デジタライゼーションにおける 暗号資産とブロックチェーン

12月10日（月）

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, Inc. Chief Technology Officer

仮想通貨・Blockchainとのかかわり:

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

Japan Digital Design - 会社概要

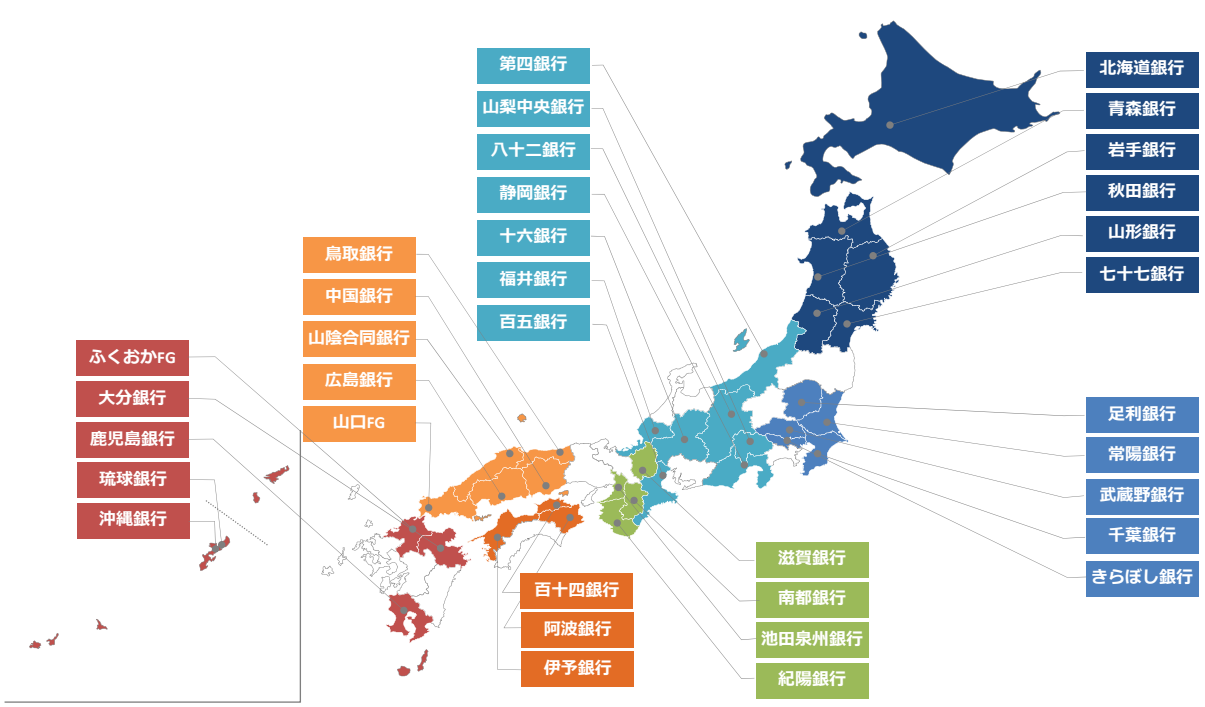
Japan Digital Design

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階
設立	2017年10月2日
代表取締役CEO	上原　高志
資本金	31億円（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 96.7% 三菱UFJリサーチ&コンサルティング株式会社3.2%
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

Japan Digital Design: 地域金融機関との連携

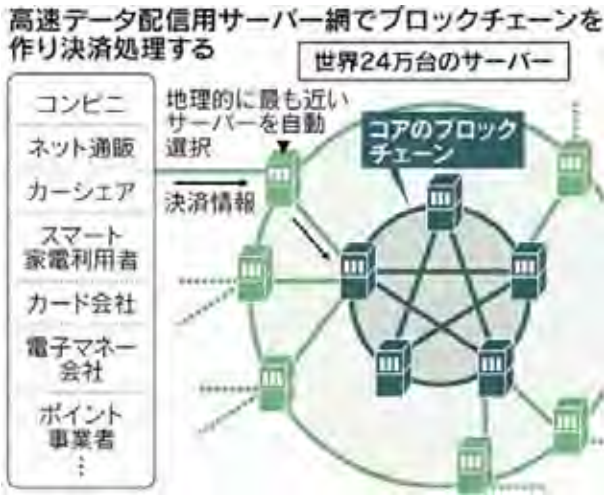
Japan Digital Design

全国の地域金融機関35行・グループと提携



MUFGの取り組み: 超高速ブロックチェーン

Japan Digital Design



Public Chain	Private Chain	既存決済
BTC 5 tps ETH 25 tps BCH 30 tps	Ripple 1.5K tps Fabric 2K tps NEM 4K tps **1M tps に目途**	全銀 800 tps Master 39K tps VISA 89K tps

ISO/TC307 Blockchain and Distributed Ledger echnologies

Japan Digital Design

2017年4月　シドニーで初会合

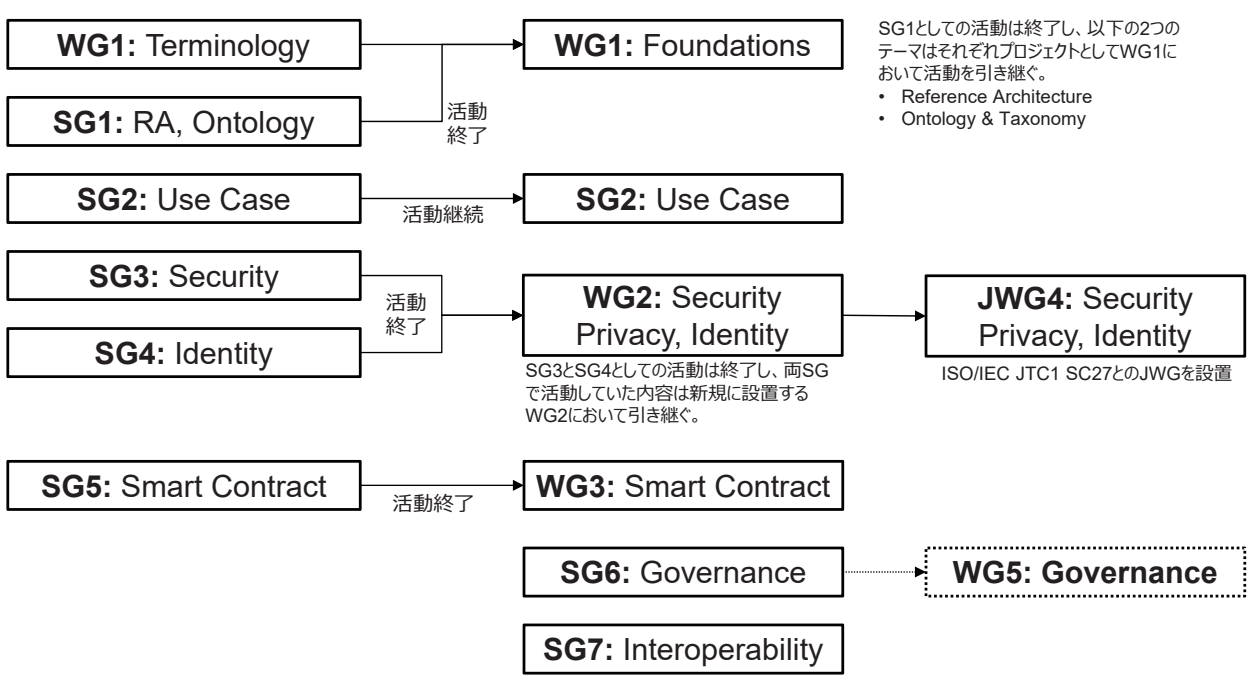
2017年11月　東京会議

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



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

交換業者・プラットフォーム	拠点	攻撃日	損失額（単位：100万ドル）
Coincheck	日本	Jan. 2018	$535
Mt. Gox	日本	Jan. 2014	$450
BitGrail	イタリア	Feb. 2018	$170
Bitfinex	香港	Aug. 2016	$77
NiceHash	スロベニア	Dec. 2017	$70
DAO	ドイツ	April 2016	$55
Coinrail	韓国	June 2018	$40
Youbit	韓国	April 2017	$35
Parity	英国	July 2017	$32
Bithumb	韓国	June 2018	$32
Bancor	イスラエル	July 2018	$24

Zaif Sep. 2018 $60M

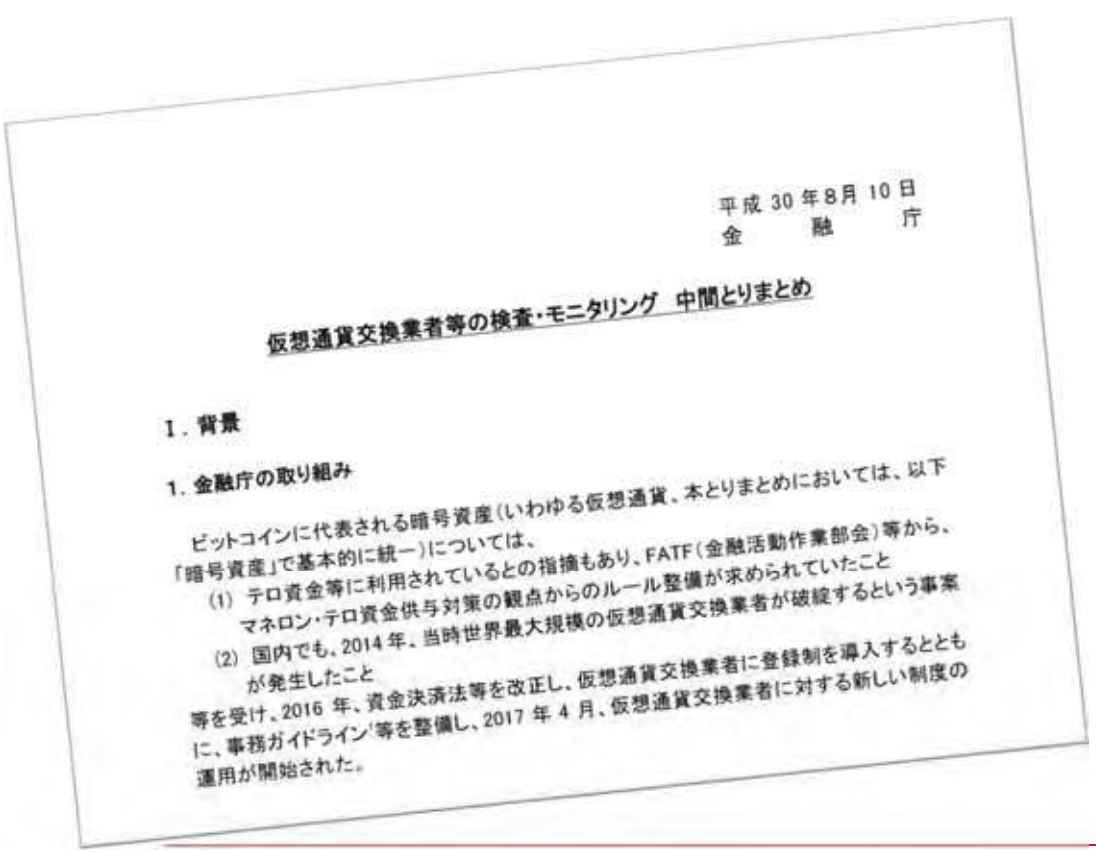
Note: DAO was created by German-based Slock.it.

Sources: Autonomous Research, staff reports

https://jp.wsj.com/articles/SB10366962949814344587904584351594067532808

仮想通貨か、暗号資産か

Japan Digital Design



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。

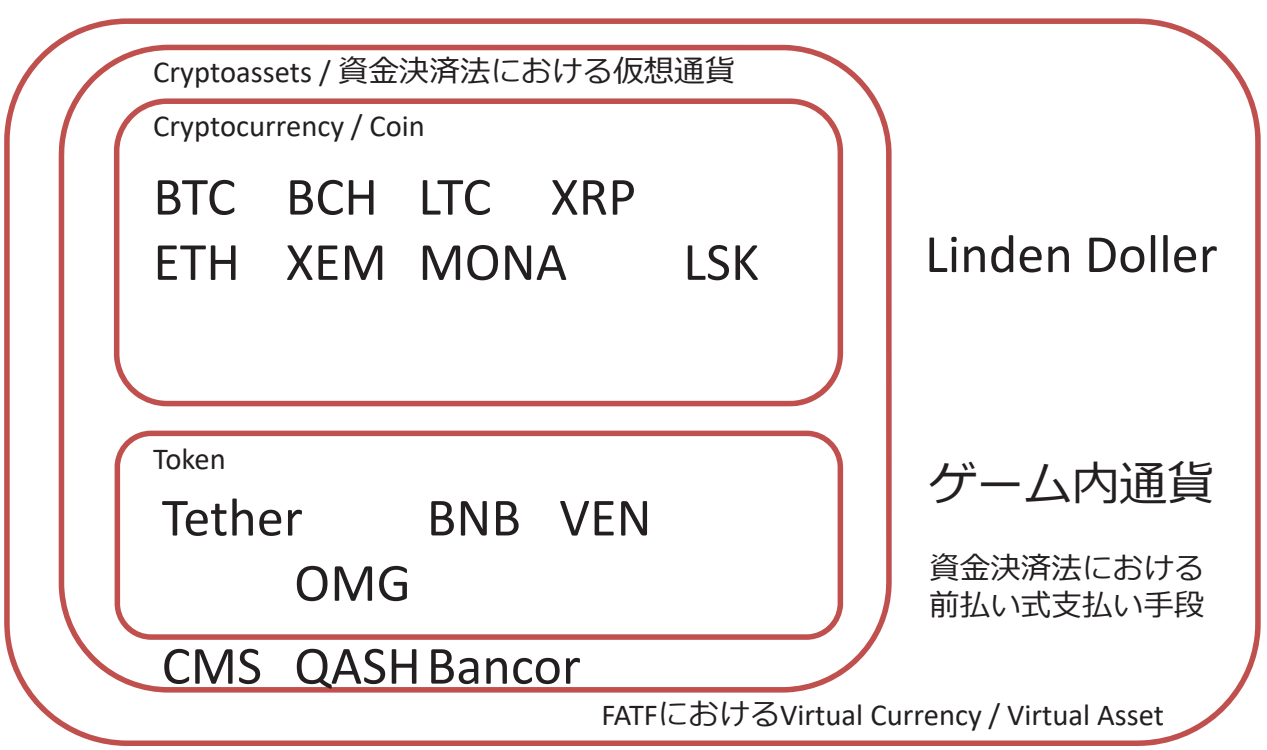
今後のBitcoin他に対する今後の呼称について

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

Japan Digital Design

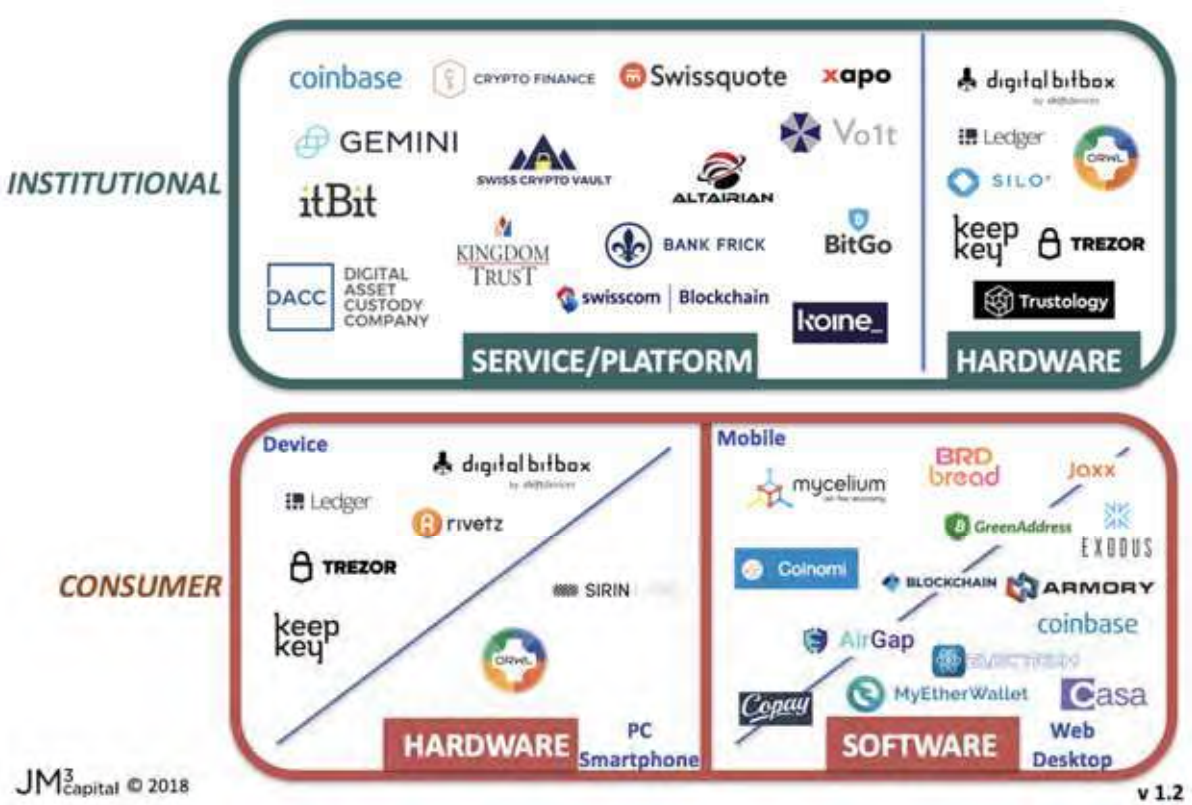
Given the urgent need for an effective global, risk-based response to the AML/CFT risks associated with virtual asset financial activities, the FATF has adopted changes to the FATF Recommendations and Glossary that clarify how the Recommendations apply in the case of financial activities involving virtual 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



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:

Direct line :

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

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

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

Internet DraftとISO/TC307 TRをゴール

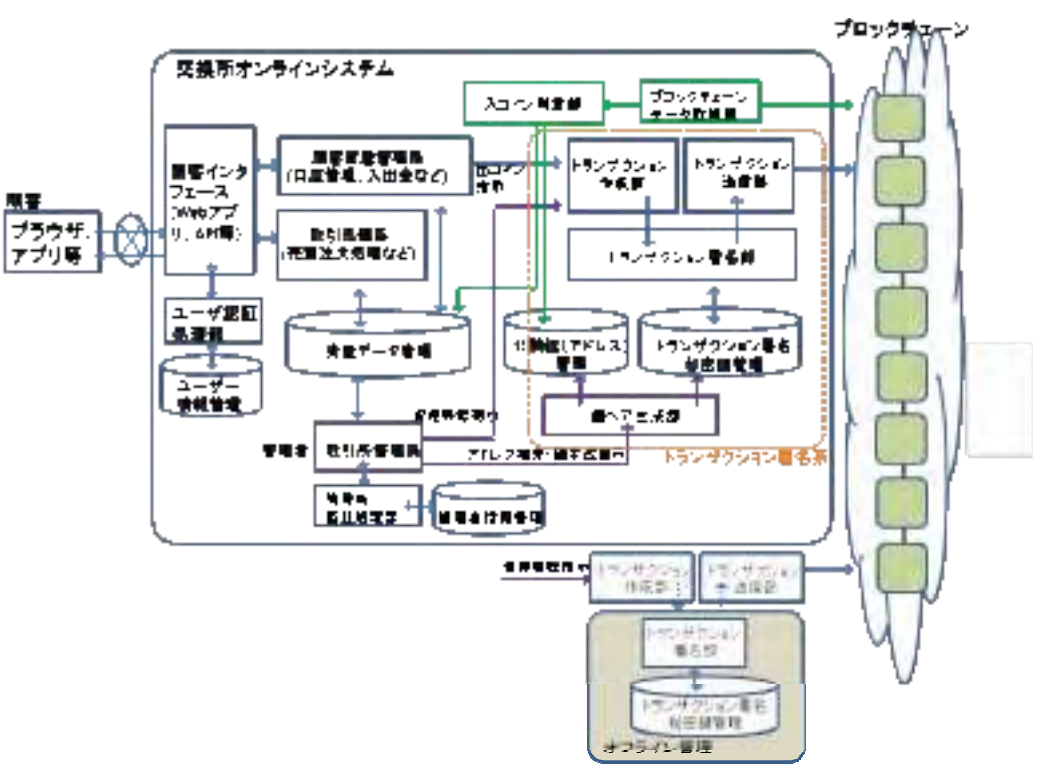
パブリックドラフトを公開

https://goo.gl/xyeYy9

管理会計WGも準備中

仮想通貨交換業者のリファレンスモデル（案）

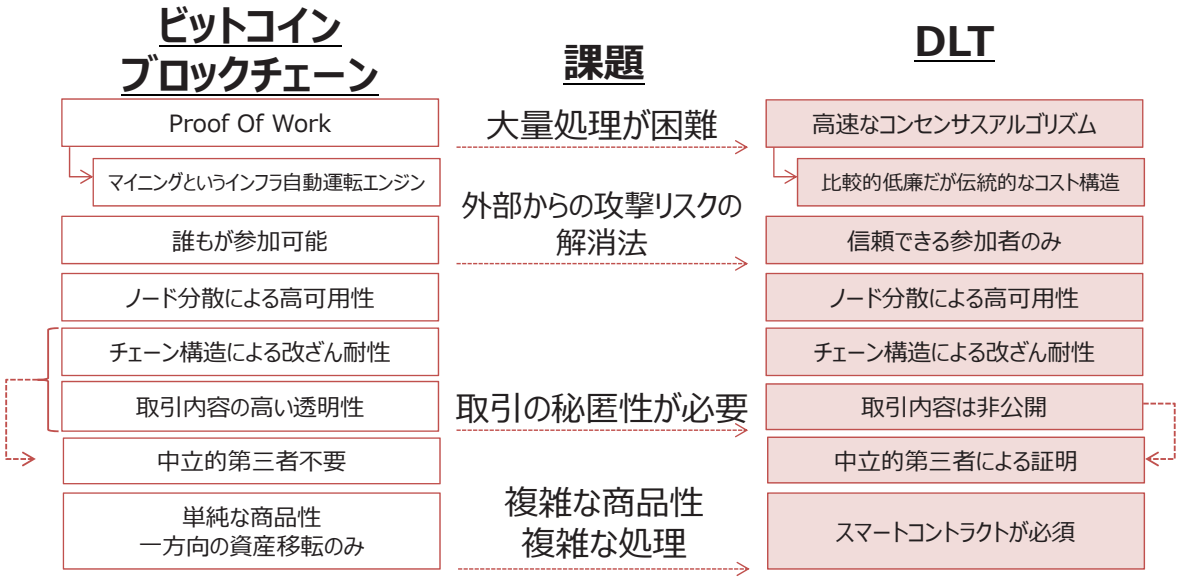
Japan Digital Design



金融業界におけるDLTのニーズと機能要件の違い

Japan Digital Design

- 金融市場への適用を考えた場合に幾つかの課題が存在しており、その技術的解決を目指した規格が多く提案されている(Fabric, Corda, Quorum等)
- コアインフラ適用は時間がかかるが、非効率性が存在している業務は有力な候補



出典：日本取引所グループ

現時点でBlockchainは何に使われているのか

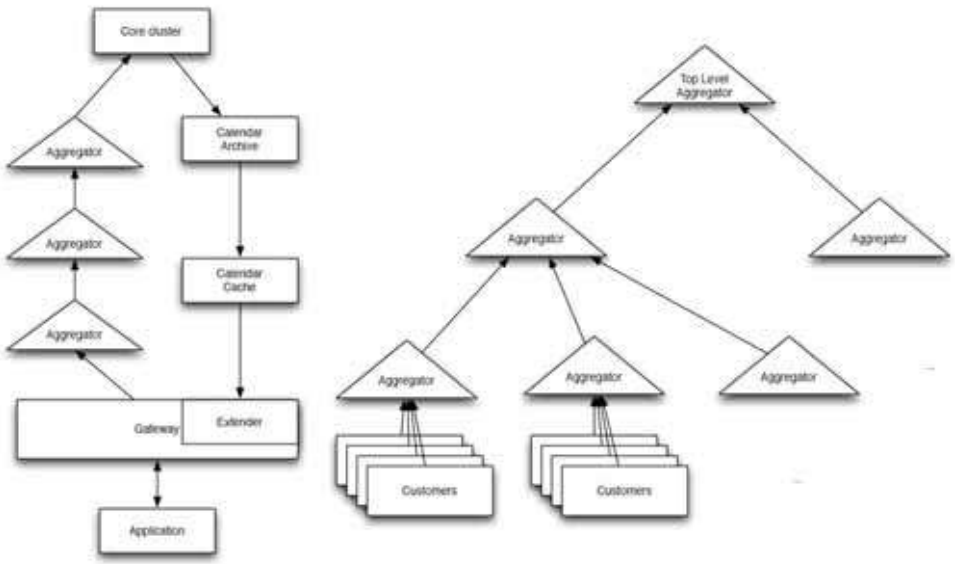
Japan Digital Design

段階	使途	メリット	課題
実用	仮想通貨 ICOトークン管理 ダークウェブ上の取引 DEX（分散型交換所）	法的責任の回避 匿名での越境取引 情報と価値移動の連動	速度・スケーラビリティ マネーロンダリング対策
PoC	地域通貨・ポイント 中央銀行デジタルマネー 国際貿易の信用状 サプライチェーン トレーサビリティ シェアリングエコノミー 分散ID・証明書・KYC/AML 公文書管理・証跡保存	ICOによる資金調達 運用・責任の分担 データの改竄が困難 レガシーフリー モダンな開発プロセス EoLのコントロールが可能	まだ実装が未熟 互換性に欠ける更新 技術的な自由度が低い エンジニア単価が高い 期待通り性能が出ない データの修正が困難 コードの修正が困難 商用サポートが限定的

エストニア政府でBlockchainは使われているのか

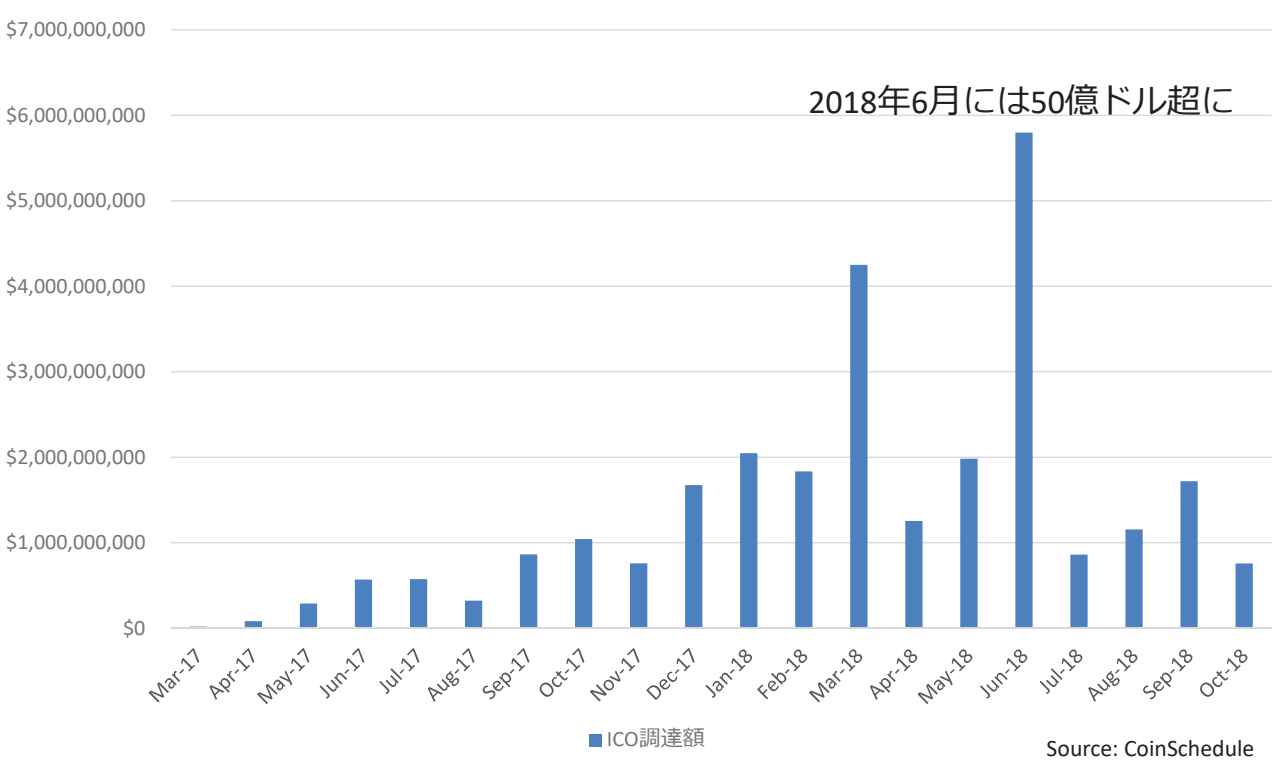
Japan Digital Design

- 実際に使われているのは実用段階にあるタイムスタンプ・キーレス署名技術
- 多数のデータ間の前後関係や整合性を管理する上でタイムスタンプの活用は有用
- マイナンバー制度の情報提供ネットワークシステムもログ保全にヒステリシス署名技術を利用



2018年に入って再び増したICOによる資金調達

Japan Digital Design



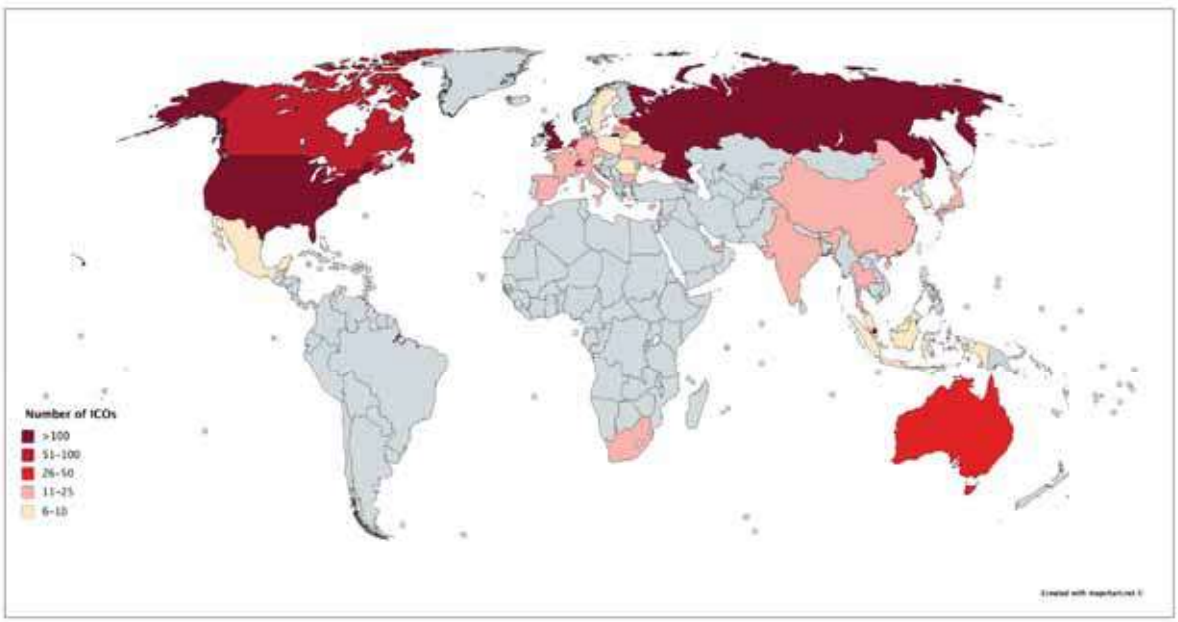
Source: CoinSchedule

ICOが活発に行われている地域

Japan Digital Design

Figure 1: World map of initial coin offerings

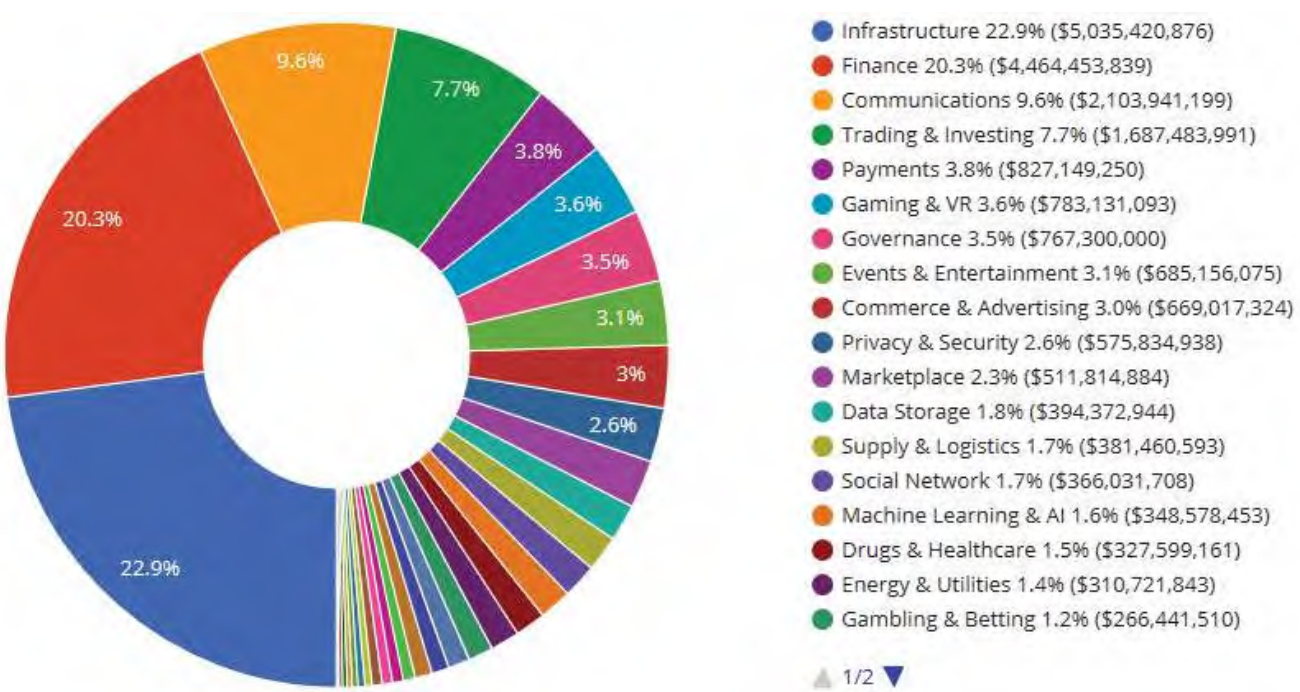
Figure 1 colors countries based on the number of ICOs that were completed in each country prior to April 30, 2018. Dark red indicates more than 100 ICOs, crimson indicates 51 to 100 ICOs, lighter red indicates 26 to 50 ICOs, pink indicates 11 to 25 ICOs, and yellow indicates 6-10 ICOs. All other countries had five or fewer ICOs.



Source: Digital Tulips? Returns to Investors in Initial Coin Offerings
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182169

2018年に行われたICOの投資対象分野

Japan Digital Design



Source: https://www.coinschedule.com/stats.html

2017年から2018年にかけてのICOの過熱

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

作者そのものが匿名だったBitcoin

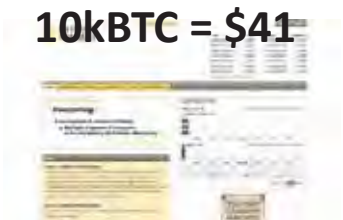
2008年11月 論文を**Cryptography ML**に投稿
2009年1月に運用開始、2010年ごろ活動を休止
2014年3月 I'm not Dorian Nakamoto"と書き込み

正体については**諸説濫立**

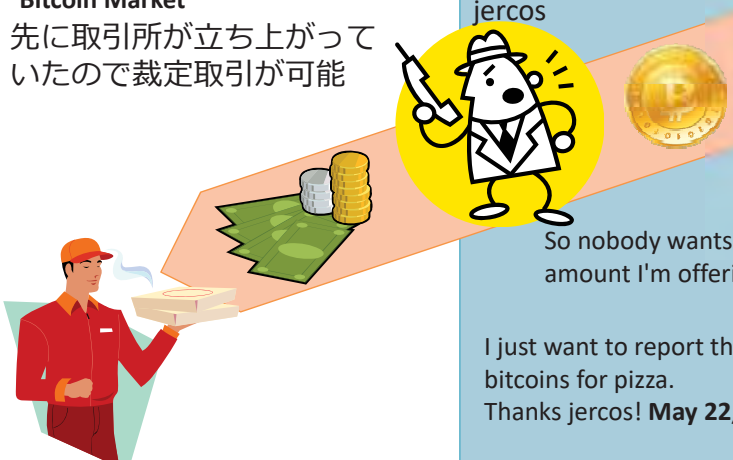
- Los近郊在住の**ドリアンナカモト**氏
- ドリアンの近所に住む**Hal Finney**
- **Michael Clear** – New Yorker
- 京大 **望月新一**教授 – Ted Nelson
- **US 20100042841 A1**の発明者
  - Updating and Distributing Encryption Keys
  - Neal King, Vladimir Oksman, and Charles Bry
- 名乗り出た**Craig Wright**

2010年5月 ビットコインで最初にモノの売買が成立

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

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

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