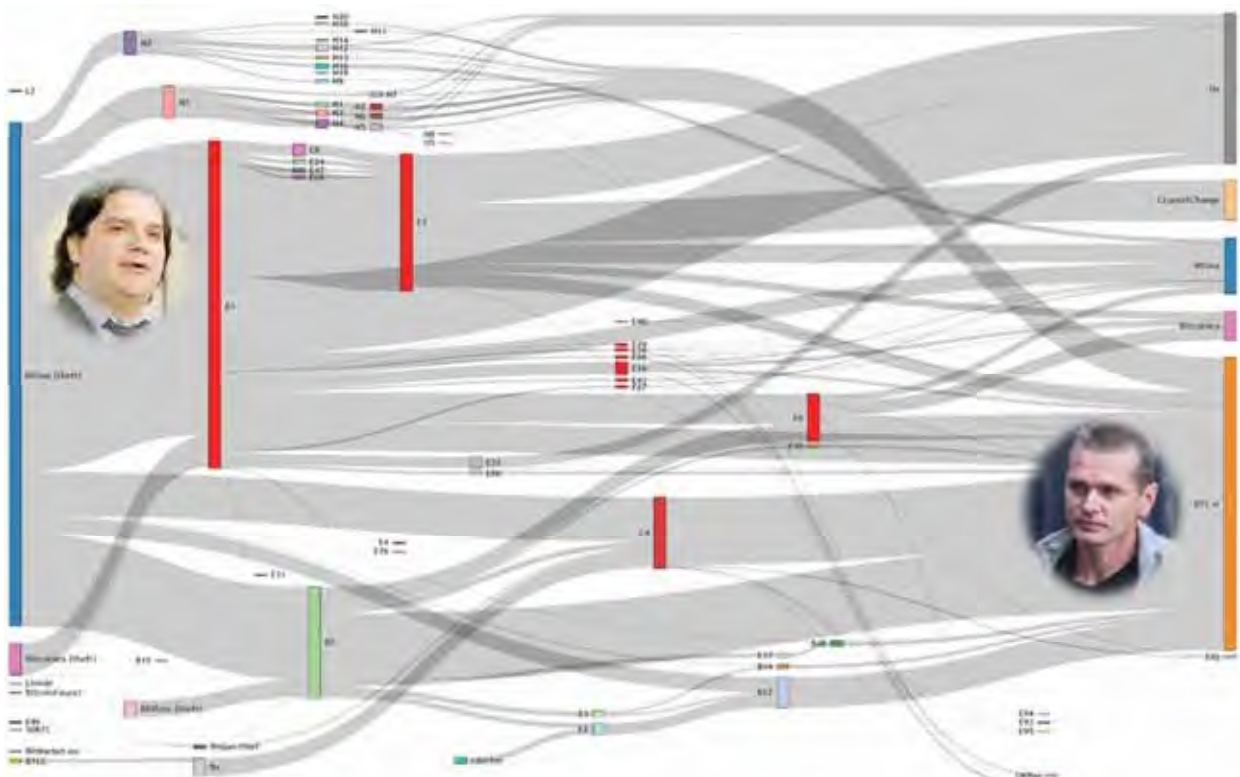


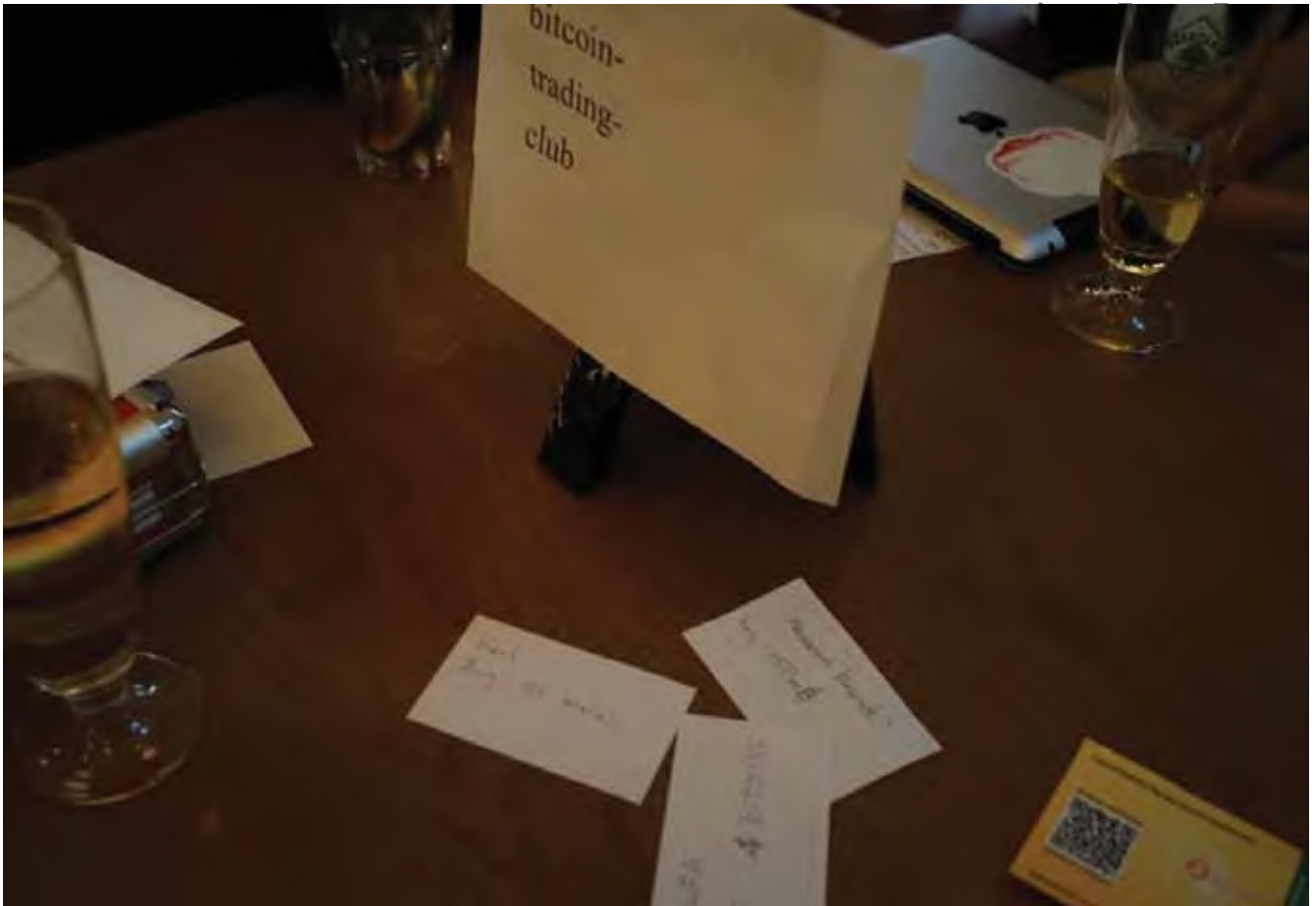


Source: <http://www.coindesk.com/price/> 2014年に閲覧

MtGOXから流出した資金の流れ (WizSecによる分析)



Source: <https://blog.wizsec.jp/2017/07/breaking-open-mtgox-1.html>



Copyright (c) 2018, Japan Digital Design, Inc., All rights reserved.

32

## 2015年 FATFガイドラインと2016年 資金決済法の改正

Japan Digital Design

- 2015年 FATFが取引所の口座開設や、仮想通貨の交換に対して**本人確認**を求める
- 2016年 勧告を受け日本でも資金決済法や犯罪収益移転防止法を改正「仮想通貨交換業者」を定義し**登録制**に
- 2017年度の税制大綱からは資金決済法に規定する仮想通貨の譲渡について**消費税を非課税**とした



Copyright (c) 2018, Japan Digital Design, Inc., All rights reserved.

33

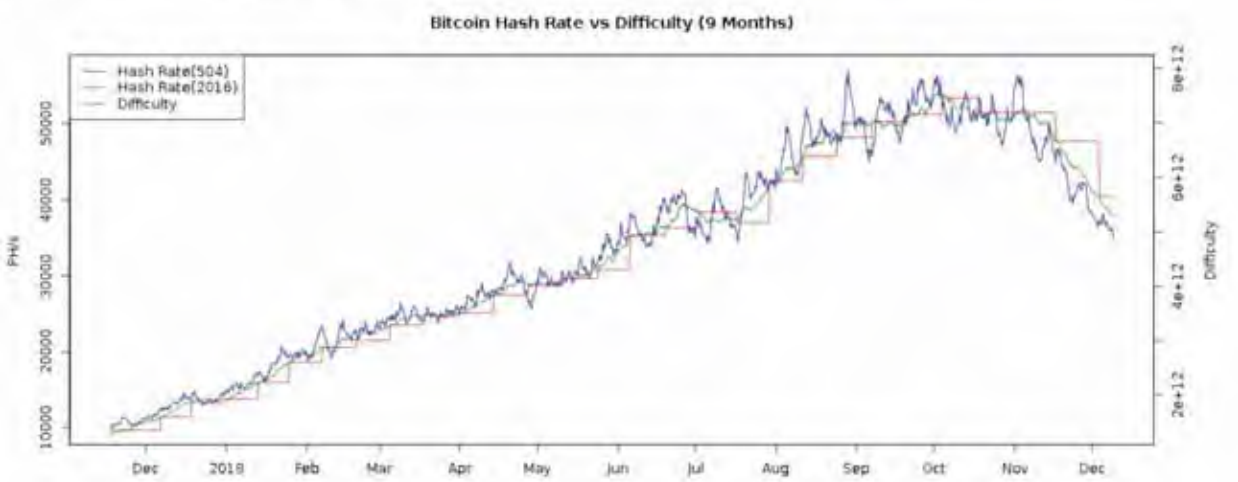


<https://www.weforum.org/agenda/2016/06/these-photos-show-you-inside-an-icelandic-bitcoin-mine>

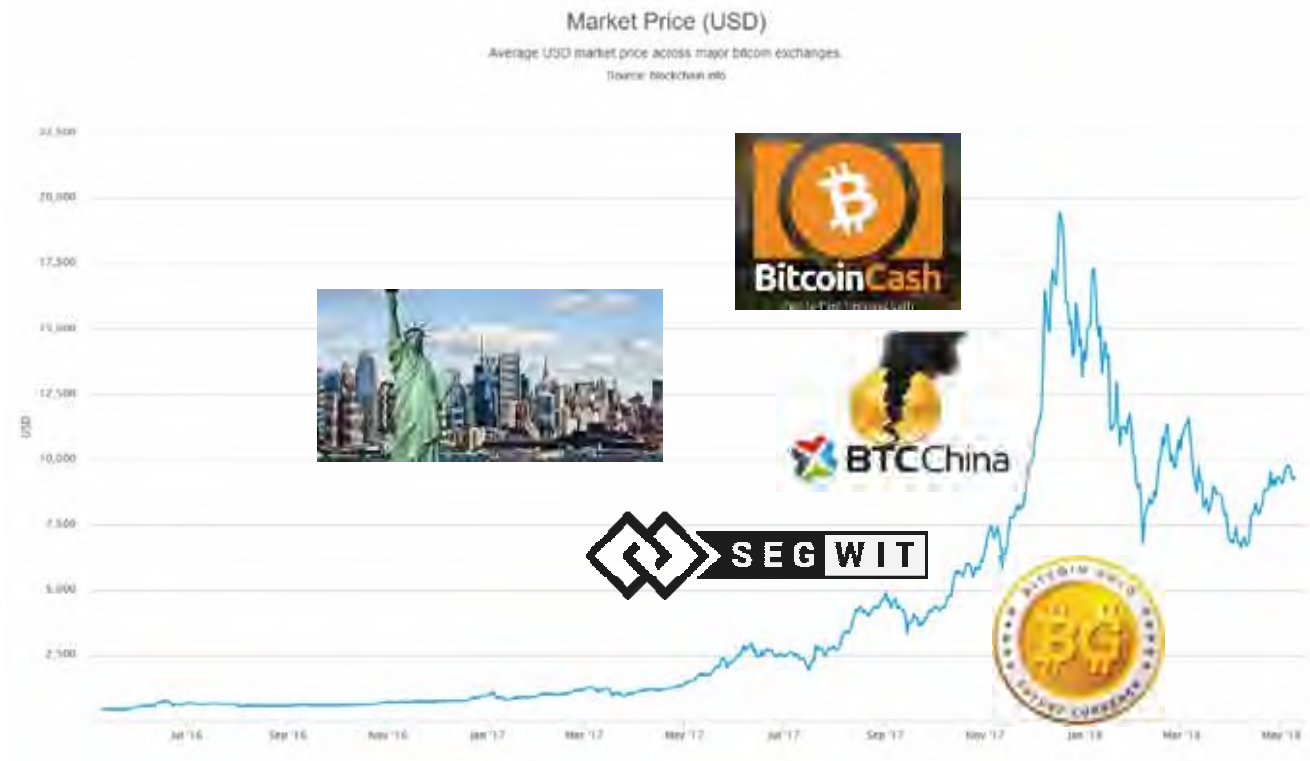
BitcoinにおけるHashrateの上昇と難易度の調整

Bitcoin Difficulty: 5,846,403,851,534  
 Estimated Next Difficulty: 5,261,178,561,254 (-8.82%)  
 Adjust time: After 1297 Blocks, About 10.0 days  
 Hashrate(2): 34,835,022,717 GH/s  
 Block Generation Time(?): 1 block: 11.1 minutes  
 3 blocks: 33.2 minutes  
 6 blocks: 1.1 hours  
 Updated: 14:45 (4.5 minutes ago)

Difficulty	5846403851534	BTC/USD	5219.5		
200000	PH/s	1.854e-8	BTC/hour	6.68665331	USD/hour
1000	MH/s	4.453e-8	BTC/day	6.0613e7	USD/day
1	GH/s	1.117e-7	BTC/week	6.082607	USD/week
1,001	TH/s	6.68666133e	BTC/month	6.064792	USD/month



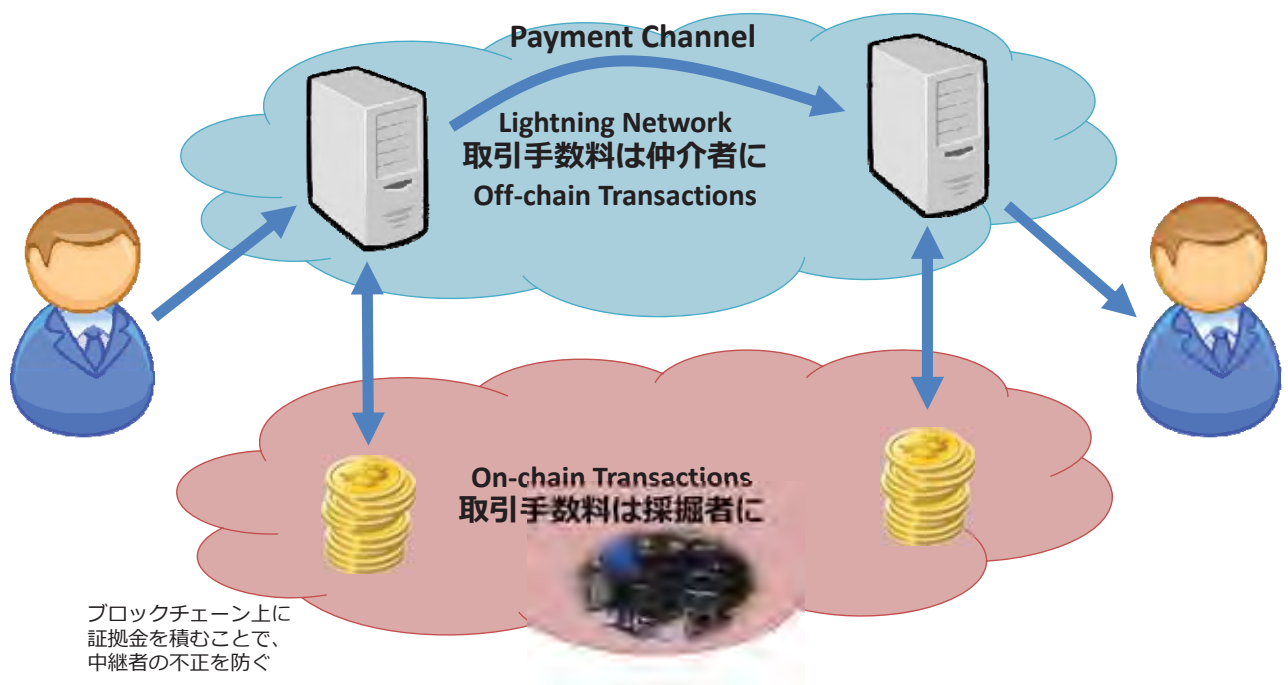
<https://bitcoinwisdom.com/bitcoin/difficulty>



Copyright (c) 2018, Japan Digital Design, Inc., All rights reserved.

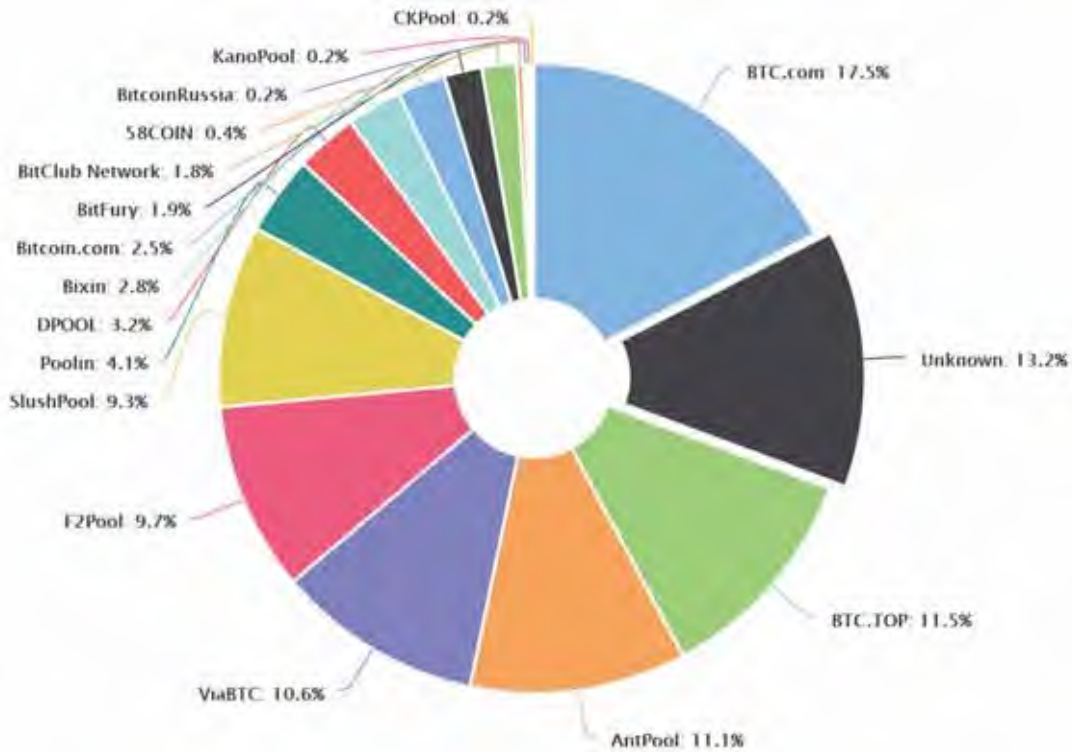
36

## 取引手数料の分け前を巡る開発者と採掘者の確執



Copyright (c) 2018, Japan Digital Design, Inc., All rights reserved.

37



Copyright (c) 2018, Japan Digital Design, Inc., All rights reserved.

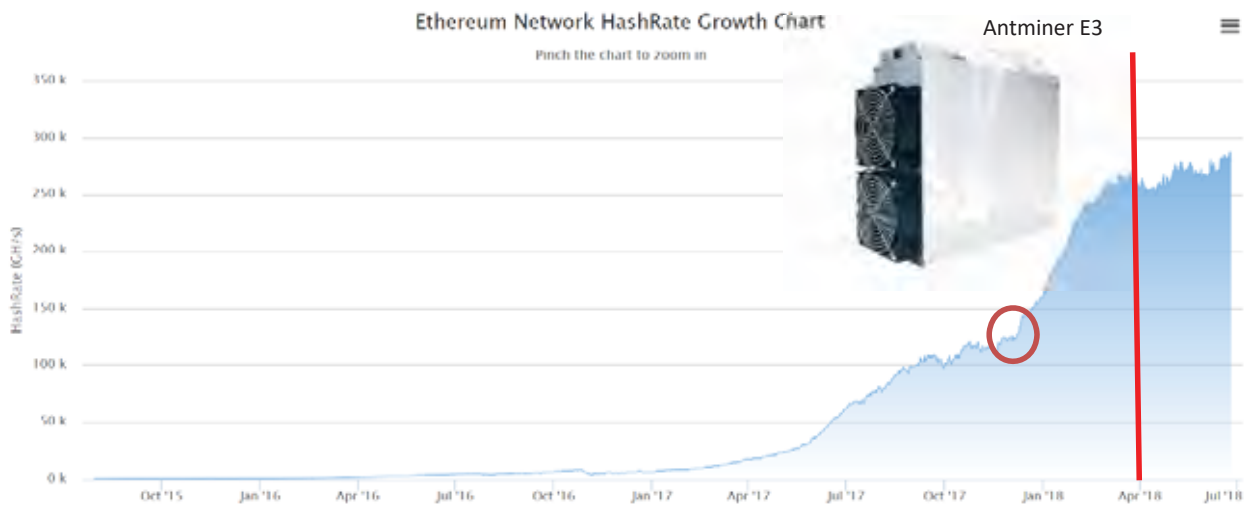
38

2018年5月から多発した仮想通貨Blockchain書換攻撃

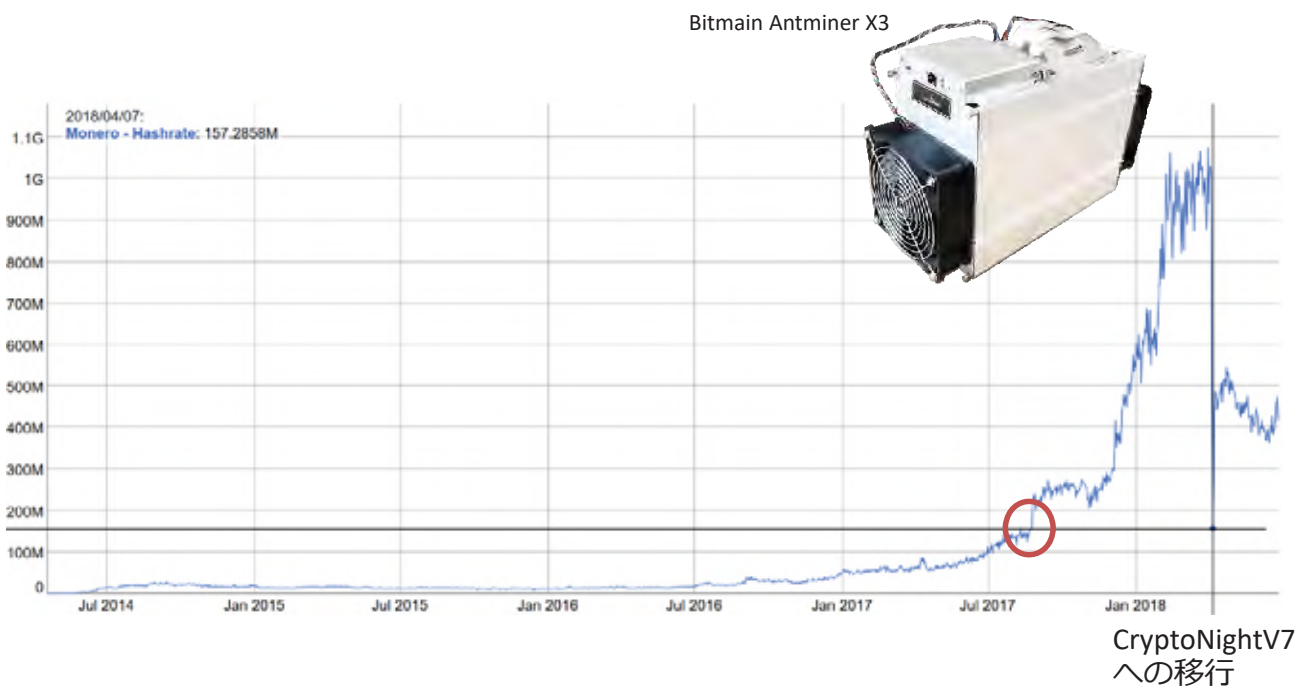
日付	銘柄	被害額
5月15日	BitcoinGold	約20億円
5月15日	Monacoin	約1000万円
5月22日	Verge	約2億円
6月4日	ZenCash	8000万円

Copyright (c) 2018, Japan Digital Design, Inc., All rights reserved.

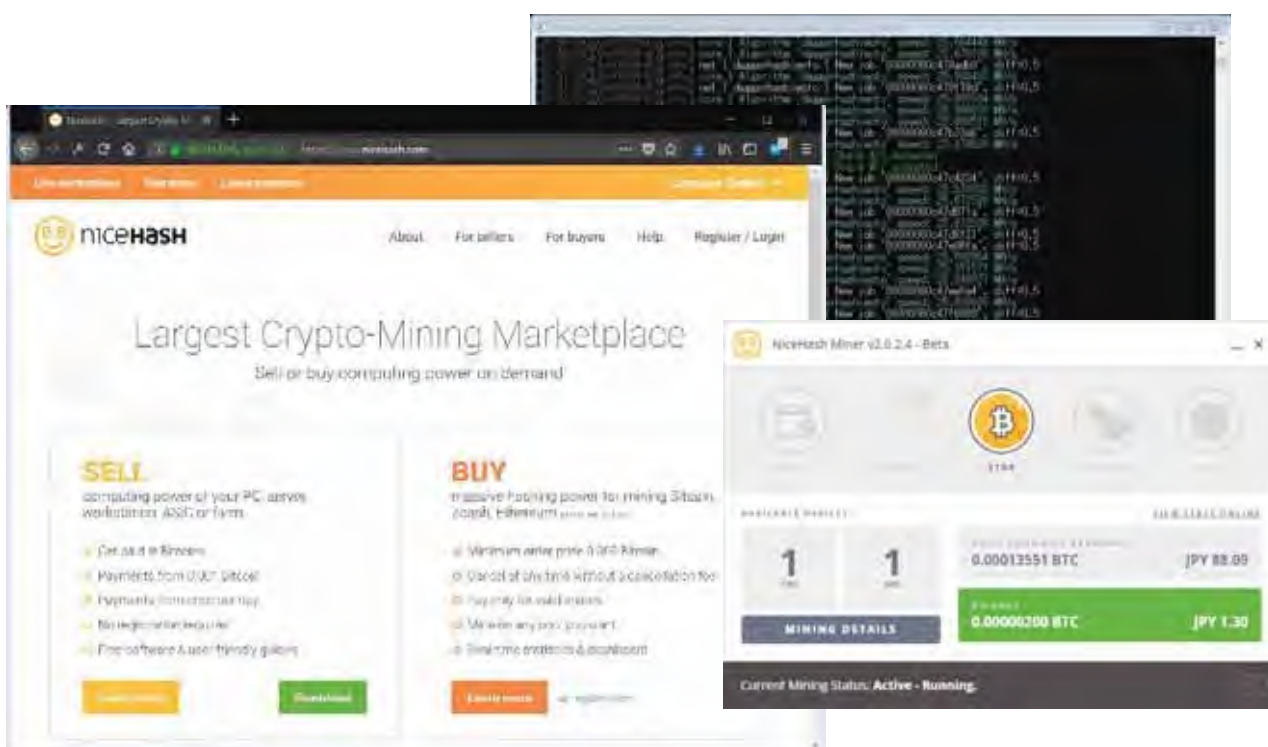
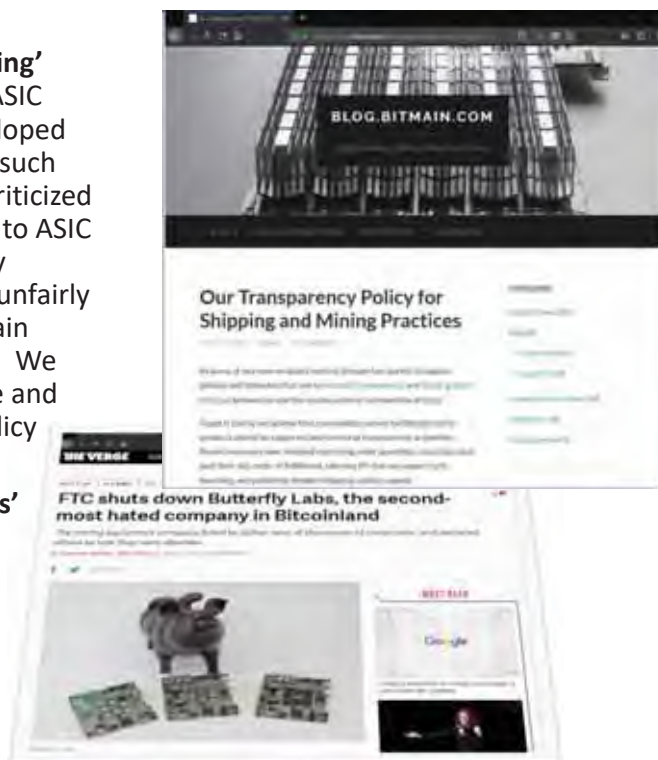
39



- ASICによるHashrate増を価格下落によるGPU採掘撤退が打ち消した？
- 製造元では2017年末からASIC Miningが増えていたのだろうか？



1. **Disclosure policy on self-mining**
2. **Zero tolerance policy against ‘secret mining’**  
 ‘Secret mining’ is a practice whereby an ASIC manufacturer may mine with newly developed equipment prior to selling or distributing such equipment to customers. This has been criticized as conferring an unfair market advantage to ASIC manufacturers over individual community member miners. Bitmain itself has been unfairly accused of this practice. In the end, Bitmain values transparency and fair competition. We therefore remain opposed to this practice and maintain our long-held zero-tolerance policy regarding same.
3. **We will never seek to mine ‘empty blocks’**
4. **We will provide shipping and volume information of new miners to the public**



Bitcoin設計時の前提	Altcoin, Fork coinの現実
世の中にはBitcoinしか存在しない	世の中には多様な仮想通貨が併存
採掘者は広く分散	採掘者は寡占化されたmining poolに所属
Minerは多くのBitcoinと採掘にしか使えない 計算機を保有	Minerは様々な仮想通貨の中で収益性の高い銘柄を 採掘
MinerにとってBitcoinの価値を毀損することの デメリットが大きい	不正によって仮想通貨が暴落しても他の銘柄を 採掘すれば良い
Hashrateは安定的な上昇傾向	ASIC MiningによるHashrateの急増 Minerの撤退、乗換によるHashrateの急減
Bitcoinの価値はマイルドに上昇する	仮想通貨の価値は乱高下する
過半数のMinerは誠実	Minerは採掘報酬と不正利得とを比較
利用者は支払時にBlockの確定を待つ	事業者は利用者ニーズや他の決済手段との競争で 十分なconfirmationを待たず決済する
発行上限は設計であらかじめ固定	相次ぐfork coinで価値は希釈化 ハードフォークで発行上限の変更も可能
発行者・運営主体はいない	フォークを決めた運営主体が実在
支払に利用される電子的な支払手段	退蔵される投機対象・資産保存手段

## 2018年1月 コインチェック事件



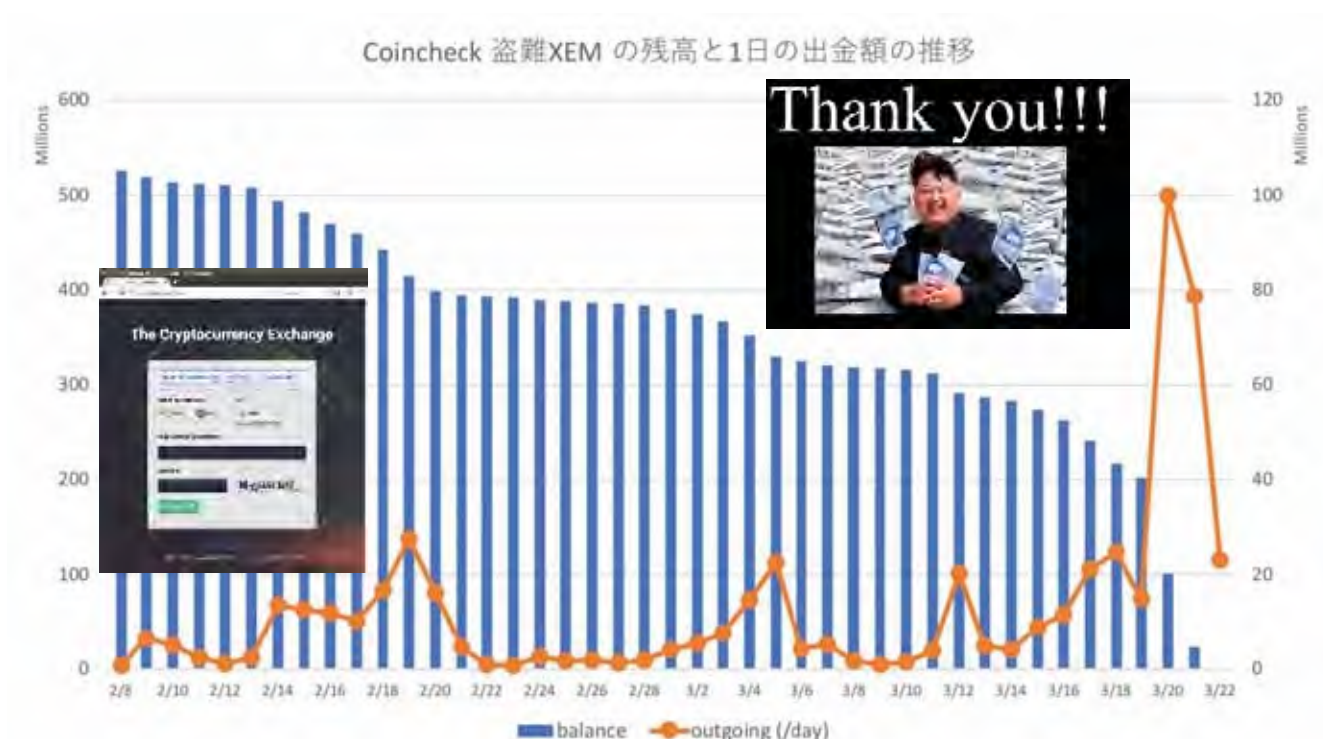
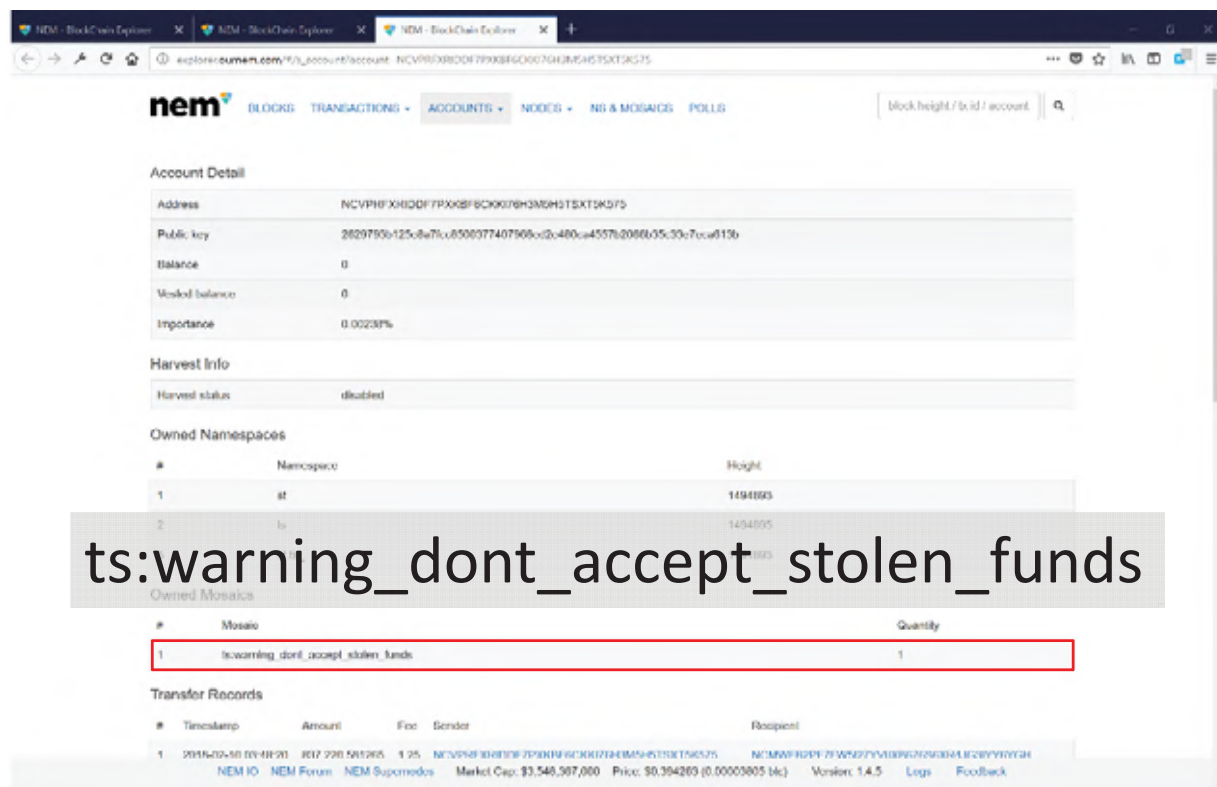


Transaction ID	Date	Amount	Fee	From	To
256	2018-01-26 05:28:44	100,000,000	1.25	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G	ND02VF32W53LW9G3V9G1C00GZVENCNR0E2ZV03H
257	2018-01-26 05:35:07	100,000,000	1.25	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G	NB4JQJ3LZVW1W9H8RUMFD0NDZ9DROV5DRC02M1
258	2018-01-26 03:14:00	100,000,000	1.20	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G	NDZL8H6JDPY5W9PYHALLWMTW9HOYTQGX53HAW
259	2018-01-26 03:02:12	700,000	1.20	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G	NBKL0YK8IVEEGAVYPLM6ZJIFH43Y8MLAPUNPM1
260	2018-01-26 03:00:33	50,000,000	1.25	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G	ND00X0W8ZGJ5M8EUKACF48HC2CB708T8V6750
261	2018-01-26 02:58:42	50,000,000	1.25	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G	NA76Z79KF6ZK927TR8G6JUBW95JH02H45P9K9W
262	2018-01-26 02:57:34	30,000,000	1.25	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G	NCT9F300VTRZ9YV1GQ3PE3M9V525KMLD53LWFQ
263	2018-01-26 00:21:14	3,000,000	1.25	NC3BDDNMR2P0E00MP2NKOQGS4KMS70YRKA5C8Z	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G
264	2018-01-26 00:10:36	20,000,000	1.25	NC3BDDNMR2P0E00MP2NKOQGS4KMS70YRKA5C8Z	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G
265	2018-01-26 00:09:22	100,000,000	1.20	NC3BDDNMR2P0E00MP2NKOQGS4KMS70YRKA5C8Z	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G
266	2018-01-26 00:08:21	100,000,000	1.20	NC3BDDNMR2P0E00MP2NKOQGS4KMS70YRKA5C8Z	NL408PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G
267	2018-01-26 00:07:04	100,000,000	1.25	NC3BDDNMR2P0E00MP2NKOQGS4KMS70YRKA5C8Z	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G
268	2018-01-26 00:06:46	100,000,000	1.25	NC3BDDNMR2P0E00MP2NKOQGS4KMS70YRKA5C8Z	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G
269	2018-01-26 00:04:56	100,000,000	1.25	NC3BDDNMR2P0E00MP2NKOQGS4KMS70YRKA5C8Z	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G
270	2018-01-26 00:02:13	10	0.05	NC3BDDNMR2P0E00MP2NKOQGS4KMS70YRKA5C8Z	NC4C6PSUW5CLTD155XAGJDDJGZNE5KFK5MCN770G

# ホワイトハッカーによる追跡劇

mizunashi.coincheck\_stolen\_funds\_do\_not\_acc pt\_trades:owner\_of\_this\_account\_is\_hacker

#	Mosaic	Quantity
1	sevendiglyphcoin	100
2	mizunashi.coincheck_stolen_funds_do_not_acc pt_trades:owner_of_this_account_is_hacker	1
3	mimblecoin	100000
4	friend_vegetable:carrot	1
5	cut_my_hair:nekoboss	11
6	nemroyan faucet	1



出典 : <https://twitter.com/MasafumiNegishi/status/976767126169010176>



## 前回の討議において複数のご意見を頂いた事項：匿名性が高いなど問題がある仮想通貨の取扱い

### ご意見

- 匿名性が高いなど、利用者保護又は交換業の適正かつ確実な遂行に支障を及ぼすおそれがあると認められる仮想通貨について、交換業者による取扱いを禁止すべき。
- 匿名性は顧客のプライバシー保護にも資するもの。また、交換業者による取扱いを禁止した場合、海外業者での取引に流れるなどのおそれもあり、規制が課される交換業者において取引がなされた方がマネロン対策の観点からも望ましい可能性。厳格な本人確認などを課した上で交換業者による取扱いを認めるべきではないか。
- 将来、仮想通貨が日銀券の代替として広く決済に使用されるような状況になった場合、匿名性のない仮想通貨が適当なのか。

### 留意点

- 仮想通貨は、インターネット経由で遠隔の個人間においても容易に移転が可能。匿名性が高い仮想通貨が流通すると、移転経路の追跡が困難となり、マネロン・テロ資金供与対策上の問題のほか、ハッキングにより流出した仮想通貨の追跡が極めて困難となるなどの問題があるか。
- 仮想通貨が日銀券の代替として広く使用されるような状況になった場合には、中央銀行による通貨管理のあり方、マネロン・テロ資金供与対策、個人のプライバシー保護のあり方など、法律体系全体の見直し自体も必要になるか。まずは、足許の状況を踏まえた対応を検討していくことが必要か。

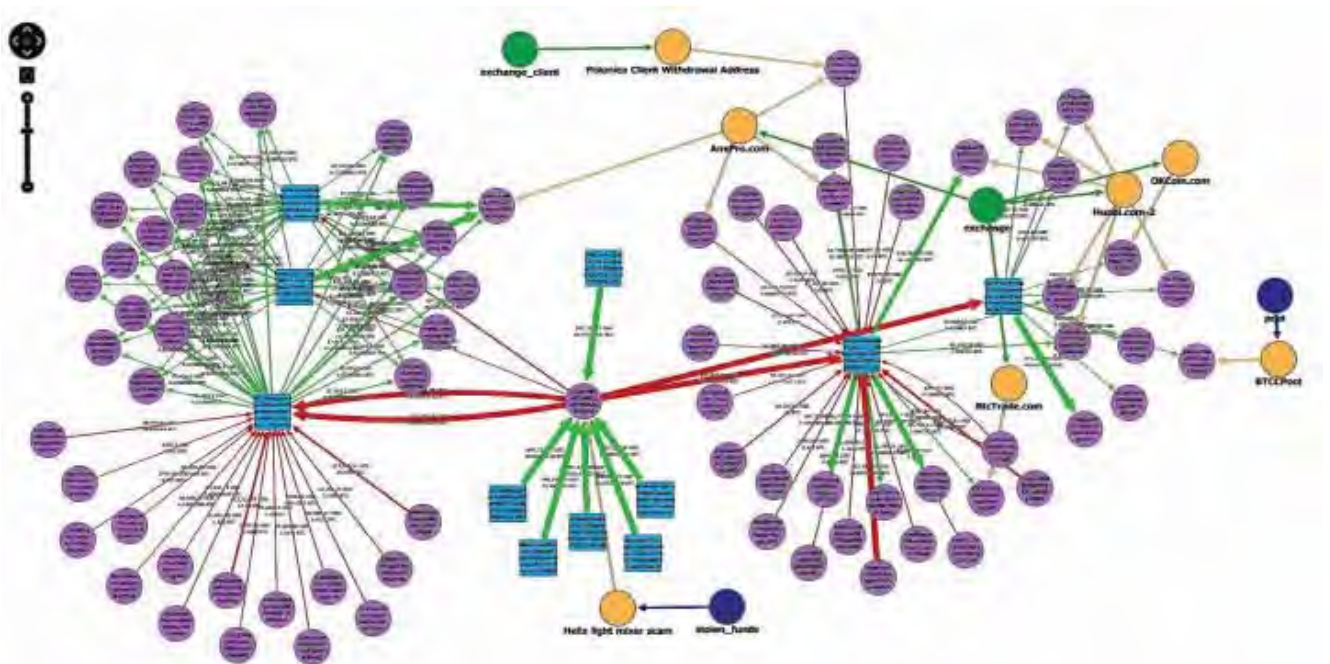
Traditional Privacy Model



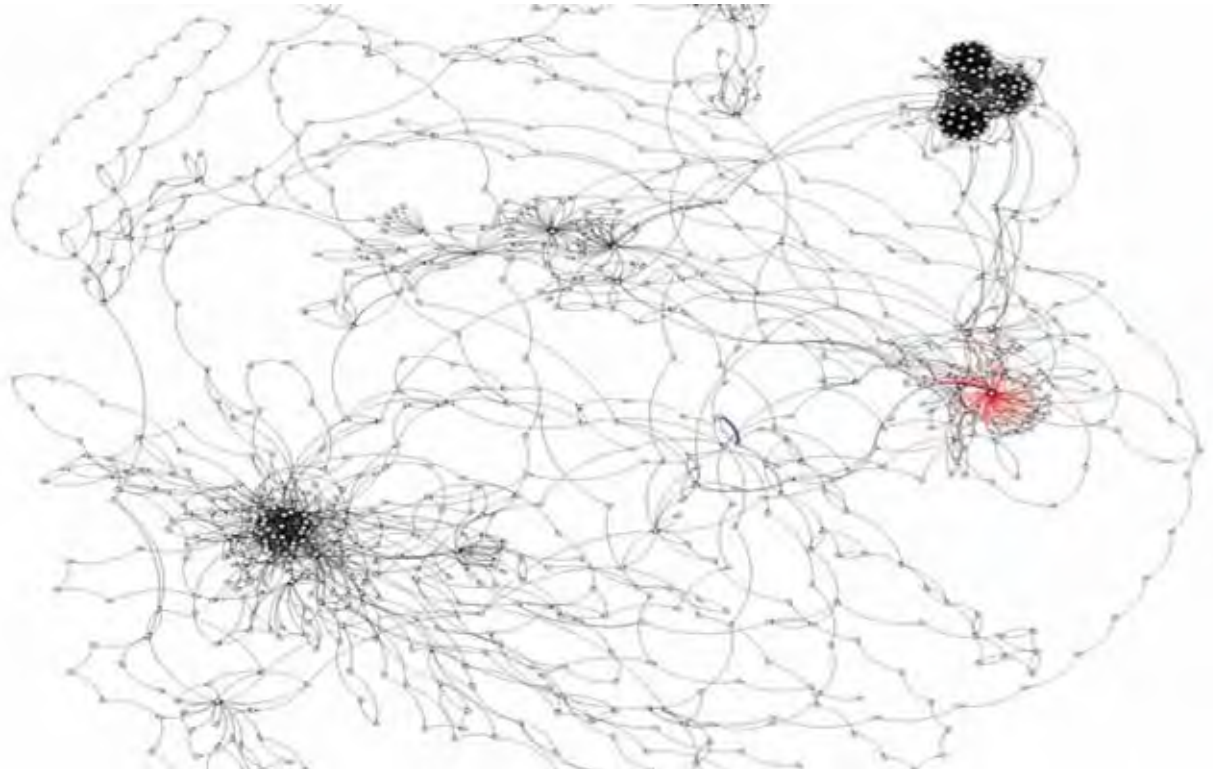
New Privacy Model



QLUEによるBitcoinブロックチェーンの可視化



QLUE検索結果例 仮想通貨の取引金額、ウォレットの関連性をリアルタイム・可視化により検索・追跡  
<https://www.value-press.com/pressrelease/187645>



近畿大学 山崎重一郎先生による分析 2014年3月

Copyright (c) 2018, Japan Digital Design, Inc., All rights reserved.

54

## Zaif事件 2018年9月14日

- 9月14日、約70億円分のBitcoin、Bitcoin Cash、Monacoinが流出
- 9月15日からBitcoinの資金洗浄が大規模化
- 9月17日 テックビューロ社が異常に気付き調査を開始
- 9月18日 テックビューロ社が近畿財務局に被害を報告
- 9月20日 事件を公表
- 10月20日、22日、流出したMonacoinの移動が開始された
- 10月26日、流出したBitcoin Cashの移動が開始された

仮想通貨	流出総額	うち顧客資産
Bitcoin	5966.1BTC (約42.5億円)	2723.4BTC (約19.4億円)
Bitcoin Cash	42327.1BCH (約21億円)	40360BCH (約20億円)
MONA	6236610.1MONA (約6.7億円)	5911859.3MONA (約6.4億円)

アッ! これなら見たことがある—— さっそくお知らせください。あなたのご協力をお待ちしています。

あなたのご協力で3億円犯人を!

犯人モンタージュ写真

3億円を積んで逃げたカローラ  
3億円を積みこんで逃げたカローラ

銀行の脅迫状に使われたもの

犯行前、犯人が着ていたもの

500円紙幣の番号(2,000枚)  
XF 227001A - XF 229000A

3億円の入ったジュラルミンの箱3個

上記の遺留品にお気づきの方は、下記へお電話ください  
0423-64-8097~9(府中署特別捜査本部)・581-2526(警視庁捜査第一課)

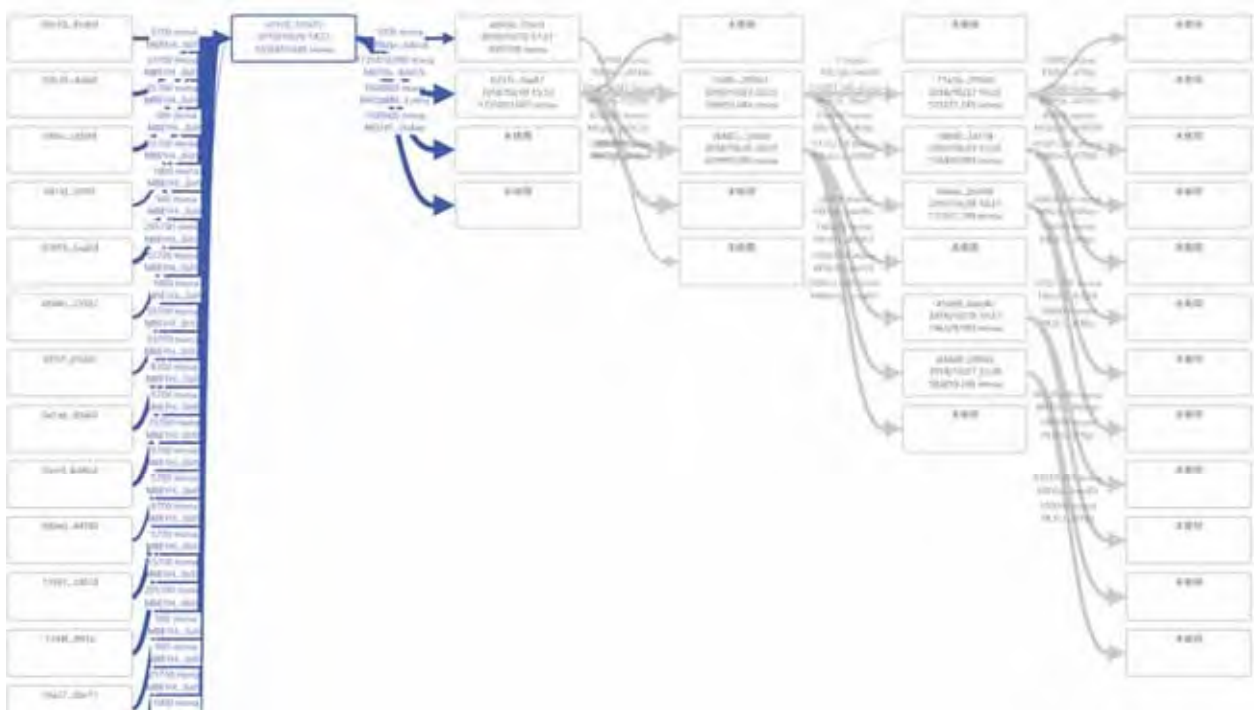
恐れ入りますが、犯人逮捕の日まで、捨てずにご保存ください。

Copyright (c) 2018, Japan Digital Design, Inc., All rights reserved.

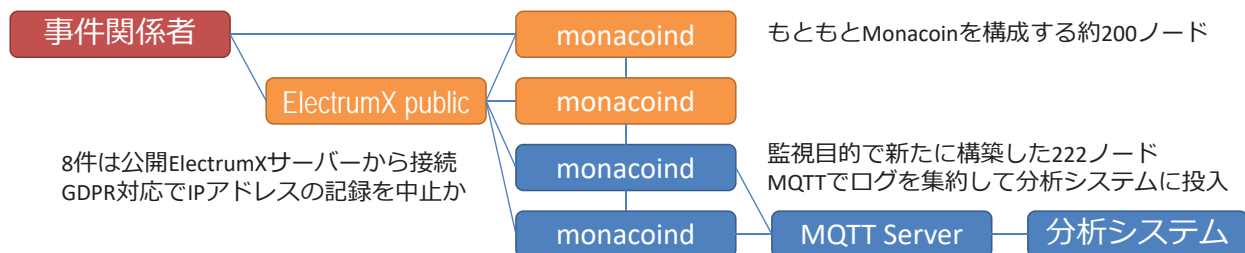
Monaco追跡Hackathon on Sep. 23rd, 24th@JDD

Japan Digital Design

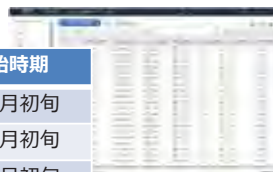




## Zaifから流出したMonacoCoinの送金指示元の逆探知



Tx日時	TxID	ノードの性質	地域	稼働開始時期
10/20 14:22	c01c...	ElectrumX public	フランス	2018年9月初旬
10/20 15:12	b237...	ElectrumX public	フランス	2018年9月初旬
10/20 17:21	a0a9...	Private Wallet	ドイツ	2018年9月初旬
10/22 20:31	9cf8...	ElectrumX public	フランス	2018年9月初旬
10/22 20:31	3bb8...	ElectrumX public	フランス	2018年9月初旬
10/27 16:22	71a1...	ElectrumX public	日本	2018年9月初旬
10/27 23:28	ddd...	ElectrumX public	日本	2017年11月初旬
10/28 10:27	45d2...	monacoind	日本	2018年10月中旬
10/28 18:21	0de6...	ElectrumX public	フランス	2018年9月初旬
10/29 23:33	588d...	ElectrumX public	フランス	2018年9月初旬



情報は2018年11月11日現在

- 暗号資産の資金移動はBlockchain上で公開されており、残高や入出金履歴は全て公開されて、何人も自由に追跡することができる。但しアドレスの持ち主までを特定することは難しい。
- 日本国内の仮想通貨交換業者に対しては法律で本人確認義務を課すことで、交換業者の管理するアドレスに関しては、所有者まで辿ることができる。
- Monero、Dash、Zcashなど、資金の流れを秘匿する仕組みを組み込んだ仮想通貨が開発されている。
- ミキシングサービスなどの匿名化サイトを利用することで、Bitcoinであっても送金元や資金の流れを秘匿することができる。
  
- 相応のコストをかければ暗号資産の送金指示元を逆探知できるケースはある。
- 辿れるのは受け付けたWalletまで、利用者のIPアドレスを特定するにはWalletサーバー運営者による協力が必要となる。
- WalletやBitcoinノードの運営者は仮想通貨交換業者と比べて零細であるケースが多く、ログが保全されていないケースも少なくない。
- 利用者がWalletへの接続にTorなどを利用した場合ログによる追跡は困難。