Blockchain Research and B-TED
- Permission-less innovation by Computer Science -

Shin’ichiro Matsuo

Grad Student Orientation

GEORGETOWN UNIVERSITY

About Me

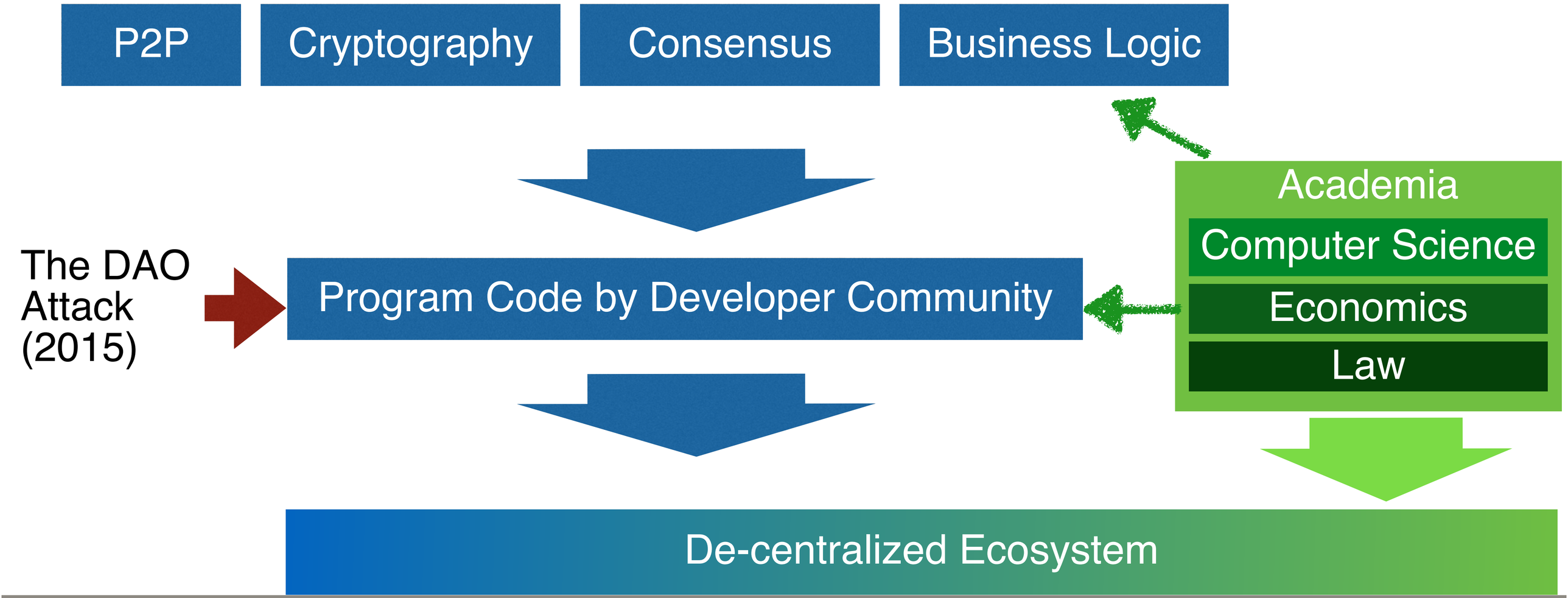
@Shanematsuo

- Cryptographer (> 20 years), digital cash (from 1997)
- Research Professor at Georgetown University
  - Director of Blockchain Technology and Ecosystem Design (B-TED) research center

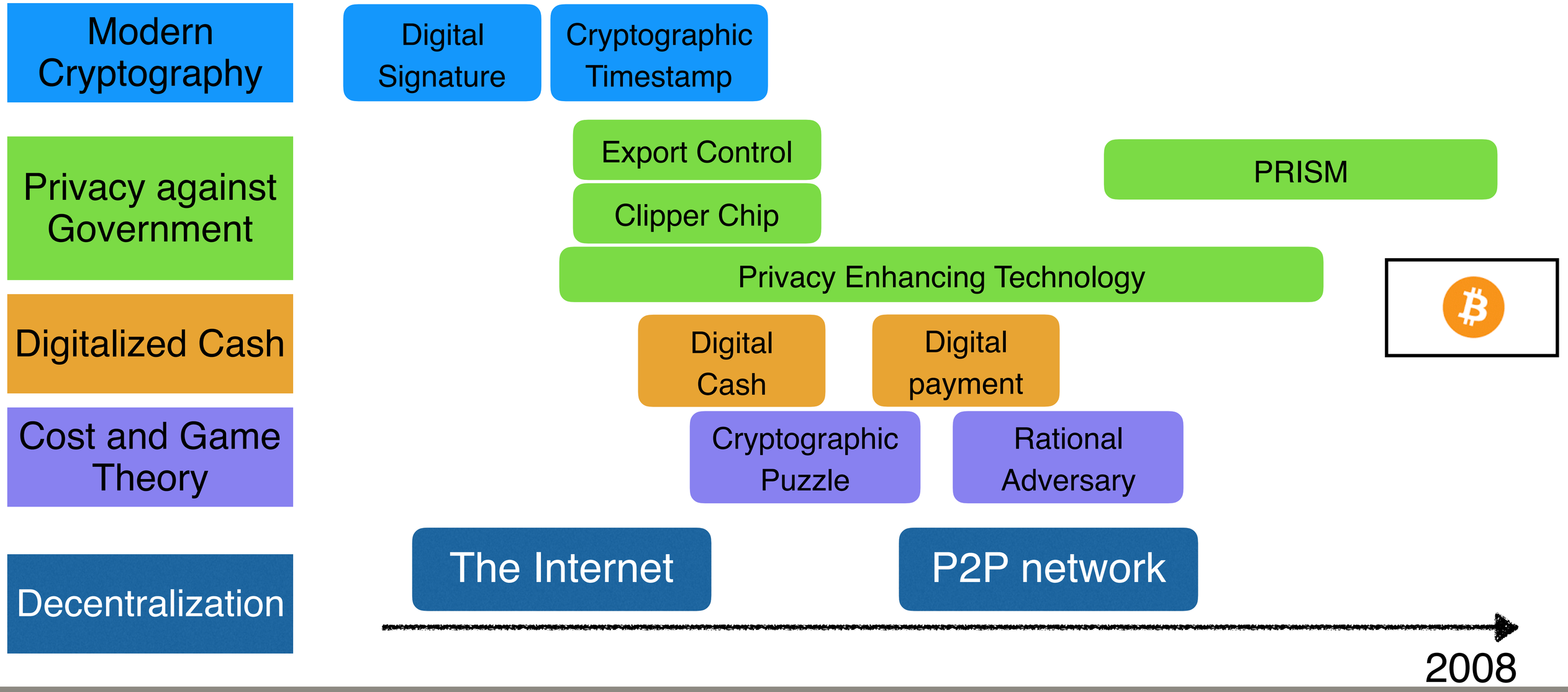
- Co-Founder of Bsafe.network (International testbed)
- Program committee and editor: Scaling Bitcoin, IEEE, ACM conferences, Ledger Journal and more…
  - Program co-chair of Scaling Bitcoin 2018
- Standardization at ISO TC307 (Blockchain and DLT)

I have no Bitcoin and any cryptocurrencies
I have no position on the exchange rate to FIAT currency.

Impact of Blockchain: CS makes De-centralization and permission-less innovation



Blockchain research is multi-disciplinary



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 ecosystem by designing better incentive/economic model

Scalability issue

Issue

7 tx/sec (textbook Bitcoin) vs 10,000 tx/sec (VISA)

Need to consider the trade-offs among scalability and security

Recent selfish minings on Monacoin and Bitcoin gold warns us again

Two directions

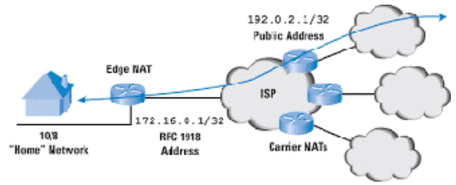
Off-chain vs On-chain

Lightning Network

Scalable, Instant Bitcoin/Blockchain Transactions

BitcoinCash

Like IPv4+NAT and IPv6



Difficult to scale blockchain without loss of permission-less nature:
Fundamental problem from computer science view

Research directions

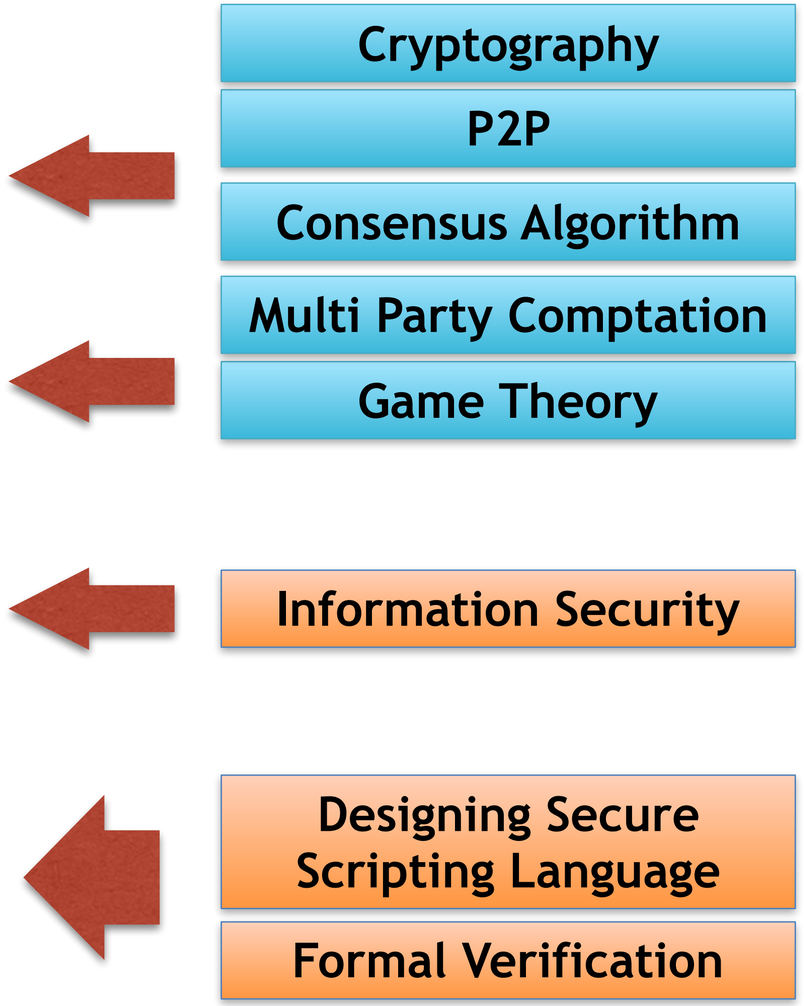
	Research Challenge	Needed/relevant computer science research
Blockchain Application	Securing Blockchain application and smart contract	Domain Specific Program Language Design Formal Analysis Computational Model Information Secuirty
Blockchain Foundation	Enhancing Scalability Enhancing Privacy without loss of decentralization	Cryptography Multi Party Computation Information Secuirty Distributed Computing Consensus Mechanism Game Theory P2P Network Security Ecnomics

B-TED (Blockchain Technology and Ecosystem Design) Research Center

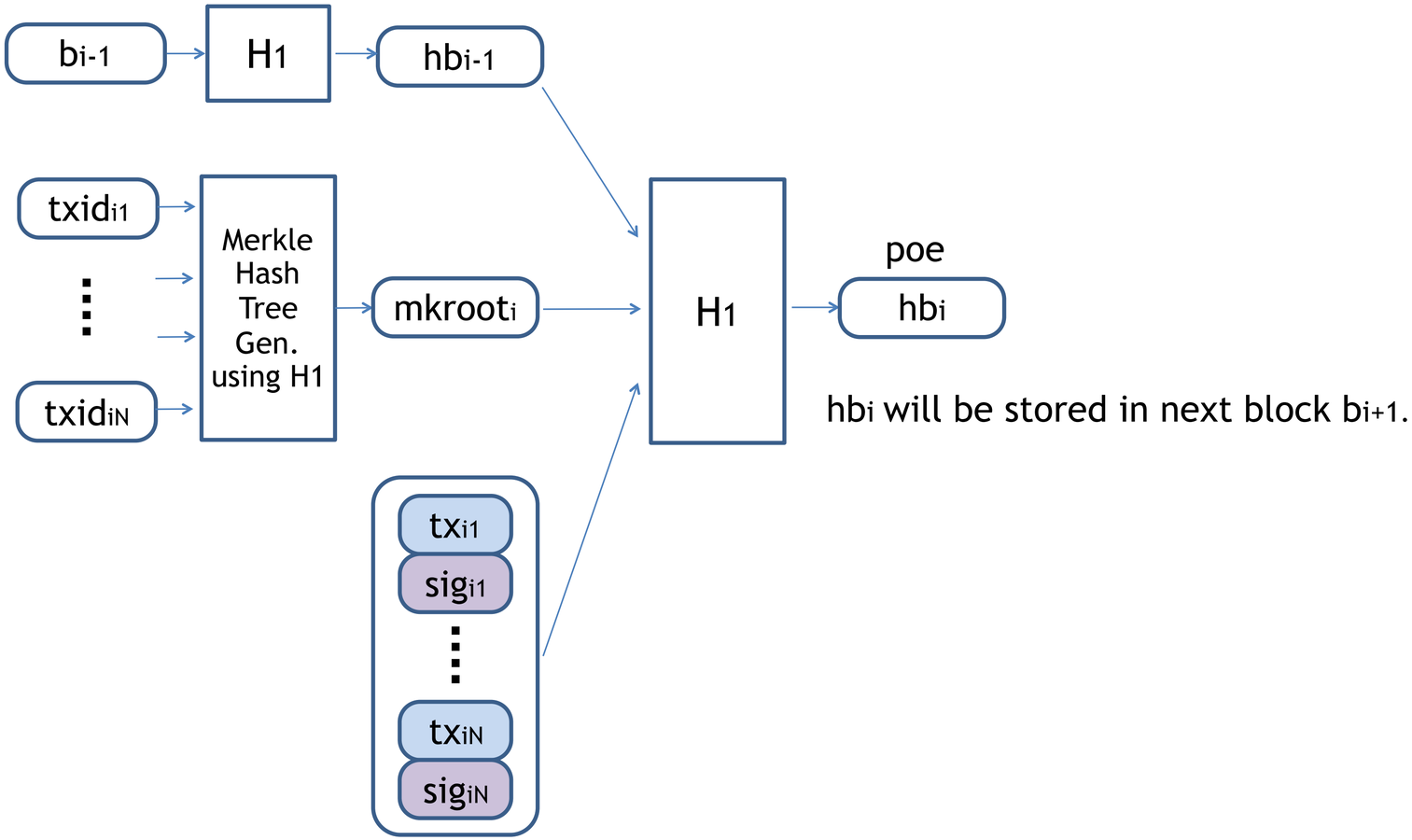
- **Be a trusted Industrial - academic research platform and anchor**
  - NSFNet and BSD for Blockchain
  - Provide independent, academic and neutral evaluation criteria for Blockchain technology
- **Provide research results and IPR to Affiliates and public (3 universities, 7 affiliates now, and more)**
  - Multi-disciplinary research, International connection
  - Technology and ecosystem design: tech, economics, legal and connection to industry, government and regulators
  - Applications and their deployment
- **Contribution to Standardization**
  - IETF, ISO, IEEE, etc.
- **Show Case Event: September 14 @ Healey Family Student Center**

Research projects at B-TED

- **Foundation of Blockchain**
  - **Technology Evaluation - Security/Privacy/ Scalability Trade-off**
  - **Game Theory and security economics**
  - Open Source Community governance
- **Applications of Blockchain**
  - **Blockchain x Security : Output to ISO Standard**
  - New forms of finance and economy
  - Blockchain x Supply Chain and Logistics
  - Blockchain x IoT, Fog
  - **Blockchain x Medical Record and Insurance**



Extending validity of Blockchain when compromise of underlying cryptography happens



hb_i will be stored in next block b_{i+1}.

ISO Technical Documents from BTED

ISO/NP TR 23245

ISO TC 307/WG 2

Secretariat: XXXX

Blockchain and DLT - Technical Report on security risks and vulnerabilities

WD stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

To help you, this guide on writing standards was produced by the ISO/TMB and is available at https://www.iso.org/iso/how-to-write-standards.pdf

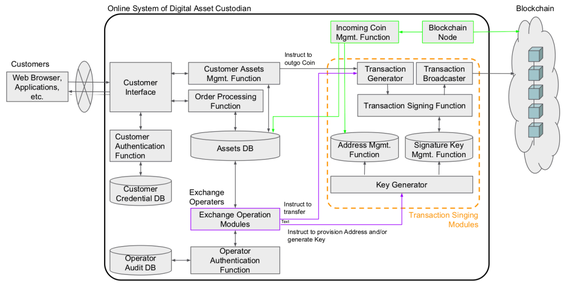
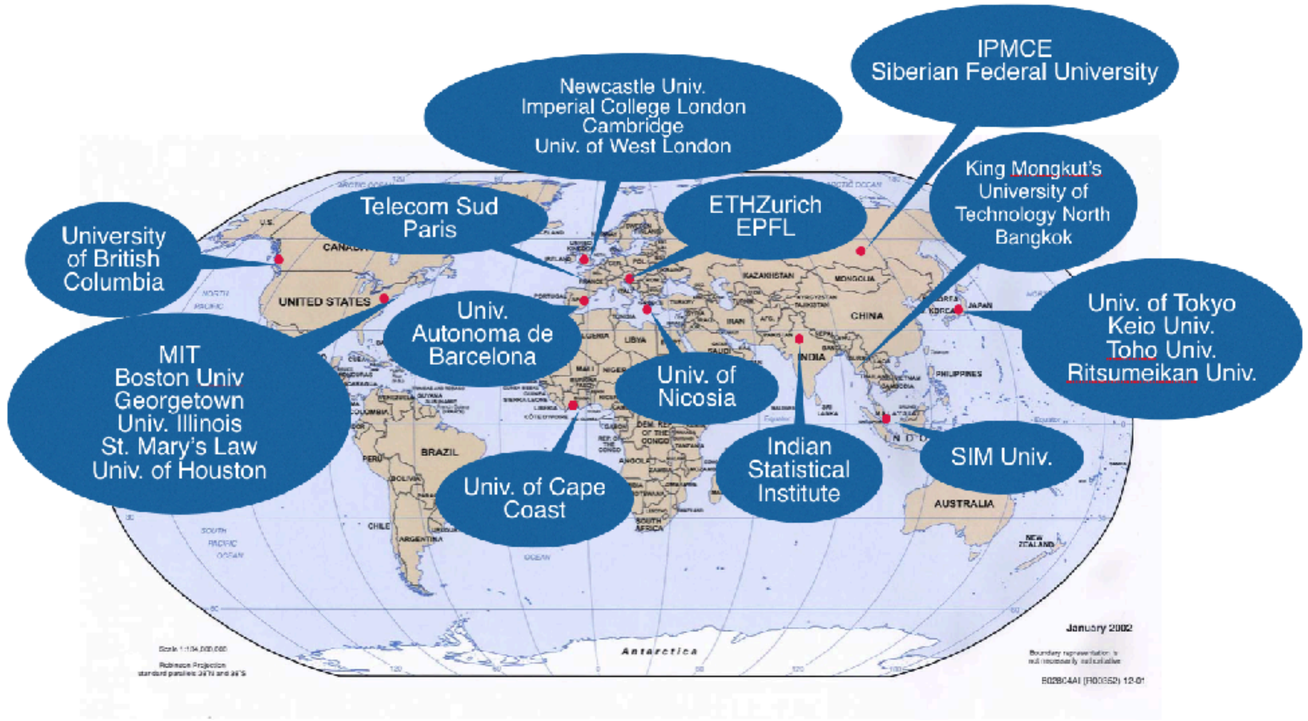


Fig. 5-1 Basic model of a digital asset custodian

Functional components	Explanation
Customer Interface	Provides screen and input functions such as login process, account management (deposit/withdrawal instruction etc.) and trade instruction for the customers(users). Web application, API, etc.
Customer Authentication Function	Performs user authentication process for login to the digital asset custodian and exchange.
Customer Credential Database	Manages required IDs for login and verification information related to user authentication process (eg. password verification info.) .
Customer Assets Management Function	A group of functions to manage customer accounts. Receive instructions for deposit or withdrawal (outgoing coins) and perform processing according to the user instructions. Refer or update asset data.
Blockchain Node	Connects to another blockchain nodes to retrieve blockchain data.
Incoming transaction management Function	Checks transaction stored in blockchain and confirm whether incoming assets are involved in the specified addresses.

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

- A **neutral**, **stable** and **sustainable** research test network for Blockchain technology <u>by international universities.</u>
- Each university becomes a blockchain node.
- Research on Blockchain and its applications
  - Not limited to Security. All aspects will be researched.
- 28 International Universities already join



12

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

Outcome to Society

US Government

金融庁 Financial Services Agency

Guide for regulation

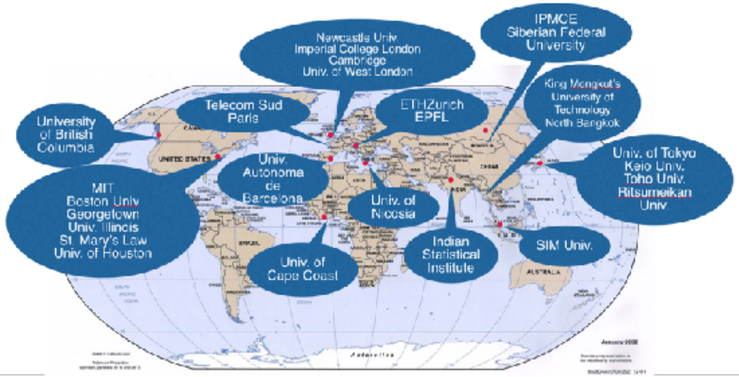
GEORGETOWN UNIVERSITY

B-TED

Computer Science

Law School Business School

BSafe network



International Research Testbed

Technology Standard

ISO

IETF

People

Faculties

Computer Science

Shin'ichiro Matsuo
(Director: Cryptography and security)

Eric Burger
(S2ERC)

Ophir Frieder
(Communication Systems)

McDonough School of Business

Reena Aggarwal
(Stock market, IPO)

James Angel
(Regulation)

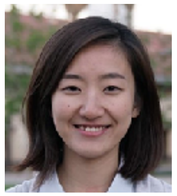
John Jacobs
(Former CMO of NASDAQ)

Perianne Boring
(FinTech and Blockchain)

Center for National Security and the Law

Clare Sullivan
(Digital identity, privacy and cyber security)

Researchers/Students



Jianna SU
(Research Assistant)

Yuta Takanashi
(Senior Fellow)

Zhi Chen
(Ph.D.Candidate)

now hiring

Staff

Paul Brigner
(Managing Director)

Ernesto Camacho
(Admin Staff)

Thanks!

Ask Me Anything!

E-mail: Shinichiro.Matsuo@georgetown.edu

Twitter: @ShaneMatsuo

https://bted.georgetown.edu

https://people.cs.georgetown.edu/matsuo/