WEHIA 2018

23rd Annual Workshop on Economic Science
with Heterogeneous Interacting Agents
International Christian University, Tokyo, Japan
June 30 (Sat) – July 2 (Mon), 2018

A crypto-currency fraud spill incident in Japan

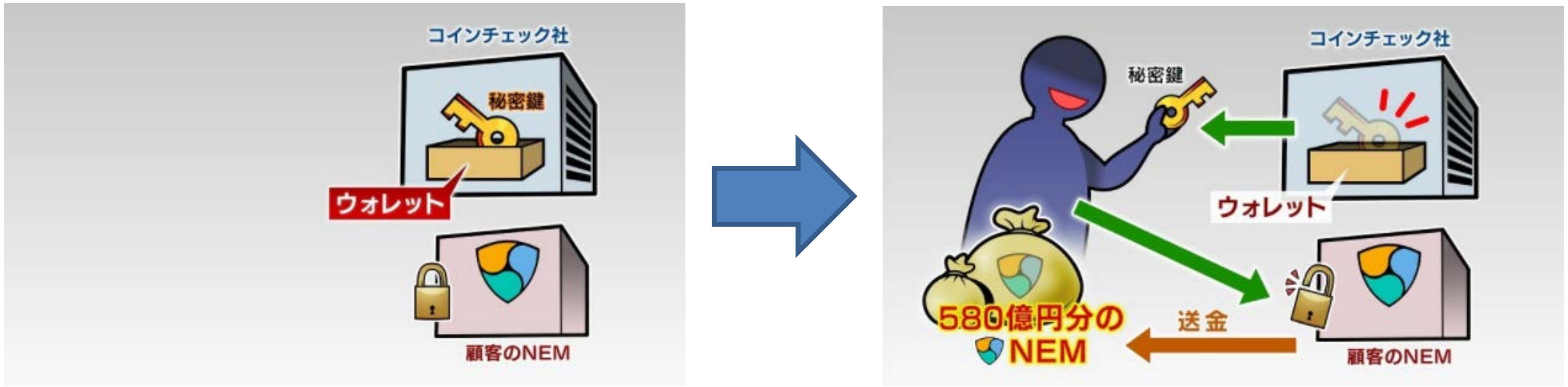
Kyoto University School of Government -
graduate program for public policy studies

Professor Naoyuki Iwashita

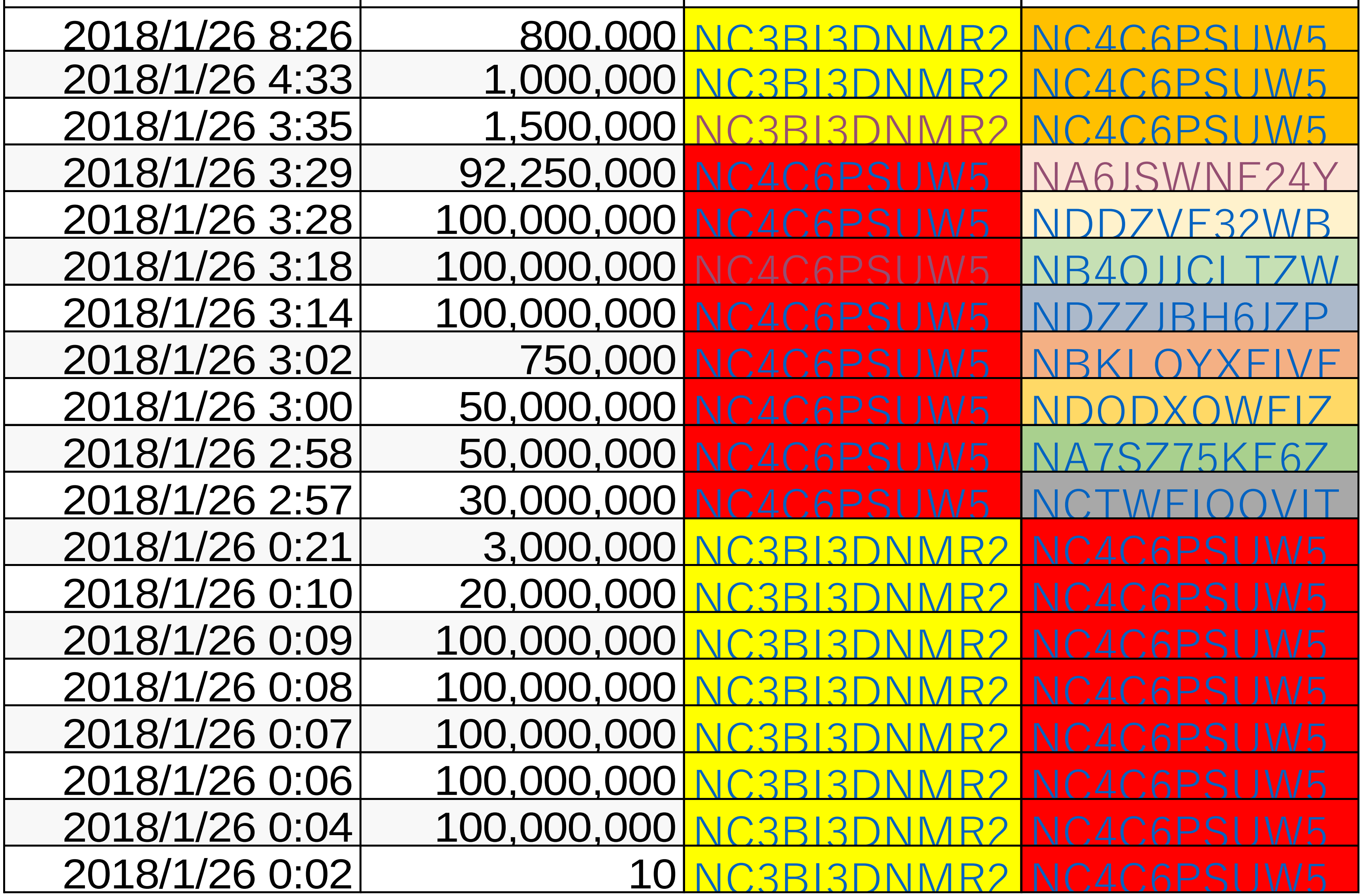
CoinCheck Incident

When and how did the incident happen?

- At very early morning on January 26 of 2018
- "NEM" equivalent of 58 billion yen was illegally remitted and leaked to someone.
- “CoinCheck” was a custodian of the NEM
- More than 260,000 customers had purchased or exchanged NEM and stored the NEM to CoinCheck.

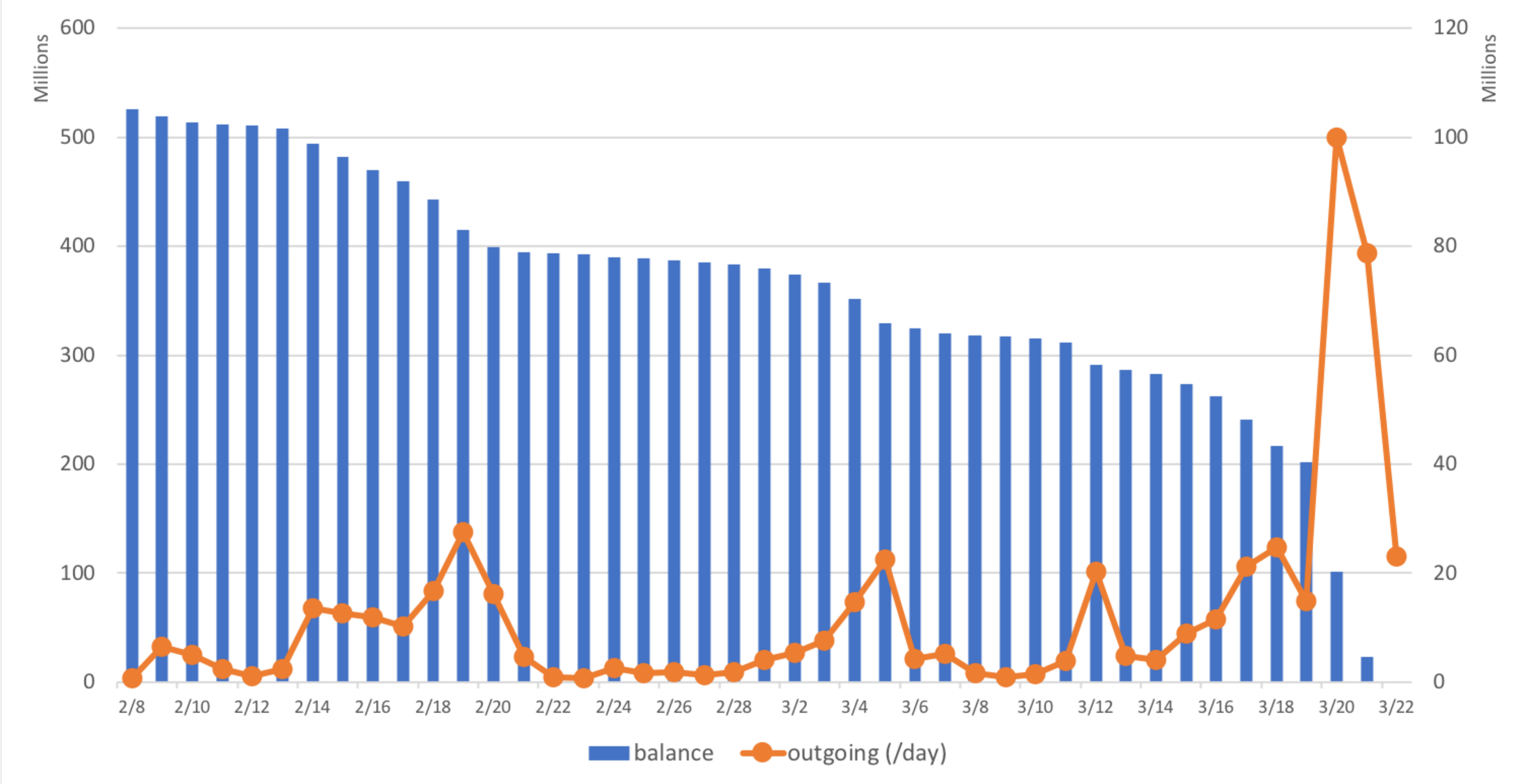


NEM transfer logs at Coincheck incident

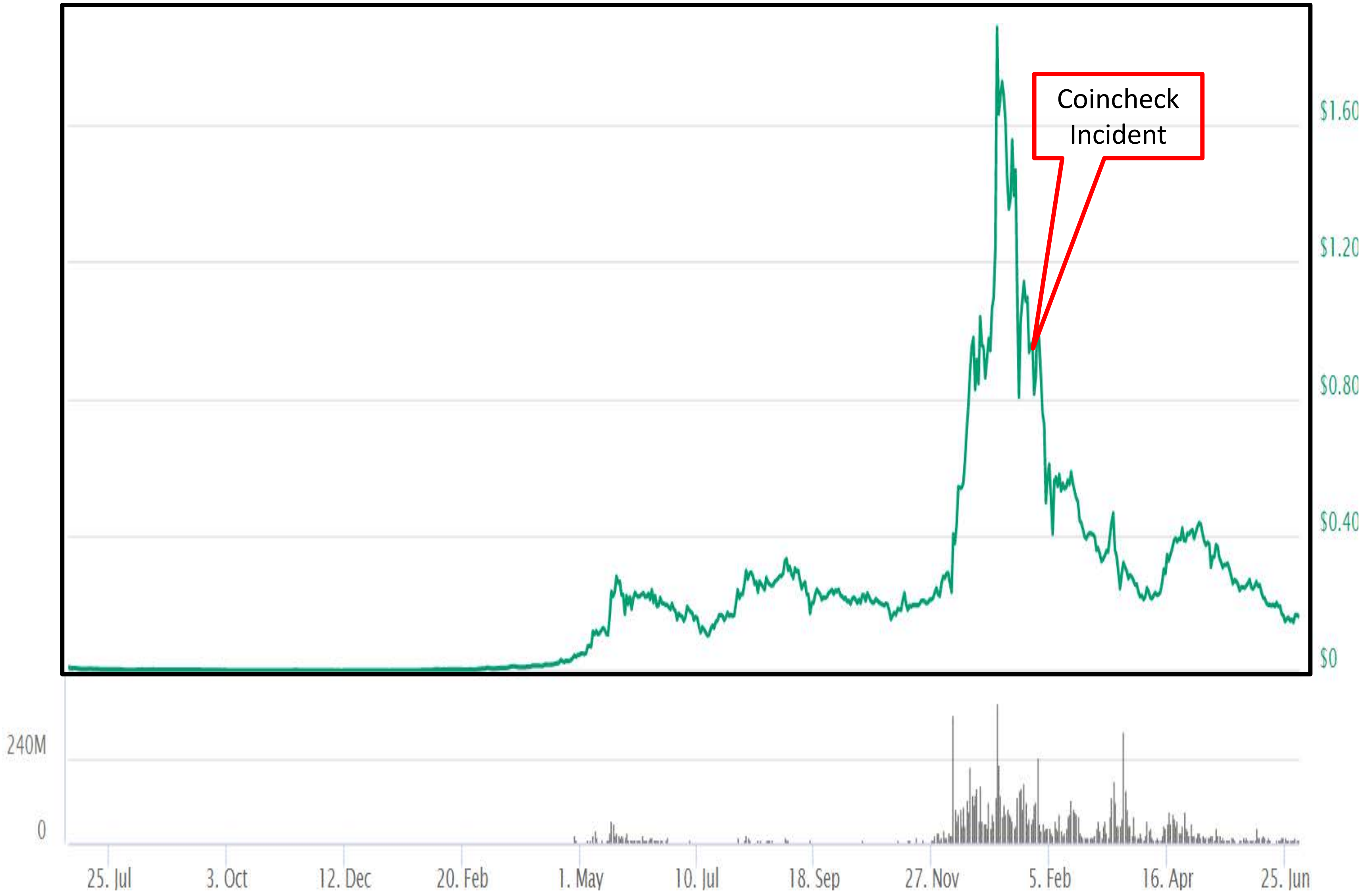


date/time	value(XEM)	sender address	receiver address
2018/1/26 8:26	800,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 4:33	1,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 3:35	1,500,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 3:29	92,250,000	NC4C6PSUW5	NA6JSWNF24Y
2018/1/26 3:28	100,000,000	NC4C6PSUW5	NDDZVF32WB
2018/1/26 3:18	100,000,000	NC4C6PSUW5	NB4QUCLTZW
2018/1/26 3:14	100,000,000	NC4C6PSUW5	NDZZJBH6JZP
2018/1/26 3:02	750,000	NC4C6PSUW5	NBKLOYXFIVF
2018/1/26 3:00	50,000,000	NC4C6PSUW5	NDODXOWFIZ
2018/1/26 2:58	50,000,000	NC4C6PSUW5	NA7SZ75KF6Z
2018/1/26 2:57	30,000,000	NC4C6PSUW5	NCTWFIOOVIT
2018/1/26 0:21	3,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:10	20,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:09	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:08	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:07	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:06	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:04	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:02	10	NC3BI3DNMR2	NC4C6PSUW5

Money Laundering of Stolen NEM

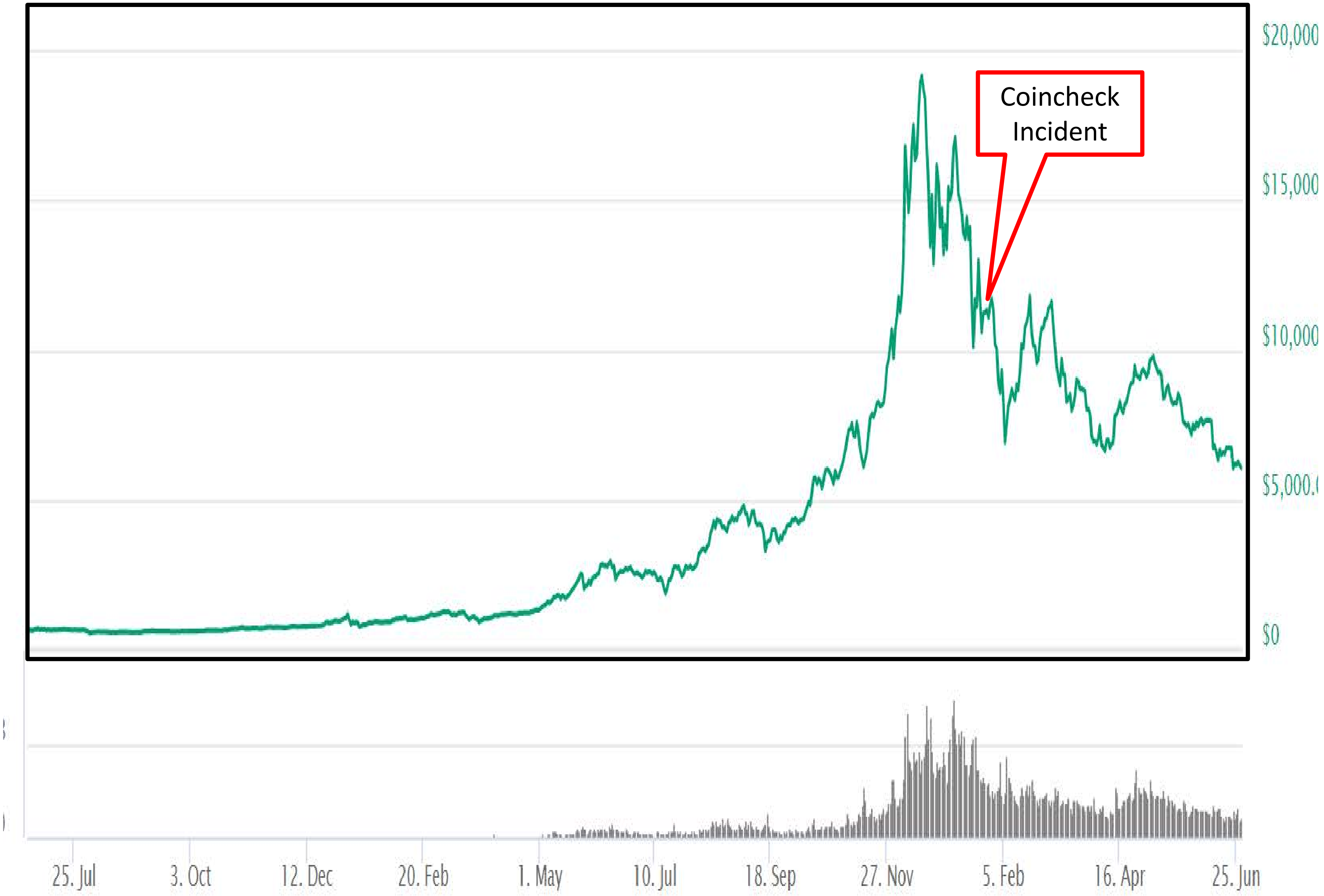


Price of NEM (2016-18)



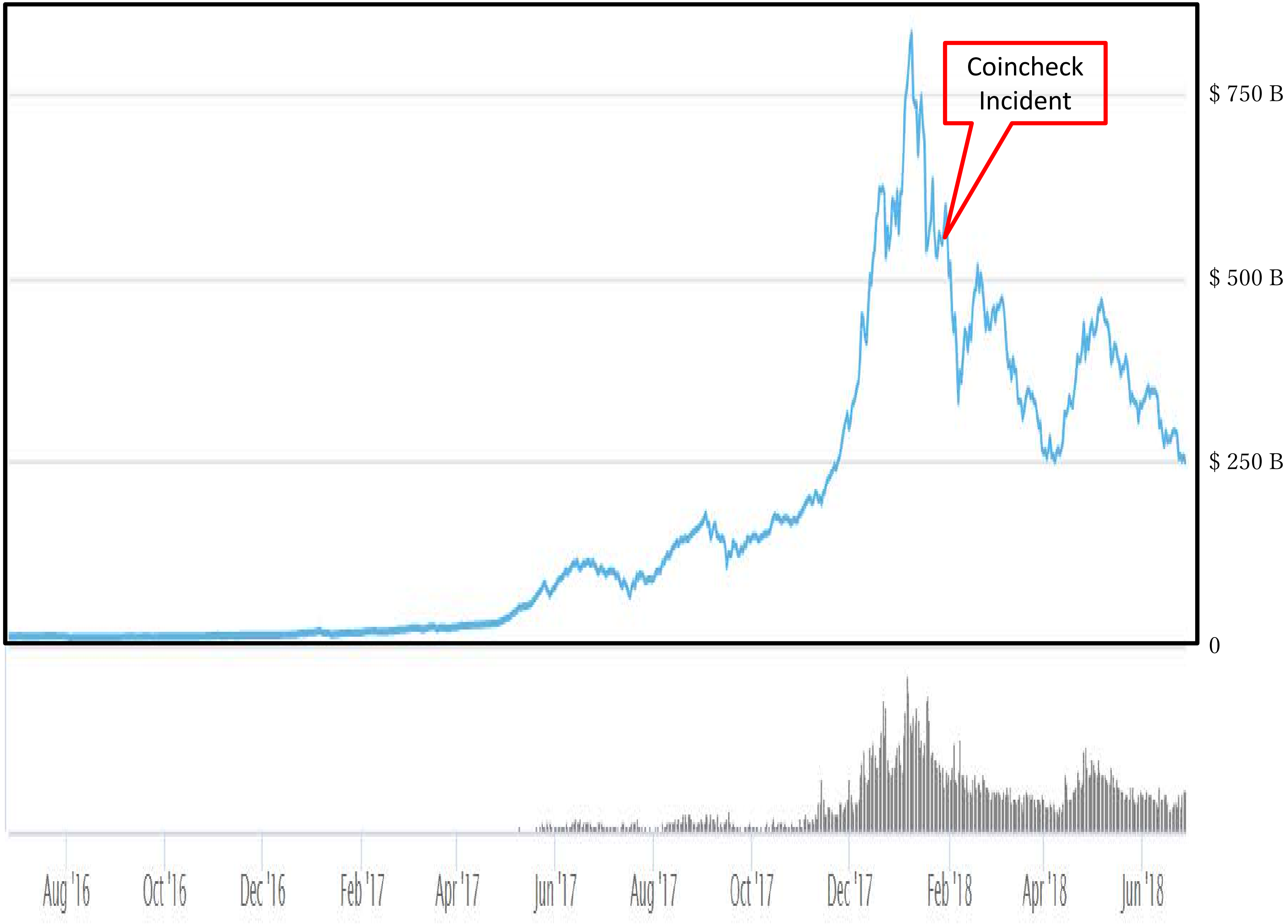
（source）coinmarketcap.com

Price of Bitcoin (2016-18)



（source）coinmarketcap.com

Market Capitalization of all Virtual Currencies (2016-18)

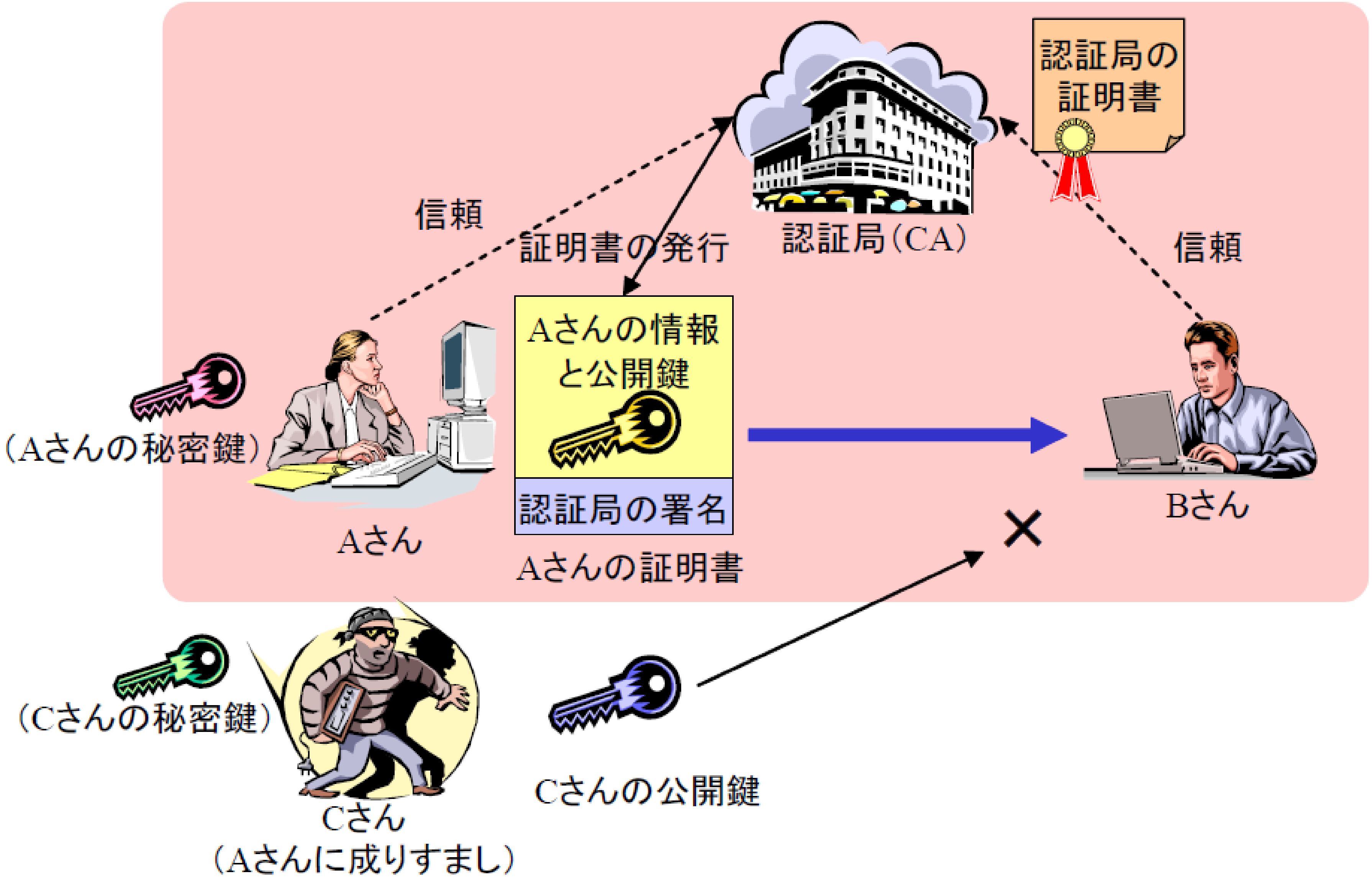


（source）coinmarketcap.com

Checkpoints of Crypto-Exchange Security

- The Cryptocurrency Act in Japan does not have a sufficient mechanism for customer protection that considers that cryptocurrency exchanges store a large amount of customers’ assets.
- Strengthening the legal regulation from the perspective of investor / consumer protection.
- Institutional measures using trust and insurance mechanisms.
- Disclosure of information on unified security standards, management structure and governance, and status of security.

PKI and Certificate Authority＝”Trusted World”



認証局の証明書

信頼

証明書の発行

認証局（CA）

信頼

Aさんの情報と公開鍵

認証局の署名

（Aさんの秘密鍵）

Aさん

Aさんの証明書

Bさん

×

（Cさんの秘密鍵）

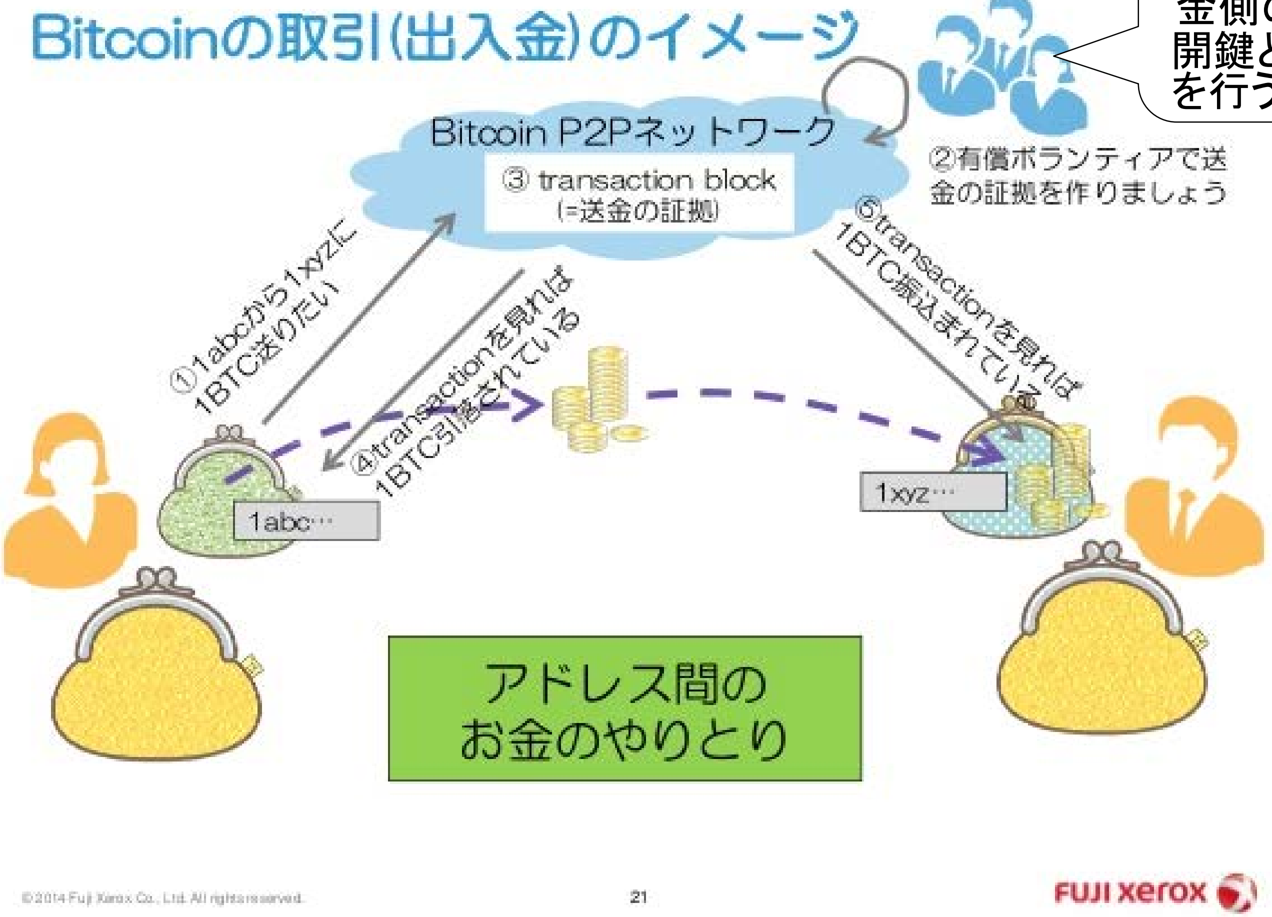
Cさん
（Aさんに成りすまし）

Cさんの公開鍵

（出典）　IPA、「PKI関連技術解説　v1.05」、2002.3.18

No PKI and CA for Bitcoin＝”Trustless World”

ビットコインの取引においては、あえてPKIを使わず、公開鍵をそのままアドレスに使用することで、信頼できる第三者機関を置かない、センターを置かないというポリシーを貫いている。



Bitcoinの取引(出入金)のイメージ

Bitcoin P2Pネットワーク

③ transaction block
(=送金の証拠)

②有償ボランティアで送
金の証拠を作りましょう

①1abcから1xyzに
1BTC送りたい

④transactionを見れば
1BTC引落されている

⑤transactionを見れば
1BTC振込まれている

1abc…

1xyz…

アドレス間の
お金のやりとり

©2014 Fuji Xerox Co., Ltd. All rights reserved.

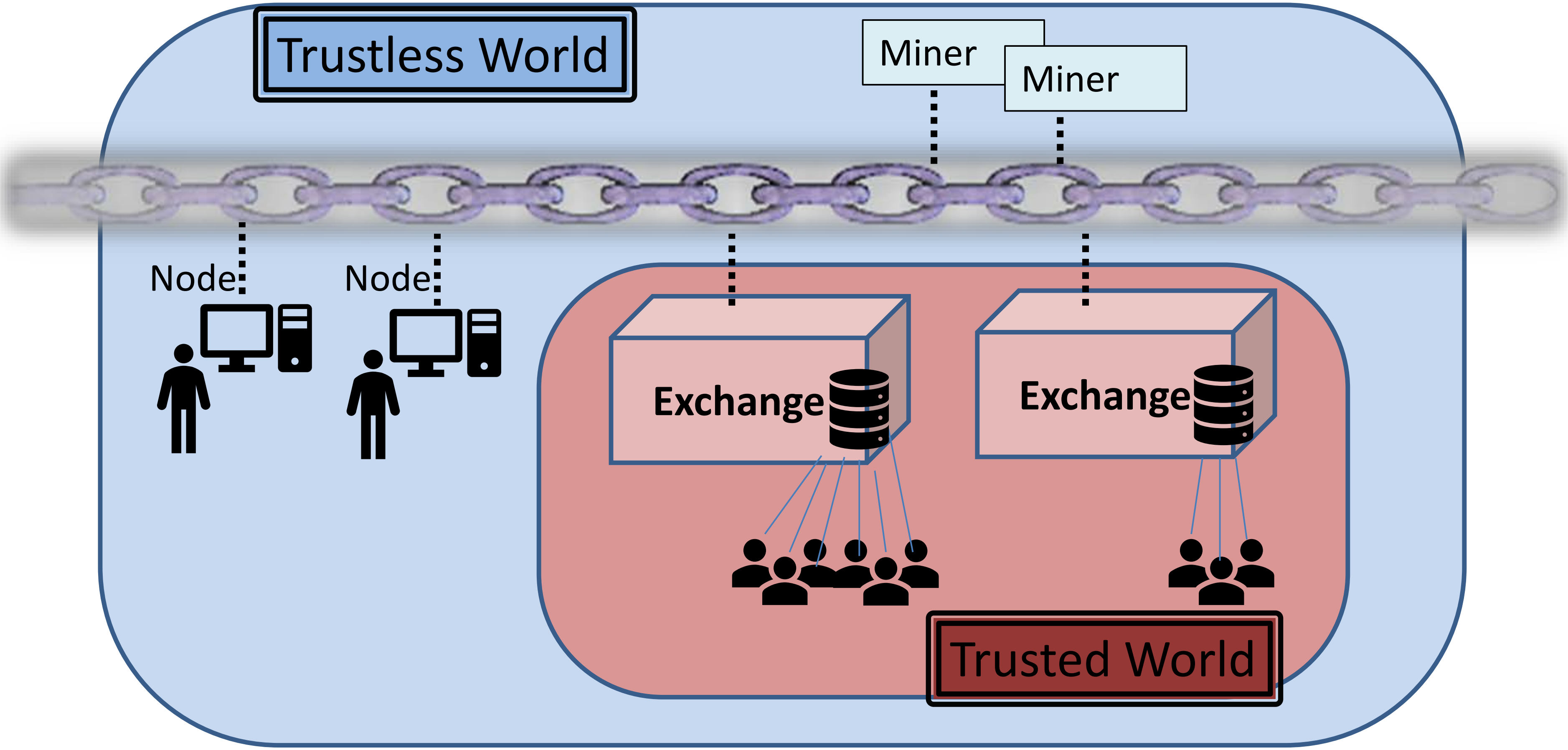
21

FUJI xerox

マイナーは、公開鍵証明書がなくても出金側のアドレスを公開鍵として署名検証を行うことができる。

（出典） 漆嶌賢二、「Bitcoinを技術的に理解する」、2014.6.2

Trusted World within Trustless World

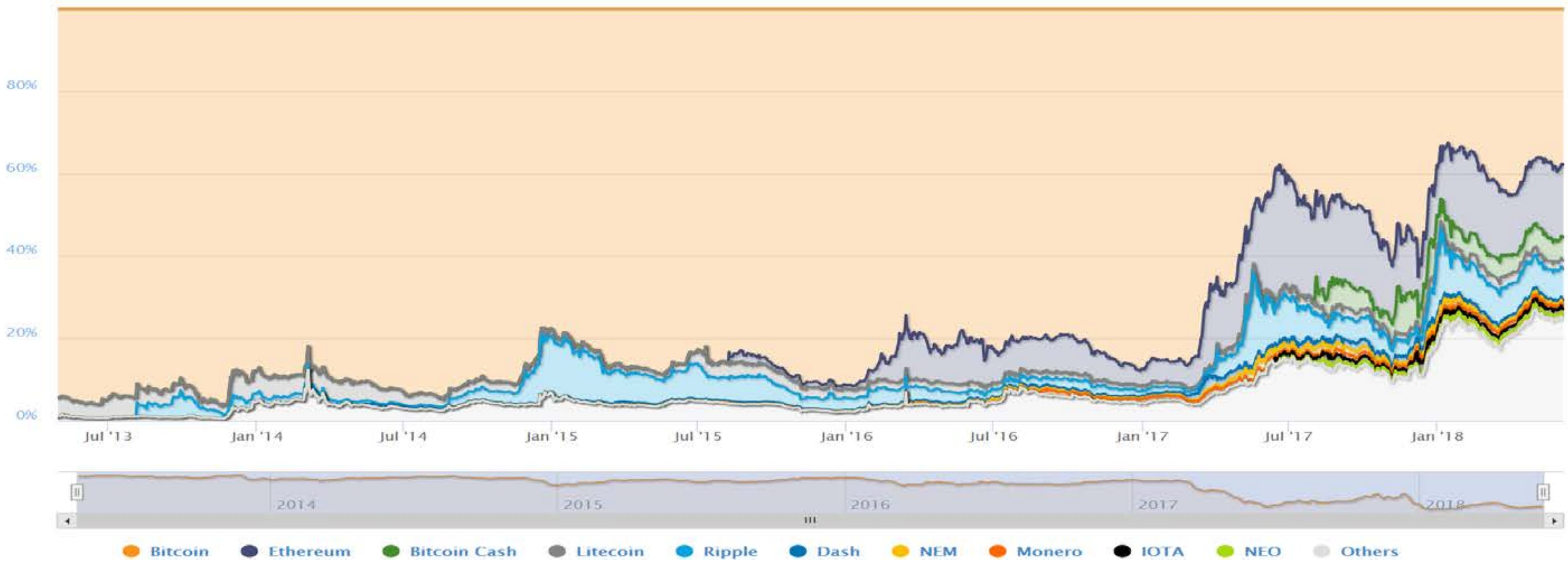


Design philosophy of “decentralization"

- Basic design concept of bitcoin = “decentralization"
  - Policy that never creates reliable central organization.
  - The cryptocurrencies with these policies were easy used internationally, by crossing over the border and differences in law and political system.
- From the perspective of the ordinary world, which is based on the existence of reliable central institutions such as governments, central banks and courts, the world of virtual currencies is extremely fragile and dangerous.
- Since NEM also has a policy to have no reliable central organization, no one can arbitrarily rewrite information including the any government agency.
- Is it possible for the government to properly control the cryptocurrencies with such a strange philosophy?

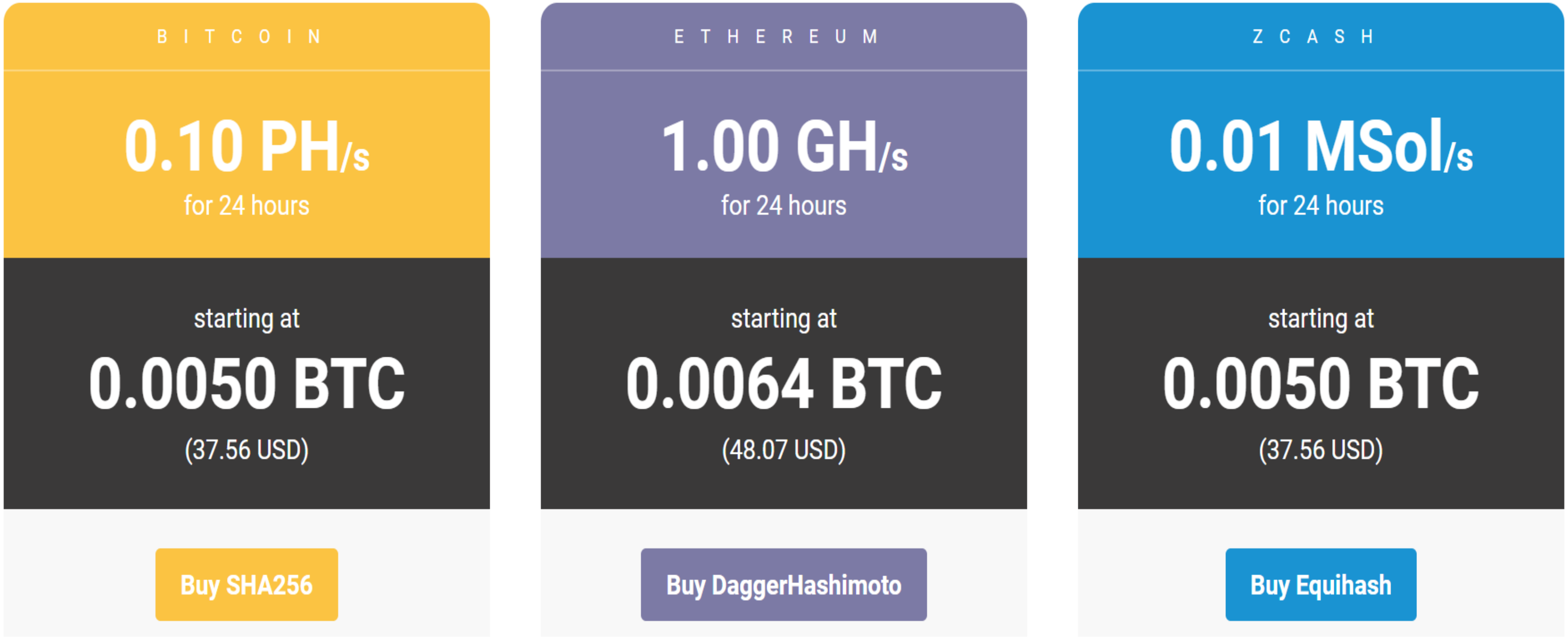
51% attack to blockchains

- A 51% attack was known to be a potential (theoretical) attack on the bitcoin network whereby an organization is somehow able to control the majority of the network mining power (hashrate). But in May 2018, Monacoin was actually attacked by using 51% mining power (selfish mining attack). In the next two weeks, Bitcoin Gold, Verge, ZenCash were also attacked. The attack methods were slightly different, all of these attacks used enormous hash power to make a longer fork and double-spend victim coins.
- One of the reasons such attack was realized was the price increase of minor altcoins.



Why was the 51% attack realized？

- Another reason for the 51% attack came from nicehash.com. NiceHash is the world’s largest crypto-mining marketplace. It is based on the concept of a sharing economy by connecting sellers and buyers of computing power from all over the world.
- Attackers can purchase vast hash powers from the marketplace to attack minor altcoins which have relatively low hashrate.



BITCOIN

0.10 PH/s

for 24 hours

starting at

0.0050 BTC

(37.56 USD)

ETHEREUM

1.00 GH/s

for 24 hours

starting at

0.0064 BTC

(48.07 USD)

ZCASH

0.01 MSol/s

for 24 hours

starting at

0.0050 BTC

(37.56 USD)

PoW 51% Attack Cost

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$126.45 B	SHA-256	37,598 PH/s	*$699,965*	1%
Ethereum	ETH	$55.85 B	Ethash	207 TH/s	*$376,501*	2%
Bitcoin Cash	BCH	$16.89 B	SHA-256	3,644 PH/s	*$67,837*	14%
Litecoin	LTC	$6.68 B	Scrypt	281 TH/s	*$61,469*	7%
Monero	XMR	$2.50 B	CryptoNightV7	426 MH/s	*$28,643*	14%
Dash	DASH	$2.47 B	X11	1 PH/s	*$11,548*	41%
Ethereum Classic	ETC	$1.56 B	Ethash	9 TH/s	*$15,975*	56%
Bytecoin	BCN	$1.20 B	CryptoNight	490 MH/s	*$1,105*	79%
Zcash	ZEC	$1.01 B	Equihash	392 MH/s	*$53,033*	17%
Bitcoin Gold	BTG	$719.79 M	Equihash	27 MH/s	$3,677	249%
Bitcoin Private	BTCP	$451.39 M	Equihash	5 MH/s	$684	1337%
Dogecoin	DOGE	$387.29 M	Scrypt	190 TH/s	*$41,641*	11%
MonaCoin	MONA	$197.63 M	Lyra2REv2	2 TH/s	$3,577	734%
Electroneum	ETN	$156.21 M	CryptoNightV7	423 MH/s	*$28,401*	14%
ZenCash	ZEN	$119.63 M	Equihash	60 MH/s	$8,053	114%

（Source） https://www.crypto51.app/