

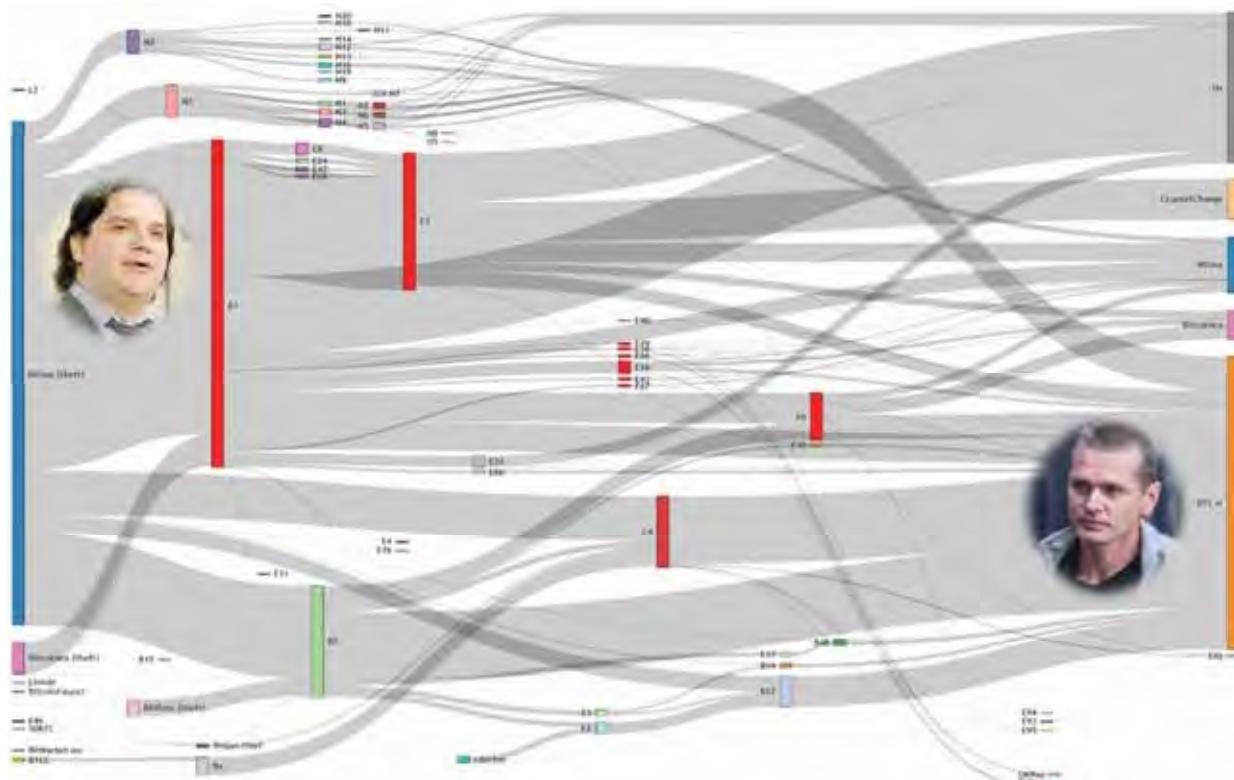


Source: <http://www.coindesk.com/price/> 2014年に閲覧

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

30

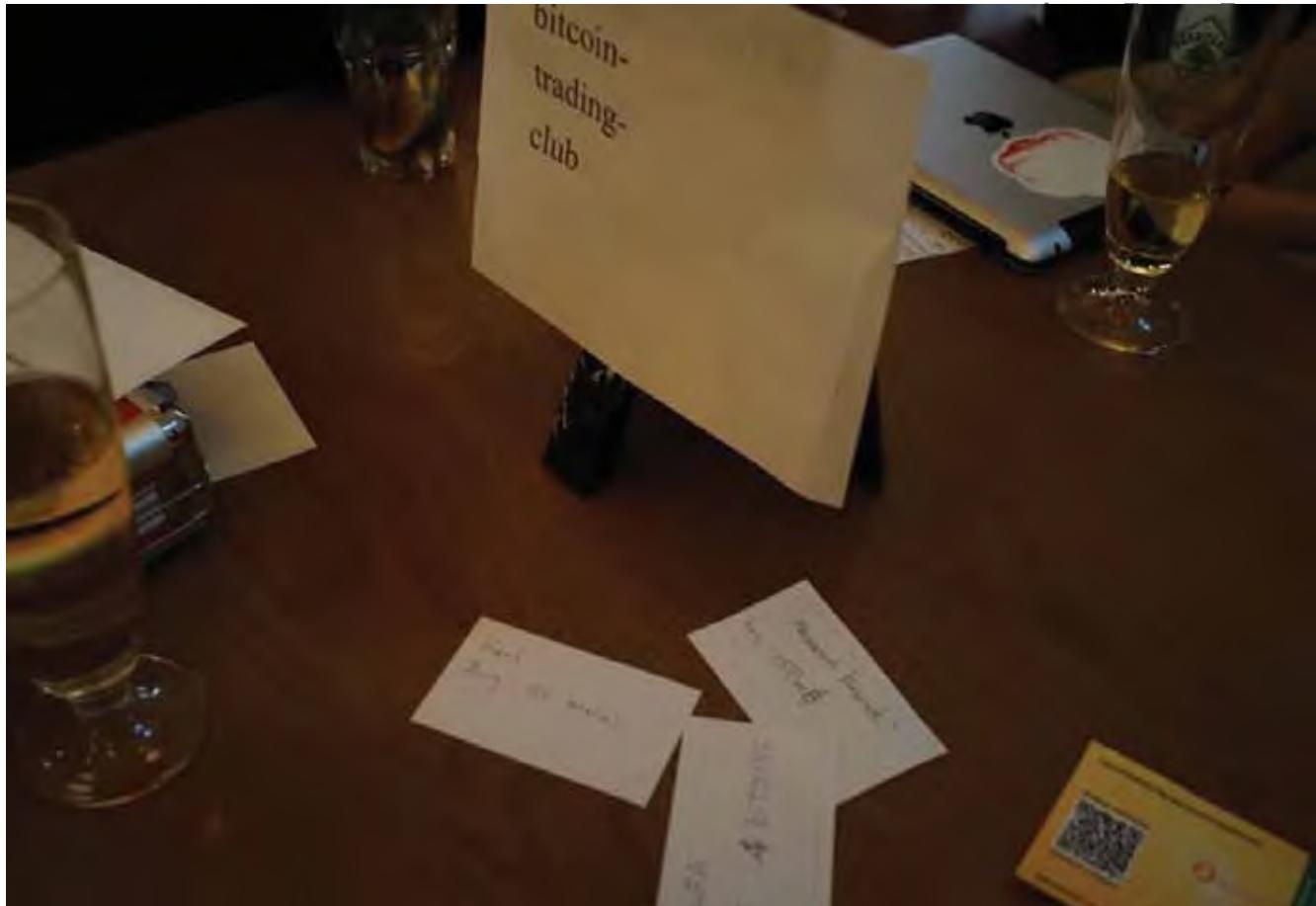
MtGOXから流出した資金の流れ（WizSecによる分析） Japan Digital Design



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

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

31

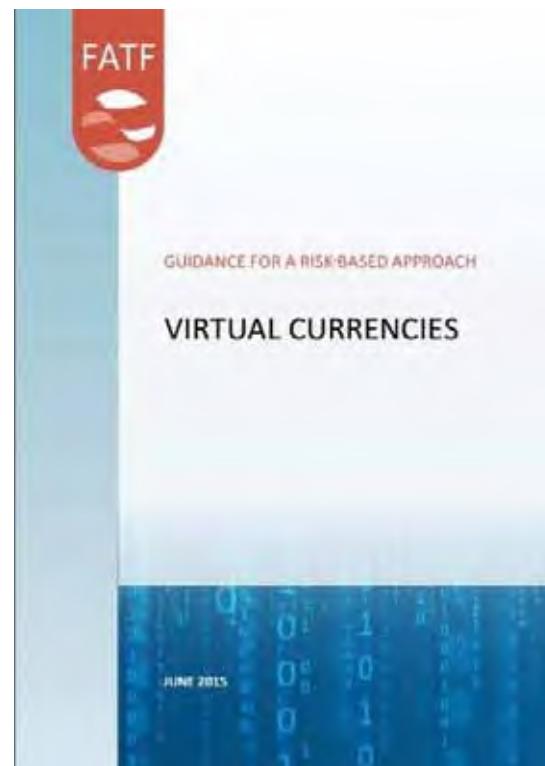


Copyright (c) 2018, Japan Digital Design, Inc., All rights reserved.

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



Jameson Lopp
@JLopp

フォローする

On stage right now: people representing approximately 90% of the Bitcoin hashing power. Truly an historic moment.

◎ 離脱を表示



143 リツイート 157 リアクション



16:06 - 2015年12月6日

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

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

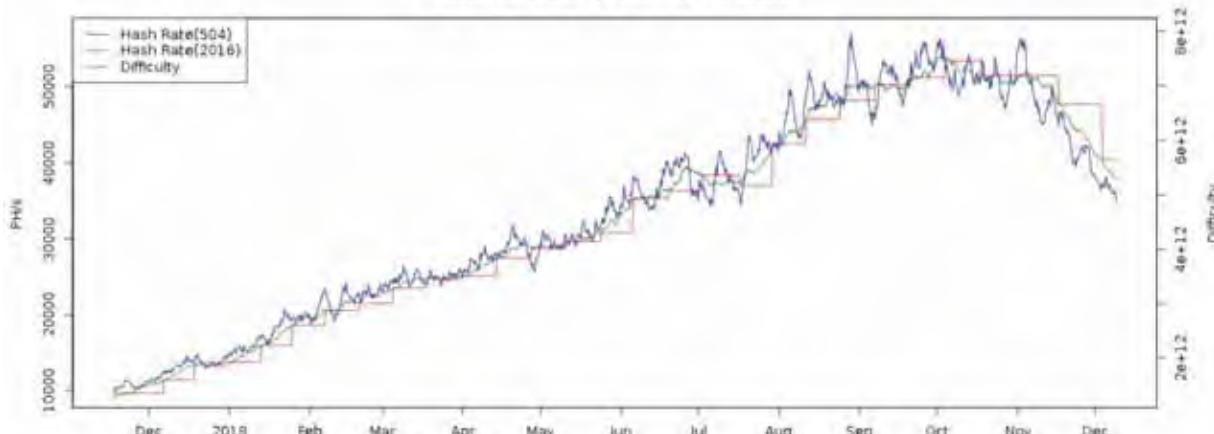
34

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 (-6.82%)
Adjust time: After 1297 Blocks, About 10.0 days
Hashrate(2): 34,835,022,717 GH/s
1 block: 11.1 minutes
Block Generation Time(2): 3 blocks: 33.2 minutes
6 blocks: 1.1 hours
Updated: 14:45 (4.5 minutes ago)

Difficulty	1640483951534	BTC/USD	9349.5		
1000000	KH/s	1.856e+9	BTC/hour	€.0000005311	USD/hour
1KH	MH/s	4.853e+8	BTC/day	€.00001567	USD/day
1	GH/s	1.127e-7	BTC/week	€.002007	USD/week
0.001	TH/s	9.090001336	BTC/month	€.004782	USD/month

Bitcoin Hash Rate vs Difficulty (9 Months)



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

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

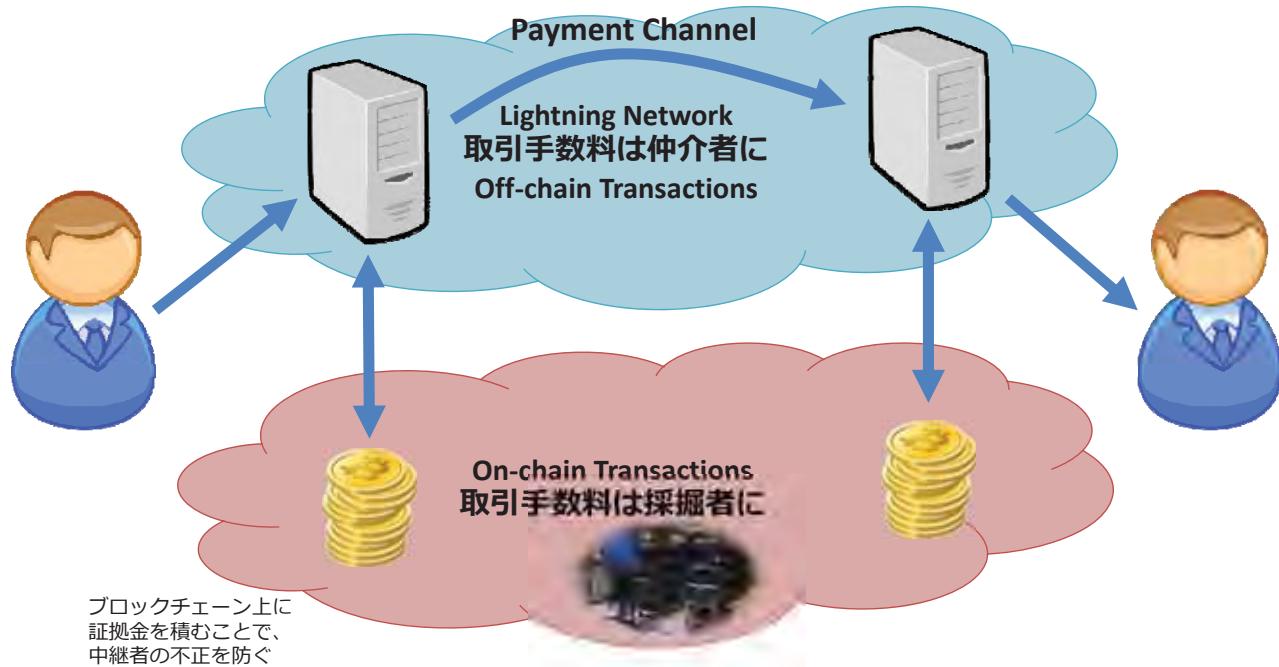
35



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

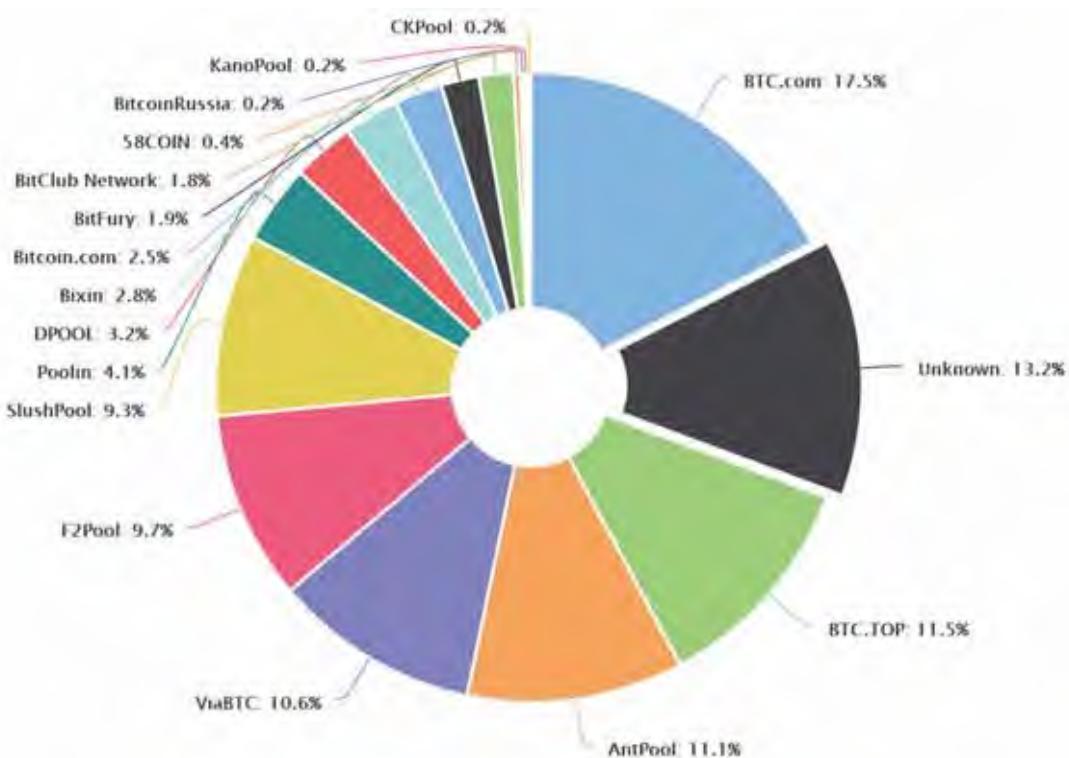
36

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

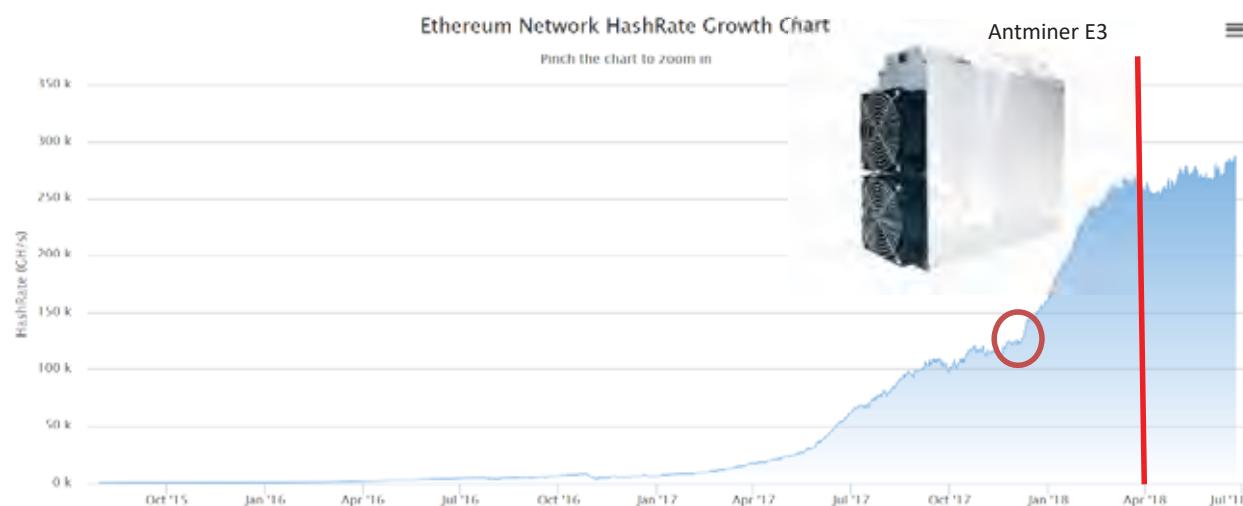


2018年5月から多発した仮想通貨Blockchain書換攻撃

5月中旬からブロックチェーンの改竄による仮想通貨の詐取が相次ぐ理由

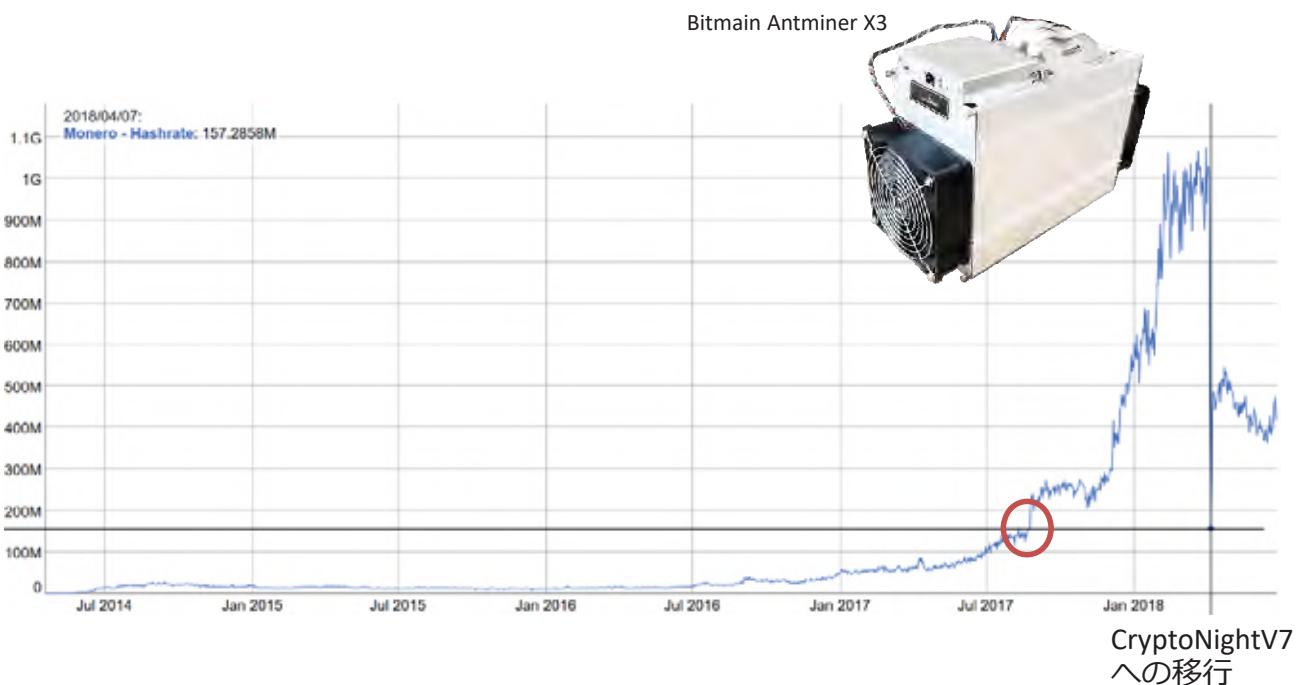
世界を発見する、想いを伝える
技術クリエイターの発信プラットフォーム
有識者・専門家がニュースに切り込む
Yahoodニュース個人欄集部ピックアップ
Yahoodニュース個人6月の月間MVAとMVCが決定

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



- 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が増えているのだろうか？

Monero: ASIC対策でHashrateが元の水準まで下落



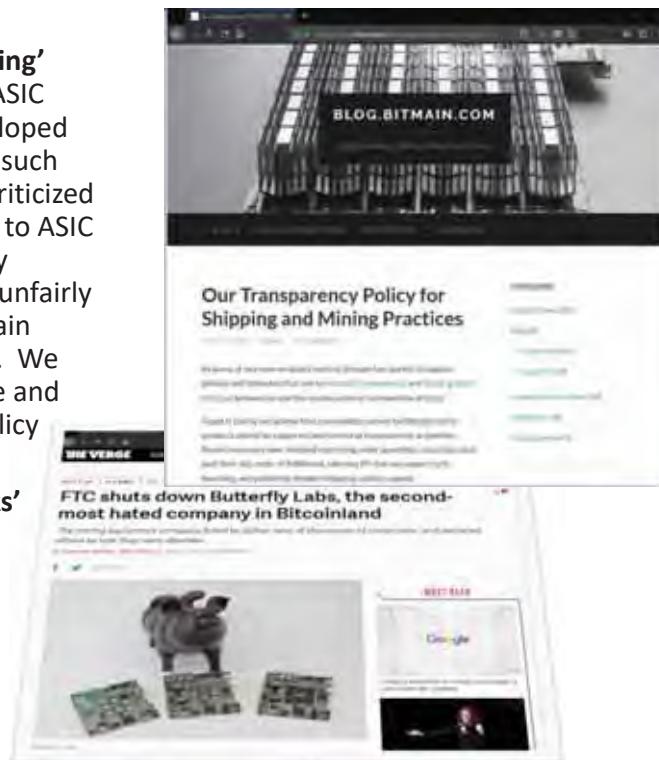
1. Disclosure policy on self-mining

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



NiceHash: ハッシュ計算能力の市場での売買が進展

The image displays the NiceHash platform, which facilitates the buying and selling of computing power for cryptocurrency mining. On the left, the NiceHash Marketplace website is shown, featuring a 'SELL' section for miners to list their available hashing power and a 'BUY' section for individuals to rent mining power. On the right, the NiceHash Miner software interface is displayed, showing real-time mining statistics and payment details.

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



256	2018-01-26 03:29:44	100,000,000	1.25	NC4C0P5UW5CLTDTSXAGJDQJGZNE5KF9MCN770G NOD2MV32W30LWNRNG3EVGHCDDGAZWEONR0E2IVCJII
257	2018-01-26 03:18:07	100,000,000	1.25	NC4C0P5UW5CLTDTSXAGJDQJGZNE5KF9MCN770G NH4QU3L3T2WVFWK9BREMI0X09-D35VSID03G2M
258	2018-01-26 03:14:09	100,000,000	1.25	NC4C0P5UW5CLTDTSXAGJDQJGZNE5KF9MCN770G NOZEBH6JZDYZSWMPYHALDWTWTHOYTQGXH3SHAW
259	2018-01-26 03:02:12	750,000	1.25	NC4C0P5UW5CLTDTSXAGJDQJGZNE5KF9MCN770G NBKLOYXEVEEGARYPLUMS2UITHASZYBMLAPU8NP1
260	2018-01-26 03:00:33	50,000,000	1.25	NC4C0P5UW5CLTDTSXAGJDQJGZNE5KF9MCN770G NOOCOXWENIZGUSMAEURXACF4IEHC2CBT0ET36VTSD
261	2018-01-26 02:58:42	50,000,000	1.25	NC4C0P5UW5CLTDTSXAGJDQJGZNE5KF9MCN770G NA7S27SKF62KK2B7TR8CJQJBW5JKIG2IASPXCRW
262	2018-01-26 02:57:34	30,000,000	1.25	NC4C0P5UW5CLTDTSXAGJDQJGZNE5KF9MCN770G NCTWFB00VTR2ZYSY10423PE3MW525MTD503EWFG
263	2018-01-26 02:51:14	3,000,000	1.25	NC3B13DNMR2P0E0MP2N0X0Q08AKMS70YRKVA5C8Z NC40SPSUW5CLTDTSXAGJDQJGZNE5KF9MCN770G
264	2018-01-26 00:10:36	20,000,000	1.25	NC3B13DNMR2P0E0MP2N0X0Q08AKMS70YRKVA5C8Z NC40SPSUW5CLTDTSXAGJDQJGZNE5KF9MCN770G
265	2018-01-26 00:09:22	100,000,000	1.25	NC3B13DNMR2P0E0MP2N0X0Q08AKMS70YRKVA5C8Z NC40SPSUW5CLTDTSXAGJDQJGZNE5KF9MCN770G
266	2018-01-26 00:08:21	100,000,000	1.25	NC3B13DNMR2P0E0MP2N0X0Q08AKMS70YRKVA5C8Z NC40SPSUW5CLTDTSXAGJDQJGZNE5KF9MCN770G
267	2018-01-26 00:07:34	100,000,000	1.25	NC3B13DNMR2P0E0MP2N0X0Q08AKMS70YRKVA5C8Z NC40SPSUW5CLTDTSXAGJDQJGZNE5KF9MCN770G
268	2018-01-26 00:06:46	100,000,000	1.25	NC3B13DNMR2P0E0MP2N0X0Q08AKMS70YRKVA5C8Z NC40SPSUW5CLTDTSXAGJDQJGZNE5KF9MCN770G
269	2018-01-26 00:04:56	100,000,000	1.25	NC3B13DNMR2P0E0MP2N0X0Q08AKMS70YRKVA5C8Z NC40SPSUW5CLTDTSXAGJDQJGZNE5KF9MCN770G
270	2018-01-26 00:02:13	10	0.05	NC3B13DNMR2P0E0MP2N0X0Q08AKMS70YRKVA5C8Z NC40SPSUW5CLTDTSXAGJDQJGZNE5KF9MCN770G

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

46

ホワイトハッカーによる追跡劇

Japan Digital Design

NEM - BlockChain Explorer NEM - BlockChain Explorer explore.nemcn.com/#/account/account_NC4C0P5UW5CLTDTSXAGJDQJGZNE5KF9MCN770G

BLOCKS TRANSACTIONS ACCOUNTS NODES MASTERS & MOSAICS POLLS

block.height / tx.id / account |

Account Detail

Address	NC4C0P5UW5CLTDTSXAGJDQJGZNE5KF9MCN770G
Public key	f0cc678d2060ca1345a2b7f704d2faaf7584:b1c250b41xj5000ff1809e051
Balance	94,015844
Moved balance	10,454075
Importance	0.02503%

Harvest Info

Harvest status	disabled
----------------	----------

Owned Namespace

mizunashi.coincheck_stolen_funds_do_not_accept_trades:owner_of_this_account_is_hacker

#	Mosaic	Quantity
1	severaliplycoin	100
2	mizunashi.coincheck_stolen_funds_do_not_accept_trades:owner_of_this_account_is_hacker	1
3	mmdeklolen	100000
4	friend.vegetable.carrot	1
5	cat_my_boss.nekoboss	11
6	nemoyen.feucol	1

NEM IO NEM Forum NEM Supmedos Market Cap: \$3,500,097,000 Price: \$0.390339 (0.00005810 Mc) Version: 1.4.5 Log Feedback

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

47

Account Detail

Address	NCVPFHXXHDDF7PXXSBCK9076H3MBH5TSXT5K575
Public key	28297505125.e71c8500377407905c02e480ce4557e208663530c70ce613b
Balance	0
Moved balance	0
Importance	0.00239%

Harvest Info

Harvest status	disabled
----------------	----------

Owned Namespaces

#	Namespace	Height
1	st	1494893
2	ls	1494895

Owned Mosaics

#	Mosaic	Quantity
1	ts:warning_dont_accept_stolen_funds	1

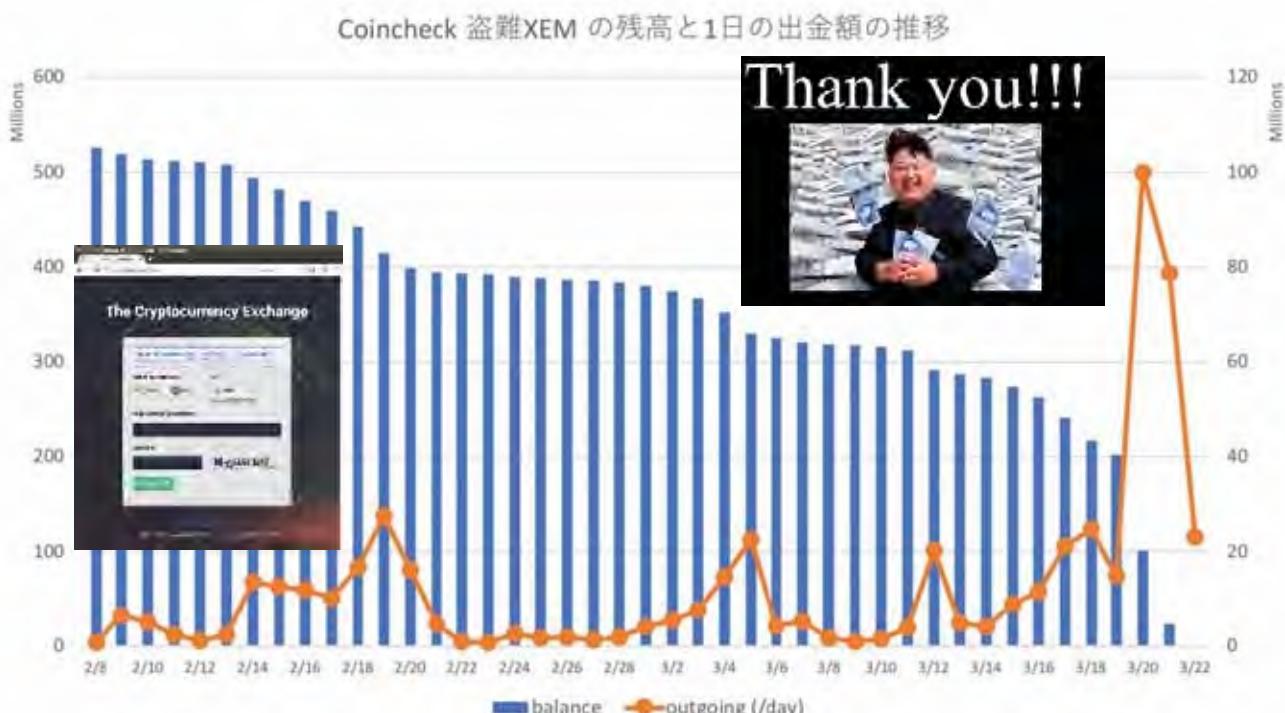
Transfer Records

#	Timestamp	Amount	Fee	Sender	Recipient
1	2017-02-20 09:49:29	3017.220 XEM	0.25	NCVPFHXXHDDF7PXXSBCK9076H3MBH5TSXT5K575	NOMWFRPFZWH9279V1D896729304L2zvYyMwA

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

48

追跡モザイクの廃止で盗難XEMの交換は一気に加速



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

一部仮想通貨の取り扱い廃止のお知らせ

2018年6月18日

今般、コインチェック株式会社（代表取締役社長：勝俣敬三、以下：当社）が運営する仮想通貨取引サービス「Coincheck」において、一部仮想通貨の取り扱いが廃止となりますことをお知らせいたします。

一部仮想通貨の取り扱い廃止について

当社は、このほど発生した不正アクセスによる仮想通貨NEMの不正送金に謝罪し、2018年3月8日、金融庁から直轄決済に関する法律第63条の16に基づく業態改善命令を受けました。今回の指摘を踏まえ、深く反省するとともに、内部管理体制及び経営管理体制等を抜本的に見直し、顧客保護を徹底した経営戦略の見直し等を進めております。

この見直しの一環として、今後さらなるAML/CFTの管理体制の整備・強化が必要となることが予想されます。少しでも懸念のある通貨を取扱うことについては、当社として適切ではないと判断し、仮想通貨の特性を踏まえた各種リスクの再検討を実施いたしました。その結果、下記の通貨の取扱いを廃止いたします。

廃止日：2018年6月18日
 詳細内容：Coincheck上における一部仮想通貨の売買、入出金、保有、当社への貸し出しの廃止
 対象通貨：XMR、REP、DASH、ZEC

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

50

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。

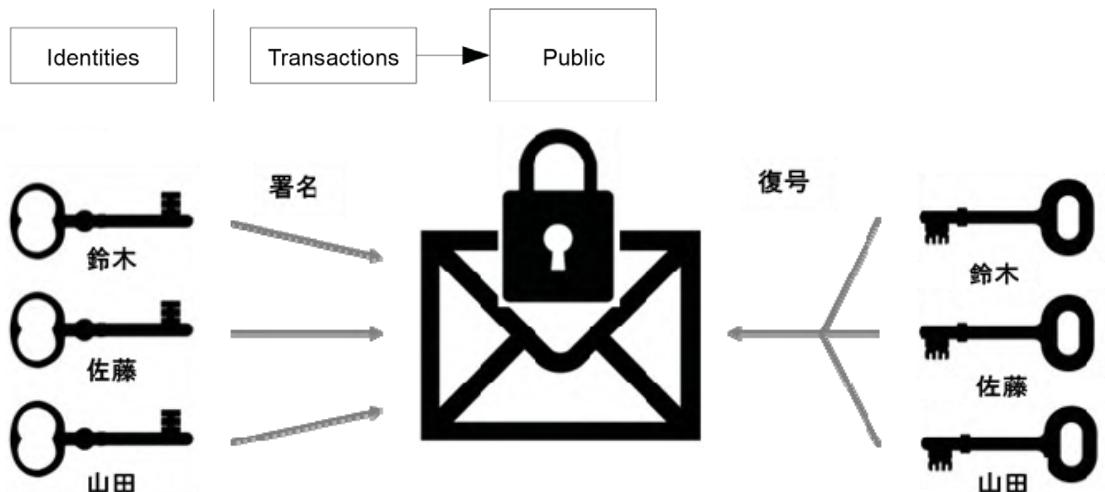
留意点

- 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。

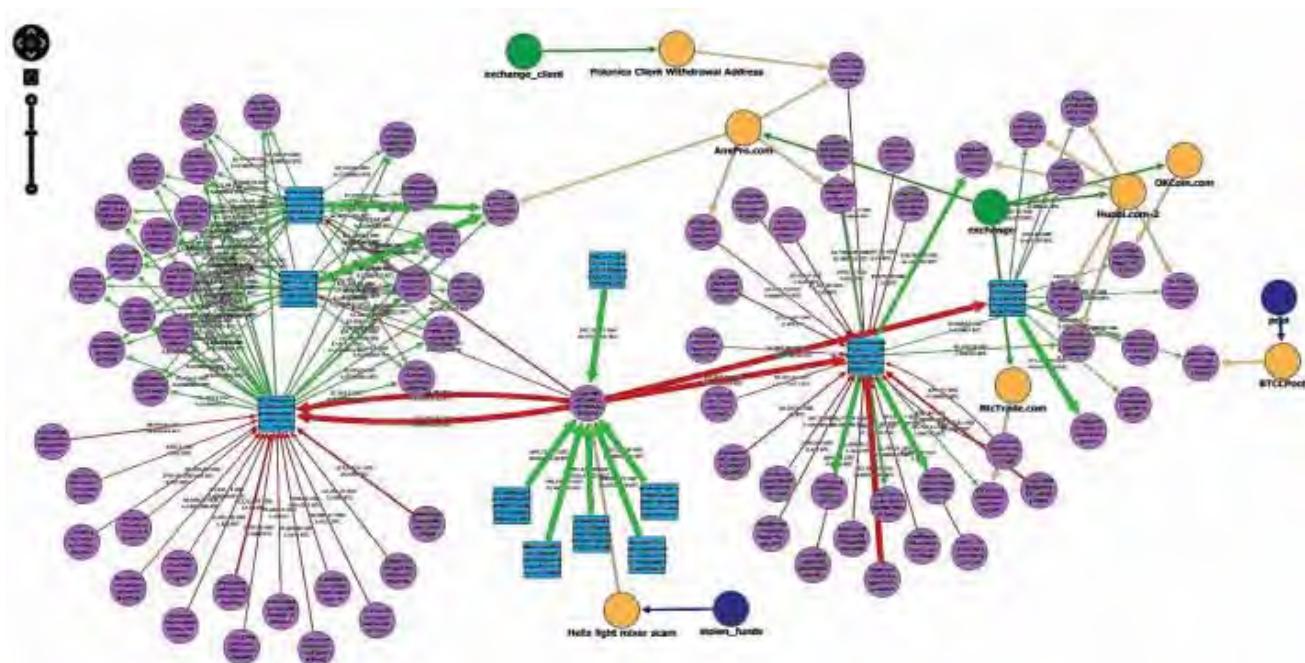
Traditional Privacy Model



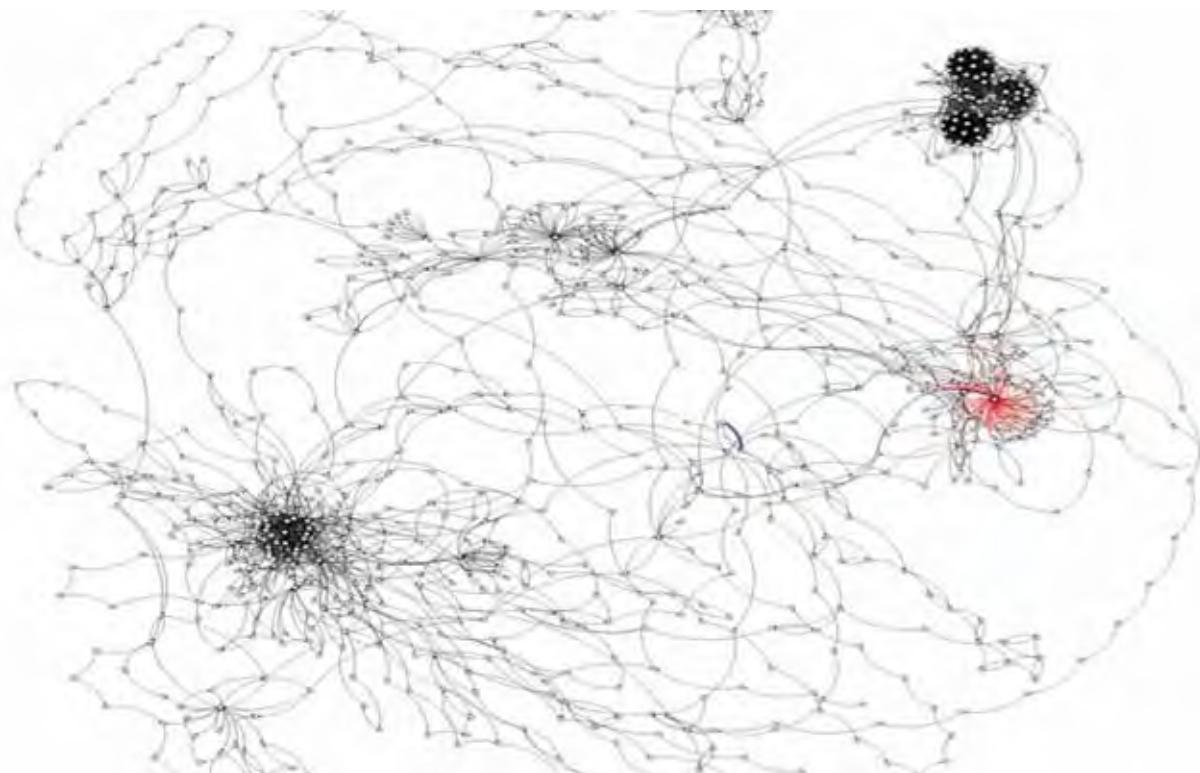
New Privacy Model



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 テックビューコロナ社が異常に気付き調査を開始
- 9月18日 テックビューコロナ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!



上記の遺留品にお気づきの方は、下記へお電話ください

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。

0423-64-8097~9(府中署特別捜査本部)・581-2526(警視庁捜査第一課)

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

56

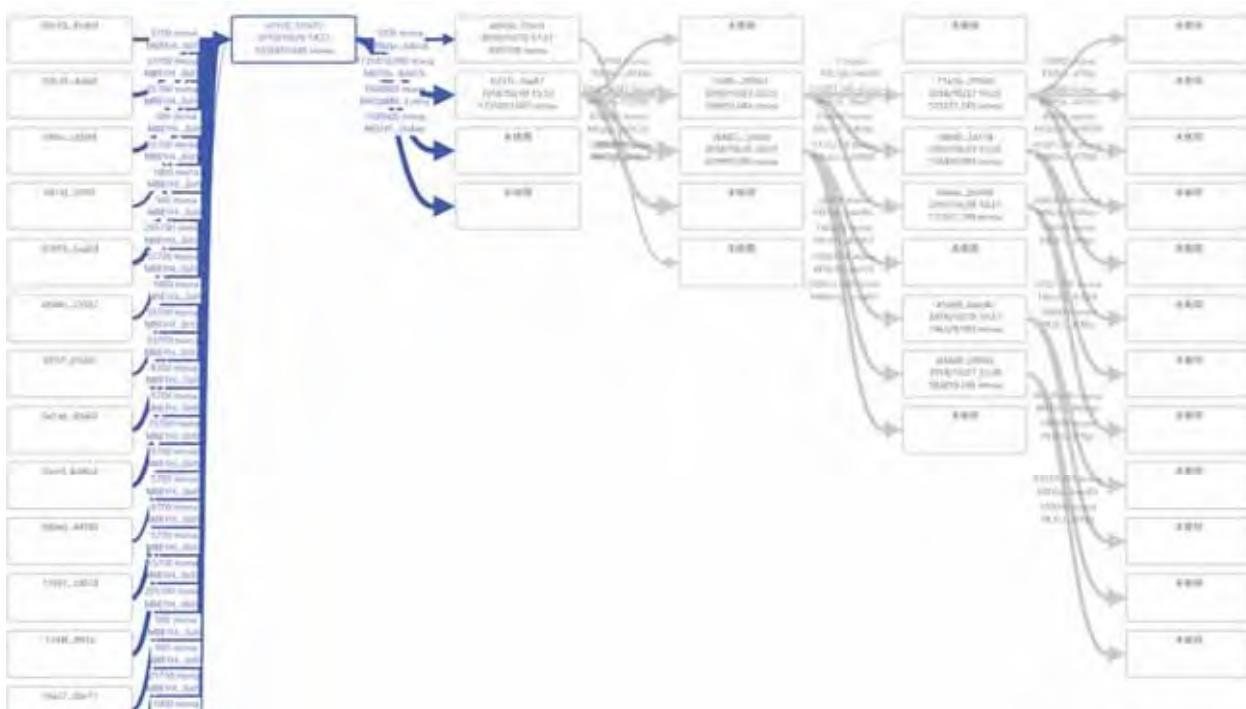
Monacoин追跡Hackathon on Sep. 23rd, 24th@JDD

Japan Digital Design



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

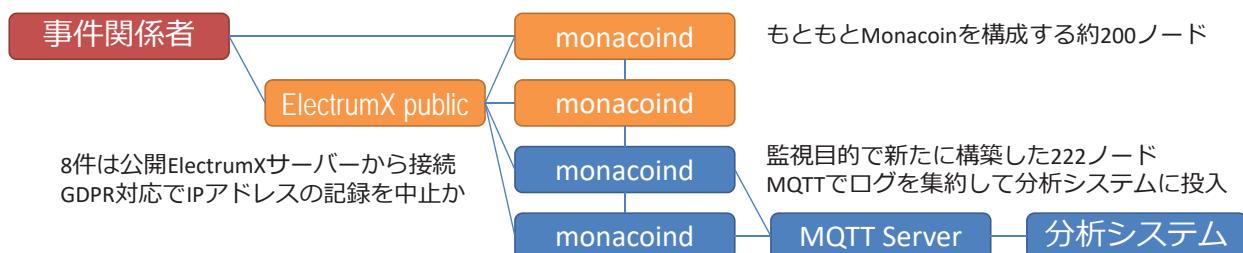
57



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

58

Zaifから流出したMonacoin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	dddd...	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してすることで、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。