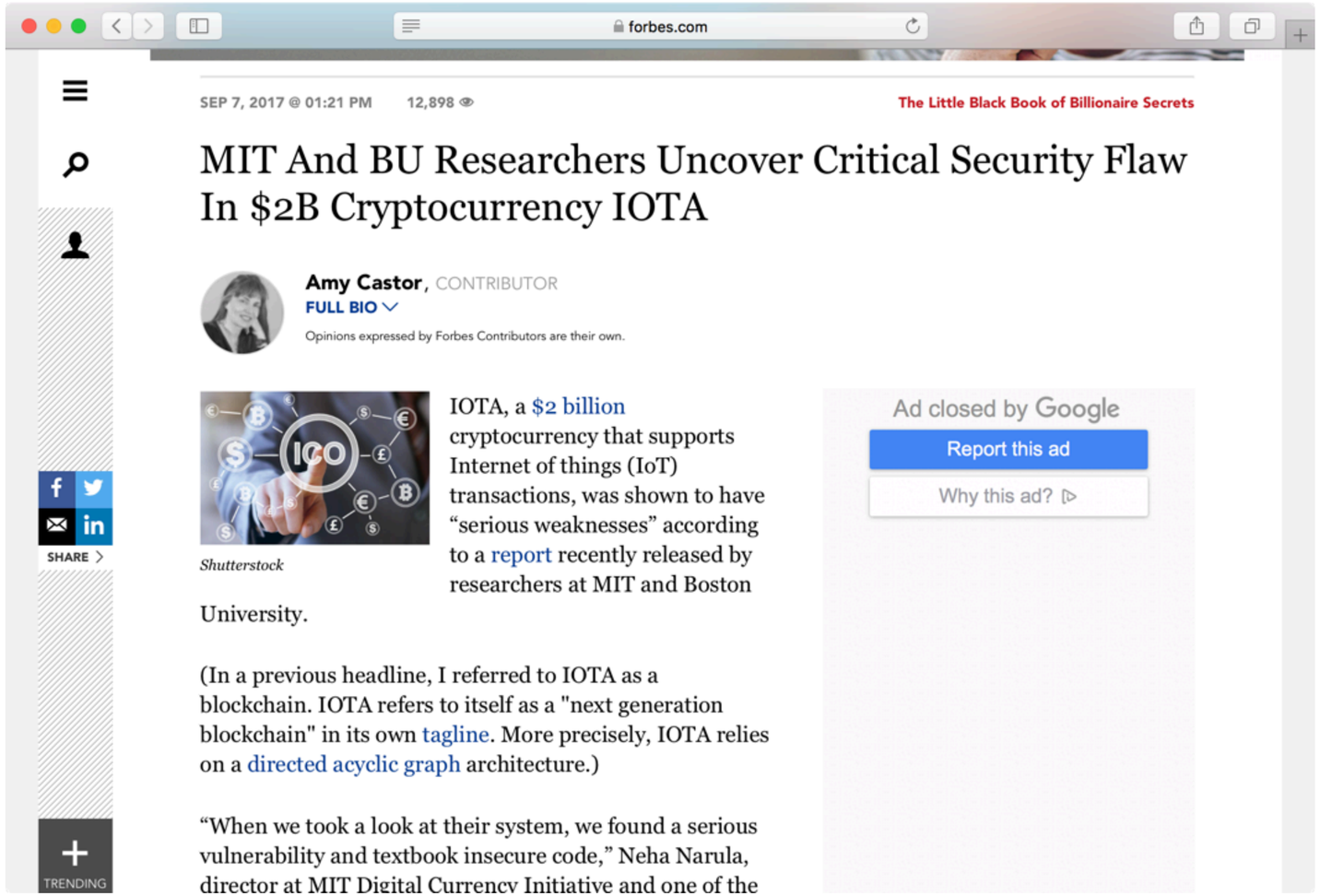
Many theoretic results and evaluations

Academic proof, Standardization by NIST, ISO/IEC, IETF(IRTF), IEEE

The case of IOTA

Use of vulnerable hash function leads vulnerability of system.

Use subset of SHA-3 instead of full SHA-3



forbes.com

SEP 7, 2017 @ 01:21 PM 12,898

The Little Black Book of Billionaire Secrets

MIT And BU Researchers Uncover Critical Security Flaw In $2B Cryptocurrency IOTA

Amy Castor, CONTRIBUTOR
FULL BIO
Opinions expressed by Forbes Contributors are their own.

Shutterstock

IOTA, a $2 billion cryptocurrency that supports Internet of things (IoT) transactions, was shown to have "serious weaknesses" according to a report recently released by researchers at MIT and Boston University.

(In a previous headline, I referred to IOTA as a blockchain. IOTA refers to itself as a "next generation blockchain" in its own tagline. More precisely, IOTA relies on a directed acyclic graph architecture.)

"When we took a look at their system, we found a serious vulnerability and textbook insecure code," Neha Narula, director at MIT Digital Currency Initiative and one of the

SHARE

TRENDING

Backbone Protocol Layer

Security goals in Blockchain

Realizing de-centralization and robustness by P2P network
Realizing consistency of transaction by consensus algorithm
Ensuring order of transaction by Merkle hash tree

Security definition, requirements and evaluation

No fixed security definition (researches are ongoing)
Evaluation by mathematical proof or formal analysis

Standard for evaluation

ISO/IEC 29128 for cryptographic protocols

Application Protocol Layer

Security goals in Blockchain

Privacy Protection
Secure data transmission
Secure transaction

Security definition, requirements and evaluation

Need application specific security definition
Evaluation by mathematical proof or formal analysis

Standard for evaluation

ISO/IEC 29128 for cryptographic protocols

Application Logic Layer

Security goals in Blockchain

Soundness and completeness in application logic

Security definition, requirements and evaluation

Checking the existence of bug

Abstract of the DAO case

The DAO is a project for Decentralized Autonomous Organization, an extreme application of smart contract, based on Ethereum Platform.

Ethereum Platform uses Solidity scripting language.

Two accounts:
- **Externally owned account: controlled by Human**
- **Contract account: controlled by code**

Action is trigged by transaction or message set off by externally owned account

Action
- **transfer or trigging of contract code**
- **Contract can trigger other contract code**

Abstract of the DAO case

When contract calls or sends money to other contract code, invoking call function.

When calling another contract, the call function provides specific function identifier and data.
When sending money to another contract, the call function has set of amount of gas (transaction fee) but no data. Thus triggers fallback function.

Abstract of the DAO case

Fallback function: does not take any argument and trigged in three cases

1) **If none of the functions of the call to the contract match any of the functions in the called contract**
2) **When the contract receives ether without extra data**
3) **If no data was supplied**

Abstract of the DAO case

Example:
we have two contracts: (i) the contract Bank (vulnerable contract) and (ii) the contract BankAttacker (malicious contract).

(1)The hacker does is send ether (75 wei) to the vulnerable contract through the *deposit function* of the malicious contract. This function calls the *addToBalance function* of the vulnerable contract.

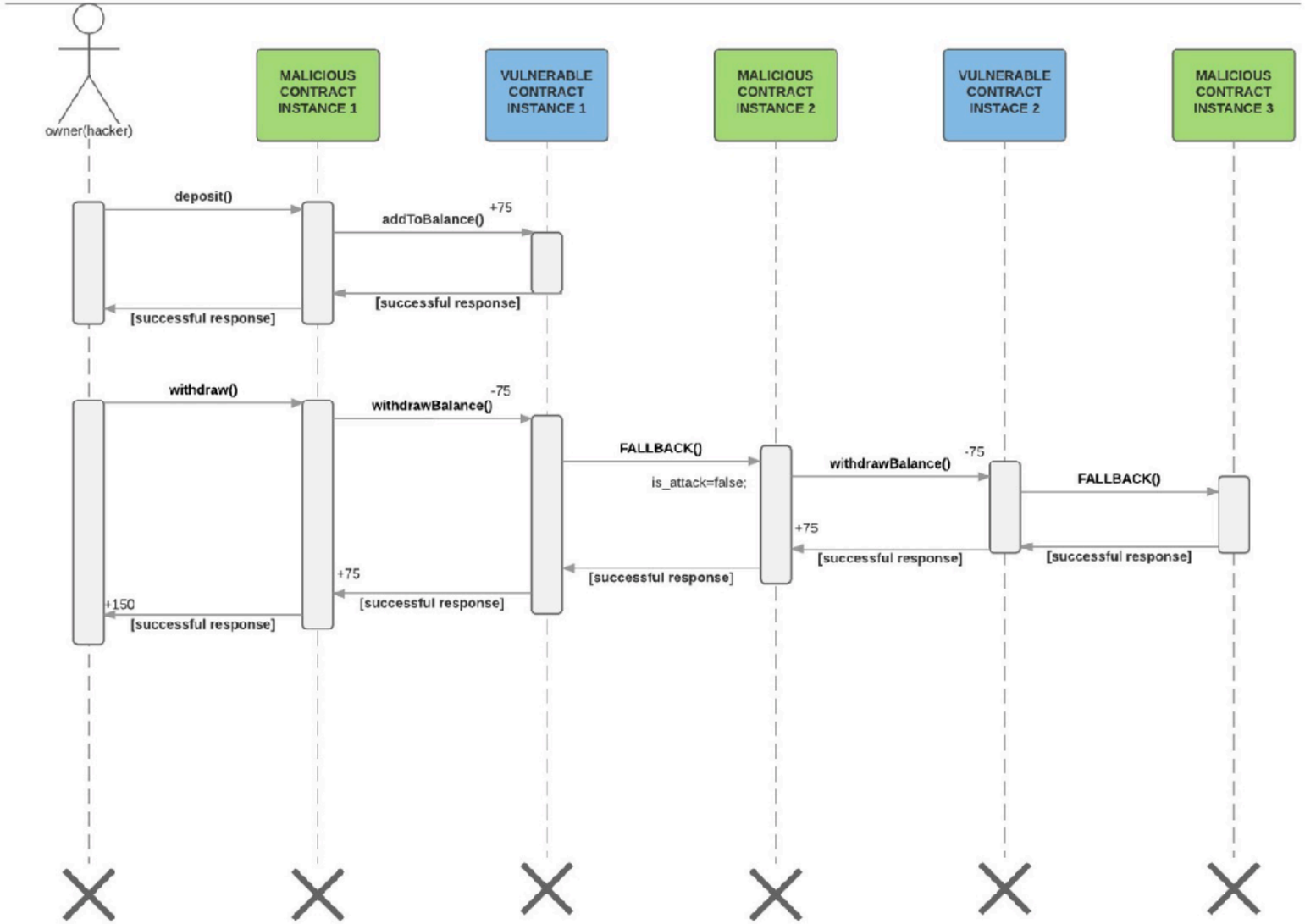
(2) The hacker withdraws, through the *withdraw function* of the malicious contract, the same amount of wei (75), triggering the *withdrawBalance function* of the vulnerable contract.

Abstract of the DAO case

(3) The *withdrawBalance function* first sends ether (75 wei) to the malicious contract, triggering its fallback function, and last updates the *userBalances* variable (that this piece is done last is very important for the attack).

(4) The malicious fallback function calls the *withdrawBalance function* again (recursive call), doubling the withdraw, before the execution of the first *withdrawBalance function* finishes, and thus, without updating the *userBalances* variable.

Abstract of the DAO case



Implementation Layer

Security goals in Blockchain

Protection of signing key and prevent forgery of digital signature
Against black box attacker (main channel), gray box attacker (side channel) and white box attacker (rooted device)

Security definition, requirements and evaluation

Capability of the adversary

Standard for evaluation

ISO/IEC 15408

Operation Layer

Security goals in Blockchain

Key management
Audit of operation

Security definition, requirements and evaluation

Need (unified) security policy

Standard for evaluation

ISO/IEC 27000 Series (Information Security Management System)

HOW WE CAN APPLY FORMAL EVALUATION AND VERIFICATION

Formal Analysis and Formal Verification

Formal Analysis

Evaluating the possibility of attack on the specification of the protocol, products or system by conducting some mathematical formalization of the security requirements, specifications and operational environment (an adversarial model).

Formal Verification

To verify the correctness of the specification of the protocol, products or system formal methods such as automated axiomatic theorem proving or model checking.

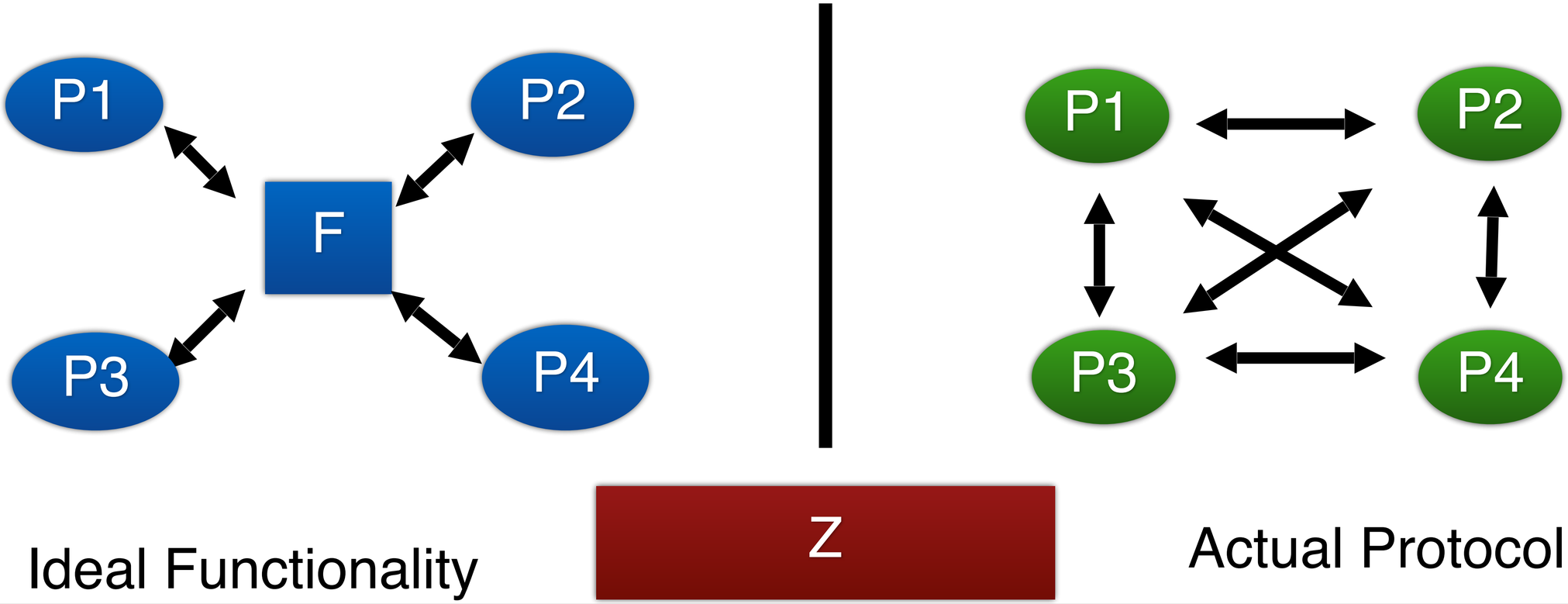
Current Results of Formal Analysis

		Formalization	Formal Analysis	
			Coq	Others
Security	Anti-double spneding	[GKL15]	[B15], [G14]	Not found
	Anti-Money Laundering	Not found	Not found	Not found
Privacy	Unlinkability	[AKRSC13]	Not Found	Not Found
	Taint-resistnat	[MO15]	Not Found	Not Found

60

Mathematical Proof: Universal Composability

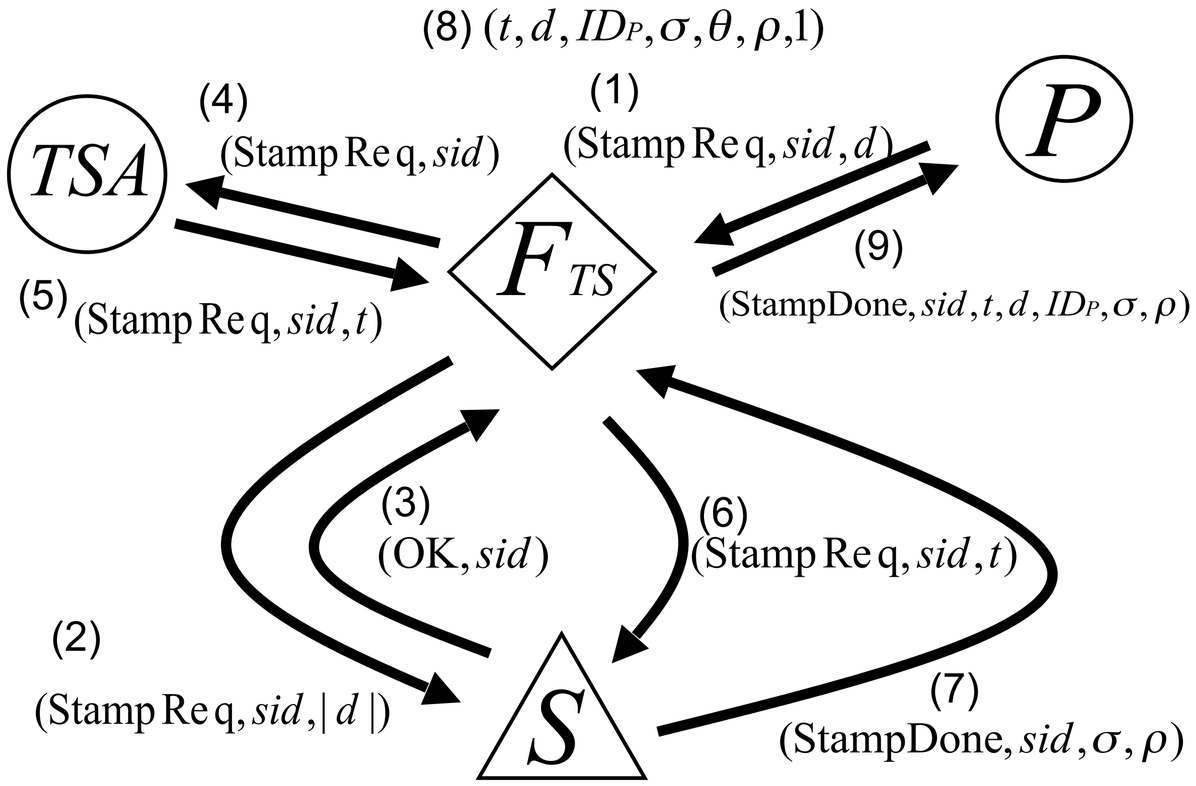
- Define the ideal functionality, then prove that the actual protocol is indistinguishable against the ideal functionality.



Universal Composability of Time-stamping protocol [MM05]

Giving Ideal Functionality of Cryptographic Timestamping

Proposal of protocol realization



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

Applicability of formal verification

Operation	Key Management, Audit, Backup	ISO/IEC 27000
Implementation	Program Code, Secure Hardware	ISO/IEC 15408
Application Logic	Scripting Language for Financial Transaction, Contract	Secure coding guides
Application Protocol	Privacy protection, Secure transaction	ISO/IEC 29128
Backbone Protocol	P2P, Consensus, Merkle Tree	ISO/IEC 29128
Cryptography	ECDSA, SHA-2, RIPEMD160	NIST,ISO

Formal analysis of Implementation

Both software/ hardware implementation

Security mechanisms which use cryptographic algorithms, protocols, random number generator and key management mechanisms

Target of Evaluation

Crypto-token wallet (Hardware/Software)

HSM (Hardware Security Module)

Examples and Standards for Implementation

<u>Industrial Standard</u>
Common Criteria (ISO 15408)
Define seven EALs (Evaluation Assurance Levels)

EAL6 requires semi formal analysis on the design and implementation
EAL7 requires fully formal analysis on design and implementation

Example of formal analysis for implementation
EAL6

FeliCa IC chip RC-SA00
Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG
Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B

Analysis of Cryptographic Protocols: Formal Verification vs UC Framework

Formal Verification

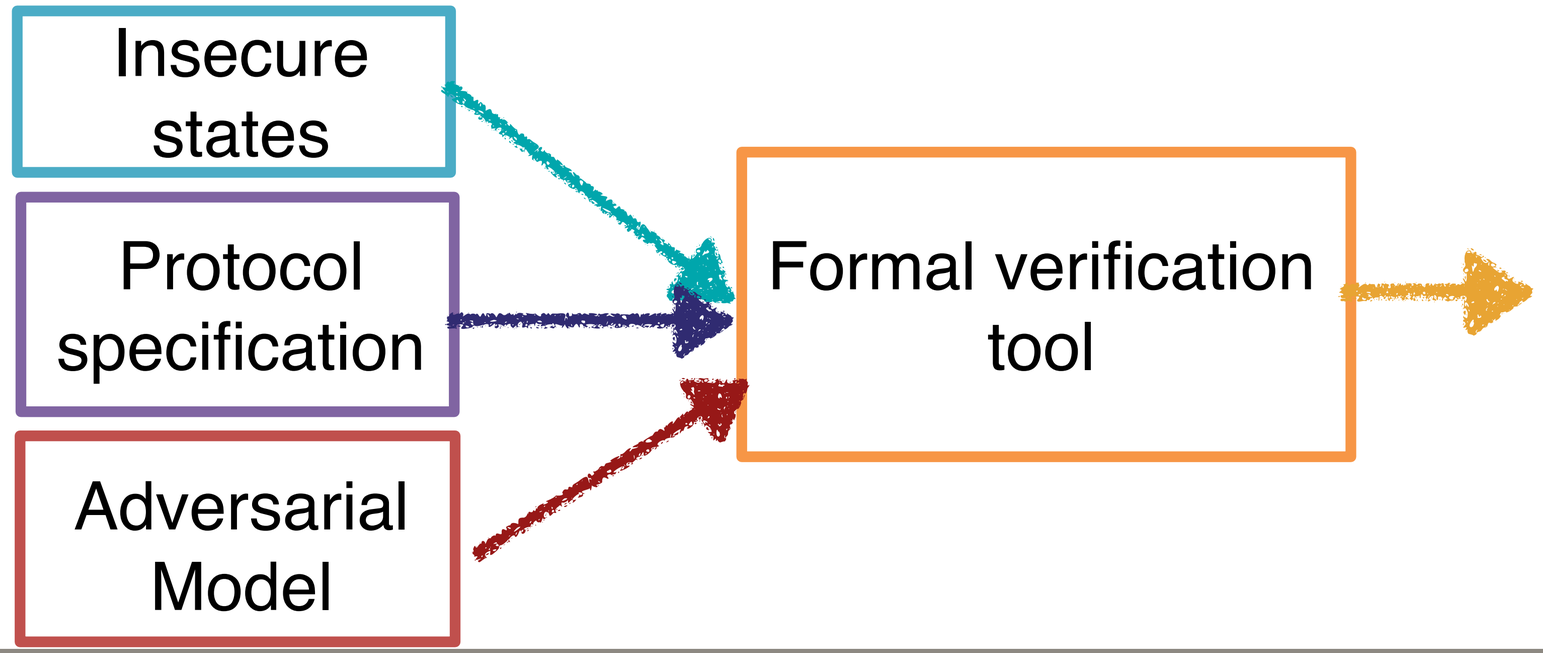
- Formal method
- Find the existence of insecure state
- Automated verification
- Tool-aided

Mathematical Proof

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

Formal Verification of Cryptographic Protocols

- Check if the insecure state may happen in execution
  - Protocol specification
  - Adversarial model
  - Insecure states to be avoided



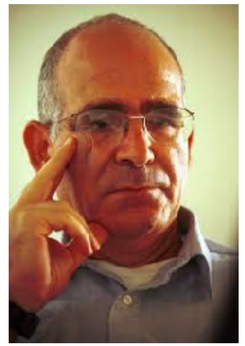
- Output if the insecure states may happen.
- If yes, output trace by which the insecure state is happen.

Formal Verification of Backbone protocols and application protocols

Explore the existence of state against security goals (Security Properties)

Dolev-Yao Model

- Basically Cryptographic algorithm is idealized
- 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.



Formal verification methods and tools

	Model checking		Theorem proving
Symbolic	NRL FDR AVISPA	SCYTHER ProVerif AVISPA (TA4SP)	Isabelle/HOL
Cryptographic		CryptoVerif	BPW(in Isabelle/HOL) Game-based Security Proof（in Coq)

Unbounded

Combination of Formal Analysis and Mathematical proof

- **Combine the merit of formal verification and mathematical rigorous proof.**
- **Many researches from 2002**
  - **Game-based evaluation**
  - **Crypto-verif**

International Standard: ISO/IEC 29128

Accuracy

Protocol Assurance Level	PAL1	PAL2	PAL3	PAL4
Protocol Specification	PPS_SEMIFORMAL	PPS_FORMAL	PPS_MECHANIZED	
Adversarial Model	PAM_INFORMAL	PAM_FORMAL	PAM_MECHANIZED	
Security Property	PSP_INFORMAL	PSP_FORMAL	PSP_MECHANIZED	
Self Assessment Evidence	PEV_ARGUMENT	PEV_HANDPROVEN	PEV_BOUNDED	PEV_UNBOUNDED

Security consideration for smart contract

Need completeness and soundness as an application logic

The DAO case was caused by bug

Checking program code is well-known application of formal analysis

Language for Smart Contract

Solidity
Flexible and General purpose language

Bhargavan et al. proposed a framework to analyze both the runtime safety and functional correctness of a Solidity contract

Introducing intermediate functional programming language suitable for verification

At this time, not covered all EVM functionalities

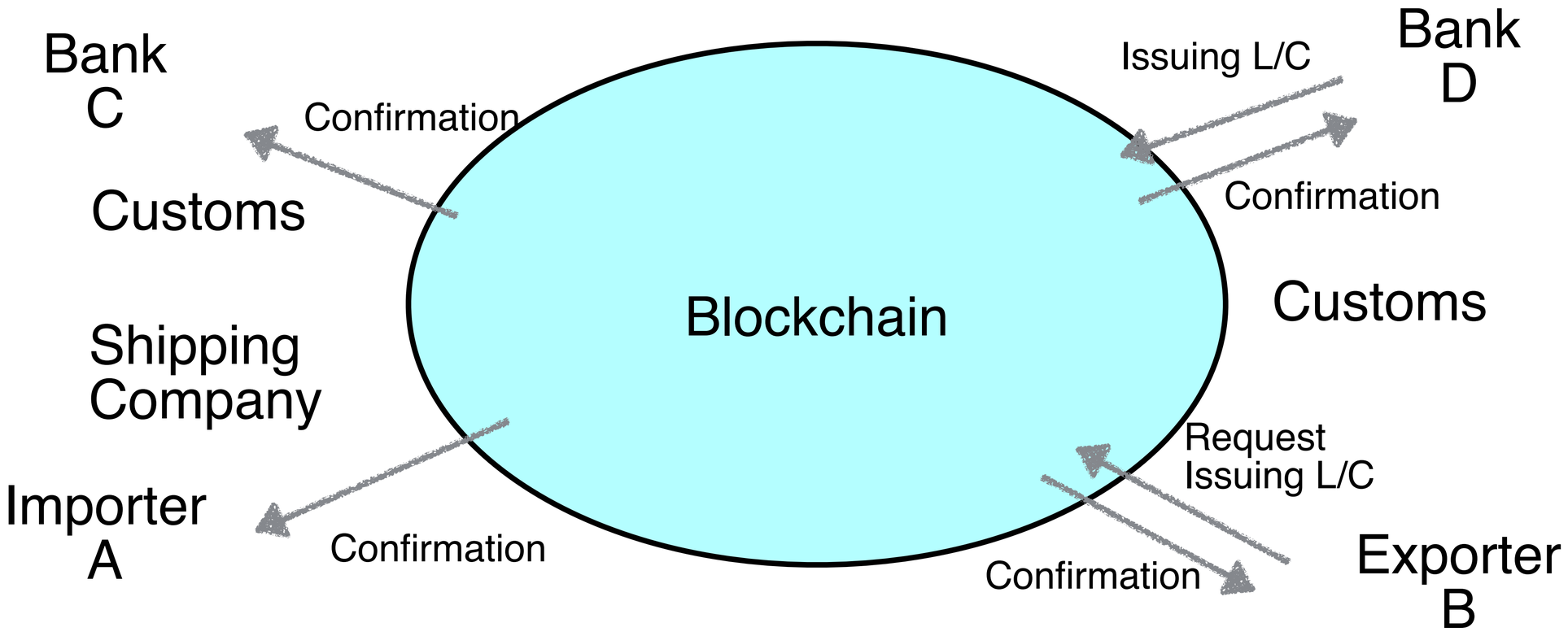
Designing Domain Specific Language

To limit possible execution states, which include “insecure” states, create new domain specific language

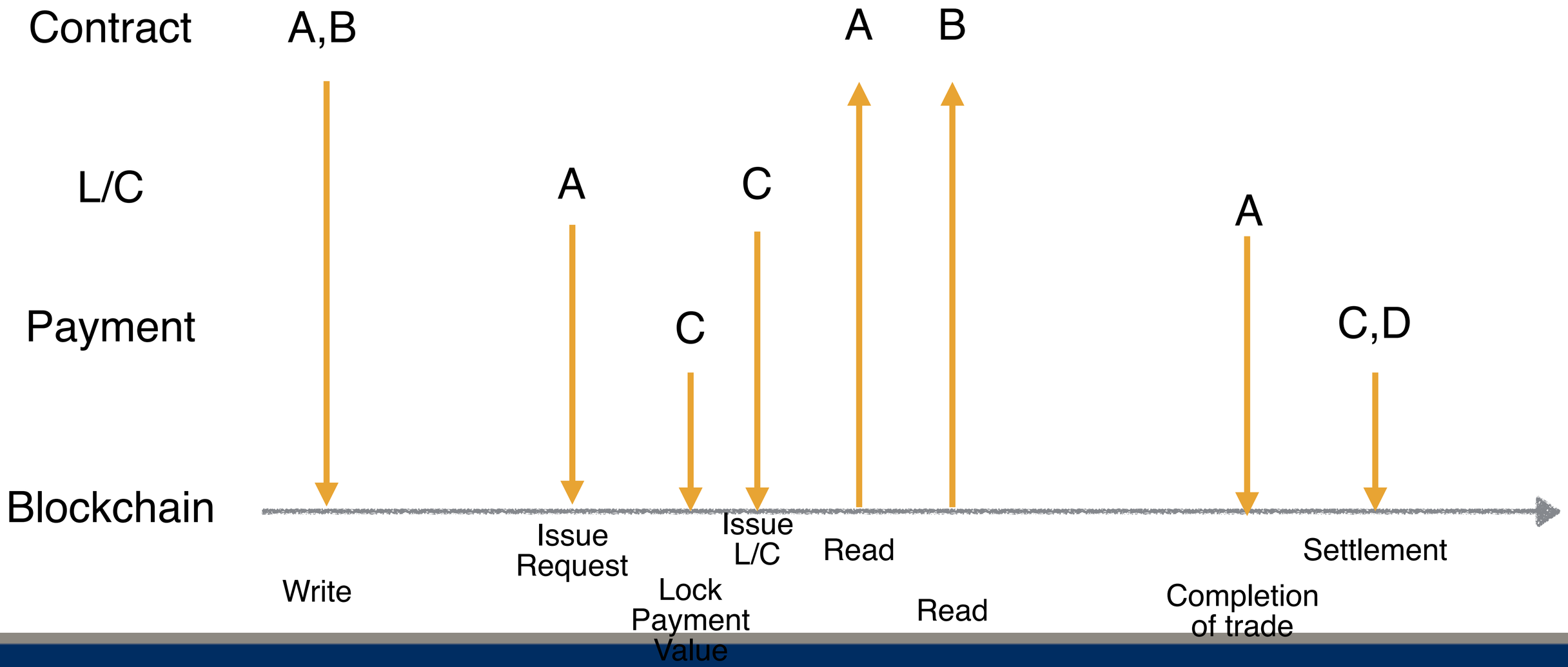
Has enough capability to write business logic

Suitable for formal verification

Letter of Credit (L/C) and Trade Finance over Blockchain

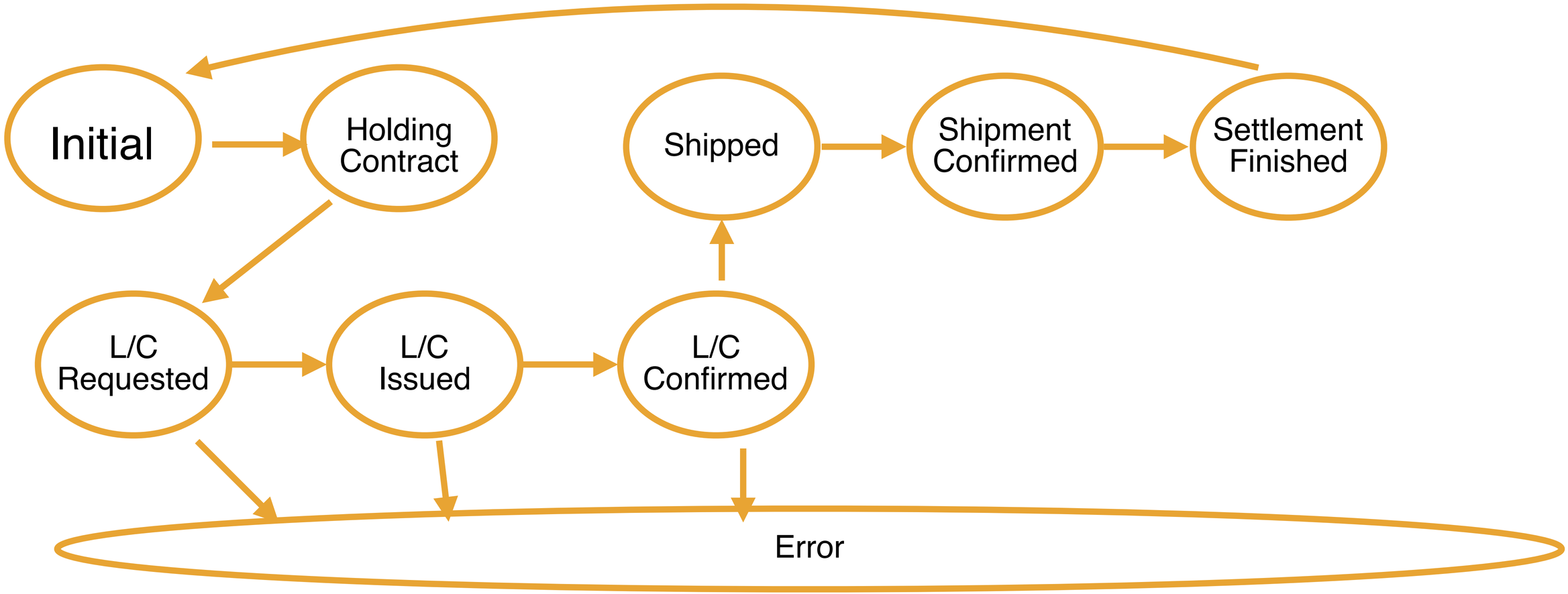


Sequence of process



State Transition

Four variables for state representation: Contract, L/C, Payment, Shipment
Create language from state transition and constraints



Limitation of Formal Analysis/Verification

Limitation of automated tool
Upper bound of memory, .,,
Not sufficient for complicated protocols

How can we verify the correctness of formalization?

Formal verification does not assure the security in most cases

Need template and languages which are suitable for formal verification

The case of SSL/TLS

Many attacks/vulnerabilities are found during this 5 years.

Heartbleed, Poodle, FREAK, DROWN, CCS Injection

Problems

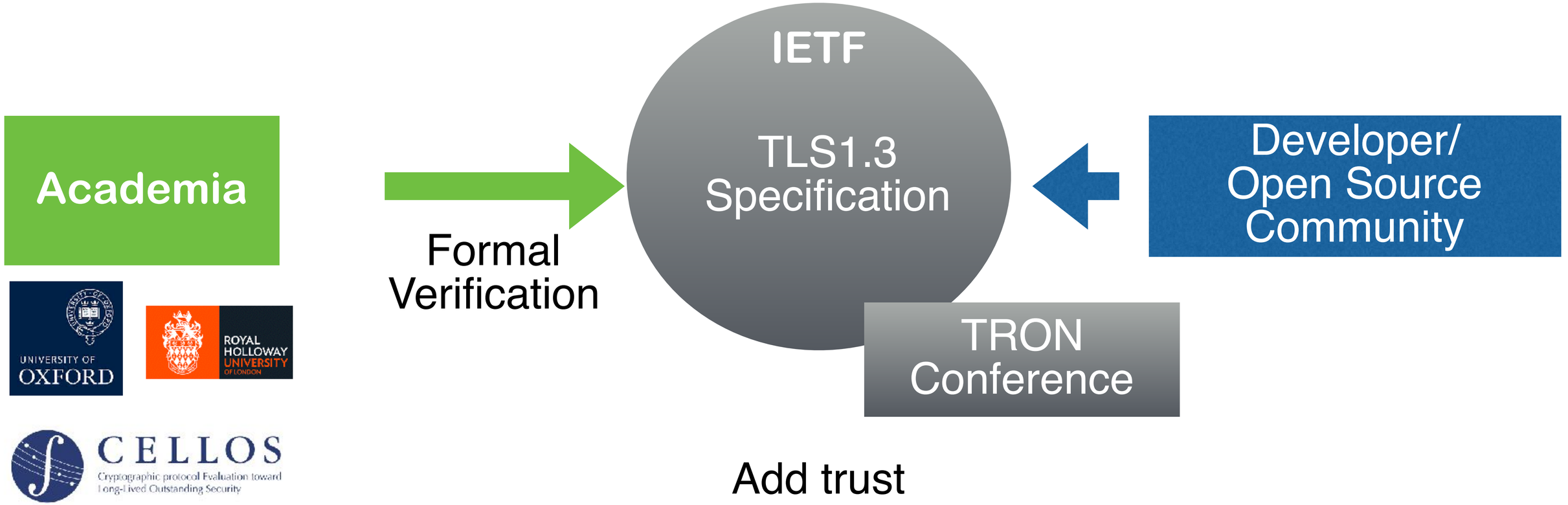
No security proof

No procedure for verification of technology.

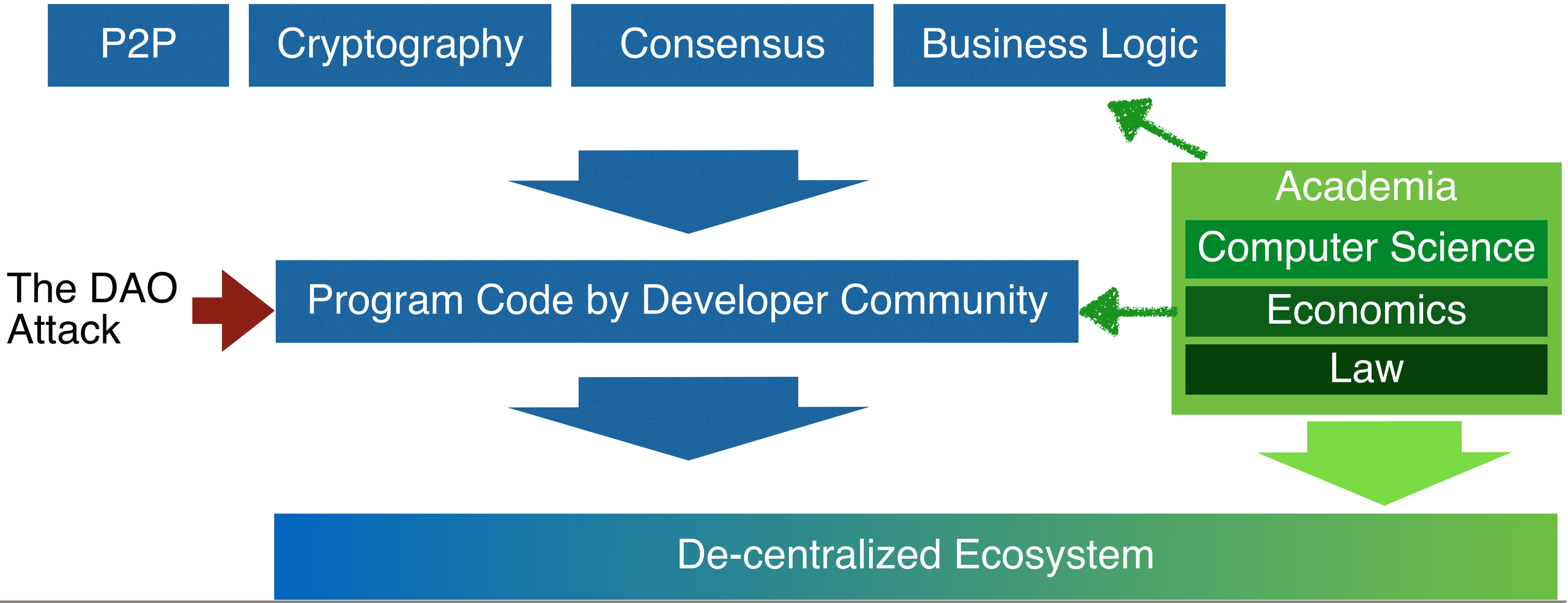
No experts on the verification of cryptographic protocols

Insufficient quality assurance of program code

The case of TLS 1.3



Decentralization by Diversity



Collaboration among Bitcoin developers and academia through BSafe.network

Bitcoin developer community

Bitcoin software

BIP
(Bitcoin Improvement Proposal)

Experiments
Competition

Research Results

BSafe.network

Academia

Research

BRR
(Bitcoin Research Request)

Conclusion

Analyzing Bitcoin/Blockchain is complex problem.

Reviewing Entire Blockchain-based systems

Formal analysis/verification is applicable for many part of blockchain-based system

Protocol,Application Logic and Protocols
Possibility to define specific language for Application Logic Layer

We are at the early stage of academic research.

Thank you!

GEORGETOWN UNIVERSITY