

Cyber Security Center@22th Jan, 2015

Our Cyber Security “Research” inspired from “Bitcoin”



Prof. Dr. Kouichi SAKURAI

Kyushu University

Slides Cooperated with S. Matsumoto and H. Anada
Institute of Systems, Information Technologies
and Nanotechnologies (ISIT)



KYUSHU
UNIVERSITY

In the end of the investigation..

- “Mt. Gox”
 - Once the world's biggest Bitcoin exchange
 - Bankruptcy (Feb 28, 2014)
 - Lost 650 thousands bitcoins (= \$210million)
 - Attacks from the outside?
- → Insider!?! (Jan 1, 2015)
 - Failed in asset use!?



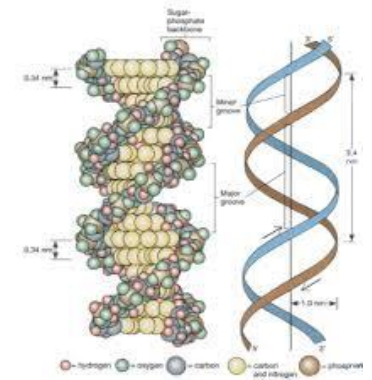
<http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228>

Interder-discrepancy research from Bitcoin

Information & Communications Technology



Privacy



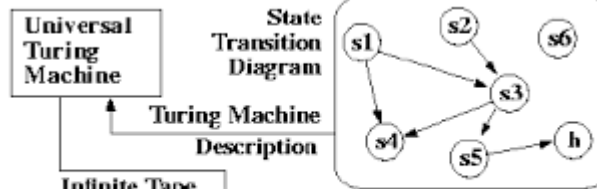
Business & Economics



Mathematics & Cryptography



Cyber Law



Computer Science

History of Electronic Money & Currency(I)

■ 1st Period

- “PayPal”

- Via Internet



■ 2nd Period

- “Edy” “Suica” (Japanese Galápagos)

- With Noncontact Technology



■ 3rd Period

- “Square”

- With Smartphone



■ 4th Period

- “Bitcoin”?



History of Electronic Money & Currency(II)

Year	Country	Name	Method	Feature
1989	Netherland	e-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 ?



So, let's have a look to the latest price

\$ **560.46** ▼ **-0.30%**

Today's Open	\$562.13	Change	-\$1.67 ▼
Today's High	\$561.96	Market Cap	\$7.256B
Today's Low	\$560.32	Total BTC	12,945,875

1h 12h 1d 1w 1m **3m** 1y All

Mar 26, 2014

to

Jun 26, 2014

Export



www.coindesk.com

From the Web site - <http://www.coindesk.com/price/>

Bitcoin vs. Gold

■ Bitcoin



- Total Currency Limited
- Stable
- Division, Conjunction
- Miner

■ Gold



- Total Currency Limited
- Stable
- Division, Conjunction
- Miner

=



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



History of Bitcoin

- 2008: **Satoshi Nakamoto** uploaded his paper on Bitcoin
 - A man of about 60 years old in California
- 2009: Service in Operation
 - Basic Algorithms Developed
- 2011: Bitcoin is known widely
- 2013, Apr: Total Currency: 10 billion USD
- 2013, July: “**Illegal**” in Thailand
- 2013, Aug: “**legal**” in USA
- 2013, Aug: USD ATM service for Bitcoin in Operation



Headline on Bitcoin

■ Regulations for Bitcoins

- in Singapore
- in China
- in Japan(Liberal Democratic Party)

■ Abuses, Crimes and Lawsuits

- Bitcoin mining malwares
- Malware spread via Skype works as Bitcoin miner
- Mt. Gox Bankruptcy

■ Getting Popularity and Utility

- First Bitcoin ATM in Singapore
- World Cup betting system “Bitkup”

Regulations for Bitcoins (1/3)

- “Singapore clamps down on Bitcoin exchanges with new regulations” ...PC world, Mar. 13, 2014
 - Singapore plans to regulate local Bitcoin exchanges to stop the virtual currency from being used in money laundering and terrorist financing schemes, authorities said.

Regulations for Bitcoins (2/3)

- “Bitcoin set for fresh **Chinese** regulatory attack” ...Financial Times, Apr.2, 2014
 - Bitcoin exchanges in China are braced for yet another blow from the central bank that would imperil their survival.
 - The People’s Bank of China is considering whether to **order the country’s banks to close Bitcoin trading accounts**, according to people familiar with the matter.

<http://www.ft.com/intl/cms/s/0/ed3ee914-ba4f-11e3-aeb0-00144feabdc0.html#axzz35iWYg57F>

Regulations for Bitcoins (3/3)

- “Japan's ruling party drops Bitcoin regulation plans” ... zdnet, June 19, 2014
 - Japan's Liberal Democratic Party, the current leading power in the country, **will not regulate** Bitcoin -- at least for now.
 - Takuya Hirai, an LDP lawmaker and leader of the Japanese party's Internet media unit, said:
 - “Basically, we concluded that we will, for now, **avoid a move towards legal regulation.**”

Cyber Research from Bitcoin

- From Economics
- From Regal Aspect
 - Promote or Restrict
- Bit(coin)nomics !?

Abuses, Crimes and Lawsuits (1/3)

■ “**Bitcoin-mining malware** reportedly found on Google Play” ... cnet.com, Apr.24, 2014

- **Fake wallpaper apps** turned phones into **bots** for the power- and computationally intensive process of producing crypto-currency, a mobile security firm warns.

<http://www.cnet.com/news/bitcoin-mining-malware-reportedly-discovered-at-google-play/>

2014/6/30



<http://androidfreeware.net/download-beating-heart-live-wallpaper.html>

Abuses, Crimes and Lawsuits (2/3)

- “Trojan Turns Your PC Into Bitcoin Mining Slave” ... Wired, Apr., 5, 2014
 - New Trojan - spotted just yesterday and spreading via Skype - that takes control of infected machines and forces them to do known as Bitcoin mining, a way of earning digital currency.



<http://www.wired.com/2013/04/bitcoin-trojan/>

Abuses, Crimes and Lawsuits (3/3)

- “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, saying it may have **lost nearly half a billion dollars worth** of the virtual coins due to hacking into its faulty computer system.



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

Cyber *Security* Research for Bitcoin

- Cyber Crime

- Against “Insider” Threat [内部不正脅威]

- Network Security

- Computer Security

- Physical Security

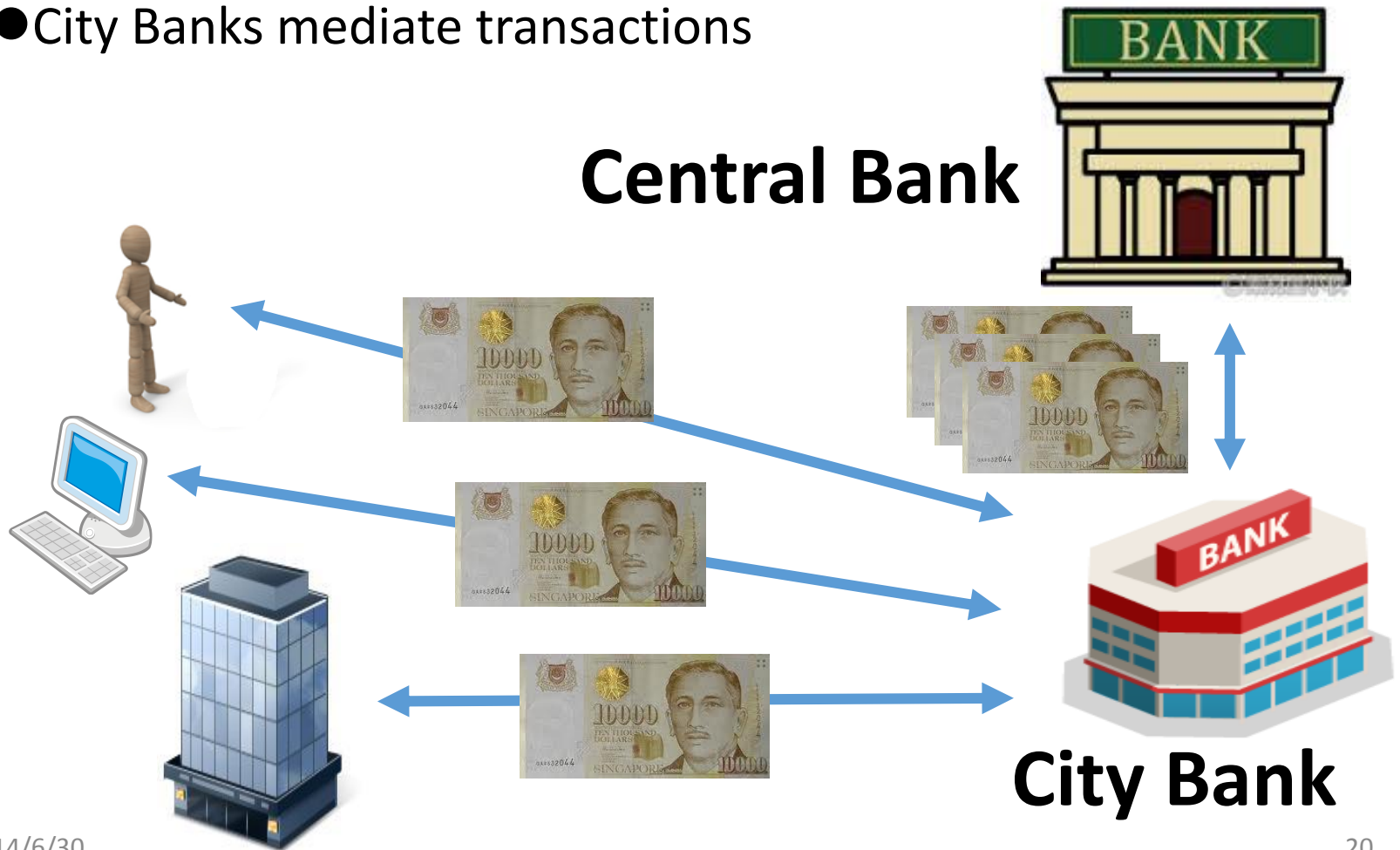
- Human Security [← PSYCHOLOGY]

Mechanism on Bitcoin

- Centralized Currency vs. Bitcoin
- Bitcoin vs. Real Currency
- Bitcoin vs. Gold
- Mining Bitcoin
- Transaction Mechanism
- Security
- Problems

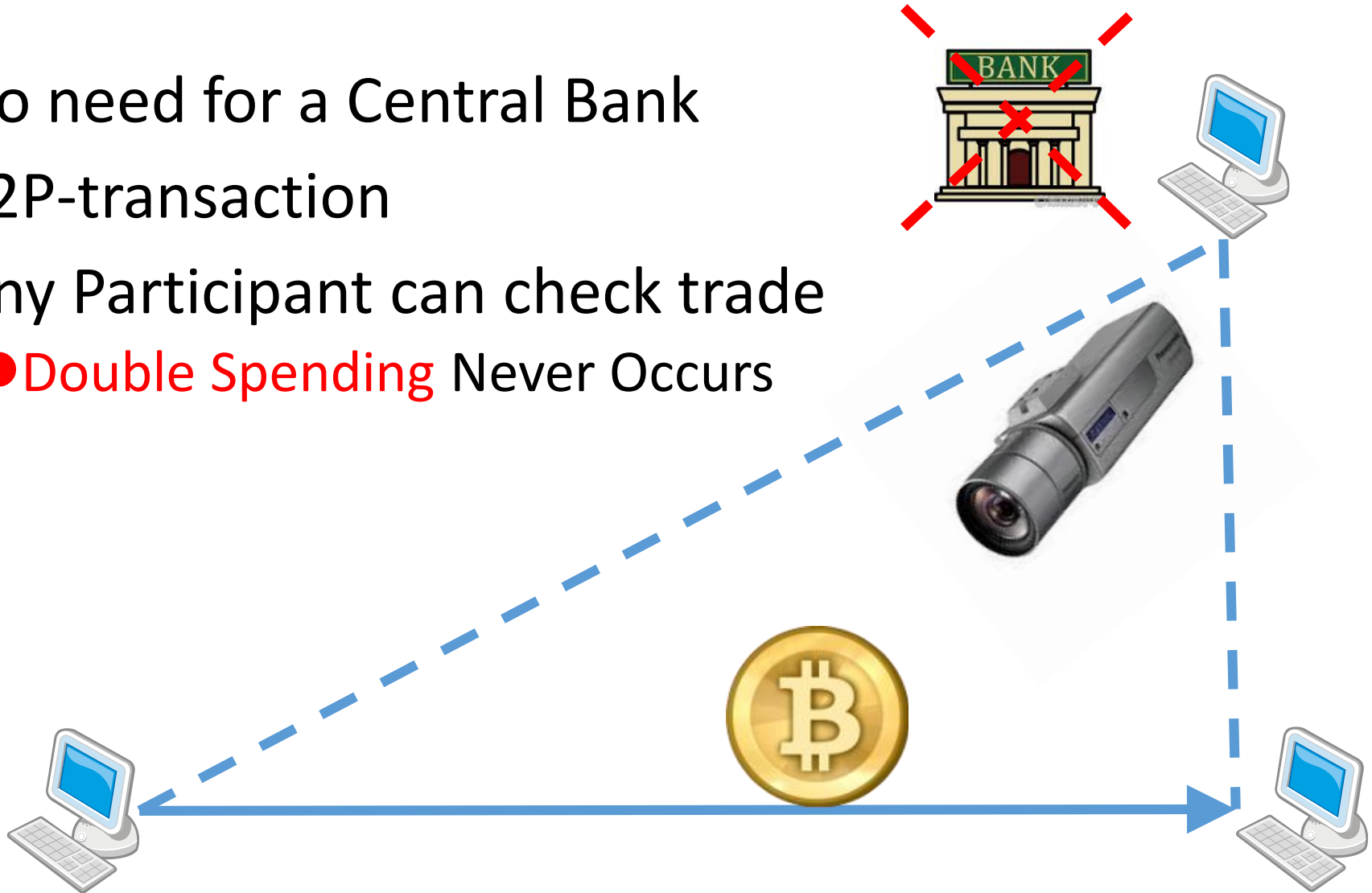
Centralized Currency

- Central Bank has a right to control currency
 - City Banks mediate transactions





Bitcoin: Decentralized Currency

- No need for a Central Bank
- P2P-transaction
- Any Participant can check trade
 - **Double Spending** Never Occurs



Bitcoin vs. Real Currency

	Money-Type	Currency-Type	Manager/Issuer	Total Currency
	Real Currency	Centralized, Physical	Country / National Bank	Not Limited
	Bitcoin	Decentralized, Virtual	Participants / Miner	Limited

Bitcoin vs. Gold

■ Bitcoin



- Total Currency Limited
- Stable
- Division, Conjunction
- Miner

■ Gold



- Total Currency Limited
- Stable
- Division, Conjunction
- Miner

=



Mining Bitcoin



- **Miners** try to solve a Math Problem
- Very Hard even for fast Computers



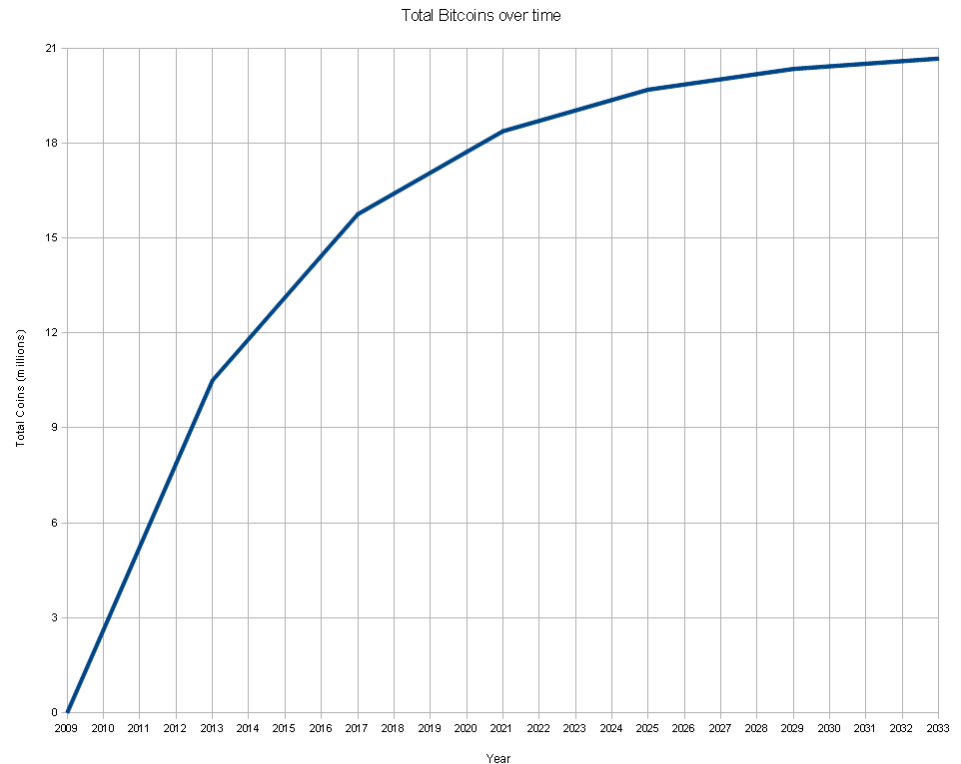
Total Currency of Bitcoin

■ Increasing by Mining

- 4 years : 10,500,000 BTC
- 8 years : 15,750,000 BTC
- 12 years: 18,375,000 BTC

■ 2140: the Limit

- 21,000,000 BTC



Foundation with Bitcoin

- Mining BitCoin [発掘]
 - Need powerful computation
 - with Super Computer
- Security with Computationally hard problem
 - Computer Science
 - Crypto-Mathematics

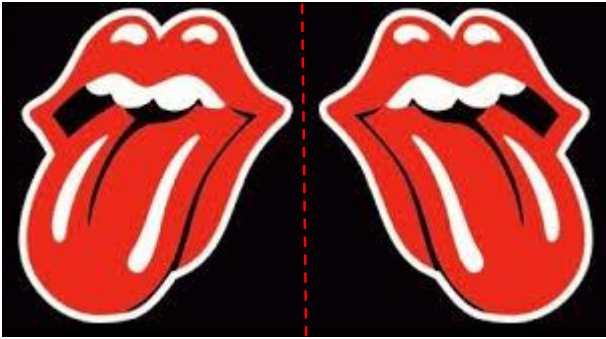
Bitcoin resolve the [The Byzantine Generals'](https://bitcointalk.org/oldSiteFiles/byzantine.html) Problem(!?) (<https://bitcointalk.org/oldSiteFiles/byzantine.html>)

- A number of Byzantine Generals each have a computer and want to attack the King's wi-fi by brute forcing the password, which they've learned is a certain number of characters in length. Once they stimulate the network to generate a packet, they must crack the password within a limited time to break in and erase the logs, lest they be discovered. They only have enough CPU power to crack it fast enough if a majority of them attack at the same time.
- They don't particularly care when the attack will be, just that they agree. It has been decided that anyone who feels like it will announce an attack time, which we'll call the "plan", and whatever plan is heard first will be the official plan. The problem is that the network is not instantaneous, and if two generals announce different plans at close to the same time, some may hear one first and others hear the other first.

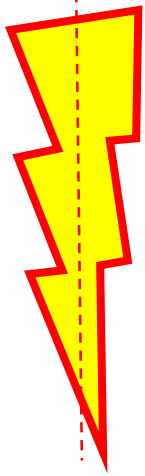
The Byzantine Problem: How can we block “double-tongued”



Go



No Go



Where from academic papers around BITCOIN

- Workshop on Bitcoin Research
 - 1st @2014, 2nd@2015: with Financial Cryptography
- Workshop on Economics of Information Security (WEIS): 12th @2014
 - Bitcoin-papers from 2013 & 2014
- IACR-eprint
 - Keyword with “Bitcoin”: 1st = 2012/248
 - 3-papers@2012, 7-papers@2013, 16-papers@2014
- Arxiv.org [80-papers by now from]
 - **A static theory of promises** [Jan A. Bergstra, Mark Burgess](#)
 - (Submitted on 18 Oct 2008 ([v1](#)), last revised 30 Jan 2014 ([this version, v5](#)))

Sorry,.... Why ? [**we may discuss**]

- No accademic paper about BITCOIN from JAPAN nor by Japanese !
 - Only by S.NAKAMOTO [?]
- By Adi Shamir
 - ePrint@2012&2013
 - → Financial Crypto 2013&2014
- Researchers on Computer Science & Crypto from US & EC



After BITCOIN

- Revisit P2P-infrastructure

- File sharing with P2P
 - [%a negative] Winney around 2005.....

- Digital Right Management (DRM)

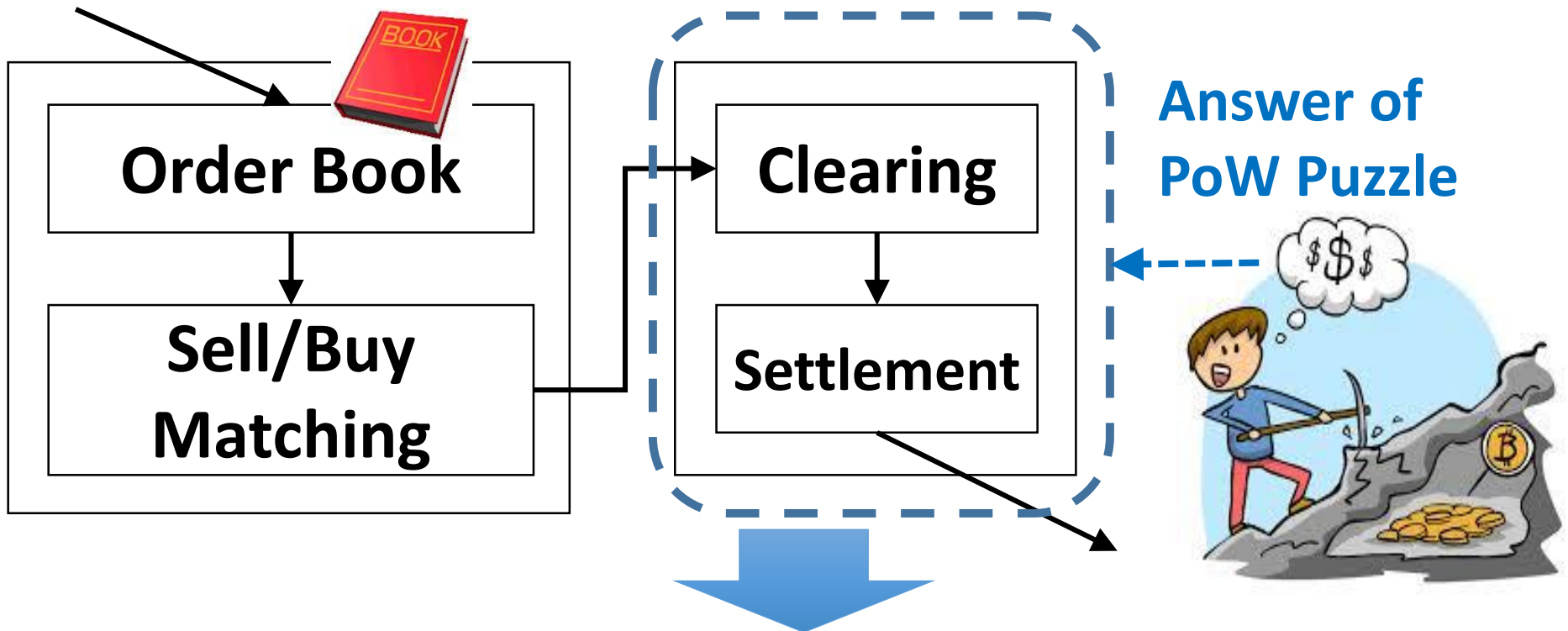
- Protecting illegal-copy
Promoting content-distribution
 - %Apple vs. Japan

vs.

- “Peer2Peer Facilitators” @RSA-conf.2015April

- On Decentralizing Prediction Markets and Order Books **WEIS2014**
 - J.Clark¹, J.Bonneau², E.W. Felten², J. A. Kroll², **A. Miller³**, and A.Narayanan²
 - 1 Concordia Univ. 2 Princeton Univ. 3 **Univ. of Maryland**

Decentralizing Order-Books System



Principle: Employ “Hash-based Proof-of-Work Puzzle”:

$Hash(\text{Nonce} | \text{Previous Hash Val.} | \text{Present Block}) < 2^d$
of All Trans. in a Time Unit

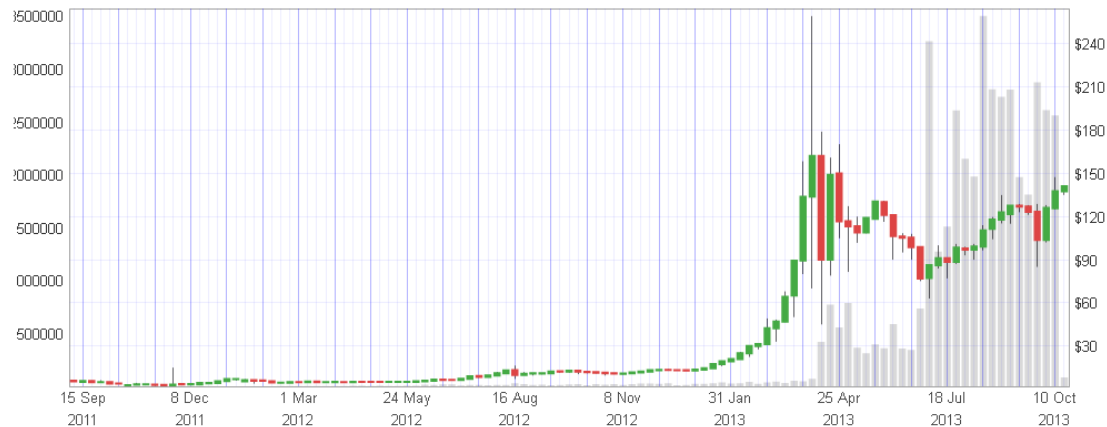
Nonce: A String found by a Miner (**Answer of PoW Puzzle**)

Strong Points of Bitcoin



1. Fast Transaction
2. Low Fee
3. High Anonymity
4. Easy to Use by Smartphone
5. Available Abroad → International Research Collaboration
6. Suitable as Escape Place of Money
7. Rise in Market Place

interval	min	max	open	last price	change (all time)	market	price
all time	\$2.00	\$259.34	\$2.00	\$141.08	+6954.00%	bitstamp	\$141.08



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



Finally

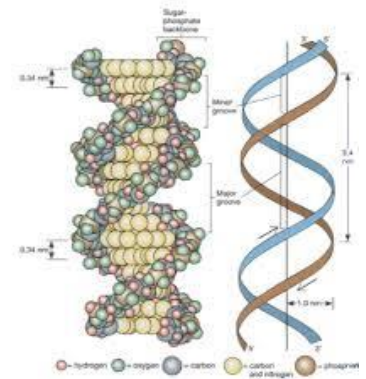
- The current stage of Bitcoin is a kind of 1st stage of Internet [before/around 1980~]
 - Developing without well-organization beyond the border of Government
- Need International Joint Research
 - UM & UMBC ↔ Kyushu Univ.

Thank you for your attention

Information & Communications Technology



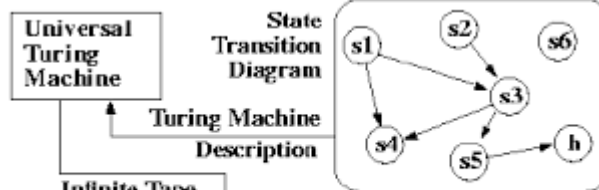
Privacy



Mathematics & Cryptography



Business & Economics



Cyber Law

Computer Science

- Thank you for your attention

Other Problems on Bitcoin

■ Prob.1: Transaction Malleability might invite **Theft**

● Mt.Gox



■ Prob.2: Anonymity might cause **Illegal Use**

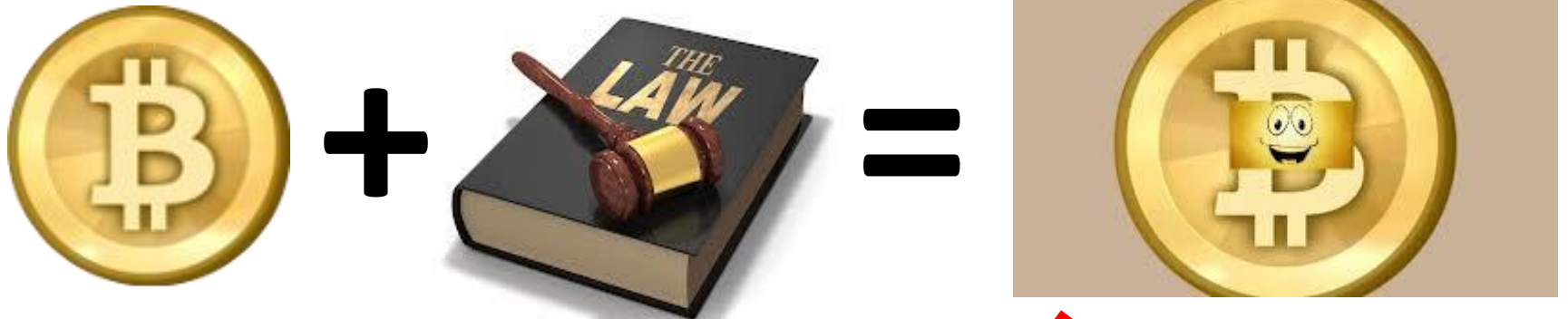
● Drug, Weapon, Malware



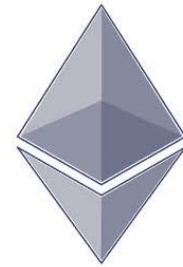
Bitcoin needs a Law ?

■ To prevent Illegal Use;

● We have to combine Bitcoin with Law



ETHEREUM



Bitcoin: Revisited

■ Cryptocurrency 1.0

- P2P Currency
- Distributed Ledger System(blockchain)
- Transaction /w Digital Signature



Bitcoin: Substantially Problem

■ Cryptocurrency 1.0

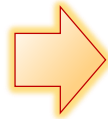
● Value Security

= Difficulty of Hash Calc.

● Many investments make much money

Software impl.(slow)

ASIC impl.(accelerated)

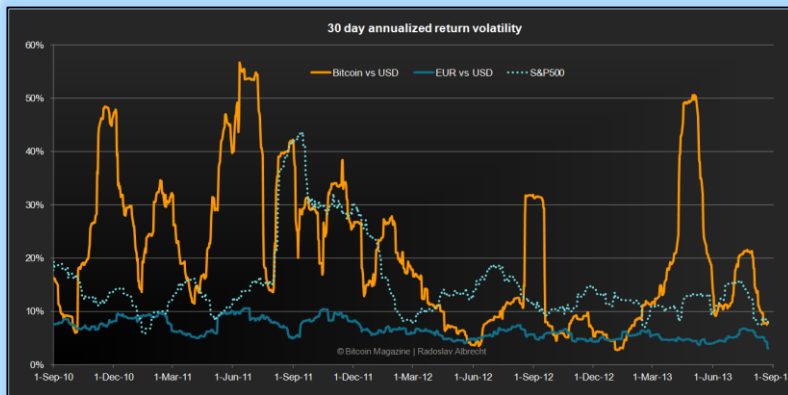


Two Aspects of Bitcoin

■ Digital currency
w/o central bank
(but price gyrates)



creates many
“altcoins”



from the article 'Bitcoin Volatility – The 4 perspectives'
In Bitcoin Magazine, by Radoslav Albrecht, on Aug. 27, 2013



integration



pursue the concept

■ “blockchain” as public
ledger of transactions

Ethereum.org

who?

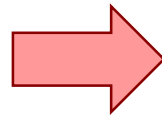
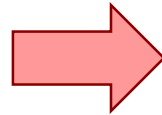
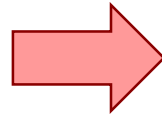
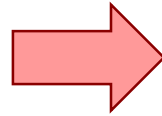
 Vitalik Buterin Founder GitHub Twitter Google+ LinkedIn	 Charles Hoskinson Founder Facebook Twitter Google+ LinkedIn Instagram	 Anthony Di Iorio Founder Twitter LinkedIn Instagram	 Mihai Alisie Founder Twitter LinkedIn
 Gavin Wood Founder GitHub Twitter LinkedIn Instagram	 Joseph Lubin Founder Twitter Google+ Facebook Instagram	 Jeffrey Wilcke Founder Twitter Google+ GitHub LinkedIn Instagram	 Amir Chetrit Founder
 Neal Koblitz Advisor WordPress	 Ralph Merkle Advisor WordPress	 Stephan Tual Communications GitHub Twitter LinkedIn Instagram	 Taylor Gerring Development GitHub Twitter LinkedIn Instagram
 Jeremy Wood Administration	 Mathias Grønnebak Development	 Ryan Taylor Development	 Nicolas Fierro Development

16 of 33 members
from Web page

2014/6/30

What is Ethereum?

Application
Platform



Next-gen.
distributed
applications

Programming
Language

Any developer to build
and publish new apps.

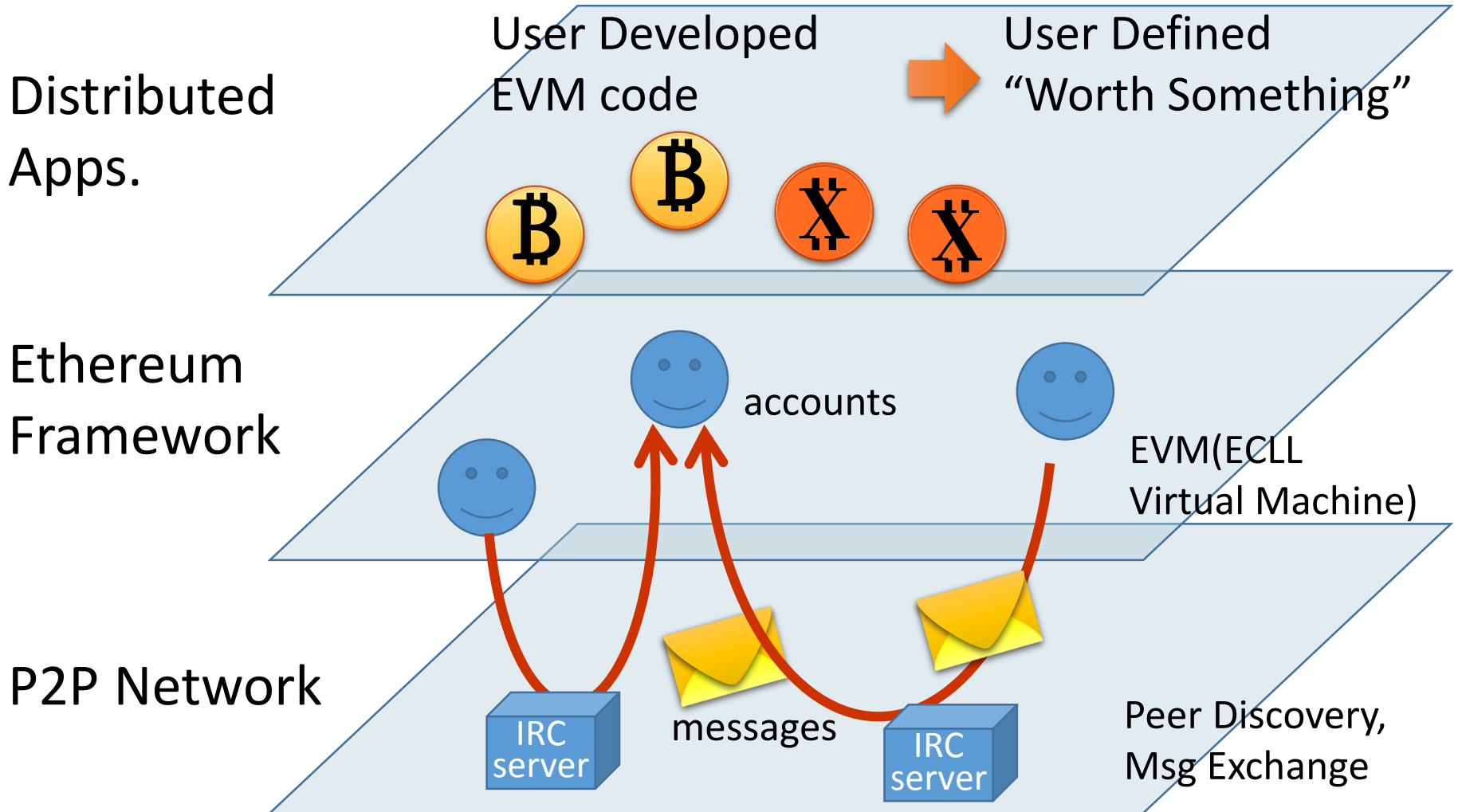
Ethereum: Cryptocurrency 2.0

- Foundations to develop apps.
 - blockchain + programming lang.
(Turing-complete)
 - For describe “contract”(=encoded arbitrary state transition function)
- Equality regardless of the amount of investment



New hash algo.
(other than SHA-256)

Structure of Ethereum



Ethereum Programming Lang.

■ Bitcoin Script

- Forth-like stack based language
- Not Turing-complete (no loop syntax)

■ Ethereum Programming Lang.

- Turing-complete
- Runs on EVM

Example of Applications

- Token Systems
- Financial derivs. and Stable Currencies
- Identity and Reputation Systems
- Decentralized File Storage
- Decentralized Autonomous Orgs.

Example 1: Token Systems

- Most Simple example

```
from = msg.sender
to = msg.data[0]
value = msg.data[1]

if contract.storage[from] >= value:
    contract.storage[from] = contract.storage[from] - value
    contract.storage[to] = contract.storage[to] + value
```

- act as a transaction
 - transfer “value” from “sender” to “to”

Example 2: Financial Derivatives

- Need to reference external price picker
 - Undisturbed by volatility of Cryptocurrency
 - Need to embed compensation mechanism.

Example 3: Identity & Reputation System

- Utilize storage in account
 - Name registration example

```
if !contract.storage[tx.data[0]]:  
    contract.storage[tx.data[0]] = tx.data[1]
```

- Can develop advanced reputation system


APPENDICES

Ethereum's Accounts

“account” object

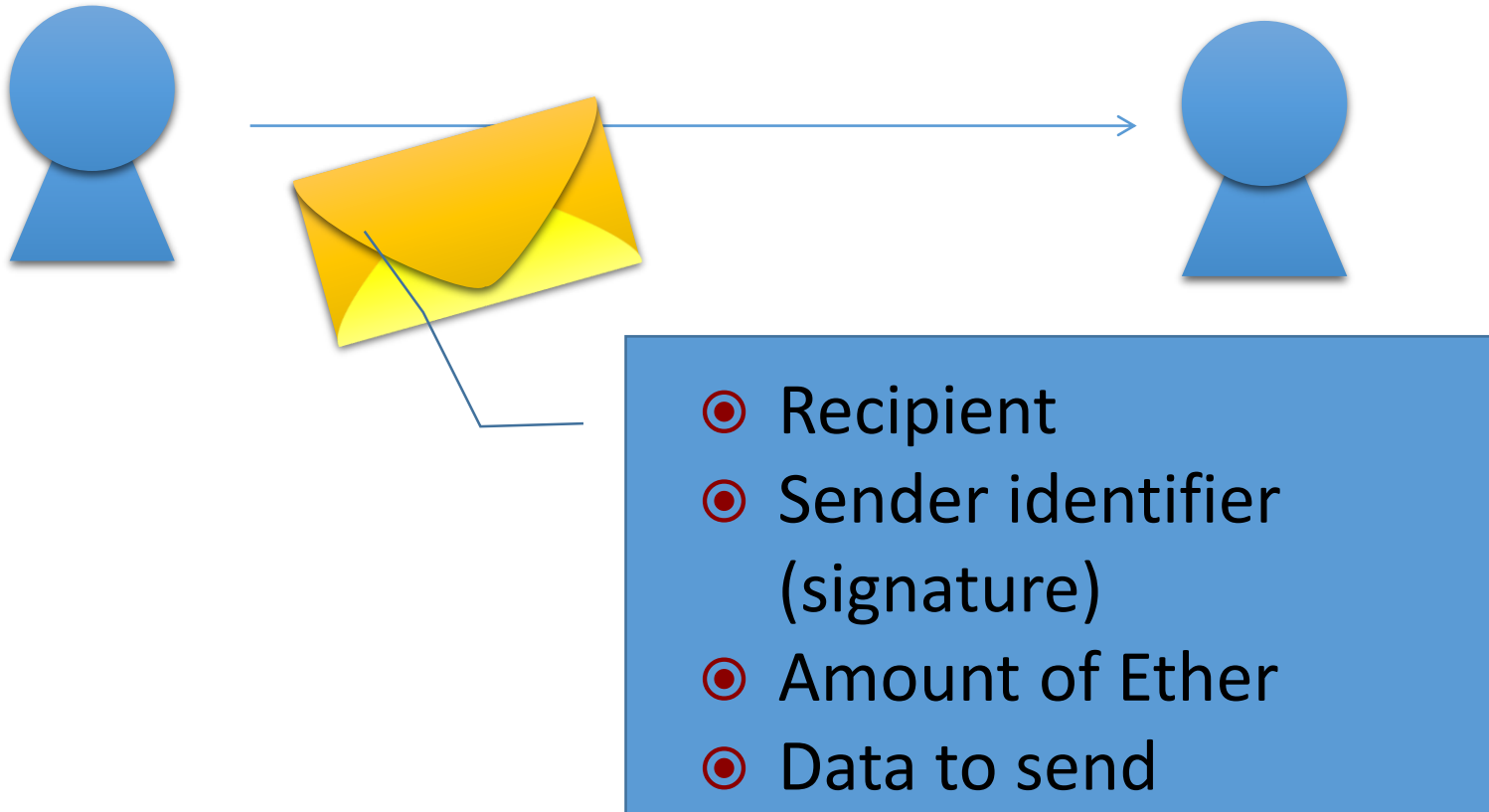
- nonce
- Ether balance
- contract code *optional
- storage

crypto-fuel in Ethereum
used to pay transaction
fee



Ethereum's Transaction

- Not same in Bitcoin.



Ethereum's Messages

Difference between Bitcoin's Transactions

- Creator
 - Ethereum msg: external entity or contract
 - Bitcoin transaction : external entity only
- Data containment
 - Ethereum msg can contain data optionally.
- Message Response
 - Recipient of Ethereum msg can send response (optionally)

Thanks for Attention!

Kouichi SAKURAI

Kyushu University /

Institute of Systems, Information Technologies
and Nanotechnologies (ISIT)



Transaction: Sending

■ Sending a Bitcoin = “Hash & Sign”



User(i)



Send

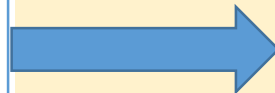


= Hash & Sign

User(i+1)



...
Hash val. & Signature (i-1)



...
Hash val. & Signature (i-1)
Hash val. & Signature (i)

Secret Key(i)

PK(i+1)

Transaction: Receiving



■ Receiving a Bitcoin

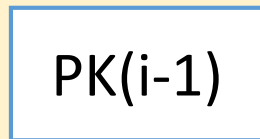
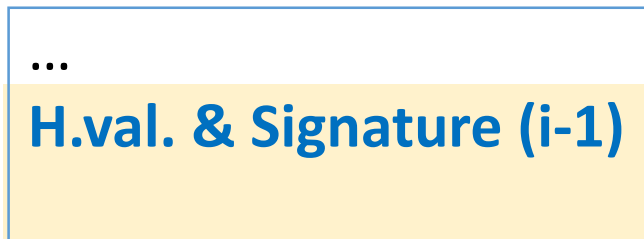
= Verify Hash val. & Signatures Repeatedly



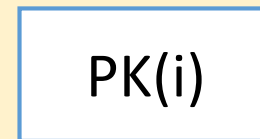
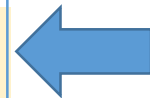
User(i+1)



Repeatedly



Verify Hash val.
& Signature



Verify Hash val.
& Signature

Problem1: Theft: Why Stolen?



■ CEO of Mt.Gox Tokyo;

- Coding of Transaction is **NOT Secure**
- Besides, Never Tested if he can Recover bitcoins



Transaction-Malleability might invite Theft

■ Lower Fee → Longer Transaction-Time

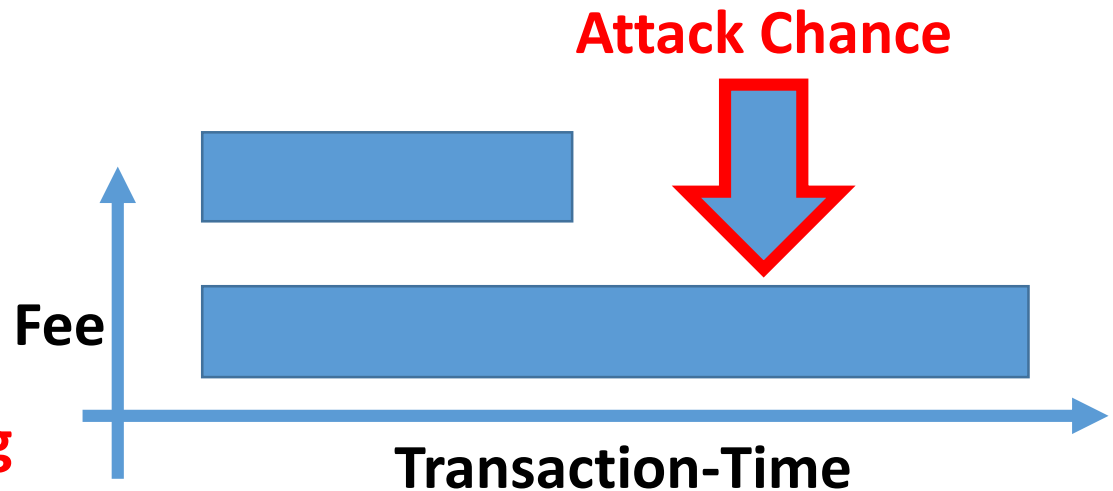
■ If Code is **Not Secure** then

● Longer Transaction-time gives **chance to be Attacked**

● = **Transaction Malleability**



Not-Secure Coding



Transaction Malleability

Problem 2: Illegal Use of Bitcoin



- **Anonymity** might cause Illegal trade
 - Drug
 - Weapon
 - Malware

Anonymity of Bitcoin

- Many Accounts Can be made from your ID
 - Pseudonym Technique
- One-Time Account enables Perfect Anonymity

