Japan Digital Design

仮想通貨から暗号資産へ
ビットコインの社会的受容とサイバーセキュリティ

Japan Digital Design株式会社 CTO
ISO/TC307 国内委員会 委員長
楠 正憲 masanori.kusunoki@japan-d2.com

自己紹介 – 楠 正憲（くすのき・まさのり）

Japan Digital Design

Japan Digital Design, Inc. Chief Technology Officer

仮想通貨・ブロックチェーンとの関わり:

学生時代から電子マネーを研究、日経デジタルマネーシステムで編集記者

2013年からBitcoinを調査、 MtGOX、 The DAO、 Coin Check事件などを報じる

2016年 ISO/TC307 Blockchain and Distributed Ledger Technologies 国内委員会 委員長

2017年 一般社団法人 日本ブロックチェーン協会 アドバイザー

2018年 金融庁「仮想通貨交換業等に関する研究会」メンバー

主な社外での活動:

一般社団法人 OpenID Foundation Japan 代表理事

内閣官房 IT総合戦略室 政府CIO補佐官（番号制度担当）

内閣官房 番号制度推進室 番号制度推進管理補佐官

内閣府（本府）情報化参与 CIO補佐官

東京大学大学院 情報理工学系研究科 非常勤講師

福岡市 政策アドバイザー (ICT)

国際大学GLOCOM 客員研究員

会社概要

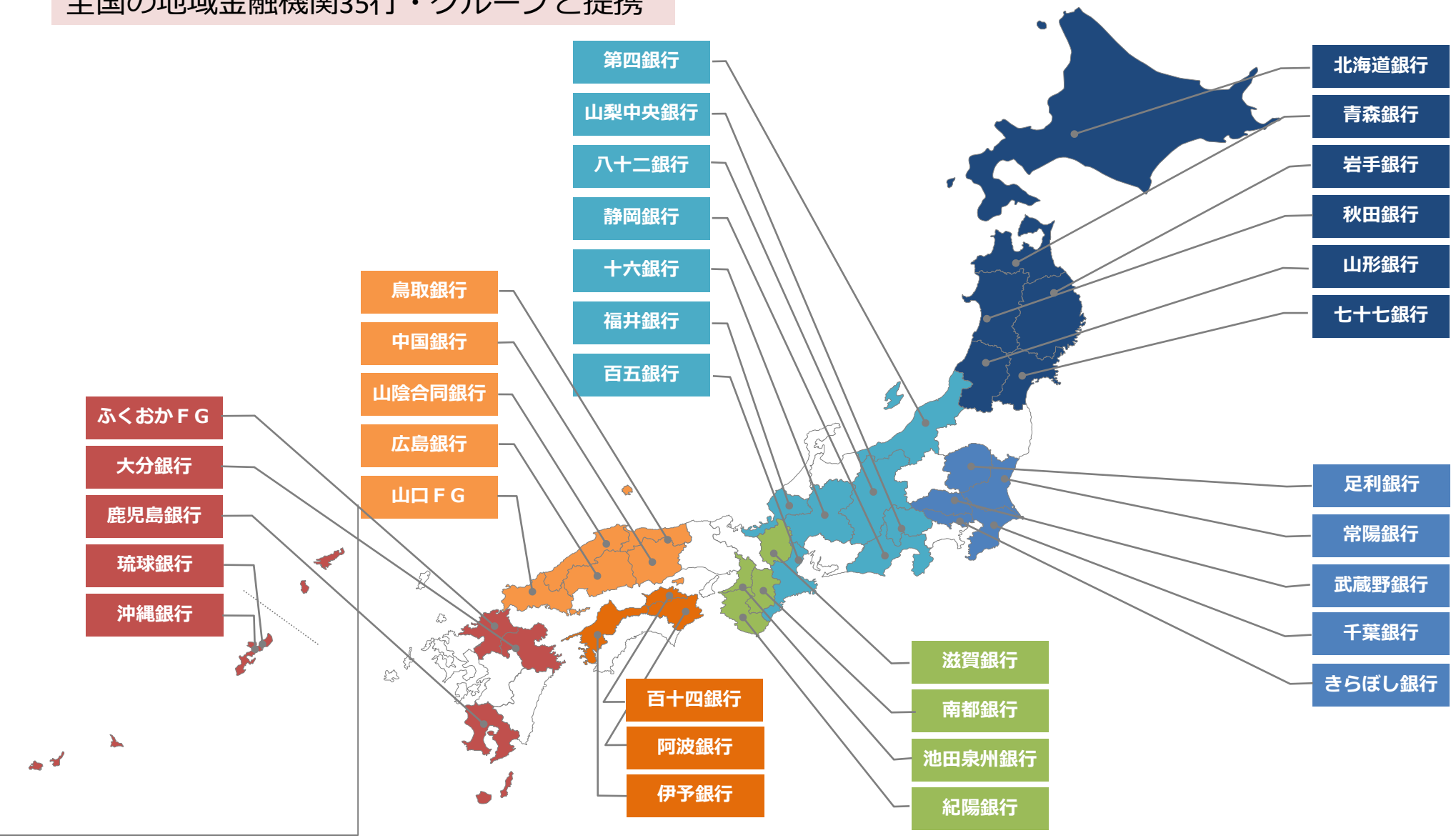
社名 (英文名)	Japan Digital Design株式会社 (Japan Digital Design, Inc.)
本社所在地	〒103-0021 東京都中央区日本橋本石町三丁目3番5号　日本橋トークビル6,８,９階
設立	2017年10月2日
代表取締役CEO	上原　高志
資本金	36億円（含む資本準備金）
株主構成	株式会社三菱UFJフィナンシャル・グループ　83.33% 株式会社三菱総合研究所　13.89% 三菱UFJリサーチ＆コンサルティング株式会社　2.78%
事業内容	① 銀行業高度化等に資する調査、研究、および技術開発 ② 銀行業高度化等に資するシステム開発、販売、および運用 ③ 銀行業高度化等に資するコンサルティングおよび人材育成 銀行法第52条の23第6項の規定により金融庁申請、認可取得済
電話	03-6225-5020
WEB	www.japan-d2.com

多様なバックグラウンドを持つエンジニアを採用

パートナー35行から1名ずつ出向を受け入れ

Japan Digital Design

全国の地域金融機関35行・グループと提携



経済産業省委託事業 ブロックチェーン ハッカソン

Japan Digital Design

教育・就労環境

1)半永久性な（例えば大学や会社が消滅しても可能な）学歴・職務履歴の証明
2)e－Learningなどにおける証明書発行
3)海外の大学と単位交換
4)分散化ID（DID）を活用した学位・職務履歴管理
5)ブロックチェーン技術を活用した長期証明
6)学歴・経歴検証におけるコスト削減

研究データ管理

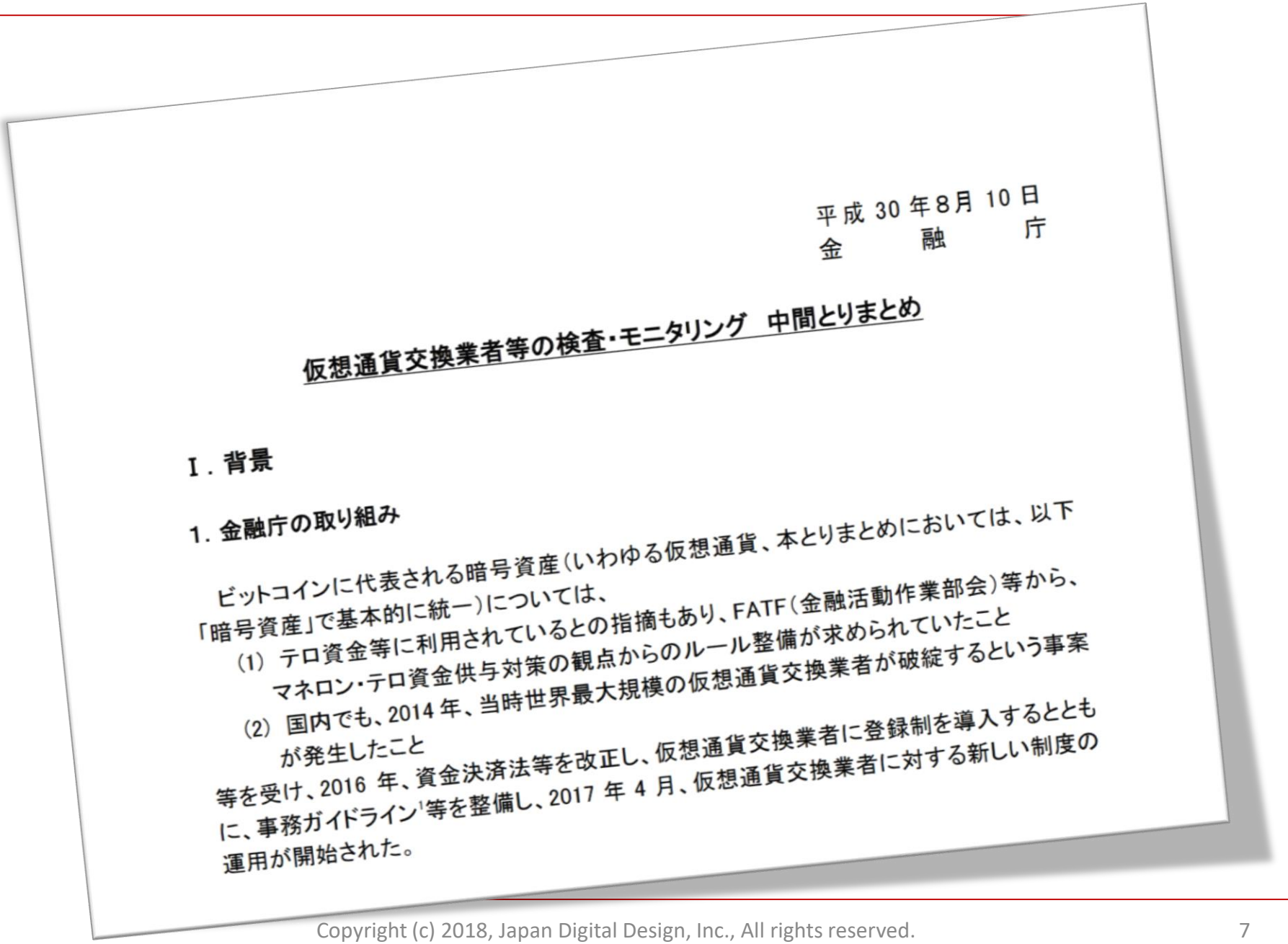
1)研究データ不正がシステム上不可能なデータ管理基盤
2)Open Data構想を導入した研究データ管理
3)IPFSなどのデータ管理用のプロトコルを活用したデータ管理基盤
4)臨床試験のデータ管理におけるブロックチェーン技術の活用
5)データの量が拡大していくときのブロックチェーン技術の活用
6)プライバシーを担保するデータ管理基盤
7)被験者（データプロバイダー）や研究者に対するインセンティブ設計

仮想通貨の交換業者やPFを狙った主なサイバー攻撃

Japan Digital Design

時期	被害を受けた事業者	被害額	要因
2014.2	MtGOX – 日	**約470億円**	交換所に対する不正アクセス
2015.1	BitStamp – SVN	約5億円	交換所に対する不正アクセス
2016.6	The DAO – 独	約50億円	Smart Contractの脆弱性を悪用
2016.8	Bitfinex – 香港	約65億円	交換所に対する不正アクセス
2017.11	Thether – 米	約34億円	交換所に対する不正アクセス
2017.12	Youbit – 韓	約18億円	交換所に対する不正アクセス
2017.12	NiceHash - SVN	約68億円	採掘プールに対する不正アクセス
2018.1	CoinCheck – 日	**約580億円**	交換所に対する不正アクセス
2018.2	BitGrail – 伊	約181億円	交換所に対する不正アクセス
2018.5	BitcoinGold	約20億円	51%攻撃を使った二重払い
2018.6	Coinrail – 韓	約40億円	交換所に対する不正アクセス
2018.7	Bancor	約23億円	運営者Walletからの流出
2018.9	Zaif – 日	**約70億円**	交換所に対する不正アクセス
2019.2	QuadrigaCX – 加	約160億円	運営者急死による署名鍵の滅失

仮想通貨か、暗号資産か



平成 30 年8月 10 日
金　　融　　庁

仮想通貨交換業者等の検査・モニタリング　中間とりまとめ

Ⅰ．背景

1．金融庁の取り組み

ビットコインに代表される暗号資産（いわゆる仮想通貨、本とりまとめにおいては、以下「暗号資産」で基本的に統一）については、

（1）テロ資金等に利用されているとの指摘もあり、FATF（金融活動作業部会）等から、マネロン・テロ資金供与対策の観点からのルール整備が求められていたこと

（2）国内でも、2014 年、当時世界最大規模の仮想通貨交換業者が破綻するという事案が発生したこと

等を受け、2016 年、資金決済法等を改正し、仮想通貨交換業者に登録制を導入するとともに、事務ガイドライン[1]等を整備し、2017 年 4 月、仮想通貨交換業者に対する新しい制度の運用が開始された。

「仮想通貨交換業等に関する研究会」報告書の概要

顧客の仮想通貨の流出事案が複数発生

価格が乱高下し、仮想通貨が投機の対象になっている、との指摘

事業規模の急拡大に業者の内部管理態勢の整備が追いついていない実態

仮想通貨を用いた新たな取引（証拠金取引やICO）の登場

適正な自己責任

仮想通貨交換業者を巡る課題への対応

◆仮想通貨の流出リスク等への対応

- ●オンラインで秘密鍵を管理する顧客の仮想通貨相当額以上の純資産額及び弁済原資（同種・同量以上の仮想通貨）の保持を義務付け
- ●顧客の仮想通貨返還請求権を優先弁済の対象とする仕組みを整備
- ●財務書類の開示を義務付け

◆業務の適正な遂行の確保

- ●取引価格情報の公表を義務付け
- ●投機的取引を助長する広告・勧誘を禁止
- ●自主規制との連携（自主規制規則に準じた社内規則を策定していない自主規制機関未加入業者の登録拒否・取消し）

◆問題がある仮想通貨の取扱い

- ●利用者保護や業務の適正かつ確実な遂行に支障を及ぼすおそれがある仮想通貨の取扱いを禁止
- ●取り扱う仮想通貨の変更を事前届出に見直し

仮想通貨証拠金取引等への対応

◆証拠金取引であることを踏まえた対応

- ●外国為替証拠金取引（FX取引）と同様に業規制の対象とし、不招請勧誘の禁止などの行為規制を適用
- ●仮想通貨の価格変動の実態を踏まえ、適切な証拠金倍率の上限を設定

◆仮想通貨の特性等を踏まえた追加的な対応

- ●仮想通貨に特有のリスクに関する説明を義務付け
- ●最低証拠金を設定

◆仮想通貨信用取引への対応

- ●仮想通貨証拠金取引と同様の機能・リスクを有することを踏まえ、同様の規制を適用

ICO（Initial Coin Offering）への対応

様々な問題への指摘が多い一方で、将来の可能性への指摘も踏まえつつ、規制を整備

◆投資性を有するICOへの対応

- ●仮想通貨による出資を募る行為が規制対象となることを明確化
- ●ICOトークンの流通性の高さや投資家のリスク等を踏まえて、以下のような仕組みを整備
  - ・50名以上に勧誘する場合、発行者に公衆縦覧型の発行・継続開示を義務付け
  - ・仲介業者を証券会社と同様の業規制の対象とし、発行者の事業・財務状況の審査を義務付け
  - ・有価証券と同様の不公正取引規制*を適用
    ＊インサイダー取引規制は、今後の事例の蓄積等を踏まえて検討
  - ・非上場株式と同様に一般投資家への勧誘を制限

◆その他のICOへの対応

- ●ICOトークンを取り扱う仮想通貨交換業者に、事業の実現可能性等に関する情報提供を義務付け

◆仮想通貨の不公正な現物取引への対応

- ●不正行為・風説の流布等・不当な価格操作を、行為主体を限定せずに禁止
- ●仮想通貨交換業者に、取引審査を義務付けるとともに、未公表情報に基づく利益を図る目的での取引を禁止

◆仮想通貨カストディ業務への対応

- ●業規制の対象とし、仮想通貨交換業者に適用される顧客の仮想通貨の管理に関する規制を適用

◆業規制の導入に伴う経過措置

- ●仮想通貨証拠金取引等への業規制の導入に際し、経過措置を設ける場合には、経過期間中の業務内容の追加等を禁止

◆法令上の呼称の変更

- ●国際的な動向等を踏まえ、「仮想通貨」の呼称を「暗号資産」に変更

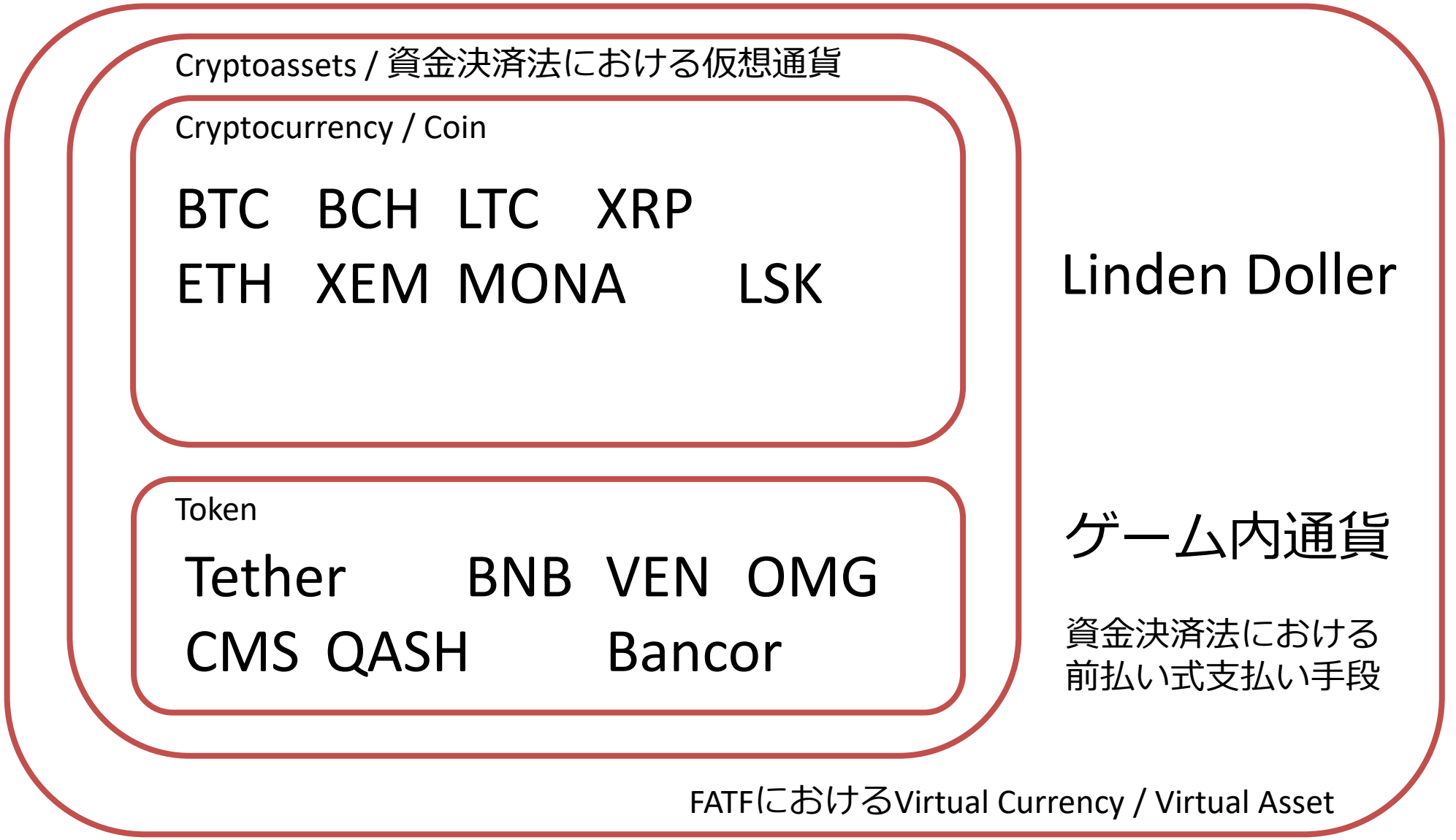
今後のBitcoin他に対する今後の呼称について

Japan Digital Design

	Crypto	Virtual
Currency	**暗号通貨 Cryptocurrency** 広くコミュニティで使われていた表現。Bitcoin、Ripple、EthereumといったDLT上で管理された価値の記録を指す。狭義でICOトークン等を含まない場合がある	**仮想通貨 Virtual Currency** 米国FinCENが2013年のガイドラインで使い始めた表現。資金洗浄対策の観点から暗号通貨だけでなくLinden Dollerなどのゲーム内通貨も含む概念。発行体による払戻義務がある電子マネー等は含まない。2015年のFATF Guidelineで使われたことから、2016年資金決済法改正でも使われた
Assets	**暗号資産 Cryptoassets** 2018年2月のG20宣言で使われた表現。Bitcoin他が値上がり期待から退蔵され、決済手段ではなく投機の対象となっている実態、法定通貨とは法的位置づけが異なることを明確にするため、通貨ではなく資産であることを強調した。一般にERC-20トークン等も含む	**仮想資産 Virtual Assets** FATFが2018年10月のRecommendationsで使い始めた表現。通貨ではなく資産であることを明確にするところでG20との平仄を取りつつ従前のVirtual Currencyと同様ゲーム内通貨等をカバーする意図があったと推察

それぞれの用語がカバーする範囲（個人的理解）

Japan Digital Design



2018年10月19日 FATF Weekでの仮想資産規制の進展

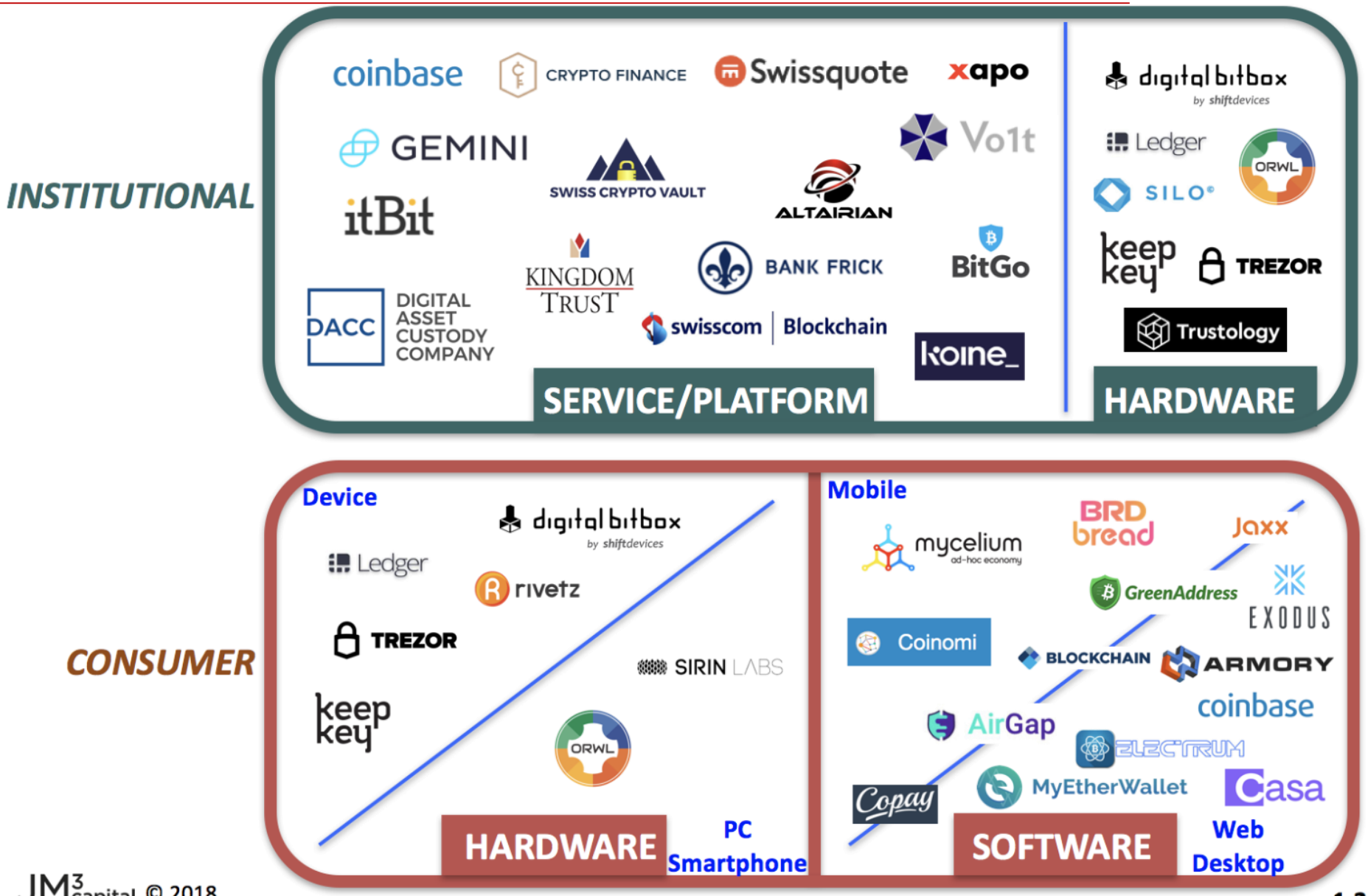
Given the urgent need for an effective global, risk-based response to the AML/CFT risks associated with virtual asset financial activities, the FATF has adopted changes to the FATF Recommendations and Glossary that clarify how the Recommendations apply in the case of financial activities involving virtual assets. These changes add to the Glossary new definitions of "virtual assets" and **"virtual asset service providers"** – such as exchanges, certain types of wallet providers, and providers of financial services for Initial Coin Offerings (ICOs). These changes make clear that jurisdictions should ensure that virtual asset service providers are **subject to AML/CFT regulations**, for example conducting customer due diligence including ongoing monitoring, record-keeping, and reporting of suspicious transactions. They should be licensed or registered and subject to monitoring to ensure compliance. The FATF will further elaborate on how these requirements should be applied in relation to virtual assets.

Regulation of virtual assets – Oct 19th, 2018

http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html

ウォレット業者 (Cryptoassets Custodian) の業態分類

Japan Digital Design



JM3 capital © 2018

v 1.2

ISO/TC307 Blockchain and Distributed Ledger Technologies Japan Digital Design

2017年4月　　シドニーで初会合

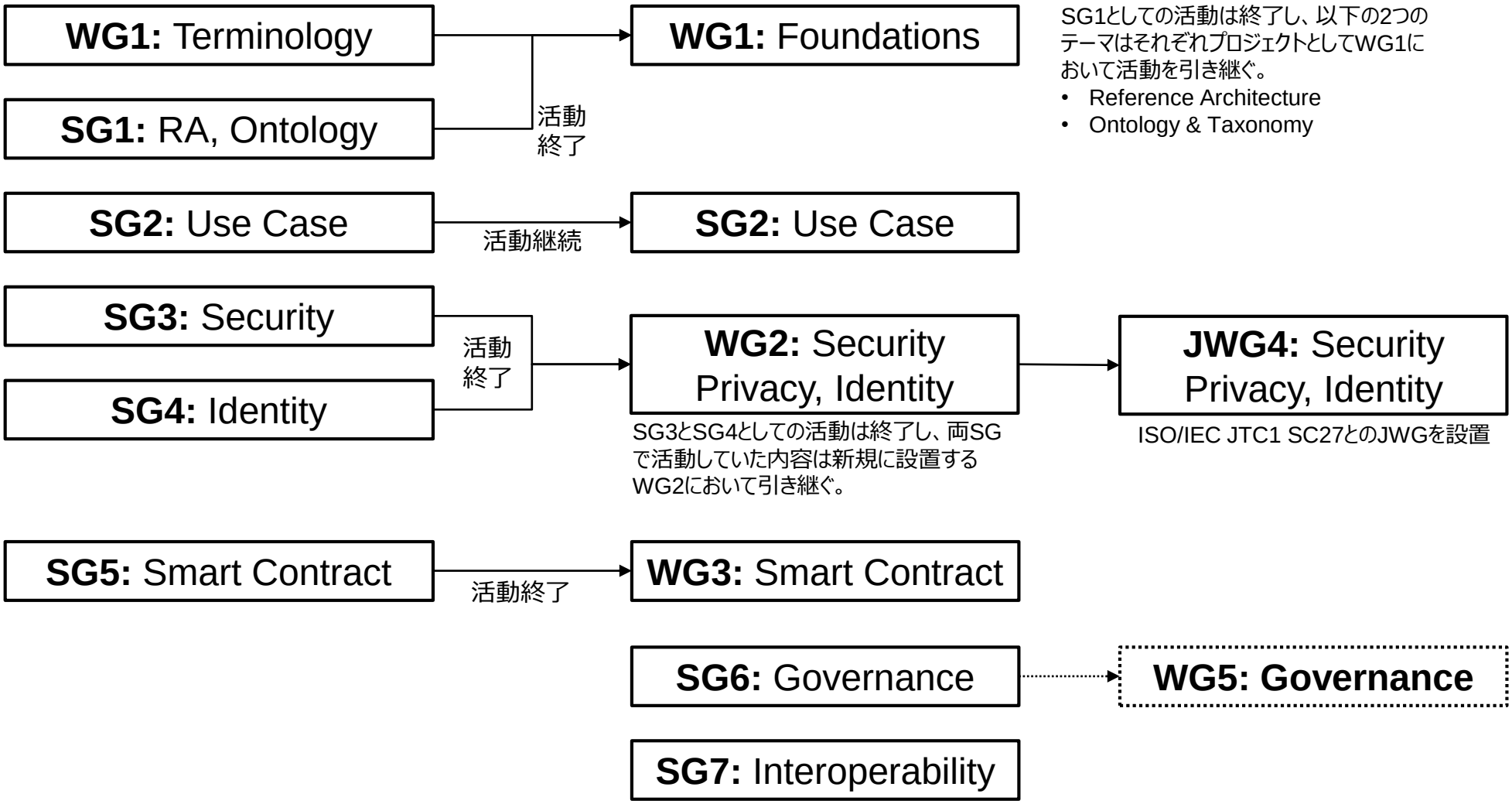
2017年11月 東京会議

2018年10月 ISO/TC307 モスクワ総会

Japan Digital Design

ISO/TC307における組織の変遷

Japan Digital Design



TR23576: Security Management of Digital Asset Custodians

Japan Digital Design

ジョージタウン大学 松尾真一郎先生をエディタとして、仮想通貨交換所のセキュリティ・マネジメント基準に関するTechnical Reportを作成

日本からの提案でプロジェクトが立ち上がり、現在Working Draft 2のフェーズ。2019年5月ダブリン総会での承認を目指して活動中

ISO

afnor NORMALISATION

Security, privacy and identity

ISO/TC 307/WG 02

Date:
2018-08-01

Doc. Number:
N 0025

Assistant: Nathalie DA SILVA
Direct line : +33 (0)1 41 62 80 30

Your contact:
Julien BRINGER
Direct line :
julien@kallistech.com

Text for Working Draft 1 – TR 23576 Blockchain and distributed ledger technologies — Security of Digital Asset Custodians

COMMENTARIES / DECISIONS: As per Decision 3 from WG2 plenary in London, please submit your comments via the online balloting application by the due date indicated (Sept. 21st)

FOLLOW UP: Comments before 2018-09-21

SOURCE: ISO/TC 307/WG2 Secretariat

ISOにおけるTechnical Reportの位置づけについて

Japan Digital Design

制定段階	略称	文書名称	
0 – 予備段階	PWI	Preliminary Work Item	予備業務項目
1 – 提案段階	NP	New Work Item Proposal	新業務項目提案
2 – 作成段階	WD	**Working Draft**	**作業原案**
3 – 委員会段階	CD	Committee Draft	委員会原案
4 – 照会段階	DIS	Draft International Standard	国際規格案
5 – 承認段階	FDIS	Final Draft International Standard	最終国際規格案
6 – 発行段階	TR	Technical Specification	技術仕様書
	TS	**Technical Report**	**技術報告書**
	IS	International Standard	国際規格

- IS（International Standard 国際標準）ISO規格として発行された文書
- TS（Technical Specification 技術仕様書）将来的にISO規格として採用される可能性があるが、標準化の対象が開発途上であるなど、ISO規格として直ちに発行できない場合に発行される文書
- TR（Technical Reports 技術報告書）通常の国際規格とは異なる種類の調査データなどを、参考文書として発行したもの

Cryptoassets Governance Taskforceについて

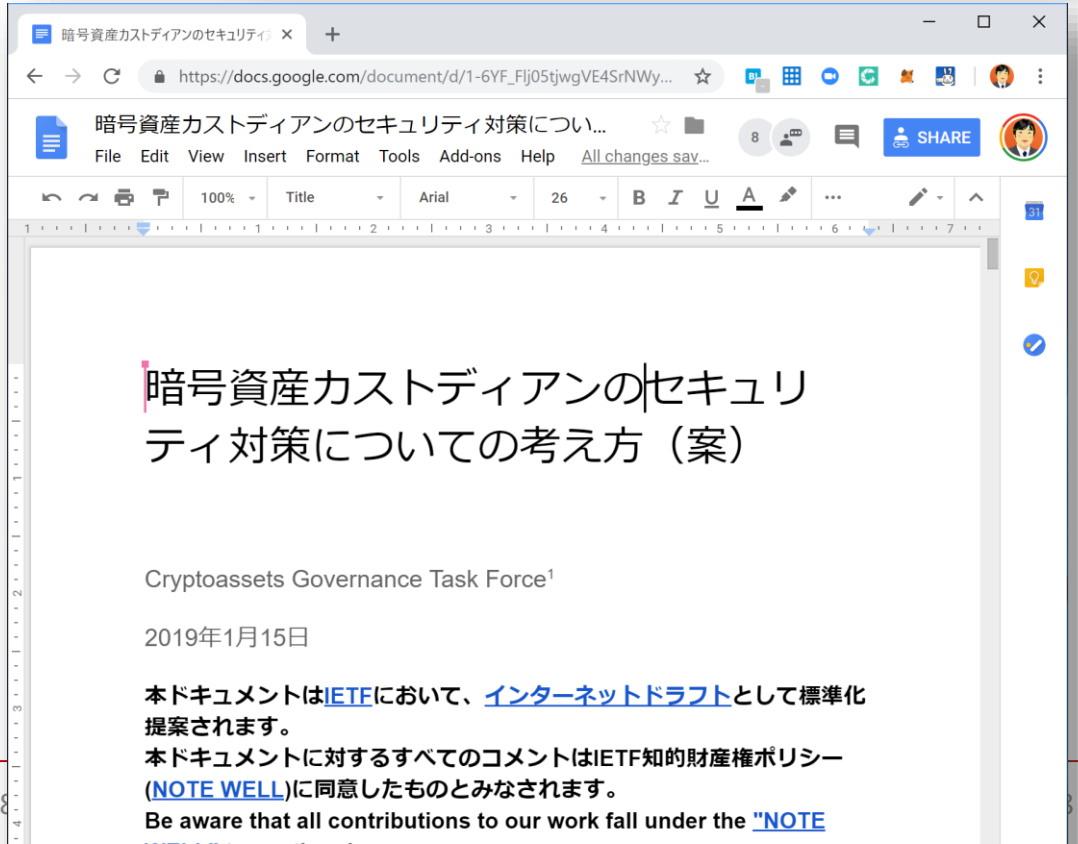
Japan Digital Design

CGTF | CRYPTOASSETS GOVERNANCE TASK FORCE

コインチェック事件後に活動を開始

仮想通貨交換業者のセキュリティ基準パブリックドラフトを公開

https://goo.gl/xyeYy9



管理会計WG等も準備中

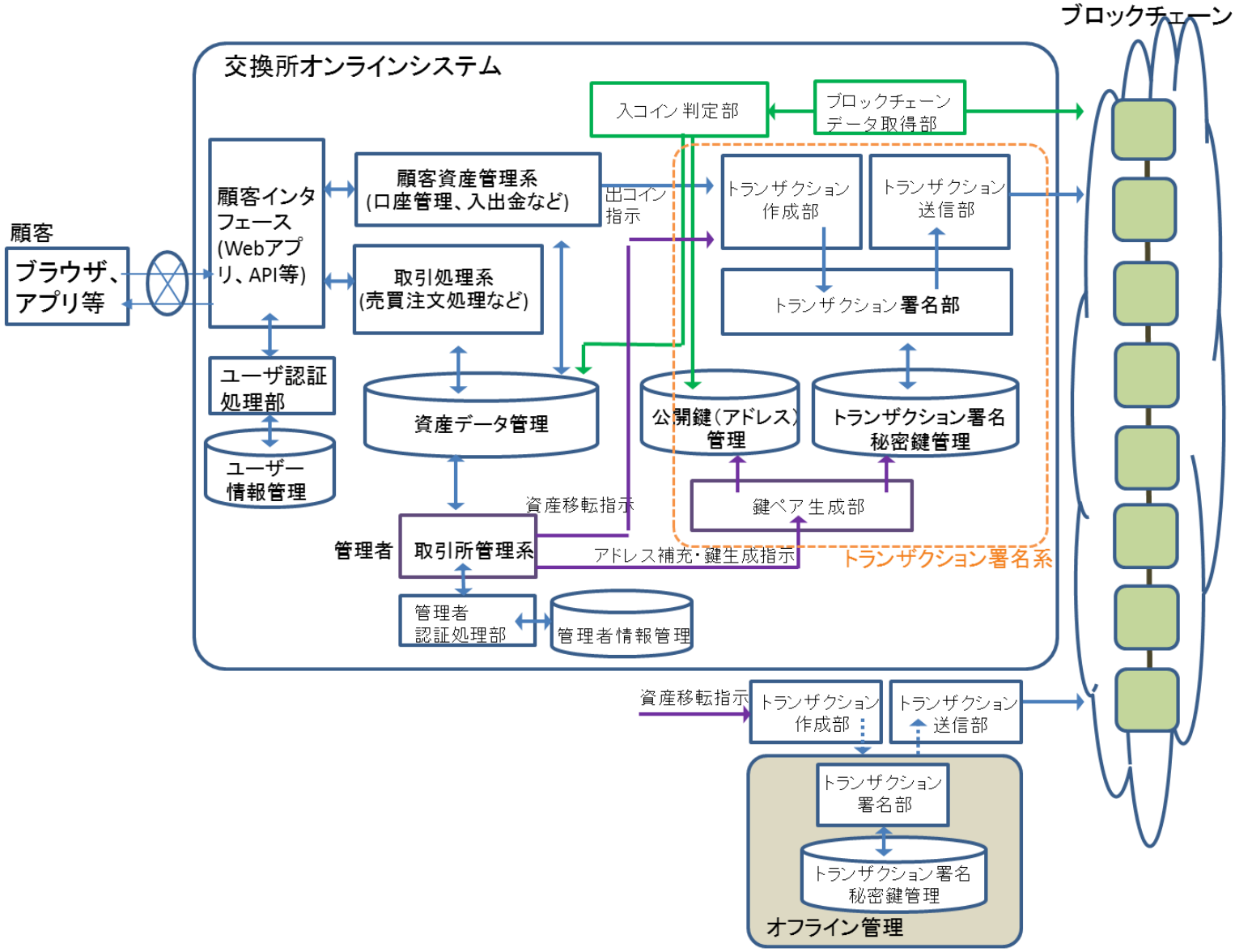
これまでの活動と今後のスケジュール（予定）

Japan Digital Design

時期	
2018年1月	コインチェック事件
2018年2月8日	第1回タスクフォースを実施、当初は週次で会合を開く
2018年5月	ISO/TC307 ロンドン会議でSecurity of Digital Asset CustodiansのTR作成を決議
2018年7月	検討中のドラフトを英訳してInternet Draftとして公開
2018年9月	Zaif事件
2018年10月	日本語版のPublic Draftを公表 Scaling Bitcoin 東京会議でVCGTFとプロジェクトについて公開 ISO/TC307 モスクワ会議で各国からのコメント処理を実施
2018年11月	IETFバンコク会議のSecDispatchで報告、メーリングリストを開設の方向
2018年12月	パブリックドラフトのコメント反映版を英訳しInternet Draftとして公開 認定自主規制団体の技術委員会に参画
2019年5月	ISO/TC307ダブリン会議でTR23576のCommittee Draft承認を目指す

仮想通貨交換業者のリファレンスモデル（案）

Japan Digital Design



Terminology: ウォレットの種類

Japan Digital Design

	自動処理	手動運用
オンライン	ホットウォレット	（ウォームウォレット等）
オフライン	（ウォームウォレット等）	コールドウォレット

- ホットウォレット
  オンラインでネットワークに接続され、鍵が活性化されており、自動処理によって仮想通貨を出コインできるウォレットのことである。
- コールドウォレット
  通常時はネットワークから切断されて鍵が非活性化され、オペレーターの明示的な操作がない限りは、出コインができないウォレットのことである。出コインの頻度は制限されている。

ホットウォレットとコールドウォレットの間には、オンラインだがトランザクションの署名時などに手動での操作が必要なウォレット、オフラインだが運用が自動化されているウォレットなど、様々な中間的な形態が考えられ、ウォームウォレットなどと呼ばれることもある。

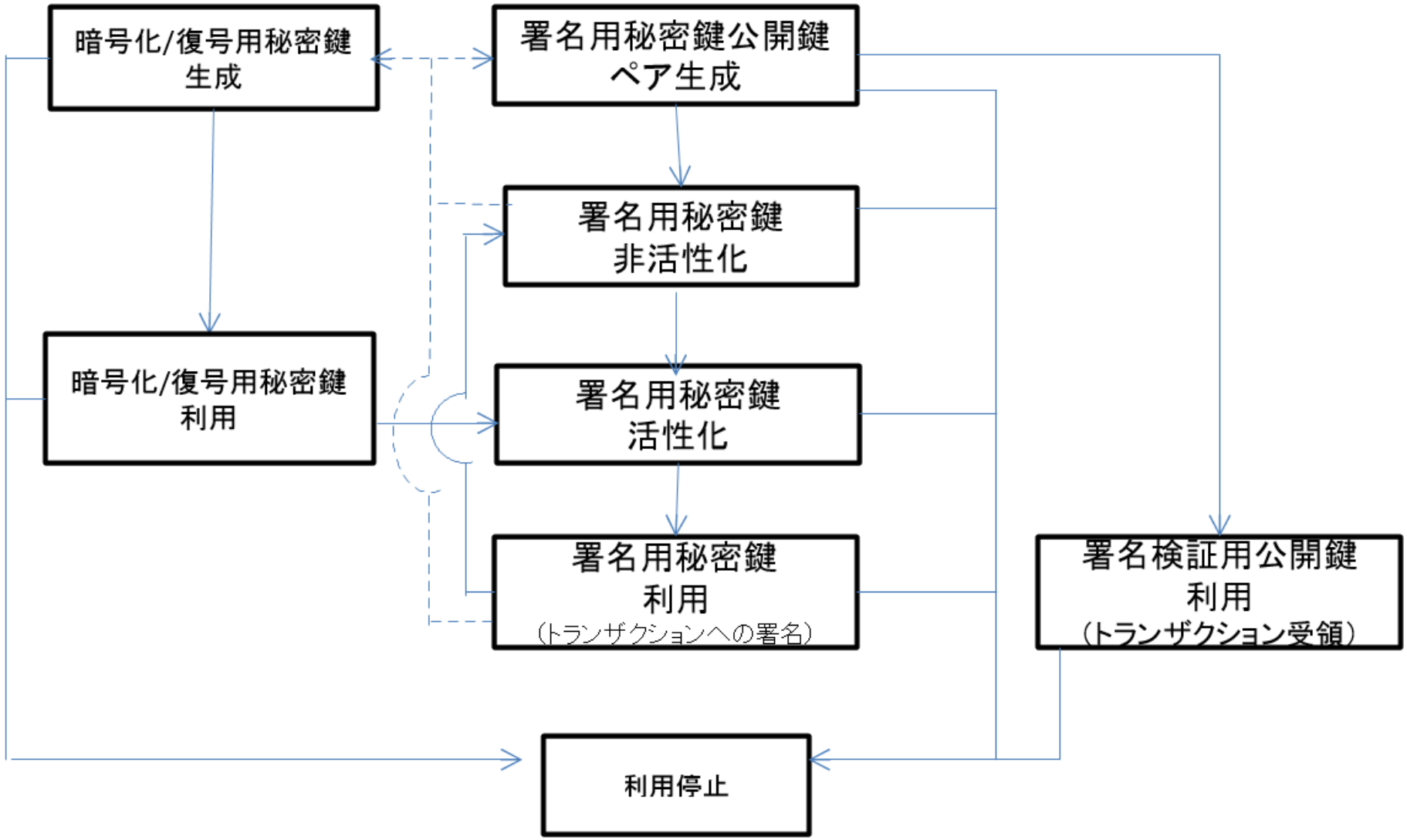
CCSSとBitLicense等の議論でコールドウォレットの定義が異なる点など要整理

交換所が管理する鍵の種類

分類	説明
署名用秘密鍵	トランザクションへのデジタル署名に用いる署名用秘密鍵（公開鍵暗号方式）
署名検証用公開鍵	トランザクションへのデジタル署名の検証に用いる公開鍵（公開鍵暗号方式）。トランザクションの宛先を指定するためのアドレスは公開鍵から生成されるユニークな値である。
署名生成用秘密鍵への暗号化/復号用秘密鍵	署名用秘密鍵を秘匿するために用いられる共通鍵暗号方式の秘密鍵
マスターシード	決定性ウォレットで署名用秘密鍵を生成するためのシード（ランダムな数値など）。

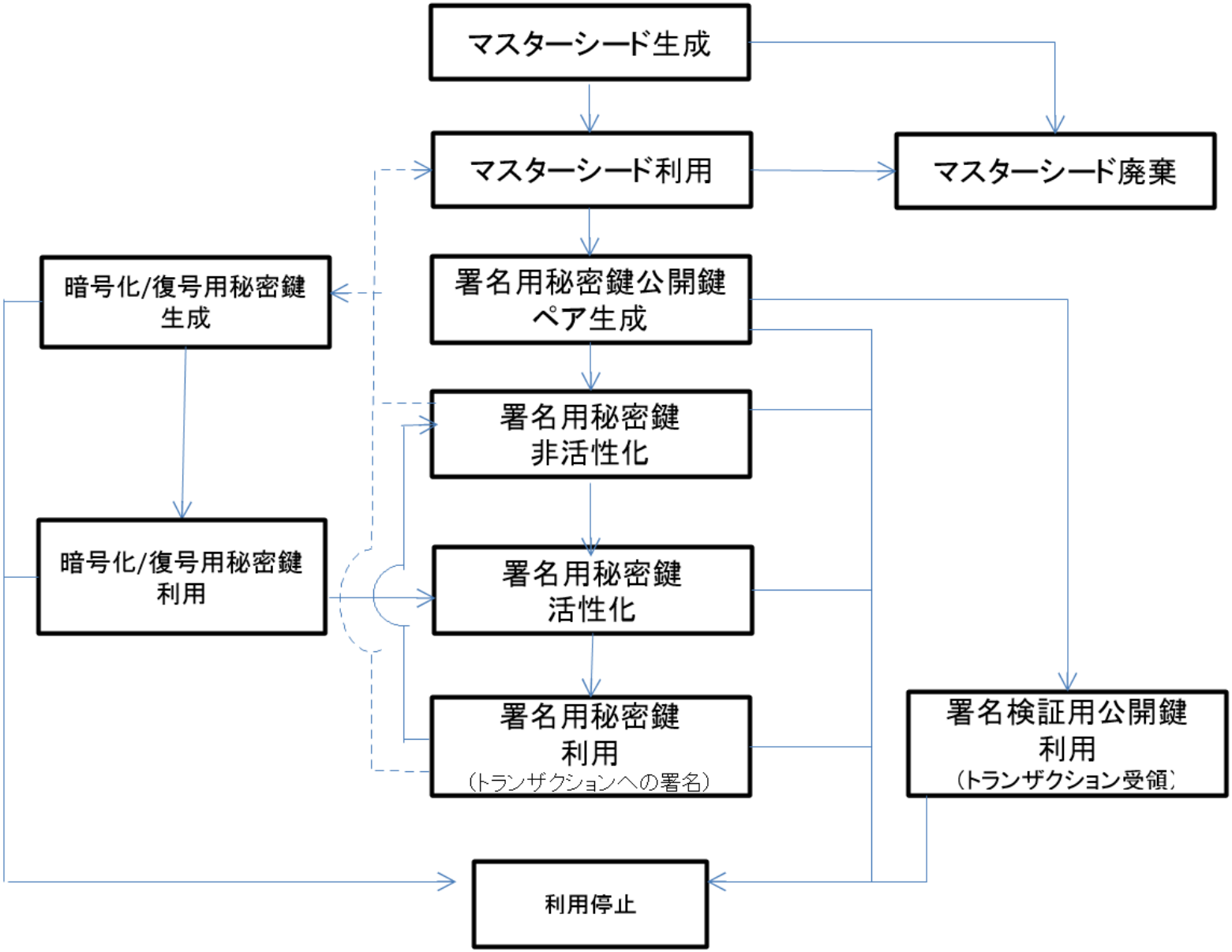
鍵管理のライフサイクル

Japan Digital Design



鍵管理のライフサイクル（HDウォレットの場合）

Japan Digital Design



仮想通貨の歴史とビットコイン価格の推移

Japan Digital Design

発明した作者が匿名だったBitcoin

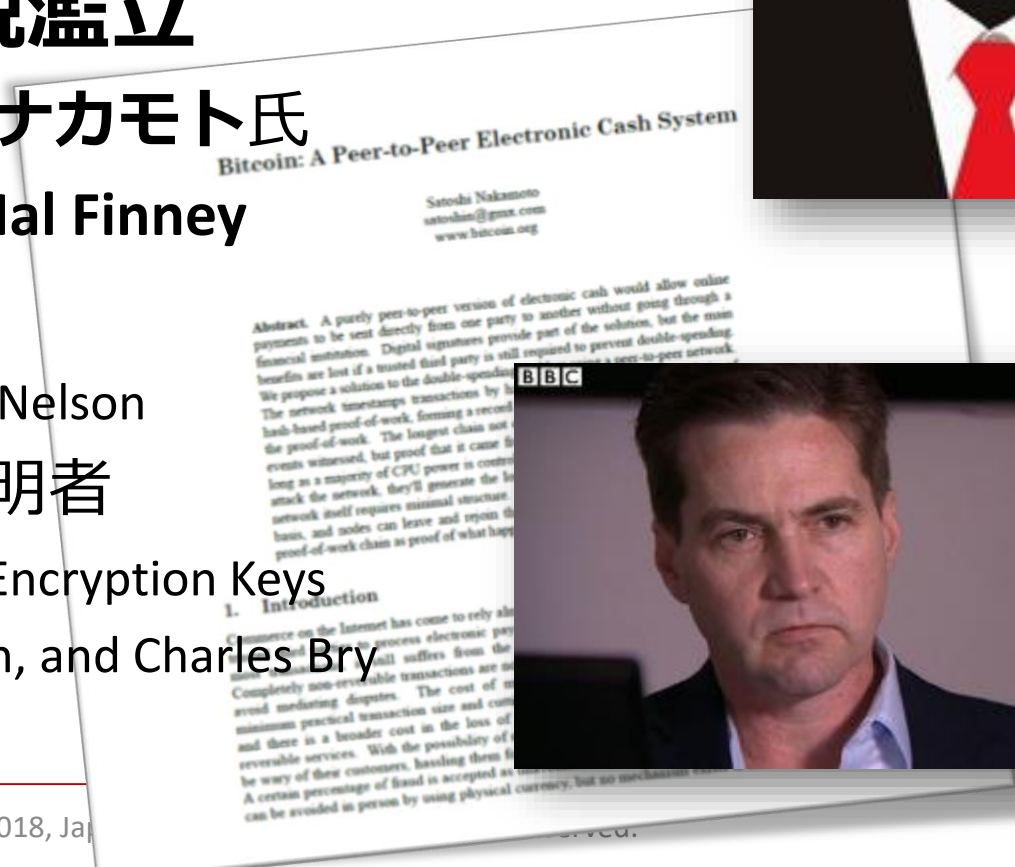
2008年11月 論文を**Cryptography ML**に投稿

2009年1月に運用開始、2010年ごろ活動を休止

2014年3月 I'm not Dorian Nakamoto"と書き込み

正体については**諸説濫立**

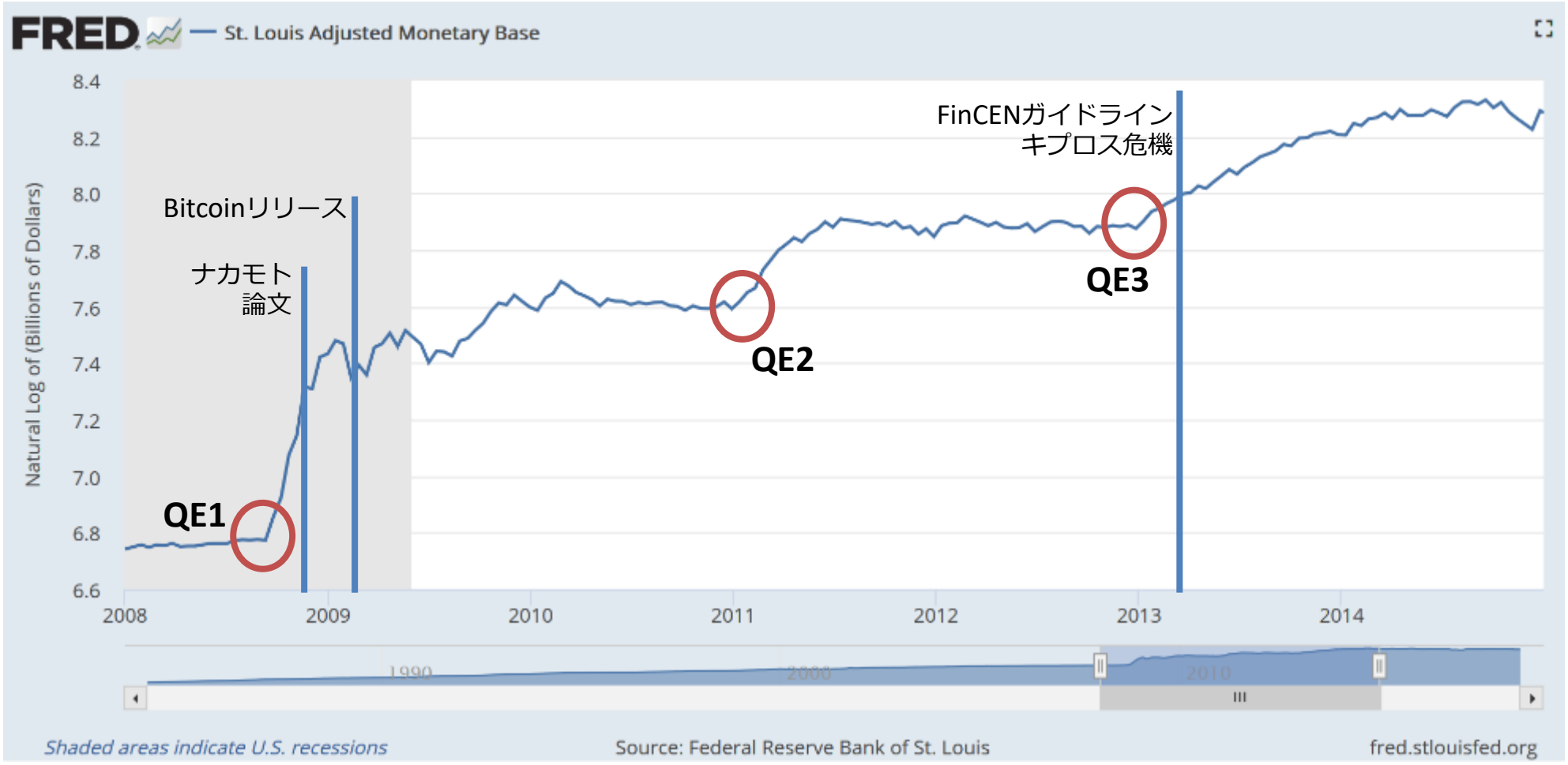
- Los近郊在住の**ドリアンナカモト**氏
- ドリアンの近所に住む**Hal Finney**
- **Michael Clear** – New Yorker
- 京大 **望月新一**教授 – Ted Nelson
- **US 20100042841 A1**の発明者
  - Updating and Distributing Encryption Keys
  - Neal King, Vladimir Oksman, and Charles Bry
- 名乗り出た**Craig Wright**



Bitcoin発明の背景 - リーマンショック後の量的緩和

Japan Digital Design

- 政府による量的緩和に対する反発を背景にBitcoinは発明されたのではないか
- キプロス危機によって資本逃避先としてのビットコインの有用性が確認され価格が高騰



2010年5月 ビットコインで最初にモノの売買が成立

Japan Digital Design

10kBTC = $41

Bitcoin Market

先に取引所が立ち上がっていたので裁定取引が可能

Pizza for bitcoins? by laszlo

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later.

May 18, 2010, 12:35:20 AM

jercos

So nobody wants to buy me pizza? Is the bitcoin amount I'm offering too low?

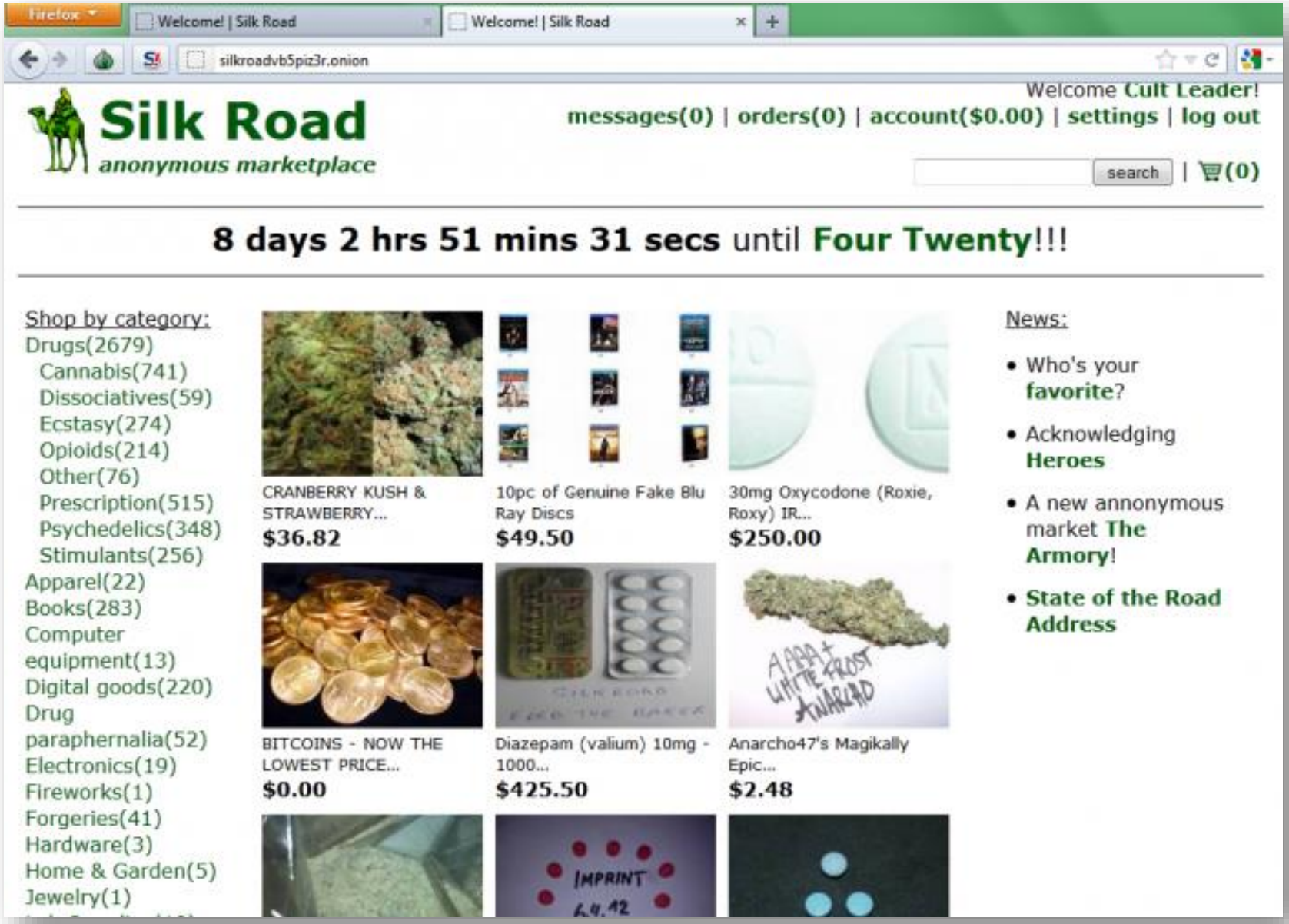
May 21, 2010, 07:06:58 PM

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Thanks jercos! **May 22, 2010, 07:17:26 PM**

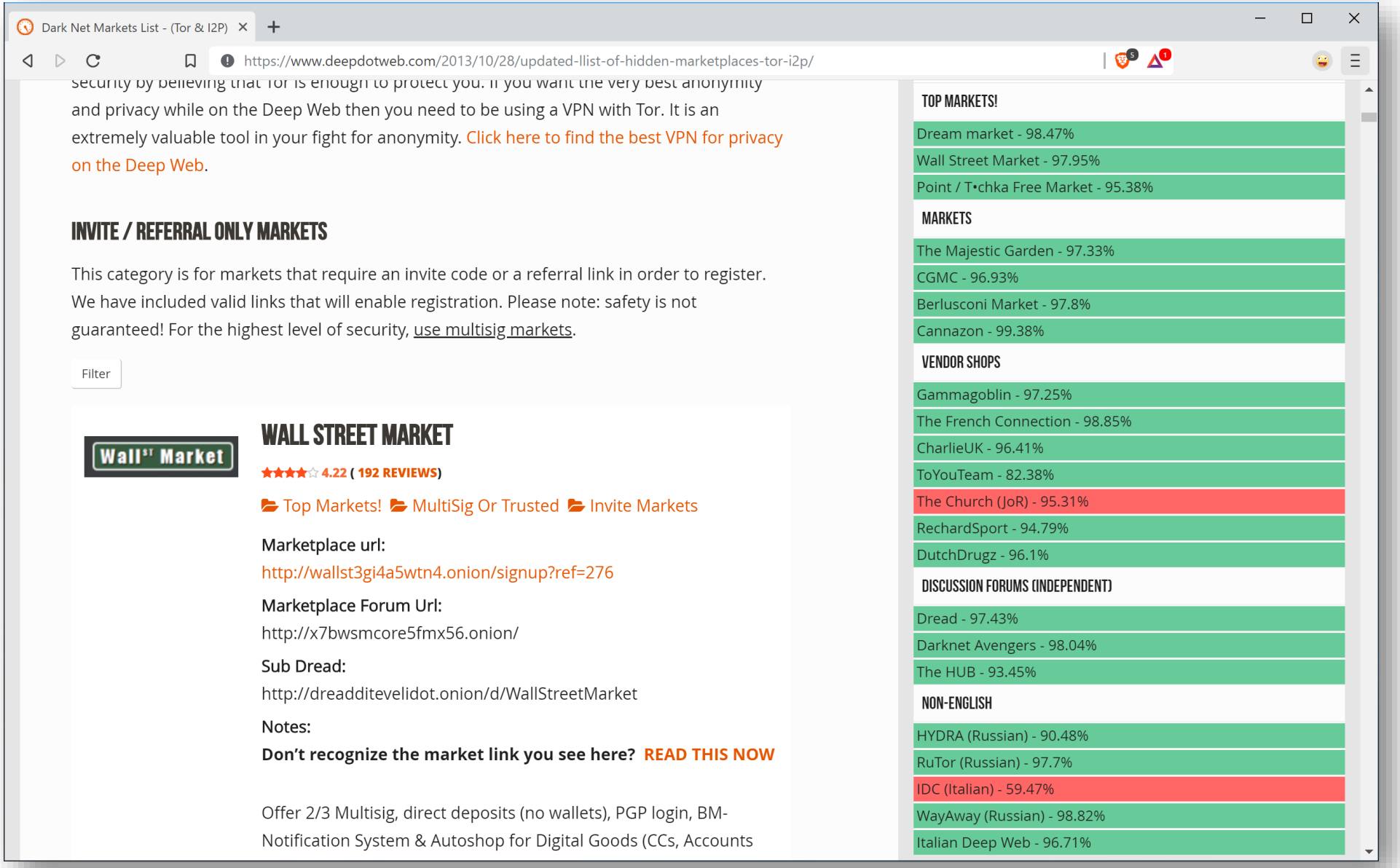
2011年 違法薬物取引サイトでBitcoin決済が普及

Japan Digital Design



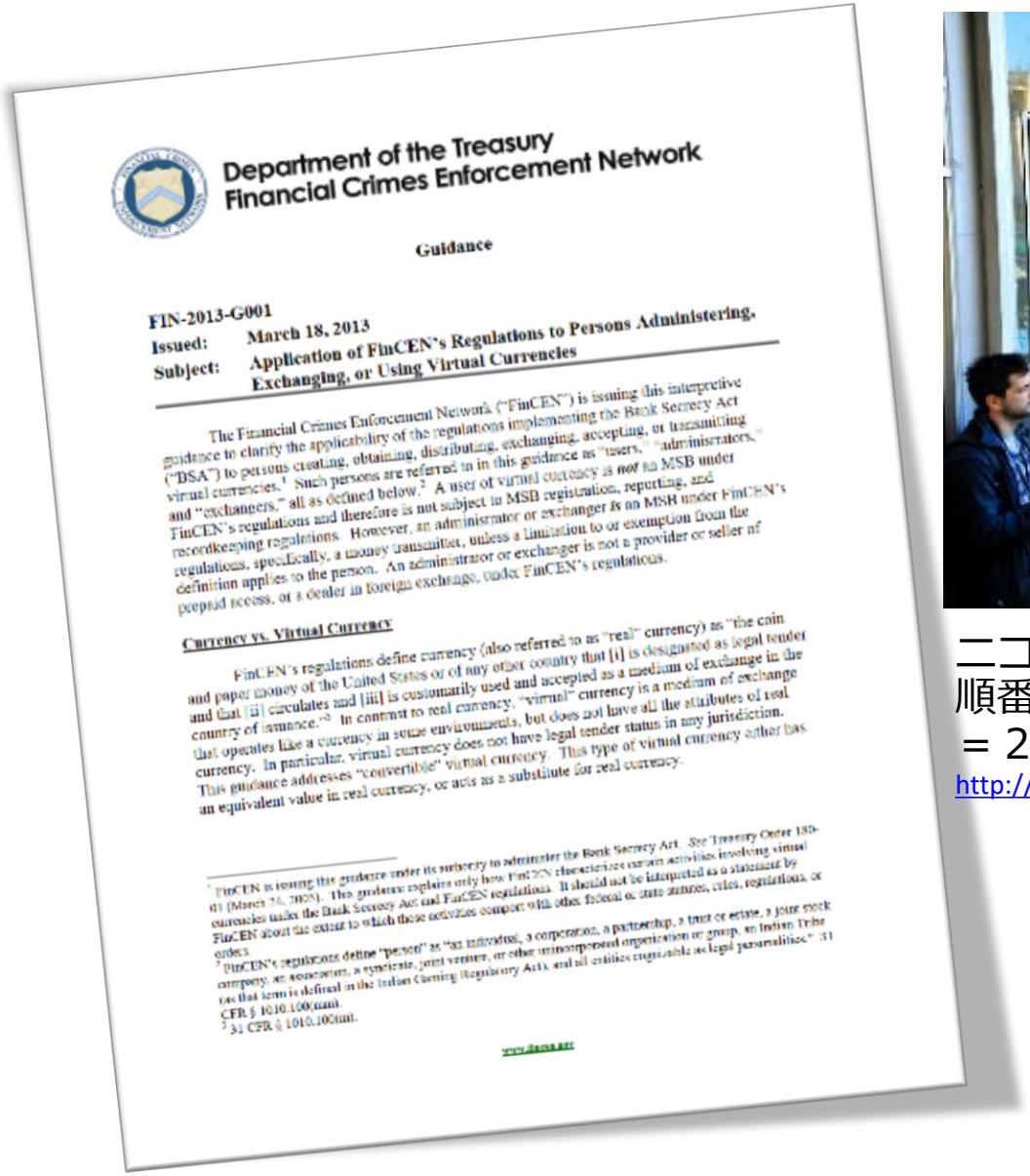
SilkRoad摘発後も百数十のDark marketplaceが現存

Japan Digital Design



2013年 FinCENガイドラインとキプロス危機で普及

Japan Digital Design



Department of the Treasury
Financial Crimes Enforcement Network

Guidance

FIN-2013-G001
Issued: March 18, 2013
Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies

The Financial Crimes Enforcement Network ("FinCEN") is issuing this interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.[1] Such persons are referred to in this guidance as "users," "administrators," and "exchangers," all as defined below.[2] A user of virtual currency is not an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations.

Currency vs. Virtual Currency

FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."[3] In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses "convertible" virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.

[1] FinCEN is issuing this guidance under its authority to administer the Bank Secrecy Act. See Treasury Order 180-01 (March 24, 2003). This guidance explains only how FinCEN characterizes certain activities involving virtual currencies under the Bank Secrecy Act and FinCEN regulations. It should not be interpreted as a statement by FinCEN about the extent to which those activities comport with other federal or state statutes, rules, regulations, or orders.

[2] FinCEN's regulations define "person" as "an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities." 31 CFR § 1010.100(mm).

[3] 31 CFR § 1010.100(m).

www.fincen.gov

ニコシア中心部の銀行支店では、店舗に入る順番を待つ預金者らをメディアが取り囲んだ＝２０１３年３月２８日、喜田尚撮影
http://webronza.asahi.com/business/themes/2913032800001.html

法定通貨による銀行預金は破綻した銀行の株式に転換されたがBitcoinで蓄財していれば数倍に膨れ上がった

2013年 ビットコインバブルと2014年 MtGOXの破綻

Japan Digital Design

$1250

$750

$500

$250

Nov '13

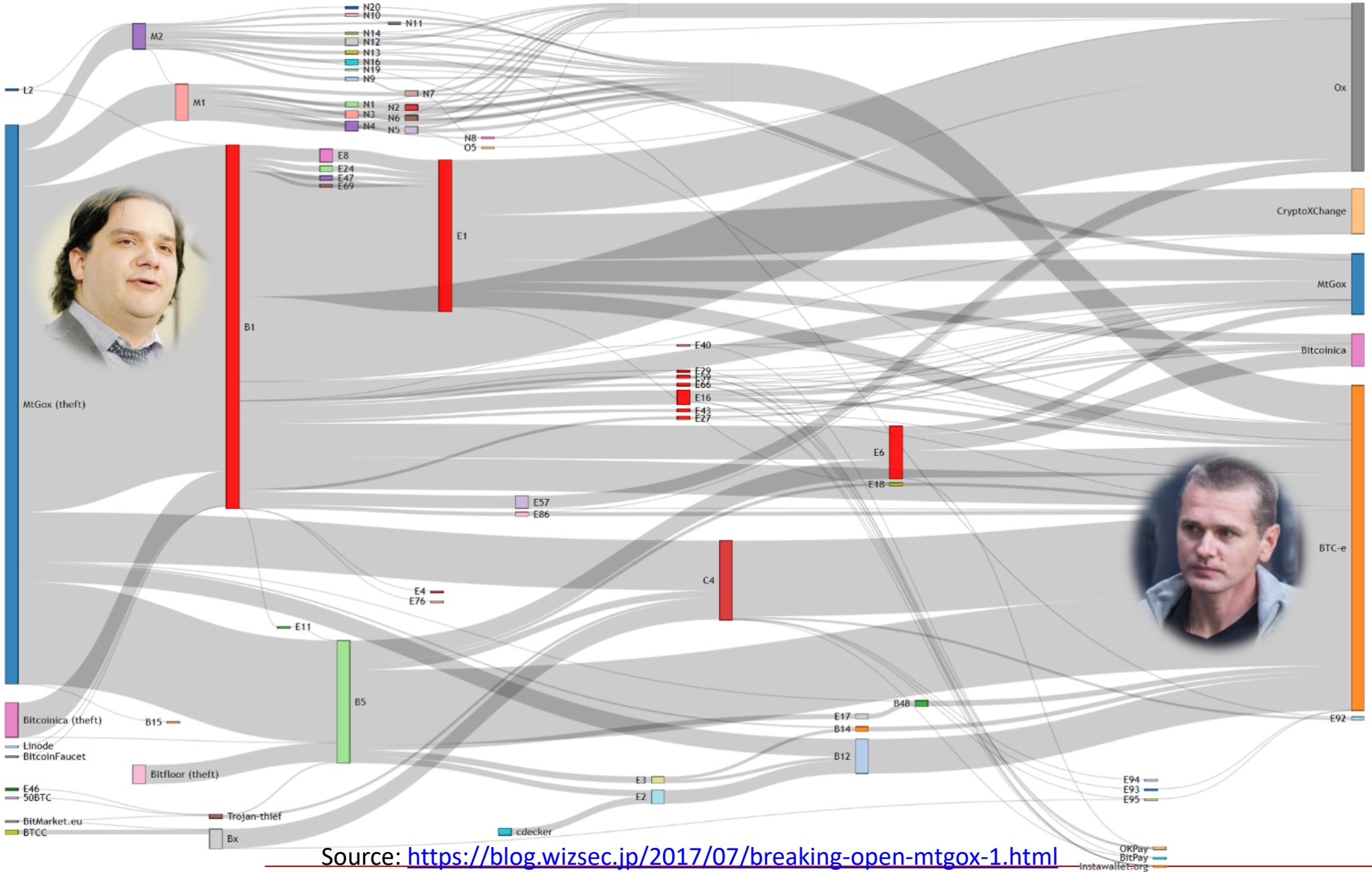
Jan '14

Mar '14

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）

Japan Digital Design



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

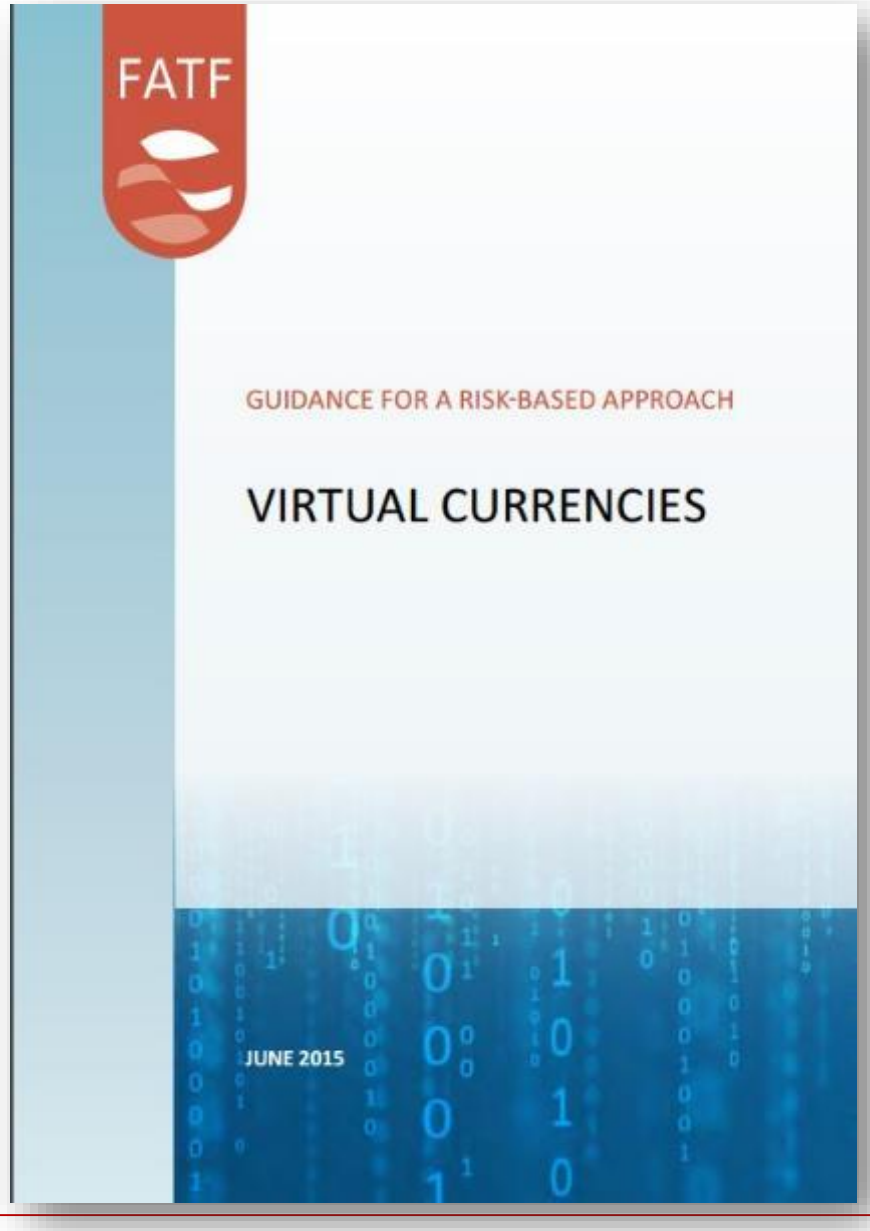

bitcoin-
trading-
club

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



中国に集積したBitcoinの採掘、Scaling問題の顕在化

Japan Digital Design

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

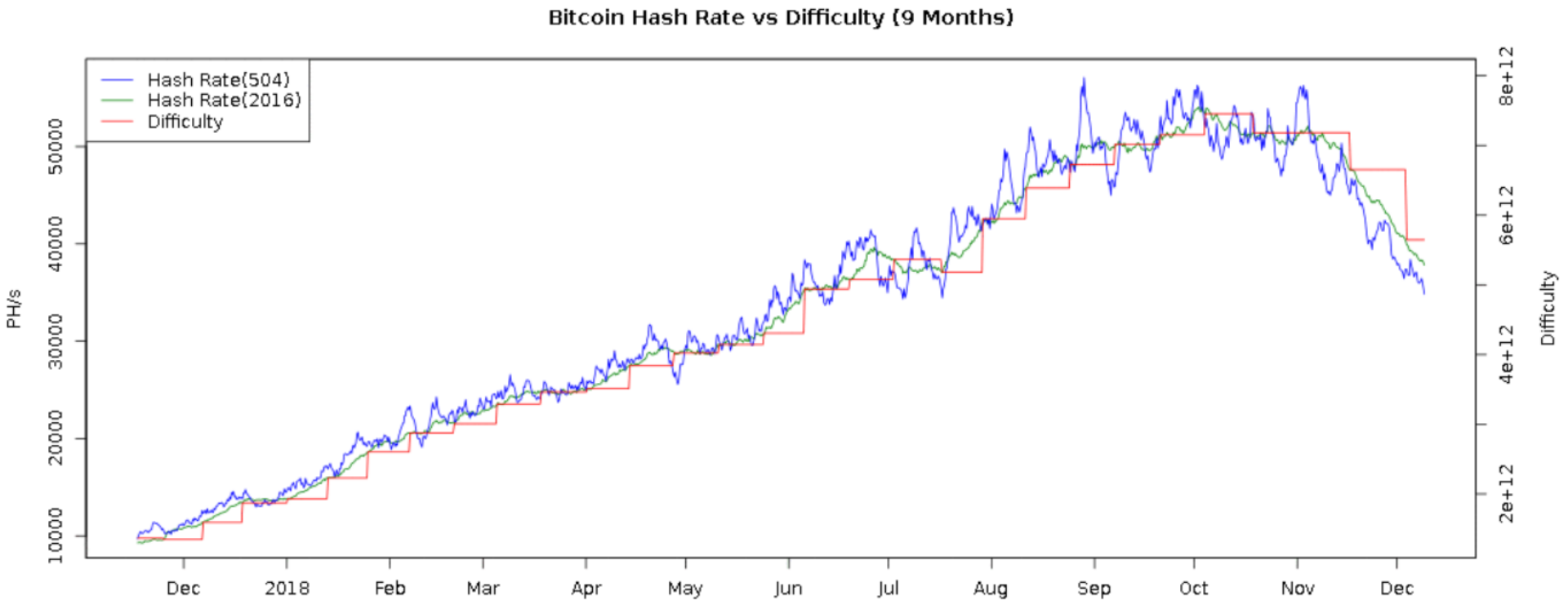
BitcoinにおけるHashrateの上昇と難易度の調整

Japan Digital Design

Bitcoin Difficulty:	5,646,403,851,534
Estimated Next Difficulty:	5,261,178,561,254 (-6.82%)
Adjust time:	After 1297 Blocks, About 10.0 days
Hashrate(?):	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: 5646403851534 BTC/USD: 3519.5

1000000	KH/s	1.856e-9	BTC/hour	0.000006531	USD/hour
1000	MH/s	4.453e-8	BTC/day	0.0001567	USD/day
1	GH/s	3.117e-7	BTC/week	0.001097	USD/week
0.001	TH/s	0.000001336	BTC/month	0.004702	USD/month



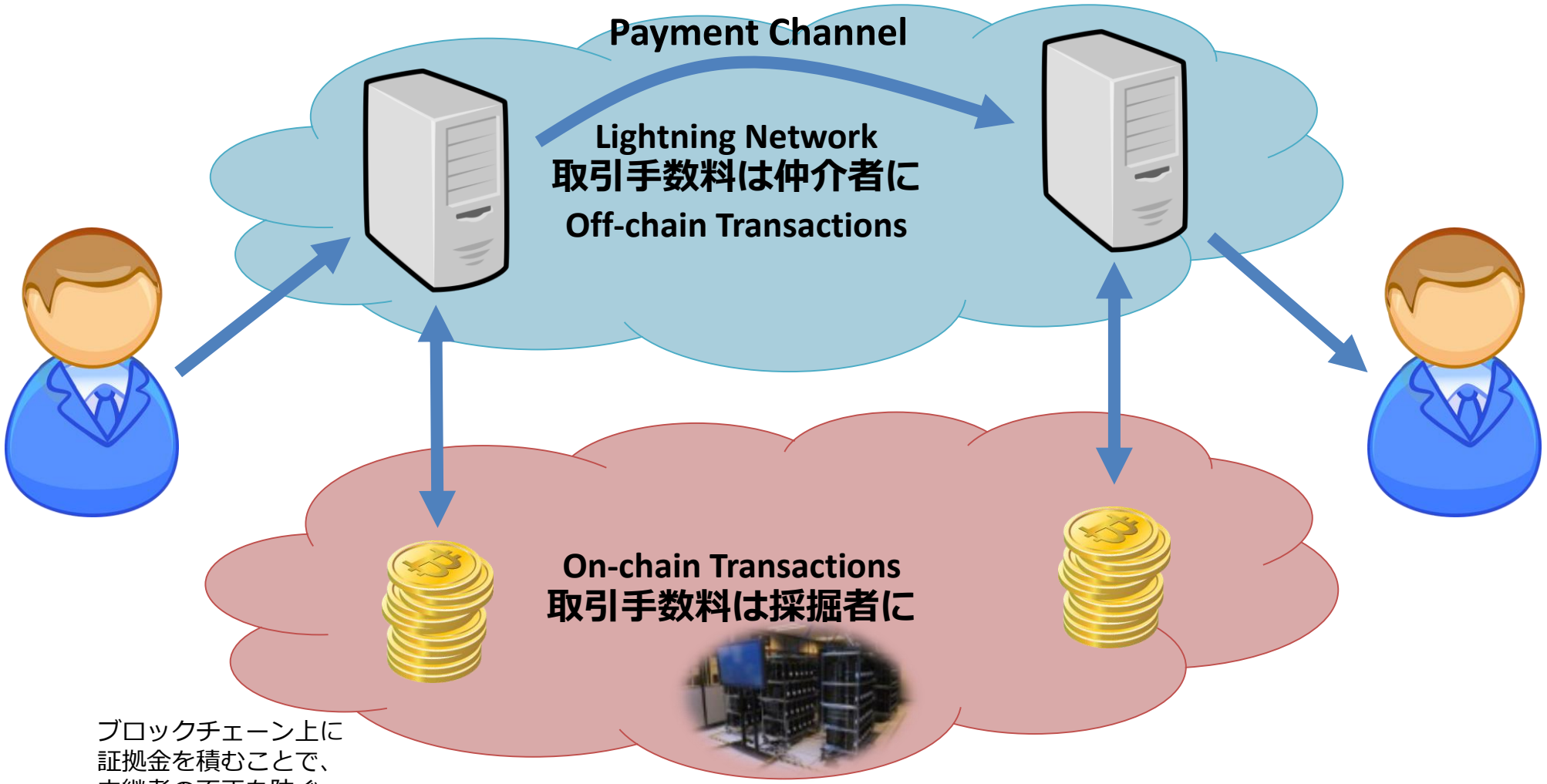
https://bitcoinwisdom.com/bitcoin/difficulty

2017年 Bitcoinバブルの再来とBitcoin Cashとの分裂

Japan Digital Design

取引手数料の分け前を巡る開発者と採掘者の確執

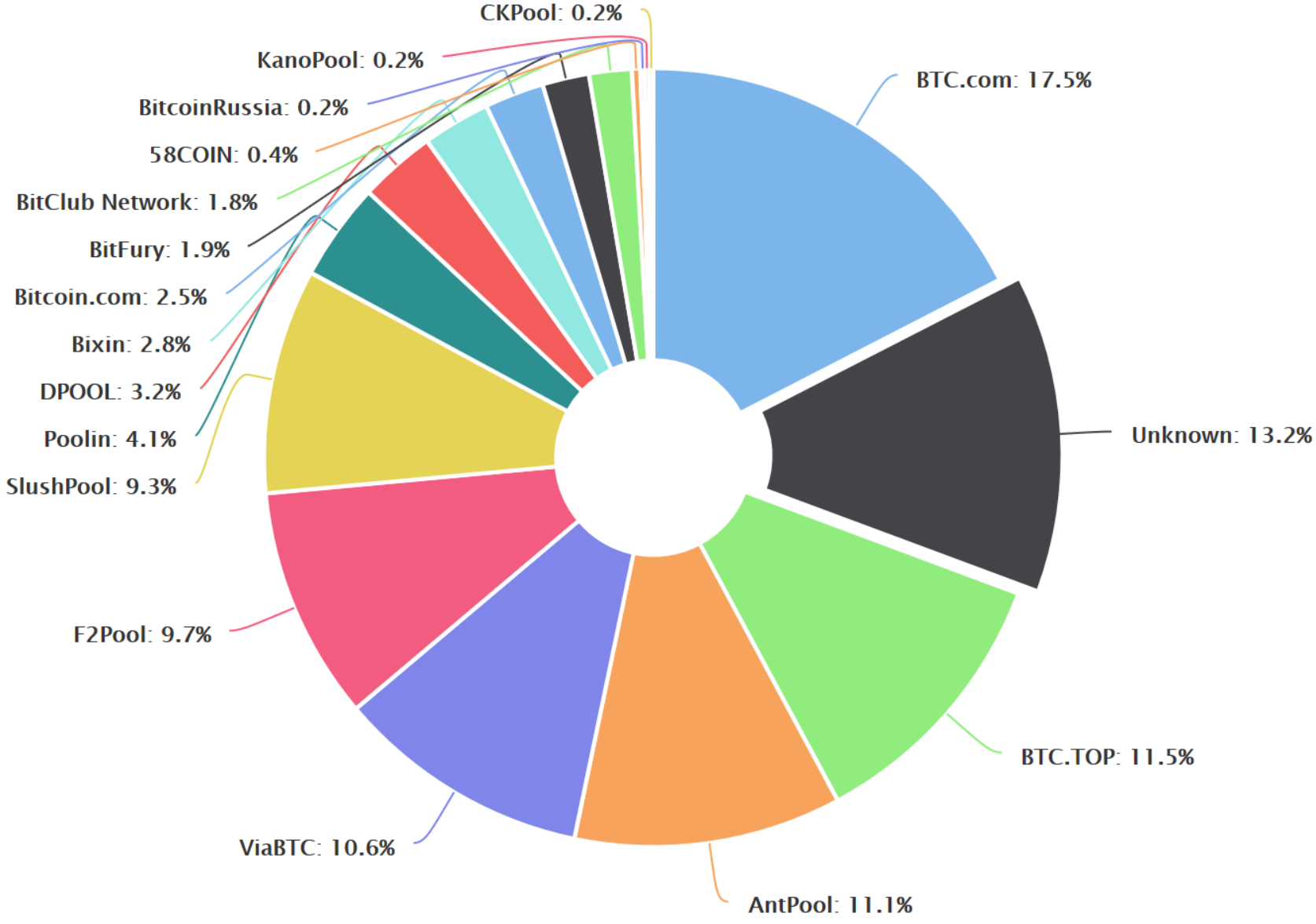
Japan Digital Design



ブロックチェーン上に
証拠金を積むことで、
中継者の不正を防ぐ

採掘プールの寡占化と51%問題

Japan Digital Design



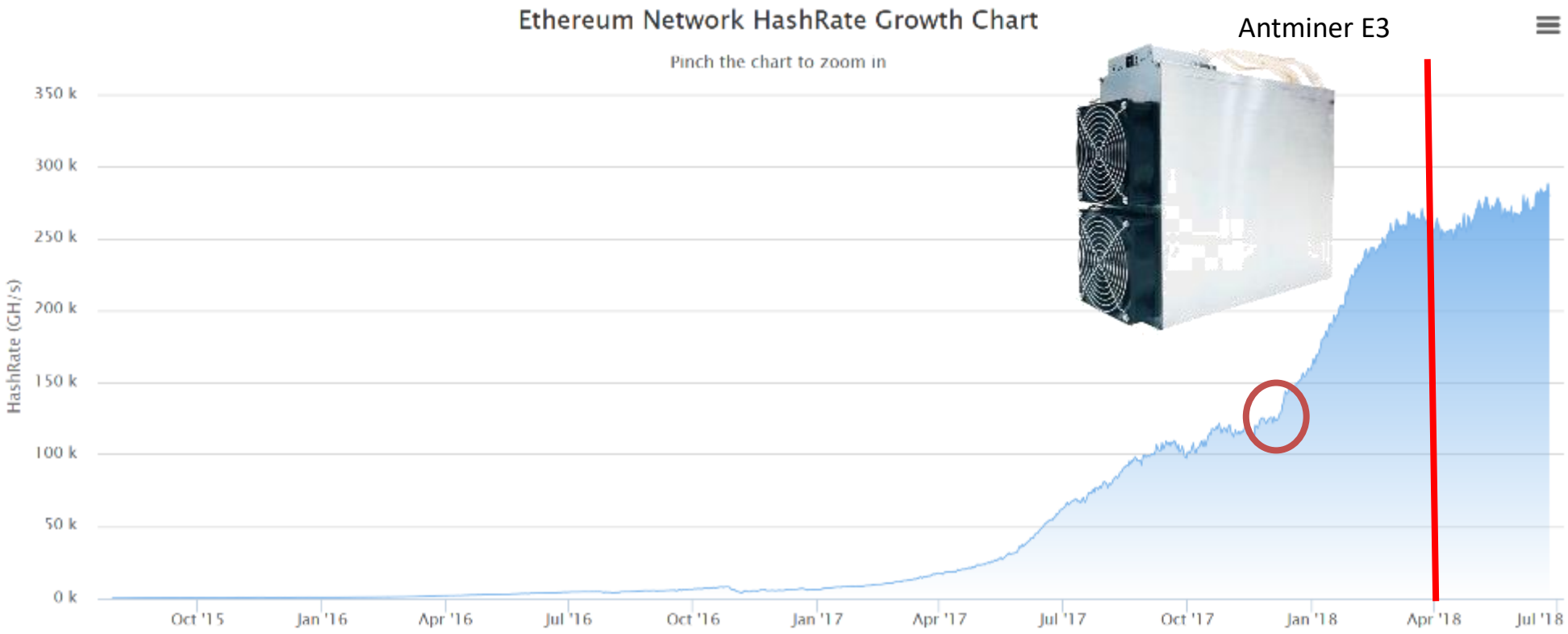
2018年5月から多発した仮想通貨Blockchain書換攻撃

Japan Digital Design

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

Ethereum: 新ASICで発売前にハッシュレートが増大

Japan Digital Design



- 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？

Monero: ASIC対策でHashrateが元の水準まで下落

Japan Digital Design

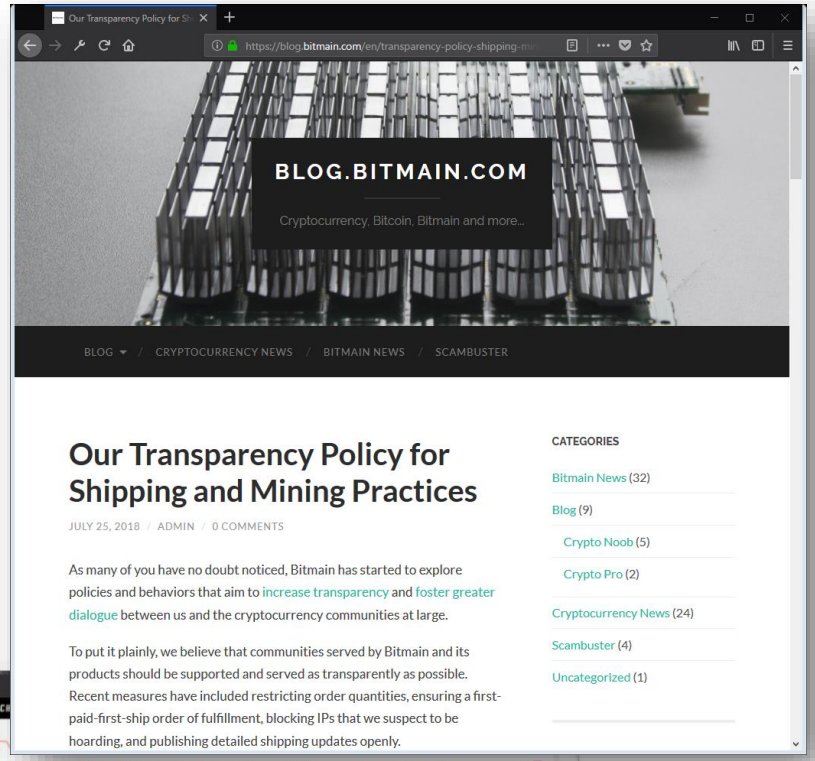
Bitmain Antminer X3

CryptoNightV7
への移行

Bitmain社が7月25日に発表した出荷・採掘方針

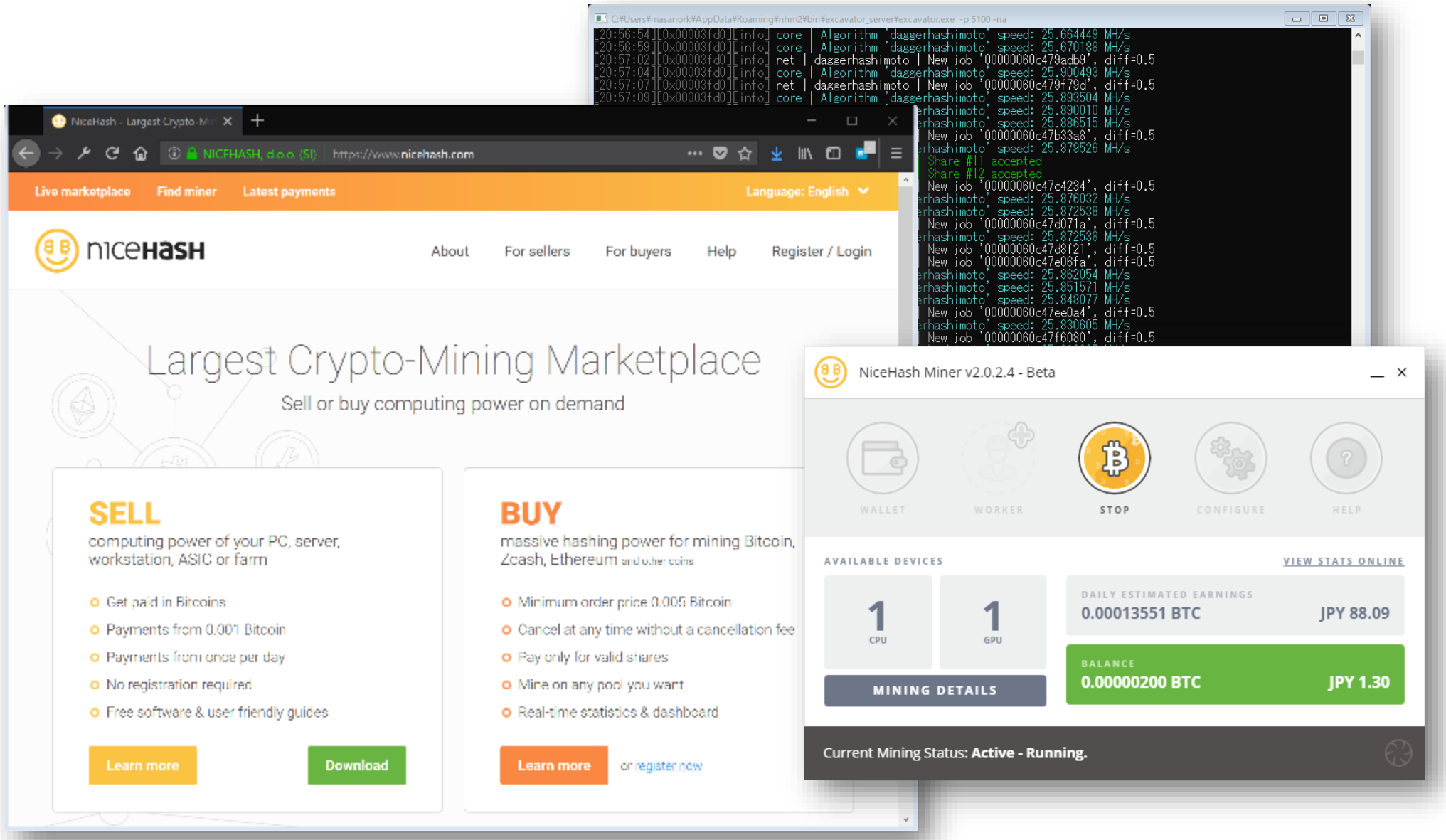
Japan Digital Design

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

Japan Digital Design



Bitcoin登場時の前提とAltcoin, Fork coinの現実

Japan Digital Design

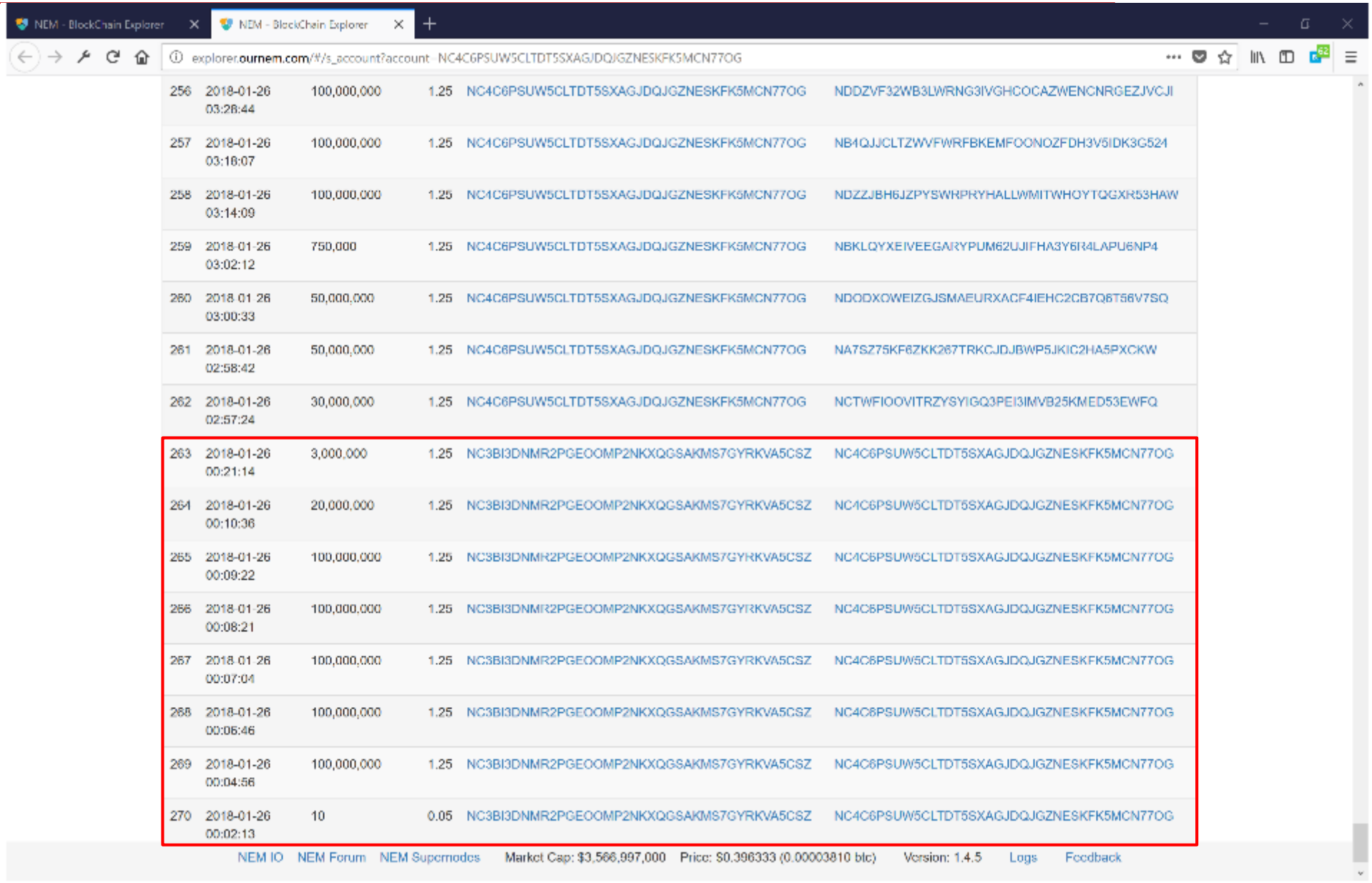
Bitcoin設計時の前提	Altcoin, Fork coinの現実
世の中にはBitcoinしか存在しない	世の中には多様な仮想通貨が併存
採掘者は広く分散	採掘者は寡占化されたmining poolに所属
Minerは多くのBitcoinと採掘にしか使えない計算機を保有	Minerは様々な仮想通貨の中で収益性の高い銘柄を採掘
MinerにとってBitcoinの価値を毀損することのデメリットが大きい	不正によって仮想通貨が暴落しても他の銘柄を採掘すれば良い
Hashrateは安定的な上昇傾向	ASIC MiningによるHashrateの急増 Minerの撤退、乗換によるHashrateの急減
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

Japan Digital Design

最初の数分で500億円分以上が盗み出された

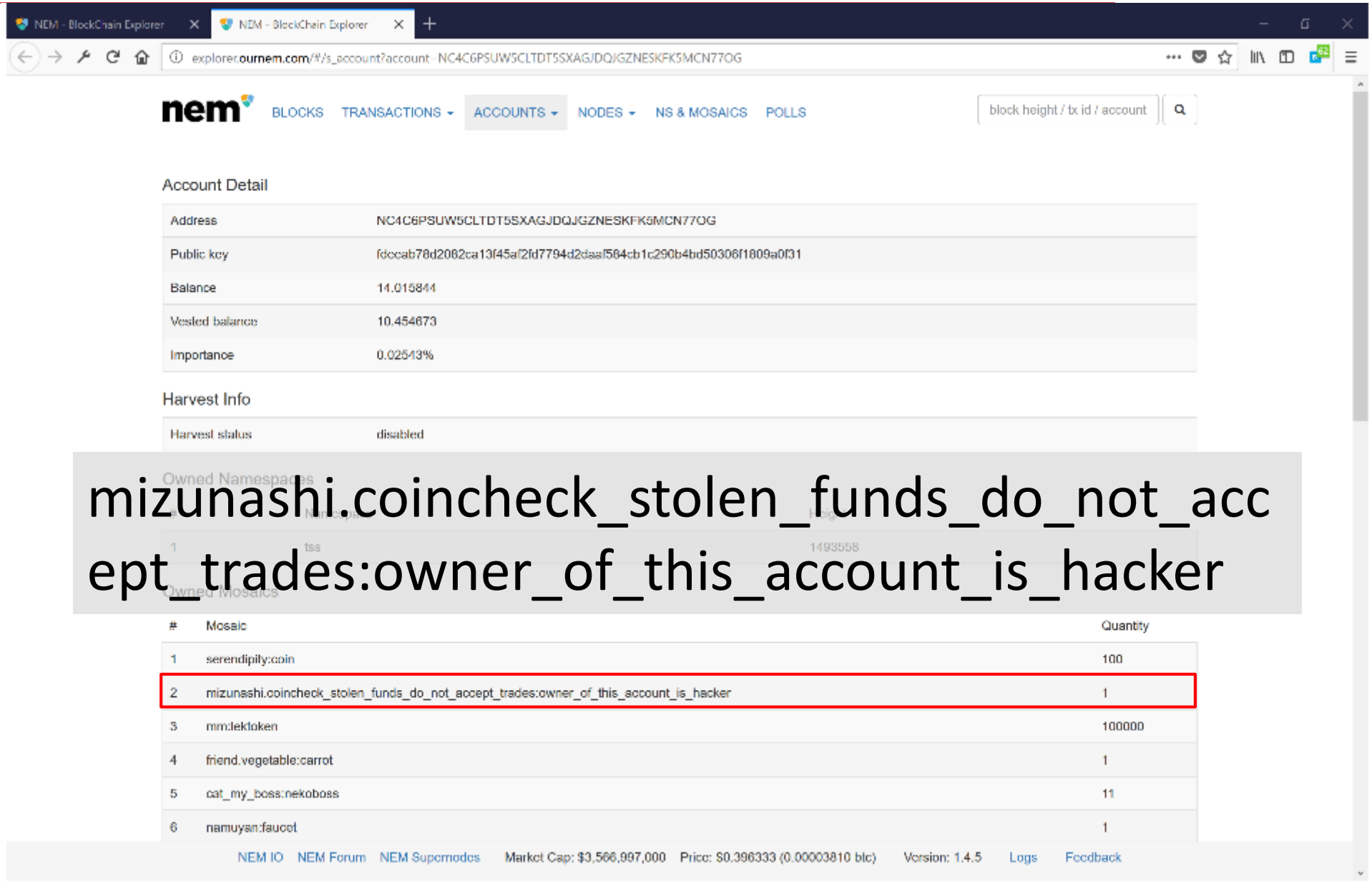
Japan Digital Design



256	2018-01-26 03:28:44	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NDDZVF32WB3LWRNG3IVGHCOCAZWENCNRGEZJVCJI
257	2018-01-26 03:18:07	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NB4QJJCLTZWVFWRFBKEMFOONOZFDH3V5IDK3G524
258	2018-01-26 03:14:09	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NDZZJBH6JZPYSWRPRYHALLWMITWHOYTQGXR53HAW
259	2018-01-26 03:02:12	750,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NBKLQYXEIVEEGARYPUM62UJIFHA3Y6R4LAPU6NP4
260	2018-01-26 03:00:33	50,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NDODXOWEIZGJSMAEURXACF4IEHC2CB7Q6T56V7SQ
261	2018-01-26 02:58:42	50,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NA7SZ75KF6ZKK267TRKCJDJBWP5JKIC2HA5PXCKW
262	2018-01-26 02:57:24	30,000,000	1.25	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG	NCTWFIOOVITRZYSYIGQ3PEI3IMVB25KMED53EWFQ
263	2018-01-26 00:21:14	3,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
264	2018-01-26 00:10:36	20,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
265	2018-01-26 00:09:22	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
266	2018-01-26 00:08:21	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
267	2018-01-26 00:07:04	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
268	2018-01-26 00:06:46	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
269	2018-01-26 00:04:56	100,000,000	1.25	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
270	2018-01-26 00:02:13	10	0.05	NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ	NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG

ホワイトハッカーによる追跡劇

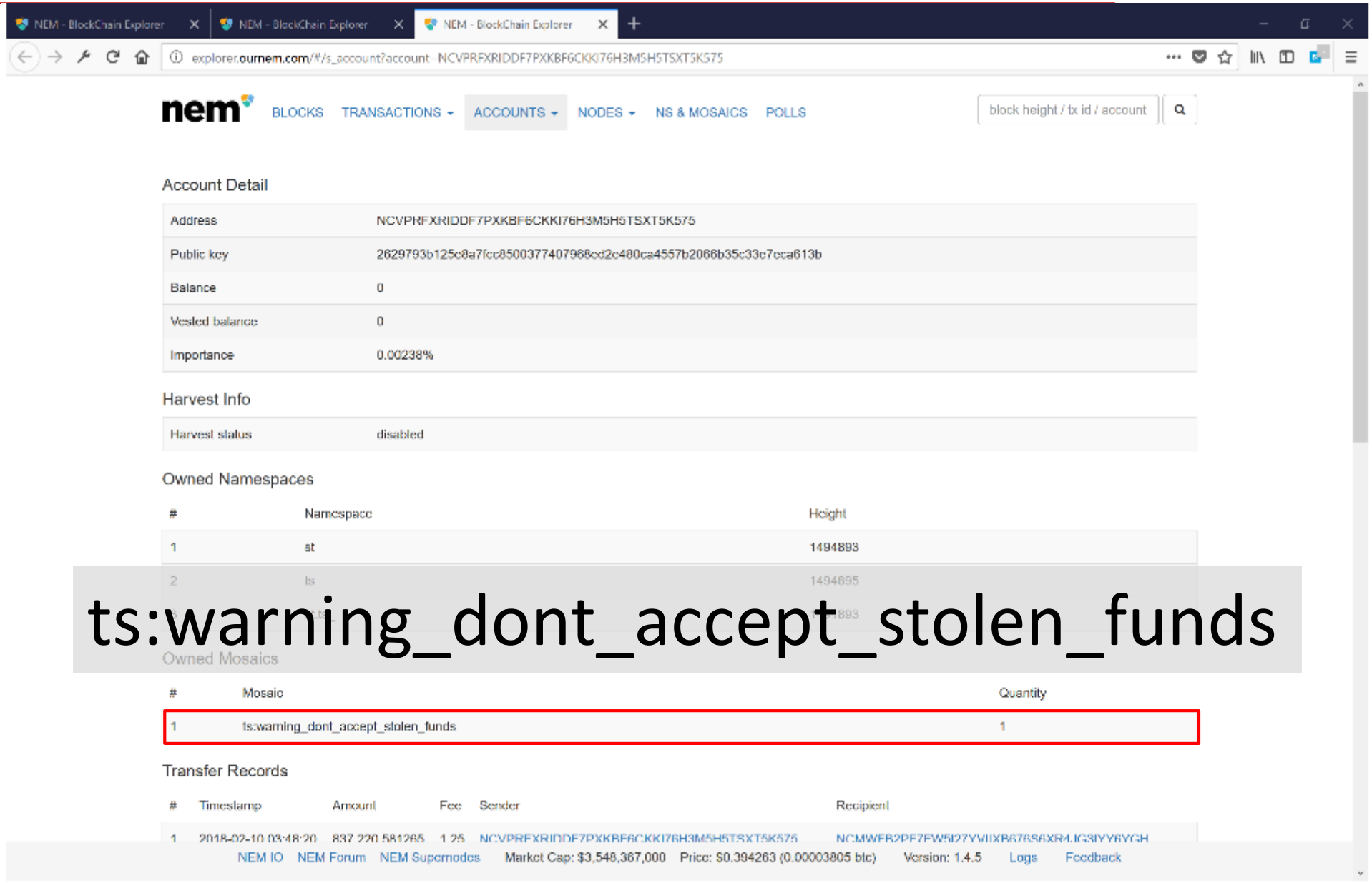
Japan Digital Design



mizunashi.coincheck_stolen_funds_do_not_accept_trades:owner_of_this_account_is_hacker

流出NEMの受取拒否を求めるメッセージ

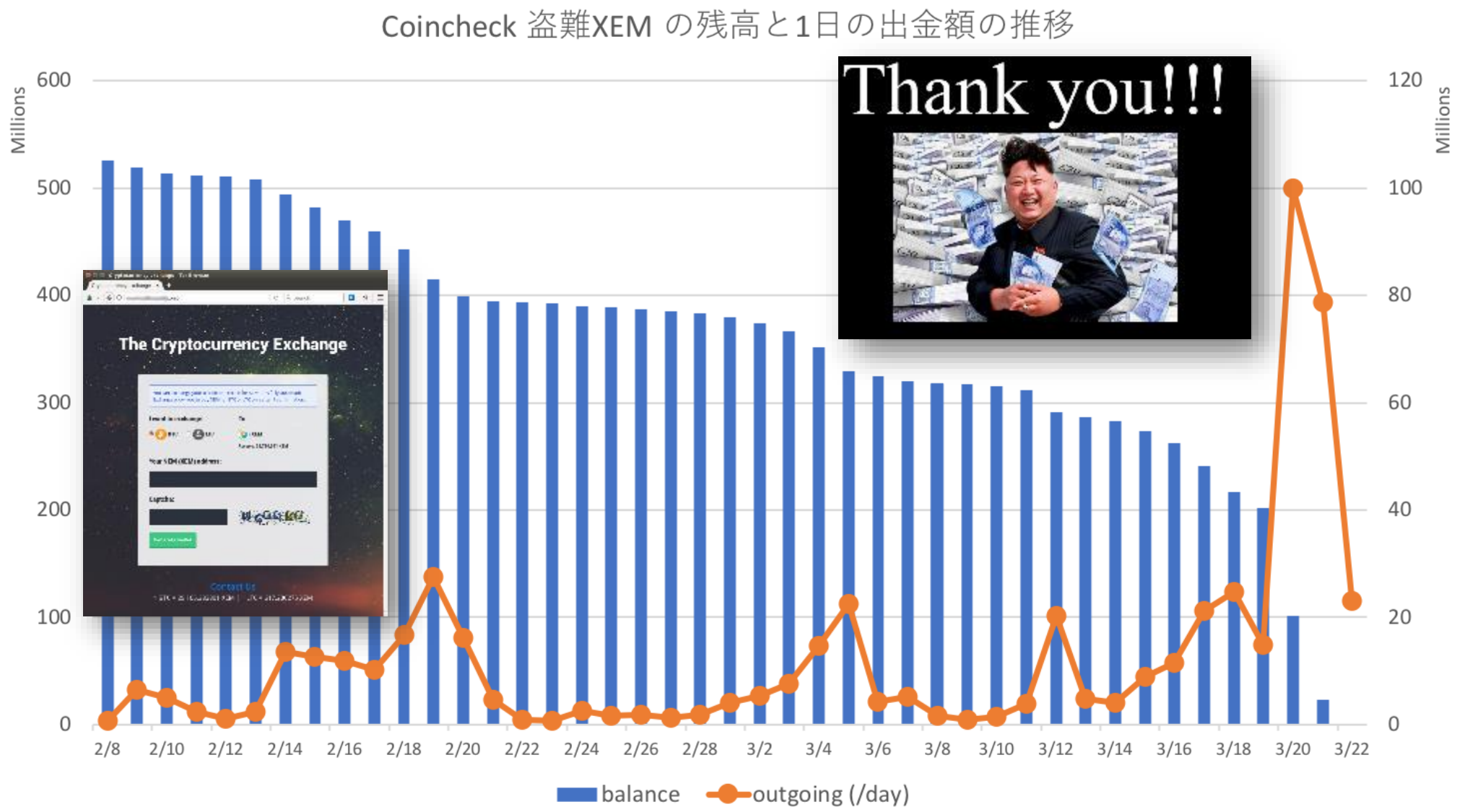
Japan Digital Design



ts:warning_dont_accept_stolen_funds

追跡モザイクの廃止で盗難XEMの交換は一気に加速

Japan Digital Design

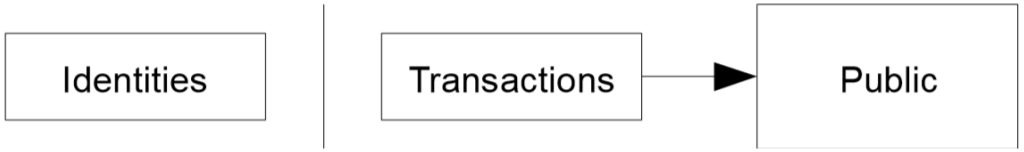


出典 https://twitter.com/MasafumiNegishi/status/976767126169010176

Bitcoinと匿名通貨との違い

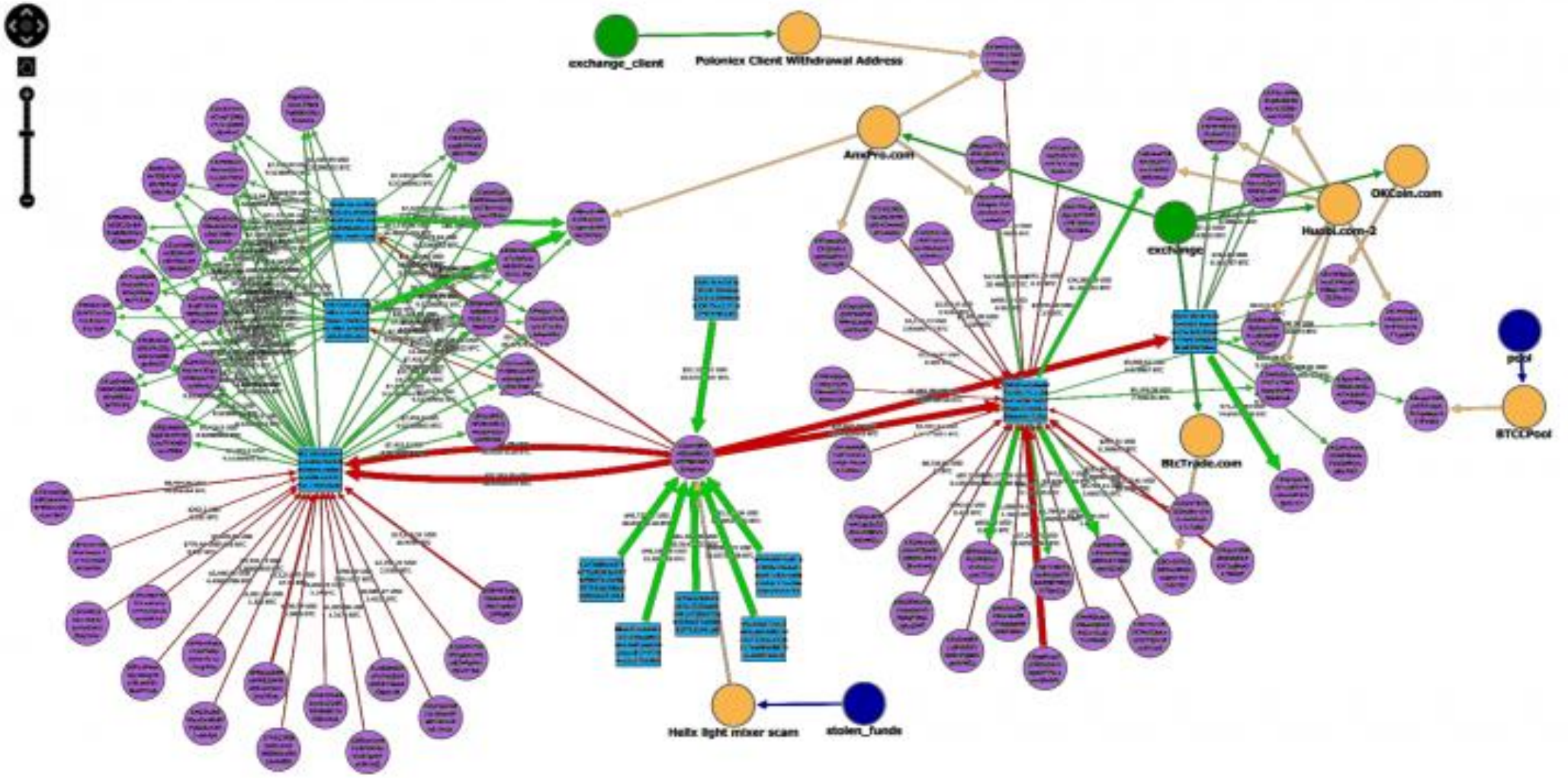
Traditional Privacy Model

New Privacy Model



QLUEによるBitcoinブロックチェーンの可視化

Japan Digital Design

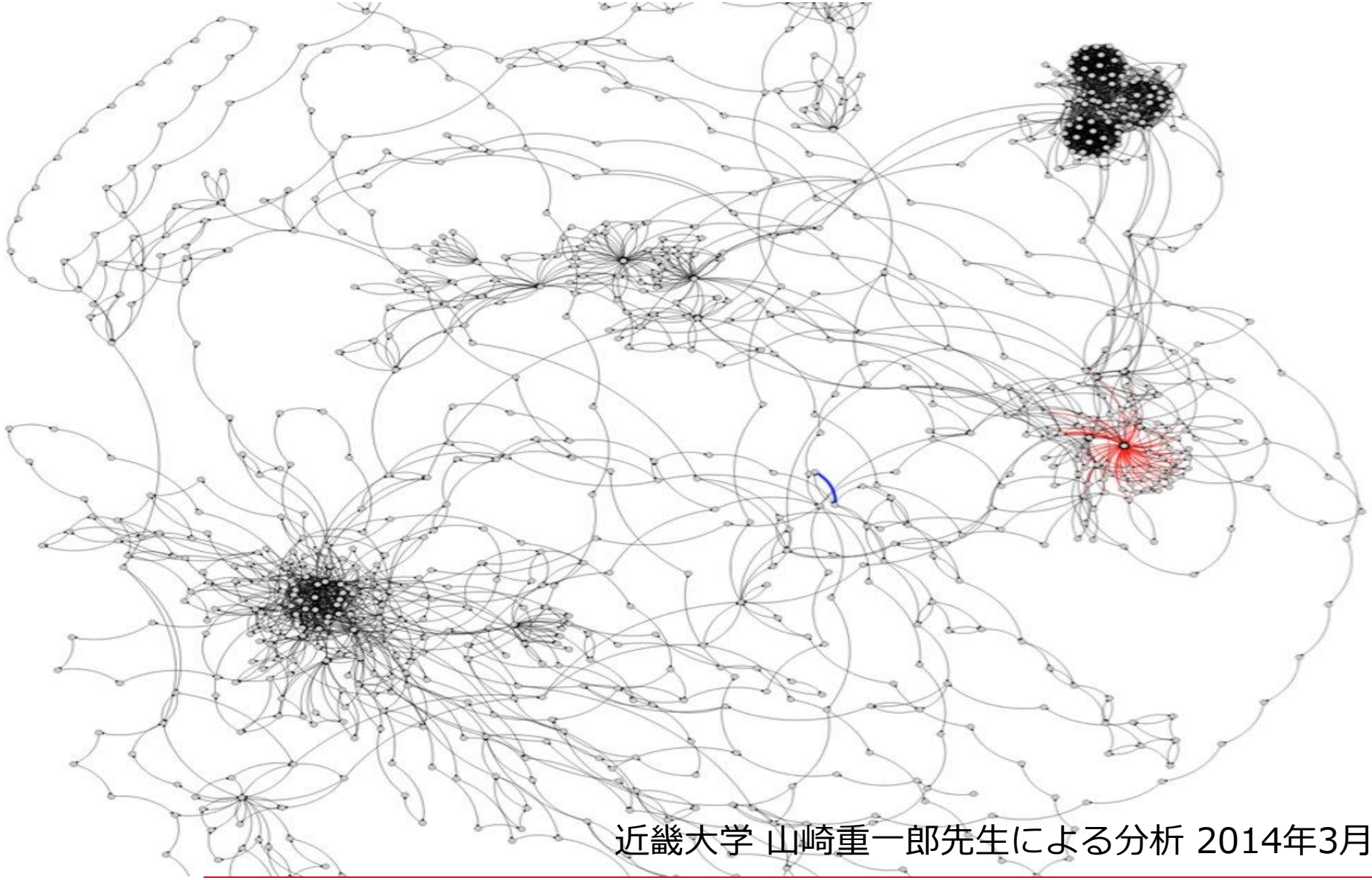


QLUE検索結果例　仮想通貨の取引金額、ウォレットの関連性をリアルタイム・可視化により検索・追跡

https://www.value-press.com/pressrelease/187645

MtGOXからのBitcoin流出とMixing Service (2014)

Japan Digital Design



近畿大学 山崎重一郎先生による分析 2014年3月

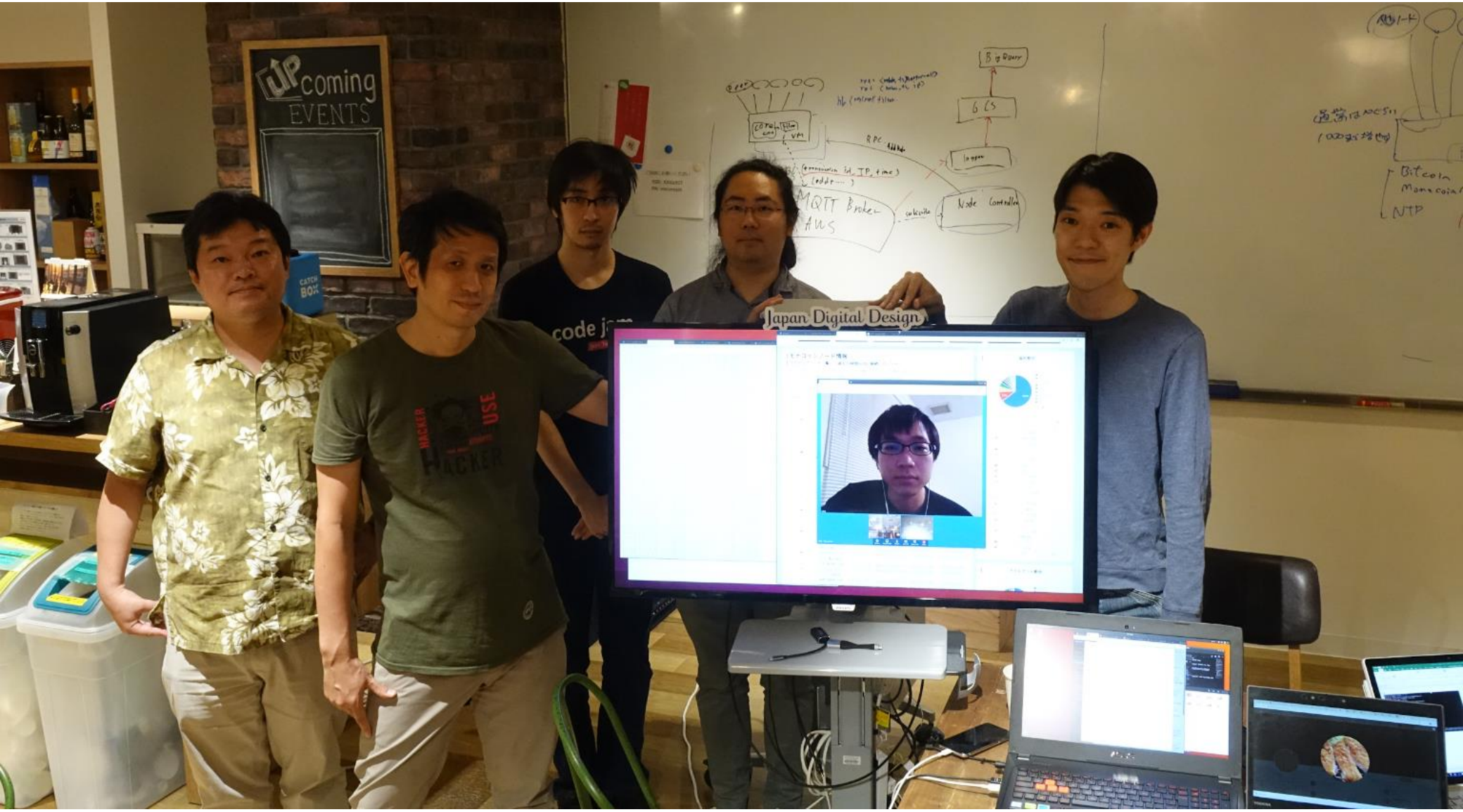
Zaif事件 2018年9月14日

- 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）

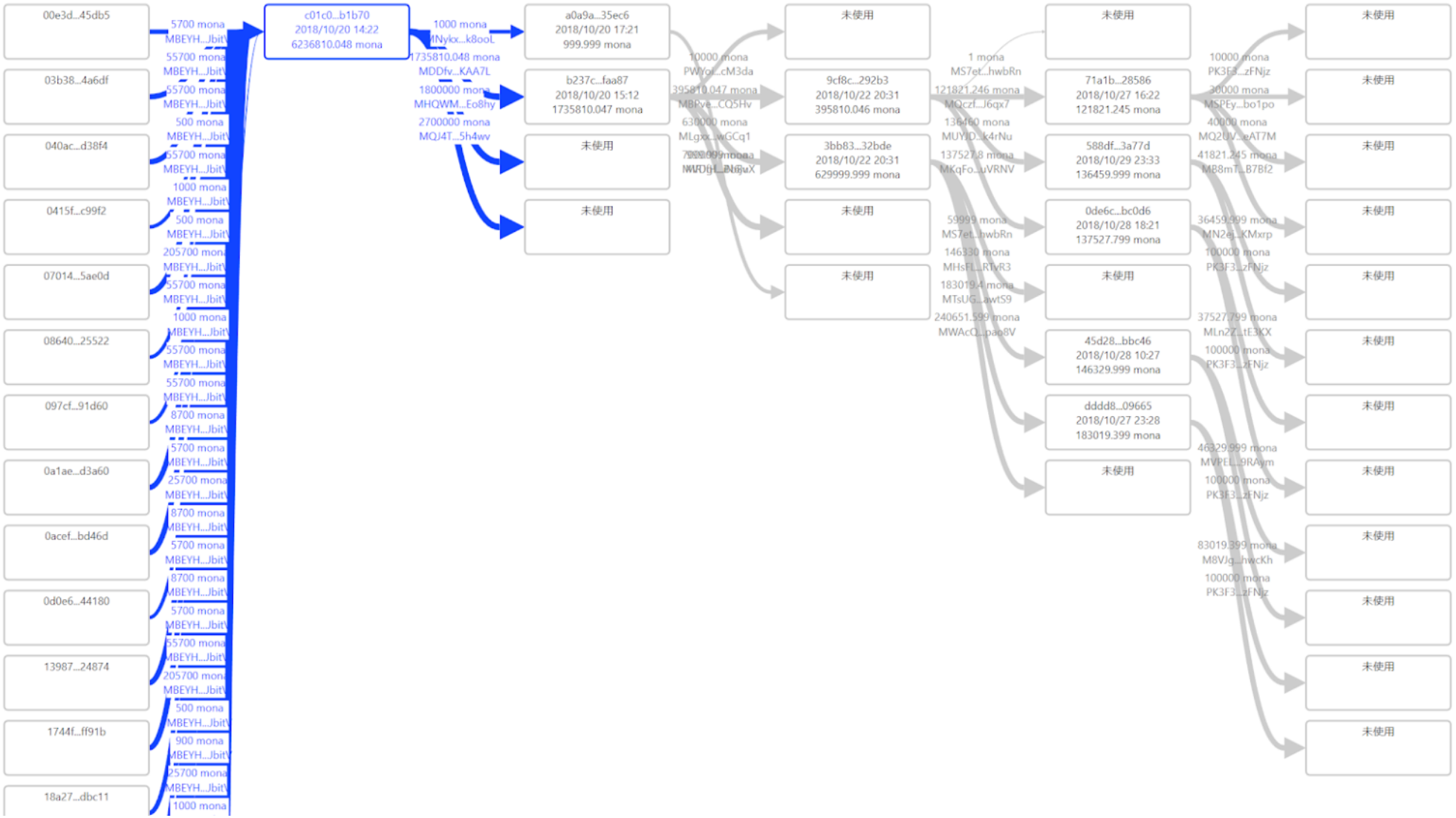
Monacoin追跡Hackathon on Sep. 23rd, 24th@JDD

Japan Digital Design



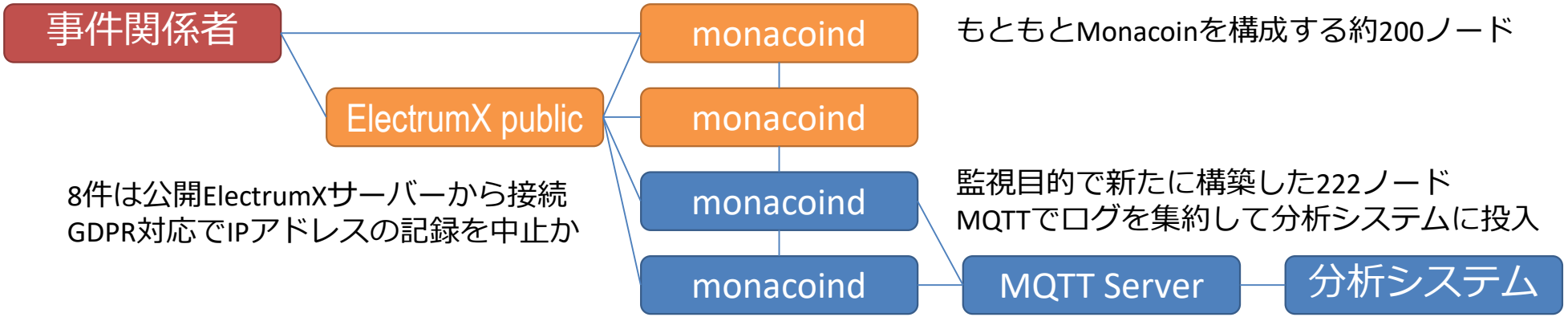
10月20日から動きはじめたMonacoin

Japan Digital Design

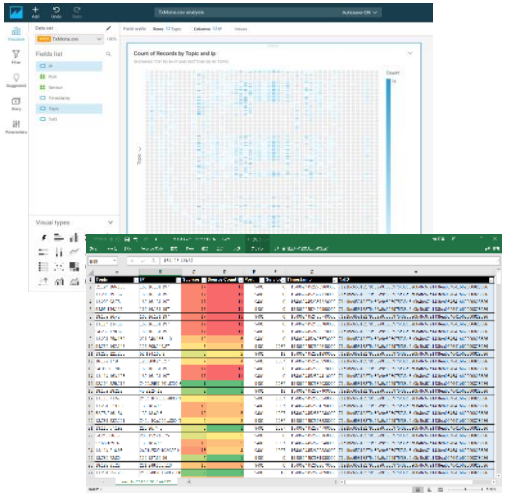


Zaifから流出したMonacoinの送金指示元の逆探知

Japan Digital Design



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

未来へ向けた投資と機会発掘とのバランス

Japan Digital Design