BlockChain Congress, Kolkata. 2018 Dec. 19th

Security, Privacy and Trust of Blockchain

--- Difficulty, Limitation, and Challenge ----

Kouichi SAKURAI
Kyushu Univ.
Dept. Informatics & CybersSecurity Cenrer

Currency should be trusted !?

- Bitcoin (2009)
  - –D. Chaum (1982) ***Digital Cash***
- Now more than 2,000 variants
  - –*Virtual* Currency
  - –*Crypto* Currency
  - –*Virtual Crypto* Currency

JAPAN Finance Services Agency Dec. 14th 2018.

- No ”Virtual” nor “Currency”
- But call CRYPTO ASSET
  - –already G-20 says “crypto asset”
    - because, virtual currency sounds too be *trusted*, whereas many cyber attacks around Bitcoin and it variants
    - to distinguish them from regal currency
    - Bitcoin’s price drastically down in this year (➔ quite unstable)

Why FinTech including Bitcoin and Blochchain so Hot in Japan ?

- **JP-Mega Bank: Restructuring with Lay-Off**
  - – Mitsubishi-UFJ plan to reduce number of employee 5/6 (=85%) [ray-off 6,000-peolpe] by 2023
  - – MIZUHO-Financial Group plan to reduce the task to 19,000-empolyees by 2026

Why so restructuring and/or Lay-off

- 1996~2001: Finance Big Bun of Japan
- Low Interest Rates
  - 1999 : 0.15%
  - 2008: "Zero" interest rates policy
- Logistical Support by FinTech including AI and BC
  - Technology reduce *COST* including Human Resource

Artificial Intelligence with Banking

- Customer Service with AI
  - Bank office counter work ➔ Chat with AI
- LOAN Review
  - Professional by Banking experts
  - But, AI may can

History of Virtual Currency Service
from David CHAUM 1989

Year	Country	Name	Method	Feature
1989	Netherland	Digi-Cash	Virtual	Cryptocurrency
1995	UK	Mondex	IC card	by UK Bank
1998	USA	*PayPal*	Server	Internet Service
2000	Japan	Edy	IC card	Noncontact
2001	Japan	SUICA	IC card	Noncontact
2004	Japan	Osaifu-Ketai	IC card, Smartphone	Noncontact, Cellphone
2009	USA	Square	Smartphone	Noncontact, Smartphone
2009	**Worldwide**	**Bitcoin**	**Virtual**	**Cryptocurrency**

1st 2nd 3rd 4th ?

5/27/2015 7

Centralized vs. Decentralized

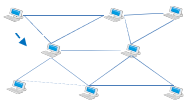
- A Rough history -

- PGP (1991〜)
  - Public-Key Crypto Suites
  - Decentralized ("Web of Trust")
- PKI (1994〜)
  - With the history of SSL, mainly
  - Centralized
- Bitcoin
  - Electronic Currency
  - Decentralized

5/27/2015 8

Decentralized vs. Distributed

- Centralized (TTP, CA, PKI)
  - ➔ Distributed CA via Secret Sharing Scheme
- ~~Decentralized = Distributed~~
- Decetralized <= BitCoin with P2P



How many nodes in your distributed (rather decentralized) systems?

- **Vs. Cloud (a kind of centralized)**
  - **Edge computing**
- **Getting Faster from 7 days To 5 sec ?**

How many nodes in your distributed (rather decentralized) systems?

- **Vs. Cloud (a kind of centralized)**
  - **Edge computing**
- **Getting Faster from 7 days To 5 sec ?**

"A pilot project
with **three** nodes @ 2016"

2018.May. New BlockChain by Mitsubishi-UFJ Financial Group with U.S. AKAMAI

- **Payment Processing time: 2 second.**
- **Transaction Processing: 1,000,000-cases/Sec.**
- **AKAMAI Intelligent Platform**
  - **130 counties,**
  - **3800 nodes**

12

PayPal[1998~] (before BC)

- US company, online transfer
  - Alternative to CHECK, or Money Order
- PayPay JAPAN was accepted after 2010,
  - A new Japanese Bank Regulation
- Cf: US Financial DeRegulation 2016~

Japanese Banks = Major Players of BC

- Three Major/Mega and many local banks
  - MEGA: Tokyo-Mitsubishi--UFJ, SMBC, and MIZUHO
  - Kyushu: 3 groups
    - Fukuoka, Nishi-Nihon City, and Kagoshima
- History of Merging, ReOrganizing
  - After 1990 ~~ still now for ***surviving***
- New Banks: Seven Bank (7-11)
  - 2001~~: ATM-based,

Japan: Major Bank vs. Local Bank

- Major issue each/new Virtual Currency
  - Assume major bank to control
- Local has no plan to his original currency
  - Just join some Banking-group with major
  - Use Distributed Ledger to reduce managing cost
- 2017: Even Tokyo Mitsubishi UFJ introduce "Cloud"

Tokyo Mitsubishi UFJ

- International Foreign Exchange
- With Ripple
- Real Service from 2018
- Among International Banks
  - USA, UK, Canada, Spain, Aurtralia

CF:SWIFT join now HyperLedger@IBM

2017 MIZUHO with IBM

- **Foreign Trade**
- **Demonstration Experiment with Pilot System**
- **IBM's HyperLedger Fabric (Linux Foundation)**

- **SMCB with IBM too**
  - **NEC with Sumitomo Group. But…..**

No Real Operation Yet

Almost all are on a kind of trial project with demonstration experiments….

Jcoin: J(apan)-COIN ! [2017.Sept.17th]

- Mizuho-Bank with Japan "***POST***" Bank
- Based on BlockChain
- Guarantee with Japanese YEN/円
  - a kind of **STABLE** coin
- ***Their plan from 2020 (by Tokyo-Olympic)***

- Against Ali-Pay@CHINA (coming to Japan)?
  - Which gets win ??

JP Electronic Company with BC

- **Two major**
  - **IBM (international) & NTT Data**
- **NEC + NEC Europe**
- **Fujitsu + Fujitsu-lab USA**
- **Small ventures**
  - **including HAW International Inc.**

BC as Financial Technology (FinTech)

- FinTECH is to study how to put FINANCES on INTERNET
  - Iwashita@Bank of Japan, now with Kyoto Univ.
  - Internet of Finance !
- FinTech + IoT
- BlockChain for
  - Energy Management
  - Privacy with Genom
- FinTech +AI

BlockChain and FinTech

- Projects with IoT
  - Your application Scinario e.g. with ROBOTICS
- With Internet
  - Information ➔ Finance (FinTech)
- With BlockChain
  - Finance (BitCoin)
  - Smart Contacts
  - *Sharing* Ecomonics/SPACE/Things
    - Distributed Cloud Storage service (MetaDisk.org)
  - Controlling Energy of Smart City
  - *Digital Right Management/Transfer (Music, Media)*

5/27/2015 22

Crimes around Bitcoin (1/2)

- "Mt. Gox files for bankruptcy, hit with lawsuit" … Reuters, Feb., 28, 2014
  - Mt. Gox, once the world's biggest bitcoin exchange, filed for bankruptcy protection in Japan on Friday

http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228

5/27/2015 23

Crimes around Bitcoin (2/2)

- "Mt. Gox
  - Lost 650 thousands bitcoins (= $210million)
  - Attacks from the outside?
- →Insider!? (Jan 1, 2015)
  - Failed in asset use!?

http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228

5/27/2015 24

Cryptocurrency exchange "Coincheck" loses JP-¥58 billion (US $532 million) in hacking attack

2018.01.26

NEM COIN from COINCHECK

- Cyber Attack ?
- 11th Trial of Illegal remittance
- NEM coin is traceable
- Converted into other COINs in DARKNET
- TIT graduated CEO

2018.April: Coincheck was M&A with Max Group.

Cyber *Security* Research for Bitcoin

- Cyber Crime
  - –Against "Insider" Threat
    - Network Security
    - Computer Security
    - Physical Security
    - Human Security [← PSYCHOLOGY]

5/27/2015 26

Weakness of Proof-of-Works 51% attack

- by a group of miners controlling more than 50% of the network's mining hash-rate, or computing power.
- 2018 MAY
  - – 51% attack did work against Bitcoin Gold and Loose US.$ 18,000,000
  - – MONA-coin was attacked by selfish-mining and Loose US $. 90,000

Cryptographic Aspects of BC

- "BC": BlockChain from BitCoin
  - – BitCoin: P2P [no-PKI], Integrity via SHA-256+ECDSA
  - – BlockChain: P2P [no-PKI] Integrity via [HASH + Digital Sign]
    - Copy Machine [Xerox],
    - Convince Super Market [7-11]
- Without Certification Authority
  - – By Using 2P2-Networking Infra.
  - – Integrity via [Crypto HASH + PubKey Digital Sign]
    - Option: Confidentiality with Encrytion

~~Public Ledger~~

- A public ledger is a tamperproof sequence of data that can be read and augmented by everyone. [Silvio MICALI @MIT]
  - PKI (CA)@Centralized vs. P2P@DeCentralized
- Distributed Ledger@R3
  - Tokyo-Mitsubishi UFJ "JOIN"
- ALGORAND by Silvio MICALI (MIT) 2017
  - Democoin, by Gorbunov and Micali,. 2015

2018/12/28 29

(*IN*-)Security of PKI

- Attacks against PKI
  - 2011 Hacking DigiNotar(Nederland' CA)
    - Forged SSL-certificates (more than #500)
    - Finally, gone Bankrupt
- Heartbleed
  - 2014: Software Bug of "Open" SSL
  - Abuse by Hackers, a kind of Zero-day attack
- Hardware PKI
  - Hardware Security Module

P2P: BC revisited

- 2000～ with Skype
- 2004-2006: Winny Scandal
  - Information leakage from users PC
  - METI plan to develop JP-original Secure OS
  - Toshiba : P2P-baed DRM
    - CD, DVD, Blue-Ray, then Next ?
    - Sorry

2018/12/28 31

After BITCOIN

- Revisit P2P-infrastructure
  - File sharing with P2P
    - [%a negative] Winny around 2005……
- Digital Right Management (DRM)
  - Protecting illegal-copy vs. Promoting content-distribution
    - %Apple vs. Japan
- "Peer2Peer Facilitators"@RSA-conf.2015April

5/27/2015 32

Tea Break

- Two Core Crypto Technology with Bitcoin
  - –HashChain
  - –ECDSA
    - *Some Patent Dispute*

BlockChain from HashChain

- Digital Time Stamping
  - – CRYPTO'90: "How to time-stamping a digital documents" by Haber-Sornetta
  - –Surety's digital service ('90)
    - With NY-times (weekend press)
  - –Patent Dispute (2000)
    - Vs. Entrust (Canada) [pki]
    - Conclusion ?

ECDSA (USA. NIST) [vs. RSA]

- Sony PlayStation 2007/07/07
- Certicom@CANADA
- IEEE Standard
- Submarine Patent
- Visit Japanese Ele. Companies
- Go to Court at US(a small city)
- Conclusion ? (with Blackberry)

SHA-256 in BitCoin

- Attack against SHA-1 CWI/NL+Google
  - – SHA-1 = SHA-160 @1995
- SHA-2 ={*SHA-256*, SHA-512}@2001
- SHA-3: {224, 256, 384, 512}@2015

- Crypto algorithm has LIFE-limitation, Never-forever
  - – DES@1977: 1994. Linear Attack
  - – SHA-1@1995: 2004.Collision Detection attack

Service Systems
How long, WHO guarantee?

- ICT
- Energy
  - Nuclear
    - UAE. AbuDhabi
    - Korean Gov. Project
      - Now 2nd stage
- BC for Energy management
  - EU project
  - JP Gov invest

The Life of BITCOIN

- How long can have BITCOIN's life ?
  - Unexpected crypto-attacks
  - ←the life of crypto-algorithms [ECDSA, SHA] !
  - 20 years or 30 years ??
  - Vs. Physical Gold

- Cf. DES → 2key-TripleDES → AES
  - NIST vs. ISO/IEC
    - VISA/Master card

Research Challenging

- Designing Crypto Algorithms with longer life (50 or 100 years more)
  - Usually within 5 or 10 years
- How BitCoin (SHA-256 & EC-DSA-256k) extend its life longer
  - Bitcoin now within 5 years or 10 years ??

  → PQcrypto !

- Diffulity control of Inversing Hash function
  - With Hash In-equality against Increasing CPU-power

  ← Elegant Idea in BitCoin

BlockChain is *Distributed* DataBase

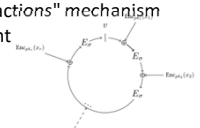
- Transaction
- Data: Search, Delete, Merge etc.
- Computer System vs. Crypto-Math
- CAP Theorem in limitation of Distributed DataBase
  - Consistency, Availability, Partition-Tolerance
- Challenge: How to design BC-oriented Database
  - Revisit: SQL (by IBM Basic Lab.)

Privacy Aspects of Blockchain

- **Bitcoin is anonymous, but no so strong privacy (e.g. linkable)**
- **Privacy Enhanced Crypto Currency**
  - **MONERO**
- **How to apply these developed techniques to Smart contracts or Social Systems**
  - **E-voting**
    - **Blockchain and Anonymous Crypto Techniques (e.g. Ring Signature)**

Ring Signatures in {Monero}

- The ring signatures [Ref] mix spender's address with a group of others
- Making it exponentially more difficult to establish a link between each subsequent transaction
- Impossible to discover actual destination
- The "ring confidential transactions" mechanism hides the transferred amount



[Ref] "How to leak a secret", Rivest, R., Shamir, A., and Tauman, Y., ASIACRYPT 2001

42

Top 20 Cryptocurrencies on Aggregate market value

- Proof of 'X' and Hash functions used -

No.	Name	BC or DAG	Proof of 'X'	Hash Algorithm	Mining Time	ASIC resist.
1	Bitcoin	BC	PoW	SHA-256	10 min	✓
2	Ethereum	BC(DAG)	(PoW,) PoS	Ehash	12 seconds	✓
3	Bitcoin Cash	BC	PoW	SHA-256	10 min	✓
4	Ripple		PoCons	80% majority	-	
5	Litecoin	BC	PoW	Scrypt	2.5 min	✓
6	Dash	BC	PoW	X11 of SHA-3 cand.	5 seconds	✓
7	NEM	BC	PoI	SHA-256	1 min	✓
8	NEO	BC	dBFT	-	20 seconds	
9	Ethereum Classic	BC(DAG)	PoW	Ehash	12 seconds	✓
10	Monero	BC(DAG)	PoW	CryptoNight	-	✓
11	IOTA	DAG "Tangle"	PoW	SHA-3, Keri	-	✓
12	Qtum	BC	PoS	-	-	✓
13	OmiseGO	BC	PoS	-	-	
14	BitConnect	BC	PoW, PoS	-	-	
15	Zcash	BC	PoW	Equihash	2.5 min	✓
16	ADA	BC	PoS	-	-	
17	Lisk	BC	DPoS	-	-	
18	Tether	BC	PoRes	-	-	
19	EOS	BC	DPoS	-	-	
20	Stellar	BC	PoCons	80% majority	-	

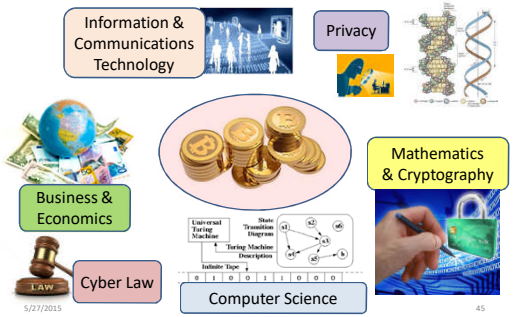
43

Analysis on MONEO

- **ESORICS 2017 Session 12: Blockchain**
- Amrit Kumar, Clément Fischer, Fischer, Shruti Tople and Prateek Saxena.
  - "A Traceability Analysis of Monero's Blockchain"
- Shi-Feng Sun, Man Ho Au, Joseph Liu and Tsz Hon Yuen.
  - "RingCT 2.0: A Compact Linkable Ring Signature Based Protocol for Blockchain Cryptocurrency Monero"
- **ProvSec2017 KeyNote by J.Liu and M.H.AU**
  - **"(Linkable) Ring Signature and its Applications to Blockchain"**
  - We will further relate linkable ring signature to Monero, one of the current largest blockchain-based cryptocurrency in the world, which is considered to be the most commercial deployment of linkable ring signature nowadays. Finally, we will discuss ways to improve the RingCT (Ring Confidential Transactions) of Monero, the linkable ring signature based protocol to provide privacy for Monero users.

44

Thank you for your attention



5/27/2015 45

Self-introduction

- **1986**: B.S. degree in MATH. From Faculty of Science, Kyushu University.
- **1988**: M.S. degree in Applied Sci. (Math) from Faculty of Engineering, Kyushu University.
- **1993**: Doctorate[論博] in Engineering from the Faculty of Engineering, Kyushu University
- 1988-1994: Research and development on cryptography and information security at the Computer and Information Systems Laboratory at Mitsubishi Electric Corporation
- 1994~ : worked for the Dept. of Computer Science of Kyushu University in the capacity of associate professor,
- 1997: One year visiting at CS-Dept@Columbia Univ (New York)
- 2002: Promotion to Full Professor there, and now.
- Also was with the Institute of Systems & Information Technologies and Nanotechnologies, as the chief of Information Security laboratory, by the of March 2017. Current as an external advisor on its Open Innovation Lab.

5/27/2015 46

Personal History with INDIA

- Asiacrypt 2005 Chennai MADORAS
- 2006 Technical Visit at ISI Kolkata with Prof. B.ROY
- IndoCR2012@Kolkata
- Jointworks with India Researchers
  - M.Nandi (research visit at Kyushu Univ.)
  - DST-JST with Prof. B.ROY, DST-JSPS with Prof. A. Adhikari & Prof. S. Ruj
  - Had Two PostDoc Researchers from Kolkata
    - S.Bag (with New-Castle UK), P.Roy (with KDDI-research lab.)
  - Now One PostDoc Researchers from Kolkata
    - Sabya Dutta

5/27/2015 47

My Research Collaboration with INDIA

- **MOU@2006:** [CRSI/Prof.B.ROY – ISIT@Ksyushu/SAKURAI]
- **DST-JST@2008-2012**: "Analysis of Cryptographic Algorithms and Evaluation on Enhancing Network Security Based on Mathematical Science "
  - Strategic Japanese-Indian Cooperative Programme on Multidisciplinary Research Field, which combines Information and Communications Technology with Other Fields
- **DST-JSPS@2014-2015**: "Computational Aspects of Mathematical Design and Analysis of Secure Communication Systems Based on Cryptographic Primitives " JSPS Biliteral program---
- **DTS-JST@2016-2021**: "IoT CyberSecurity" IIT-Delhi
  - India-JAPAN Joint Research Laboratory Program in the field of ICT
- **JICA@MOFA**: IIIT-DM-Jabalpur@2016~
  - One week teaching class "Hot Topics on Cyber Security"