Bitcoin & Blockchain概況

2018.05 by SATO

「Bitcoin2.0概況」「Blockchain2.0概況」から改題

過去11回（＋臨時1回）にわたり、ビットコイン動向とブロックチェーン応用事例トピックを整理

- **第１回（2014年10月）：**2014年7月～9月の動き
- **第２回（2015年1月）：**2014年10月～12月の動き
- **第３回（2015年5月）：**2015年1月～4月の動き
- **臨時（2015年6月）：**金融分野のトピックに絞って
- **第４回（2015年8月）：**2015年5月～7月の動き
- **第５回（2015年11月）：**2015年8月～11月の動き
- **第６回（2016年4月）：**2015年12月～2016年4月の動き
- **第７回（2016年7月）：**2016年12月～2016年7月の動き
- **第８回（2016年12月）：**2016年8月～2016年11月の動き
- **第９回（2017年3月）：**2016年12月～2017年3月の動き
- **第１０回（2017年7月）：** 2017年4月～2017年7月の動き
- **第１１回（2017年10月）：**2017年8月～2017年10月の動き
- **第１２回（2018年2月）：**2017年11月～2018年1月の動き
- **第１３回（2018年5月）：**今回

TABLE OF CONTENTS

➔ 今回は、2018年2月～4月の動きを中心に整理

分野間が連携してきていることを踏まえて、構成を見直し

1. Bitcoinエコシステムの動向

- Lightning Network
- 署名集約とScriptless Scripts
- MASTからTaproot、Graftrootへ
- Confidential TransactionからBulletproofへ
- Sidechain
- プライバシー技術
- Bitcoin Cash
- その他トピック

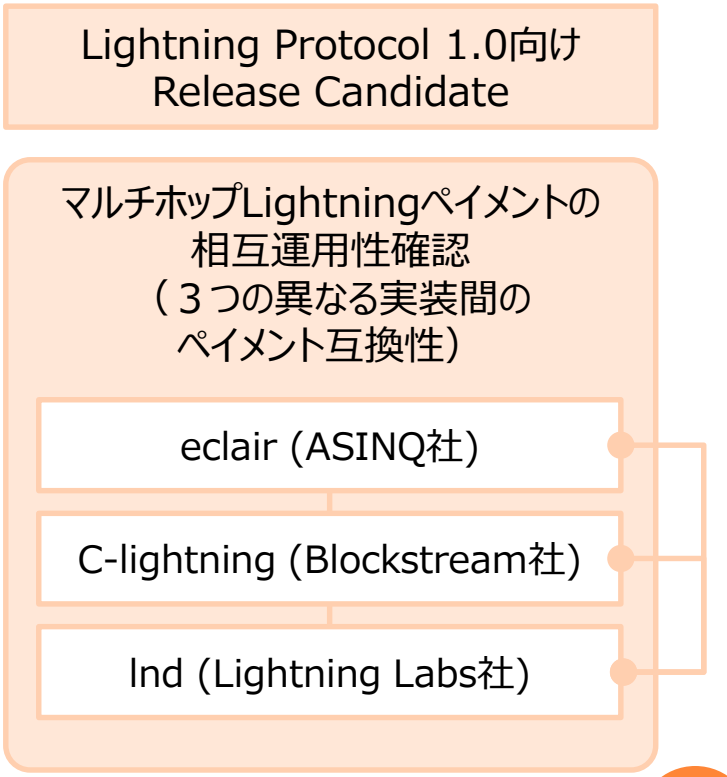
- Lightning Network
  - 概況
  - 前クールのおさらい
  - Lightning Labs、lnd0.4ベータ版をメインネットリリース
  - Lightning上でのアトミック・マルチパス・ペイメント（AMP）
  - Lightning Network関連コンテンツ

概況

- 2017年10月にはデスクトップウォレットアプリを提示した他、12月にはLightning Protocol 1.0をリリースしてプロトコル間の互換性が確保された。
- 2018年3月に、Lightning Labsから、lnd0.4ベータ版をメインネットリリースされた。
- これを受けて、Lightning Apps（LApps）開発進展が期待される。
- 今後の進化としては、Lightning上でのアトミック・マルチパス・ペイメント（AMP）の提案がなされている。これは例えば、2ドル分のペイメントチャネルを５本持っている場合に、６ドル分のペイメントをアトミックに行えるようにするようなもの。

前クールのトピックおさらい①

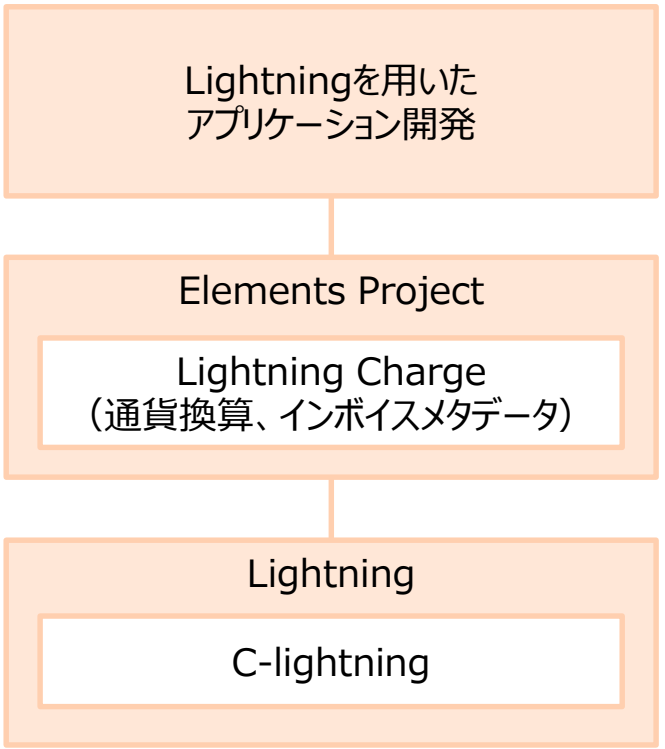
- Lightning、複数実装間のペイメントを試行
  - ３つの異なる実装間の互換性を含むLightning Protocol 1.0向けRelease Candidateをリリース。
  - ビットコインMainnet上でLightning ペイメントを行い、ASINQ（eclair）、Blockstream（c-lightning）、Lightning Labs（lnd）の３チームによりそれぞれ開発されてきたものについて、マルチホップLightningペイメントの相互運用性を確認。



→ 出典：https://medium.com/@lightning_network/lightning-protocol-1-0-compatibility-achieved-f9d22b7b19c4

前クールのトピックおさらい②

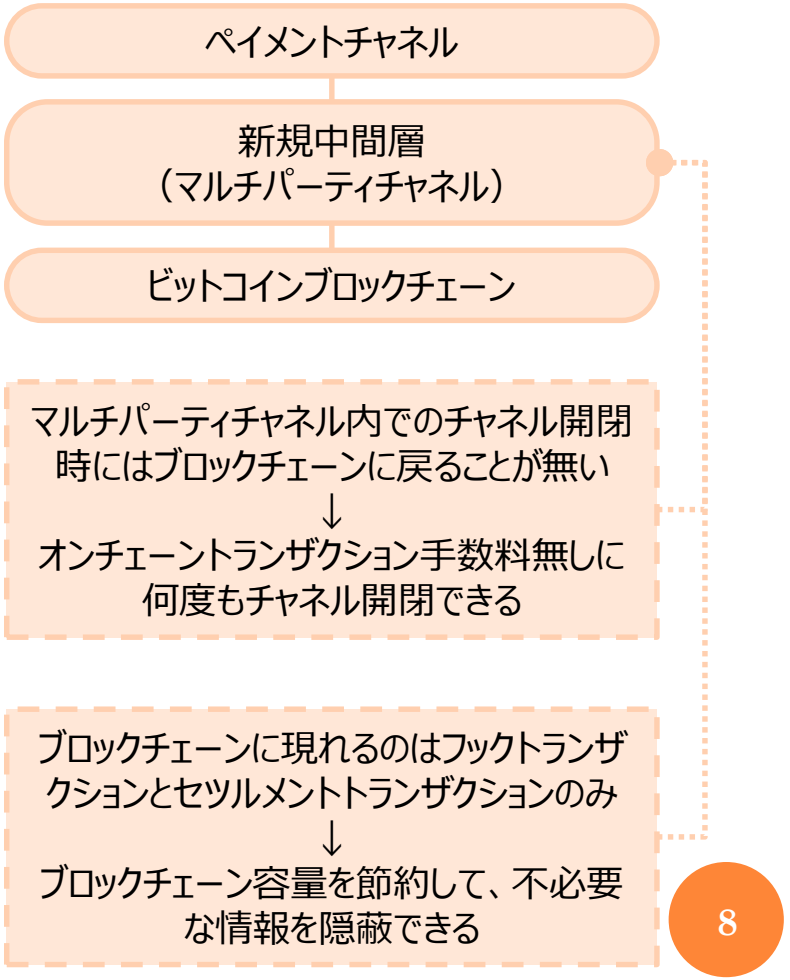
- c-lightning向け補完パッケージLightning Charge、Elements Projectへ導入
  - node.jsで書かれたマイクロペイメントプロセシングシステム。
  - Lightning Chargeは、Lightning上にアプリを構築しやすくすべく、Blockstreamと活動している個人開発者のNadav Ivgiにより設計された。
  - 通貨の換算や、インボイスメタデータなどの機能を利用可能で、c-lightningを用いてウェブペイメントインフラを独自に開発することを可能とする。



→ 出典：https://blockstream.com/2018/01/16/lightning-charge.html
→ 出典：https://github.com/ElementsProject/lightning-charge/blob/master/README.md

前クールのトピックおさらい③

- 参加者は仮想的に無数のチャネルを、追加のオンチェーントランザクション無しに開閉できるChannel Factory
  - Lightning Networkは、無数のチャネルをサポート出来ない他（今のLightningでは週あたり数百万のLightningトランザクションが限界）、チャネル開閉都度トランザクションをブロックチェーンに記録必要といった制約がある。
  - Channel Factoryは、ビットコインブロックチェーンとペイメントチャネルの中間層を作ることによってこうした制約を克服しようとするもの。
  - フックトランザクションを使ってコインをマルチパーティチャネルに送る。この中では15人までの参加者のうち2人が独立したチャネルを開設して、いったん閉じてマルチパーティチャネルに戻って改めて別の人とチャネルを開くことができる。



→ 出典：https://www.tik.ee.ethz.ch/file/a20a865ce40d40c8f942cf206a7cba96/Scalable_Funding_Of_Blockchain_Micropayment_Networks%20(1).pdf

Lightning Labs、lnd0.4ベータ版をメインネットリリース

- 4回目のメジャーリリースだが、メインネットベータ版としては初めてのもの。
- 主なハイライト
  - btcdに加えbitcoindをサポート
  - lndノードのバックアップやデータロスリカバリーを容易にする鍵生成・回復システム（新たなシードフォーマットおよび決定性鍵）
  - フォールトトレランス改善によるユーザ資金の安全性向上
  - Mission Controlと呼ばれるペイメントルート構築システムによる経路探索改善
  - コントラクト解消時のユーザ資金のウォレット返金プロセス自動化
  - SegwitおよびP2SHアドレスサポート
  - 手数料トラッキングツール提供
- ベータ版以降の方向性として挙がっているトピック
  - 無効トランザクションのモニタリングによりユーザ資金の安全性向上をはかるwatchtower
  - 大きなトランザクションを自動的に少額トランザクションに分割して決済するアトミック・マルチパス・ペイメント（AMP）
  - 一般ユーザにも利用可能性なLightning Apps
  - ルーティングノード運営者むけツール
  - クロスチェーンアトミックスワップ

→ 出典：https://blog.lightning.engineering/announcement/2018/03/15/lnd-beta.html
→ 出典：https://github.com/lightningnetwork/lnd/releases/tag/v0.4-beta

LIGHTNING上での アトミック・マルチパス・ペイメント（AMP）の提案 [1/3]

- 想定するケース
  - ２ドル分のペイメントチャネルを５本持っている。
  - ６ドル分のペイメントをアトミックに行いたい。
  - インボイスと合計がマッチするまでの間、全てのHTLCをPullするのを受け手が待てば可能に。

- 但し、いくつかの点で不都合がある
  - まず、受け手がペイメントハッシュを供給して、送り手が全てのストリームに対してペイメントハッシュを再利用することが考えられるが、このように複数のペイメントをまたいでペイメントハッシュを再利用すると、相互の関連付けが容易となる。
  - また、送り手が全てのペイメントフローを充たすことが出来ない場合でも、受け手はマネーをPull出来てしまう。

＜リスクは何か＞

- 複数ペイメントフロー横断でペイメントハッシュが再利用されることによる、関連付けられるリスク
- 送り手が全てのペイメントフローを充たすことが出来ない場合にも、受け手が支払を受け取ってしまうリスク

→ 出典：https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-February/000993.html
→ 出典：http://doublehash.me/atomic-multi-path-payments/

LIGHTNING上での アトミック・マルチパス・ペイメント（AMP）の提案 [2/3]

- そこで、Lightning上で以下 2 点を可能とすることにより、アトミックなマルチパス・ペイメントを実現する。
  - まず、ペイメントハッシュをペイメントフロー間で再利用しないこと。
    - コンセンサスレイヤーにより検証されるペイメントハッシュ（現像）はそれぞれのペイメント毎に区別される。
    - それにより、ペイメント間の関連付けを回避するほか、悪意を持つ仲介者がマネーを横取りできないようにする。
  - また、全てのペイメントフローが行き渡るまで、受け手は支払いを受けることが出来ないと保証すること。
- AMPにおいては、送り手と受け手の間のエンドツーエンドでネゴシエーションが行われるため、プロトコルに根本的変更を加えることなく、現バージョンのLightning上に機能追加するのみで実験可能な点がポイント。

リスク	複数ペイメントフロー横断でペイメントハッシュが再利用されることによる、関連付けられるリスク	対策	ペイメントハッシュをペイメント毎に区別し、再利用しない
リスク	送り手が全てのペイメントフローを充たすことが出来ない場合にも、受け手が支払を受け取ってしまうリスク	対策	全てのペイメントフローが行き渡るまで、受け手は支払を受けることがない保証

→ 出典：https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-February/000993.html
→ 出典：http://doublehash.me/atomic-multi-path-payments/

LIGHTNING上での アトミック・マルチパス・ペイメント（AMP）の提案 [3/3]

- AMPにより、ペイメントチャネルを異なるブロックチェーン横断でリンクできる。
  - ユーザーがビットコインを送り、ネットワーク上のノードが交換を望む限りは、他のユーザーはペイメントをライトコインとして受け取れる。
  - このペイメントを自分自身に対しても送ることができるので、ビットコインを送ってライトコインを受け取ることができる。
  - こうしてトラストレスな暗号通貨交換ネットワークを構築できる。

- 大きなペイメントを複数の小さなペイメントに分割し、それぞれをネットワークを通じて異なるルートを介して送付するもの。
  - このときペイメントの受け手はそれらペイメント全てを組み合わせた上で、あたかも一つのトランザクションかのように、それを受け入れたり拒否したりすることが出来る。
  - これらのプロセスを、ユーザーから見てバックグラウンド/自動で行われる点がポイント。
  - 大きなペイメントを小さくカットした上で、大きなペイメントの小さなパーツを受取人により償還することとし、秘密データがルート全体を通せない場合には、ペイメント全体をフェイルさせるようにしている点がポイント。

→ 出典：https://bitcoinmagazine.com/articles/future-bitcoin-what-lightning-could-look/
→ 出典：https://blog.lightning.engineering/posts/2018/05/02/lightning-ux.html

LIGHTNING NETWORK関連コンテンツ

- Lightning Networkに対する15の疑問に対するQA集
  - https://medium.com/@thecryptoconomy/dont-count-your-fud-before-the-lightning-strikes-15-claims-against-lightning-answered-9671d4a663a9
- 2nd layer
  - http://blog.nayuta.co/blockchain/2018/02/20/ln0172nd-layer/
- [LN#001] どこから読むか
  - http://blog.nayuta.co/blockchain/2017/11/24/ln001-どこから読むか/
- [LN#020]HTLC (1)
  - http://blog.nayuta.co/blockchain/2018/04/19/ln020htlc-1/
- Privacy in Lightning FAQ
  - https://snyke.net/post/privacy-in-lightning/
- ライトニングネットワークのビジネス展開 消費者向け少額直接広告
  - https://speakerdeck.com/takayaimai/raitoningunetutowakufalsebizinesuzhan-kai-xiao-fei-zhe-xiang-keshao-e-zhi-jie-guang-gao
- lnwalletウォレットアプリでのライトニングネットワーク受金方法
  - https://www.slideshare.net/mobile/takayaimai/lnwallet
- ライトニングネットワークの現在と未来
  - https://speakerdeck.com/takayaimai/24-1
- 2nd-layer技術（ライトニングネットワーク）
  - https://speakerdeck.com/takayaimai/24
- LNの強化：コントラクト違反時の防衛強化とSigned Sequence Commitment
  - http://techmedia-think.hatenablog.com/entry/2018/04/24/171943
- SF Cryptocurrency Devs Presents Building Bitcoin LApps with Lightning
  - https://youtu.be/zWOMyxO-YJI
  - https://youtu.be/4nKqV86i6mI

オフチェーンコントラクト向けアップデートメカニズム、ELTOO [1/2]

- 概略
  - 新しい状態について再交渉して、古い状態がオンチェーンでセツルメントされることの無いようにするオフチェーンアップデートメカニズムの提案。
  - 但しLightning Networkをリプレイスするものではないとのこと。
  - Lightning Networkのプロトコルフルスタックに係るものではなく、他スタックとの後方互換性を維持するためのアップデート機構だとしている。

- 通常のLightning
  - 新しいペイメントが作られる都度、ユーザー間のLightningチャネルは互いの残高を反映すべく更新される。このとき古い残高をブロードキャストするとペナルティとして、チャネル内の全資金を失う。ただし、古い残高をブロードキャストするのは必ずしも不正行為ではなく、ソフトウェアバグの可能性もあり、全資金喪失というペナルティは過大。

- Eltooにおける処理
  - そこで、タイムロックされたトランザクションのチェーンを構築することによってチャネルを更新することとし、各トランザクションは古いものから資金消費して最新チャネル残高を反映する。

→ 出典: https://blockstream.com/2018/04/30/eltoo-next-lightning.html
→ 出典: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-April/015908.html
→ 出典: https://www.mail-archive.com/bitcoin-dev@lists.linuxfoundation.org/

オフチェーンコントラクト向けアップデートメカニズム、ELTOO [1/2]

- 概略
  - 新しい状態について再交渉して、古い状態がオンチェーンでセツルメントされることの無いようにするオフチェーンアップデートメカニズムの提案。
  - 但しLightning Networkをリプレイスするものではないとのこと。
  - Lightning Networkのプロトコルフルスタックに係るものではなく、他スタックとの後方互換性を維持するためのアップデート機構だとしている。

- アップデートトランザクションとセツルメントトランザクション
  - eltooでは、状態を、アップデートトランザクションとセツルメントトランザクションという、二つのトランザクションセットで表す。
  - アップデートトランザクションは、コントラクトのアウトプットを消費して新しいアウトプットを生成するもの。
  - セツルメントトランザクションは、新しく生成されたアップデートアウトプットを消費して、合意した配分に従ってファンドを分割するもの。
  - アウトプットにはスクリプトがあり、新しいアップデートトランザクションに即座に紐付けられるか、若しくはタイムアウト後にセツルメントトランザクションに紐付けられる。
  - 参加者がタイムアウト前にアップデートに合意すれば、新しいアップデートトランザクションを生成して、以前のアウトプットを消費するとともに、対応するセツルメントを無効化する。

→ 出典：https://blockstream.com/2018/04/30/eltoo-next-lightning.html
→ 出典：https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-April/015908.html
→ 出典：https://www.mail-archive.com/bitcoin-dev@lists.linuxfoundation.org/

オフチェーンコントラクト向けアップデートメカニズム、ELTOO [2/2]

- SIGHASH_NOINPUTフラグ
  - eltooの肝は、中間アップデートのスキップ。
  - アップデートを短絡化（最終更新トランザクションをコントラクト生成と接続）すべく、署名にSIGHASH_NOINPUTフラグを導入することが実装上の要点である様子。
  - SIGHASH_NOINPUTフラグを導入することによって、トランザクションインプットは、マッチングスクリプトを持つトランザクションアウトプットと紐付くことが可能になると。
  - 前のアップデートトランザクションアウトプットのアウトプットスクリプトは、後のインプットスクリプトとマッチングするので、後のアップデートを前のアップデートと紐付けることができる。
  - eltooはこのようにして、SIGHASH_NOINPUTフラグ導入により中間アップデートをスキップできる。
- LN-penaltyの不要化
  - LN-penaltyと呼ばれるペナルティシステムがあるのに対し、eltooはオフチェーンコントラクトの合意された状態のみセツルメント。
  - eltooでは、無効な状態のためのハッシュ原像や、無効なHTLCは、そこに紐付くセツルメントトランザクションがブロックチェーンへコミットされることは無いため格納不用になるため、データ管理がシンプルになると。
  - 最新のアップデートトランザクションと、関連するセツルメントトランザクションと、セツルメントで消費されるHTLCのみを格納するだけで済むため、Lightning Networkにおけるデータ管理がシンプルに。
  - また、最新のアップデートトランザクションをセットアップアウトプットに紐付け、セツルメントトランザクションをブロードキャストする前に期限切れとすることによって、セツルメント自体もシンプル化されるとのこと。

→ 出典：https://blockstream.com/2018/04/30/eltoo-next-lightning.html
→ 出典：https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-April/015908.html
→ 出典：https://www.mail-archive.com/bitcoin-dev@lists.linuxfoundation.org/

WATCHTOWER

- 概略
  - Lighting Appsが用いるセキュリティシステムであり、インターネット接続が複数日にわたり切れてペイメントチャネルの一つが機能しないときの保護を提供するもの。
  - こうしたネットワークエラーが起きると、Watchtowerの一つが自動でリカバリープロセスを起動する。
- ブロックチェーンモニタリングをサードパーティにアウトソーシングするもの
  - ユーザーがチャネルを更新するときに、小さなデータパッケージをWatchtowerへ送る。
  - パッケージの最初のパートがトランザクションのヒントであり、パズルのピースとなるが、このヒントだけではトランザクションの中身は判明しない。
  - 関連するトランザクションがビットコインブロックチェーンに現れると、watchtowerはヒントを使ってそれを認識できるため、Watchtowerはブロックチェーン上のトランザクションデータを用いて、ペナルティトランザクションを再構成するために受け取ったパッケージの第二パートを使える。
  - このペナルティトランザクションはチャネル内の全資金を、それを生成したユーザーへ送るもの（eltooの場合は、正しいチャネル残高をブロードキャストするのみ）。
  - ペナルティトランザクションはwatchtowerが資金の一部を報酬として請求できるように設計されているため、ユーザーはチャネルモニタリングを複数のwatchtowerにアウトソースできる。

→ 出典：https://bitcoinmagazine.com/articles/future-bitcoin-what-lightning-could-look/
→ 出典：https://blog.lightning.engineering/posts/2018/05/02/lightning-ux.html

SPLICING

- 概略
  - オンチェーンでのビットコイン支払いを受け入れるもののまだLightningを使えないマーチャントへペイメントしたいときに使うもの。
  - チャネル自身を閉じることなく、チャネル外でオンチェーンペイメントを可能とする。
  - このとき、オンチェーンとオフチェーン（Lightning）トランザクション間のシームレスな移行ができる点が特徴。
- チャネルを開いたまま閉じる必要無しに、既存のLightningチャネルの上にファンドを積み増したり、ひきあげたりする事ができる
  - オンチェーントランザクションをLightning チャネル外で整列させることができる。
  - Lightningチャネルはトランザクション開設後、双方のユーザがチャネル内で資金移動することに同意すると、残りのLightningチャネルは、一連の後続トランザクションを構成し、それらはビットコインネットワークへブロードキャストされない。
  - Splicing inでは、オープニングトランザクションを取り出して代わりに資金を送りオープニングトランザクションをリプレイスする。このオープニングトランザクションがブロックチェーン上でconfirmされるとチャネルが積み増しされる。新しいオープニングトランザクションがconfirmされるまでは両ユーザーは新旧チャネルを同時に更新して、チャネルダウンを回避できる。
  - Splicing outでは逆に、ユーザーはオープニングトランザクションを取り出して、通常のオンチェーンアドレスへ資金送付し、その一部をチャネル内に保持可能。

→ 出典：https://bitcoinmagazine.com/articles/future-bitcoin-what-lightning-could-look/
→ 出典：https://blog.lightning.engineering/posts/2018/05/02/lightning-ux.html

- 署名集約とScriptless Scripts
  - 概況
  - 前クールのおさらい
  - Scriptless ScriptsをECDSAで行う提案

概況

- シュノア署名は、ビットコインで現在使われるECDSAの代替になりえるもの。
  - 計算が容易で安全性が高いことができるに加え、集約可能である点がポイント。
  - 加えて、MuSigと呼ばれる署名集約（複数のUTXOに付随する署名を単一署名へ集約する）への拡張が可能。
  - このように効率およびプライバシーの両面でのメリットが期待されている。

- シュノア署名により可能となるもう一つのトピックがScriptless Scripts。
  - 署名集約によって、Scriptless Scriptsといったスマートコントラクトをオフチェーンで行うものも将来的には可能になる。
  - シュノア署名を用いて、スクリプト言語の多くの機能を、スクリプト言語無しに実現するもの。

- これら以外にもシュノア署名検証により可能となるスクリプトとして、次で述べるMAST/Taproot,Graftrootがある。
  - このようにシュノア署名は応用可能性が大きく、ソフトフォークで実装可能だが、実現にはまだ数年かかる見込み。

前クールのトピックおさらい①

- シュノア署名により、複数の署名を単一の署名へと集約が可能
  - ビットコインの署名は、楕円曲線デジタル署名アルゴリズム（ECDSA）を用いているのに対して、別のデジタル署名形態（※ビットコインが用いる楕円曲線secp256k1とは互換）。
  - 計算が容易で安全性が高いことができるに加え、集約可能である点がポイント。
  - 一つの署名で複数のビットコインアドレスのインプットを証明（CoinJoinトランザクションを30-40%安価に済ますことが可能）。
  - ネイティブでマルチシグをサポートし、複数参加者が合同で単一署名を生成。これにより鍵の数や署名の数を低減。
  - 複数セットの鍵・メッセージを持つときに、一度に検証できる（バッチ検証）。
  - ソフトフォークで実装可能だが数年かかる見込み。

→ 出典：https://blockstream.com/2018/01/23/musig-key-aggregation-schnorr-signatures.html

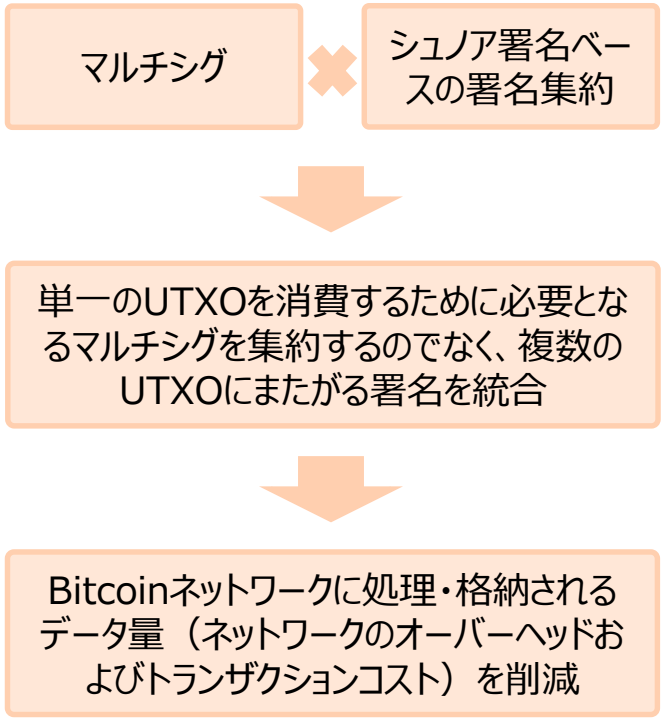
複数の署名を一つの署名へ集約
↓
トランザクションサイズ縮小の効果

関わる公開鍵インプットの判別を防止
↓
マルチシグのプライバシー向上効果

＜シュノア署名をベースとした拡張＞
- MuSigへの拡張
- Scriptless Scriptsといったスマートコントラクトも将来的には可能に
- MASTによるコントラクトのコンパクトな実現
- シュノア署名検証により可能となるスクリプト（Taproot）

前クールのトピックおさらい②

- MuSigは、シュノア署名をベースにしたマルチシグ実装
  - シュノア署名むけの効率的な署名集約スキーム。
  - 複数UTXOに付随する署名を単一署名へ集約。
  - ネイティブマルチシグをセットアップ無しに可能とするスキーム。
  - シンプルなマルチシグスキームに加えて、「カギ集約のサポート」および「プレーンな公開鍵モデルにおけるセキュリティ」という２つの特徴を、新たに組み合わせたもの。



  - コミュニケーションラウンド数に応じて、二つのバージョンがある（双方ともにおよそセキュア）。
  - 3ラウンドMuSig：ECDSAもベースとしている離散対数（DL）の仮定に基づくのみ。
  - 2ラウンドMuSig：少し強力なOMDL（One-More Discrete Logarithm）の仮定に基づく。

→ 出典: https://blockstream.com/2018/01/23/musig-key-aggregation-schnorr-signatures.html
→ 出典: https://cyber.stanford.edu/bpase18

前クールのトピックおさらい③

- Scriptless Scriptsは、シュノア署名を用いてスクリプト言語無しに、スマートコントラクトをオフチェーンで行うもの
  - 署名集約を通じてコンパクトにスマートコントラクトをエンコード出来る点がポイント。
  - スマートコントラクトのやりとりを通常のペイメントと区別なく、且つインプットも小さなものとして実現。
    - ネットワークレベルで検証・格納が必要となるデータ量を最小化することで、フルノードのオーバーヘッドを軽減できるほか、トランザクション手数料を低減できる。
  - コントラクト条件をネットワーク全体で検証せずに、参加者が検証する。
    - ブロックチェーン上に現れるのは鍵に対して支払う一つのトランザクションのみであり、両者以外はコインスワップが行われていることも知らず、チェーン上には公開鍵と署名のみのためコントラクト条件を関係する参加者以外に対して明かす必要が無くfungiblilityも向上できる。
    - ネットワークから見れば、参加者双方間のコントラクト条項を知る必要はなく、コントラクト条項が満たされたこと、および結果をもたらすトランザクションが有効であることを、参加者双方が同意したことを知る必要があるのみ。

スマートコントラクト

単一署名を必要とする標準的トランザクションの他タイムロックやマルチシグのような複雑なトランザクションが含まれる

Bitcoin Scriptを用いてオンチェーンで処理されるため、トランザクションコストやネットワークリソース、プライバシーが課題

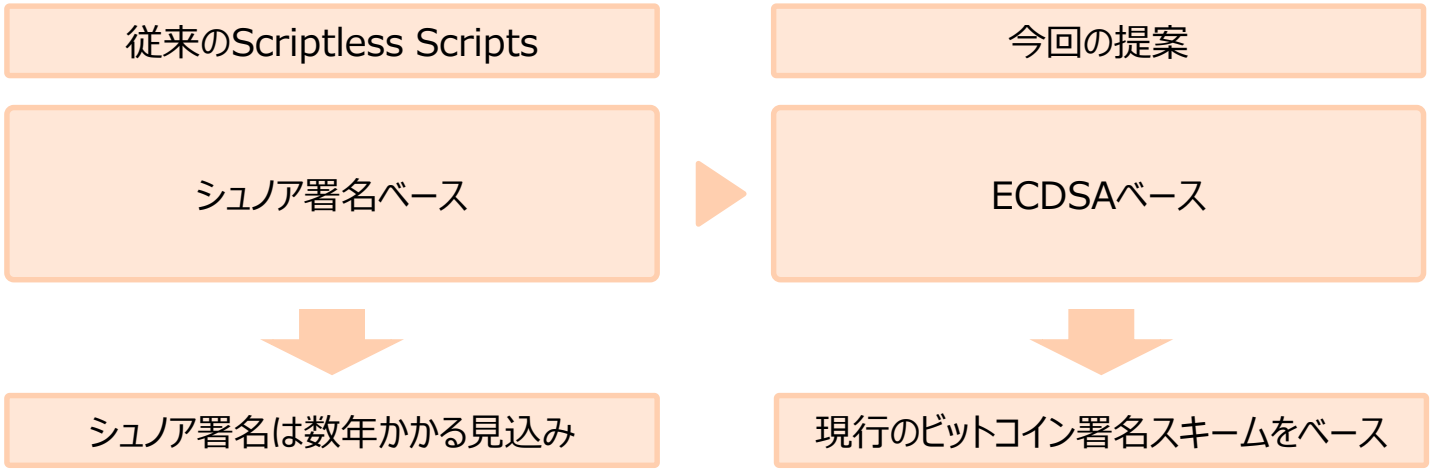
クロスチェーンアトミックスワップを行う場合、ハッシュのプリイメージを必要とし、それを明かすなどが必要。

＜Scriptless Script＞
・コントラクトの仕様・実行をオフチェーン化
・コントラクト条件は参加者のみが検証
・コントラクト実行を参加者が決定
・ネットワークレベルの格納データを最小化

→ 出典：https://medium.com/@Bitcom21/crypto-innovation-spotlight-2-scriptless-scripts-306c4eb6b3a8
→ 出典：https://bitcoinmagazine.com/articles/scriptless-scripts-how-bitcoin-can-support-smart-contracts-without-smart-contracts/

SCRIPTLESS SCRIPTSをECDSAで行う提案

- Lightning Networkで用いるアダプタ署名とコントラクトのScriptlessバージョンをECDSAにて行うというもの。
- シュノア署名を待たずにScriptless Scriptsを実現できる点が特徴。
- ECDSAベースのScriptless Scriptsが実現すると、Scriptless Lightning の様なものが可能となるかもとの見方も。



→ 出典: https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-April/001221.html
→ 出典: https://lists.linuxfoundation.org/pipermail/lightning-dev/attachments/20180426/fe978423/attachment-0001.pdf

- MASTからTaproot、Graftrootへ
  - 概況
  - 前クールのおさらい

概況

- MASTは、シュノア署名の集約特性を用いて、大きなコントラクトをコンパクトに実現するもの（スマートコントラクトの大部分をオフチェーンで処理することにより、効率性およびプライバシーを高めることが可能）。
- MASTでは、スクリプト構成を見ることにより、単純な１つの公開鍵への支払いではなく何らかのコントラクトへの支払いが含まれていることが判別可能という課題がある。
- そこで、Taprootは、アンロック条件がマルチシグ or その他のアンロック条件（ただし１つのみ）で構成されるロックスクリプトを、1つの公開鍵への支払いスクリプトに変換する。
- さらに、Graftrootでは、このアンロック条件の数を１つではなく複数持てるようにする（それら全てを列挙する必要もなく、またロック後に条件追加可能）事で、さらに柔軟なものとしようという提案。

→ 出典：https://btcnews.jp/banhwha215086/

前クールのトピックおさらい①

- MASTは、シュノア署名の集約特性を用いて、大きなコントラクトをコンパクトに実現するもの
  - ブロックチェーンにデータ追記時には、特定の使用でしか使われないスクリプトも含めて追加される。
  - 未使用の制約事項を記したデータはトランザクションサイズを増やす他、必要以上の情報開示でプライバシーを損ねたり、スマートコントラクトの使い勝手を損ねる。
  - スクリプトの未使用部分を含める必要性を無くすことが課題。
  - 制約事項を抽象構文木で分割した子スクリプトがそれぞれTrueを返し、マークルルートに繋がってマークル証明を提供することによって、トランザクション縮小・プライバシー向上できるのがポイント。

Merklized Abstract Syntax Tree

抽象構文木（AST） × マークル木

- プログラムを個別パーツに分割して分析や最適化しやすくする記法（AST）
- SPVウォレットで全ブロックをダウンロードせずにトランザクションが当該ブロックのメンバーだと検証可能（マークル木）

- 制約事項の記述を独立した二つの結果をもたらす子スクリプトに分割
- マークル木を用いてスクリプト全体無しに、制約事項を一意に識別

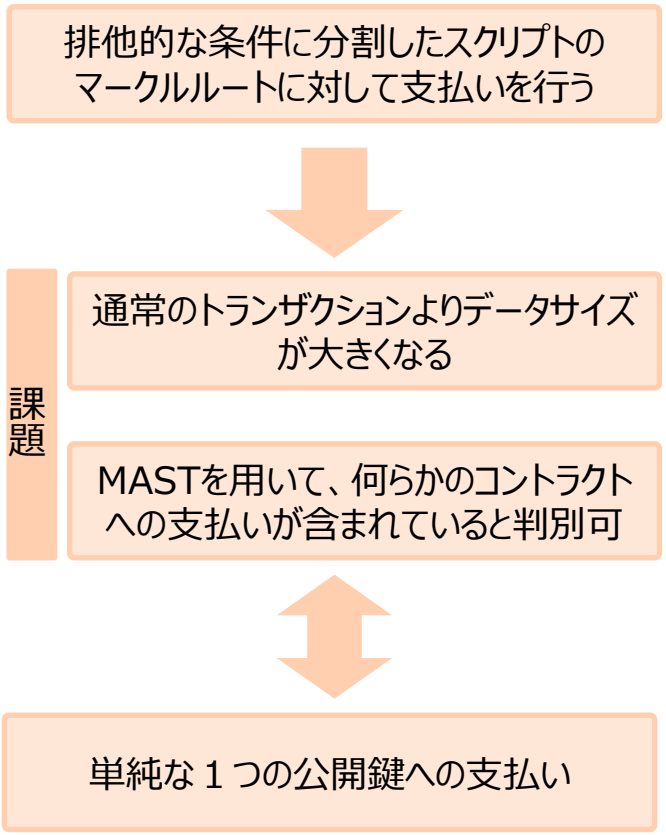
→ 出典：https://bitcointechtalk.com/what-is-a-bitcoin-merklized-abstract-syntax-tree-mast-33fdf2da5e2f
→ 出典：https://medium.com/@Bitcom21/crypto-innovation-spotlight-3-mast-e3eead7a2c6f
→ 出典：https://www.slideshare.net/knagato/20180410-blockchain-tokyo07

前クールのトピックおさらい②

- MASTには、通常のトランザクションよりデータサイズが大きくなる他、そのトランザクションでMASTを使っていることはわかってしまうため、プライバシー向上は課題

  - 利点
    - スクリプトの条件が複雑になっても、実際に実行した条件のみをブロックに取り込めばよい
    - ブロックに取り込むべきデータサイズを抑えられる
    - 大きなコントラクトを可能となる
    - ブロックに取り込まれなかったスクリプトを秘匿することができる

  - 課題
    - スクリプト構成を見ることにより、単純な１つの公開鍵への支払いではなく何らかのコントラクトへの支払いが含まれていることが判別できてしまう。



→ 出典: https://bitcointechtalk.com/what-is-a-bitcoin-merklized-abstract-syntax-tree-mast-33fdf2da5e2f
→ 出典: https://medium.com/@Bitcom21/crypto-innovation-spotlight-3-mast-e3eead7a2c6f
→ 出典: https://www.slideshare.net/knagato/20180410-blockchain-tokyo07

複数参加者間スクリプトのプライバシー向上を図るTAPROOT、GRAFTROOT

- Taprootは、アンロック条件がマルチシグ or その他のアンロック条件（ただし１つのみ）で構成されるロックスクリプトを、1つの公開鍵への支払いスクリプトに変換する。
  - MASTの条件を「シュノア署名ベースのマルチシグ or 例外処理スクリプト」というフォーマットに統一
  - 課題は、例外処理に単一のスクリプトしか指定できないほか、MASTと比較して記述柔軟性が劣る

- Graftrootは、このアンロック条件の数を１つではなく複数持てるようにする（それら全てを列挙する必要もなく、またロック後に条件追加可能）事で、さらに柔軟なものとしようという提案。
  - 例外処理を、集約鍵に対応する署名済みスクリプトでアンロック可能に
  - 例外処理スクリプトを増やしてもデータサイズ一定
  - 集約鍵による署名スクリプトをいくらでも増やせるため柔軟に条件記述可能

→ 出典：https://btcnews.jp/banhwha215086/
→ 出典：https://www.slideshare.net/knagato/20180410-blockchain-tokyo07

- Confidential TransactionからBulletproofへ
  - 概況
  - 前クールのおさらい
  - 範囲証明サイズを小さくおさめるBulletproof

概況

- Confidencial Transactionは、Pedersen Commitmentを用いてアウトプット量をリプレイスしつつ、トランザクションバランスをパブリックに検証可能とするもの。
  - トランザクションサイズは従来ビットコインのトランザクションサイズの16倍であったが、このほど３倍に縮小できると発表された。
  - 取引数量のプライバシーを向上できる一方、2400バイトのサイズとなり、この処理に14msを要するため、重たく遅いものとなる点（=コミットメントサイズの巨大さ）が短所。
  - 現時点、Elementsで可能となっているものの、ビットコイン本体への取り込みは時期未設定。

- これに対して、Bulletproofsは、Confidential Transactionと違い、トランザクション処理に要する計算パワーの大きな増加不要で軽量な点が特徴であり、トランザクション手数料の低減効果も期待できる。
  - Confidential Transactionの課題であるコミットメントサイズを小さくするものであり、これらをそれぞれ674バイト、4.2msへと縮小する、対数的な容量セーブを実現する。
  - ビットコインへの取り込みは、まだ未成熟なため時期未設定であるものの、Moneroではテストネットに取り込み済みであり、年内にメインネットリリース見込み。

前クールのトピックおさらい

- Confidential Transactionは、Pedersen Commitmentを用いてアウトプット量をリプレイス（トランザクション数量を隠蔽）しつつ、トランザクションバランスをパブリックに検証可能とするもの。
  - 取引数量のプライバシーを向上できる一方、2400バイトのサイズとなり、この処理に14msを要するため、重たく遅いものとなる点（=コミットメントサイズの巨大さ）が短所。
  - トランザクションサイズは従来ビットコインのトランザクションサイズの16倍であったが、このほど３倍に縮小できると発表された。
  - 現時点、Elementsで可能となっているが、ビットコインへの取り込みは時期未設定。

ビットコインのトランザクション数量

＜Confidential Transaction＞
- Pedersen Commitmentを用いてトランザクションアウトプット量をリプレイス
- トランザクションバランスをパブリックに検証可能
- 現在、Elements上でのみ利用可能

＜課題＞
- トランザクションサイズ（コミットメントサイズ）が巨大化
- トランザクション処理に長時間必要

→ 出典：https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-November/015283.html
→ 出典：https://www.reddit.com/r/Bitcoin/comments/7w72pq/bulletproofs_presentation_at_feb_2_milan_meetup/

範囲証明サイズを小さくおさめるBULLETPROOF

- Confidential Transactionで使われる範囲証明サイズ（nに線形比例）を改善。
  - サイズが小さくて且つtrusted setup不要な非対話ゼロ知識証明を提供して、所定のインターバル内に秘密のコミットされた値があることを証明。
  - 証明サイズがwitnessサイズの対数で済む短くて且つトラストされたセットアップ不要な、非対話式ゼロ知識証明。
  - 範囲のビット長nに対して2log(n)+9の群・体の要素のみを使うだけで済む（線形に大きくならず、対数的な伸びで済む点がメリット）。
  - 範囲証明の他、マークル証明や支払能力証明、或いはScriptless Scriptsへの利用も可能。

- トランザクション数量を隠蔽する際に、コミットされた値がある範囲内にあると示す範囲証明を小さなサイズで可能。

<効果>

- Confidential Transactionへの改善としてコミットメントサイズを小さくするものであり、これらをそれぞれ2400倍とから674バイトへと縮小する、対数的な容量セーブを実現。
- トランザクション処理に要する計算パワーの大きな増加不要であり、処理時間を14msから4.2msへ短縮。
- 証明はネットワーク全体を伝播して長期にわたり格納されるので小さなサイズの証明の方が低コストで済む。

→ 出典：https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-November/015283.html
→ 出典：https://www.reddit.com/r/Bitcoin/comments/7w72pq/bulletproofs_presentation_at_feb_2_milan_meetup/

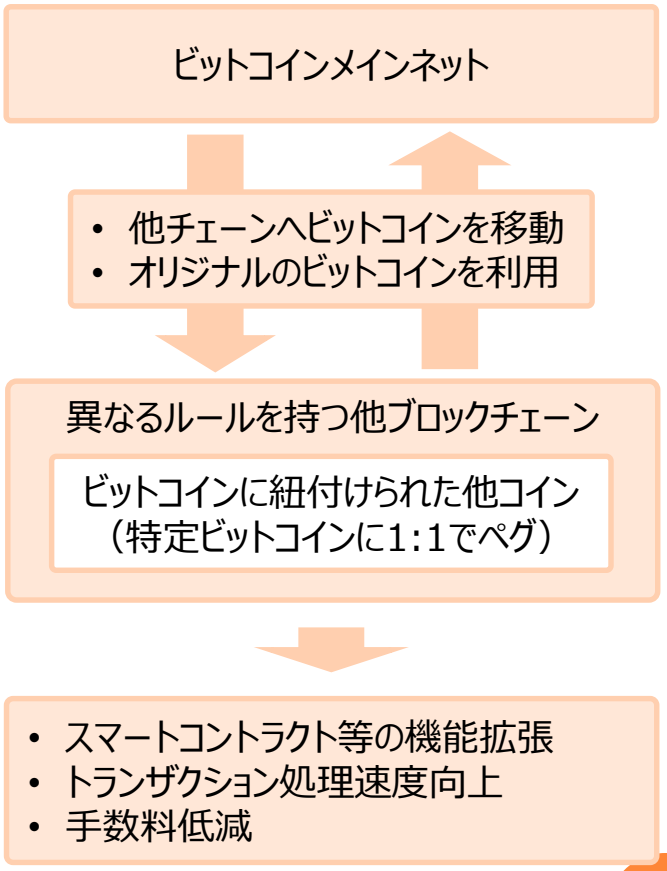
- Sidechain
  - 概況
  - 前クールのおさらい
  - Liquid、Release Candidate版を交換業者むけにローンチ

概況

- サイドチェーンとは
  - ビットコインに紐付けられた他コインを用いて、異なるルールを持つ他ブロックチェーンをビットコインメインネットへ接続するもの。
- Liquid
  - 取引所間で即時トランザクションを行うLiquidサイドチェーンがベータ版稼働済み。
  - 2018年には1.0版がリリース予定。
- RSK
  - チューリング完全のスマートコントラクトをサポートするため、Ethereumの柔軟性をビットコインに導入出来る。
  - 現在クローズドベータ版だか間もなくパブリックリリースとされる。
- Drivechain
  - LiquidやRSKがfederatedモデル（セミトラストされたゲートキーパーのグループにより安全確保されるサイドチェーン）であるのに対して、マイナーの投票により安全確保される点が特徴。
- Mimblewimble
  - トランザクションは完全にフンジブルであり、トランザクション数量および参加者の公開鍵を隠蔽。
  - ビットコインのサポートするスクリプトをサポートしないなど、ビットコインプロトコルとは全く別物のため、サイドチェーンまたはアルトコインとしての実装が想定されている。

前クールのトピックおさらい

- サイドチェーンは、ビットコインに紐付けられた他コインを用いて、異なるルールを持つ他ブロックチェーンをビットコインメインネットへ接続するもの。
  - 特定のビットコインに1:1でペグされた代替ブロックチェーンであり、異なるルールで動く他のチェーンへビットコインを移動でき、ビットコインプロトコル中のオリジナルのコインを使うことのみが可能となるもの。
  - ビットコインへのサイドチェーン導入によるメリットは、スマートコントラクト等の機能拡張およびトランザクション処理速度向上・手数料低減。



→ 出典: https://medium.com/@ianedws/roadmap-to-bitcoin-developments-f7af59b6d122
→ 出典: https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/
→ 出典: https://zoom-blc.com/sidechain

前クールのトピックおさらい

- 双方向ペグとは、ビットコインをビットコインブロックチェーンから別のブロックチェーンへ送ることに加えて、反対方向も可能とするもの。
  - 実際にはビットコインは「移動」するのでなく、ビットコインブロックチェーン上に一時的にロックされ、同量のトークンが別ブロックチェーン上でロック解除。更に、別ブロックチェーン上で同量トークンが再びロックされたときに、元のビットコインがロック解除。
  - この仕組みは、相手のブロックチェーンに決済ファイナリティがあることが前提条件のため、双方向ペグでは正直者の介在が必要。
  - 双方向ペグには、単一カストディアンによる双方向ペグ、マルチシグfederationによる双方向ペグ、そしてコンセンサスによるバリデーション利用がある。

単一カストディアンによる双方向ペグ

- 取引所などが「ロックされたビットコイン」「ロック解除された同等トークン」のカストディを務める。
- 課題は、取引所などにコントロールの集中性が残る点。

マルチシグfederationによる双方向ペグ

- マルチシグによる公証コントロールのグループを通じて、ロック解除。
- 公証認定を複数個所に分散し、単一カストディモデルより分散される。
- コントロールの集中性は残る。

コンセンサスによるバリデーション利用

- 各チェーンが相手のコンセンサスシステムを理解し、相手方チェーンにおいてロックトランザクションの証明（SPV-Proof）があればビットコインをリリースする。
  （→サードパーティー関与を減らす）
- 残る問題としては、パブリックチェーンにおいて決済ファイナリティが無く確率的である点（相手のチェーンで受け入れられたことに確証を持てない）など。

→ 出典：https://www.rsk.co/blog/sidechains-drivechains-and-rsk-2-way-peg-design

LIQUID、RELEASE CANDIDATE版を交換業者むけにローンチ

- Liquidは、取引所間で即時トランザクションを行う、アクセス可能なユーザーをコントロール可能な商用サイドチェーン。
  - 交換業者間のビットコイン移動を高速・安全・機密性高く行うもの。
  - ユーザー、ブロック署名者（マイナー同様）、観察者（ペギングプロセスによりチェーン間で安全に資金移転）という３つの参加者で構成するStrong Federationsコンセプトに基づく。
  - 2017年5月にベータ版がメインネットリリースされて試行中であり、2018年中に1.0版リリースを見込む。
  - 2018年3月にはRelease Candidate版を参加交換業者向けにローンチしている。

即時トランザクションおよびConfidential Transactionが可能

- Elementsを実装（Confidential Transactionを備えるSidechain）
- トランザクションファイナリティを二分以内で行う

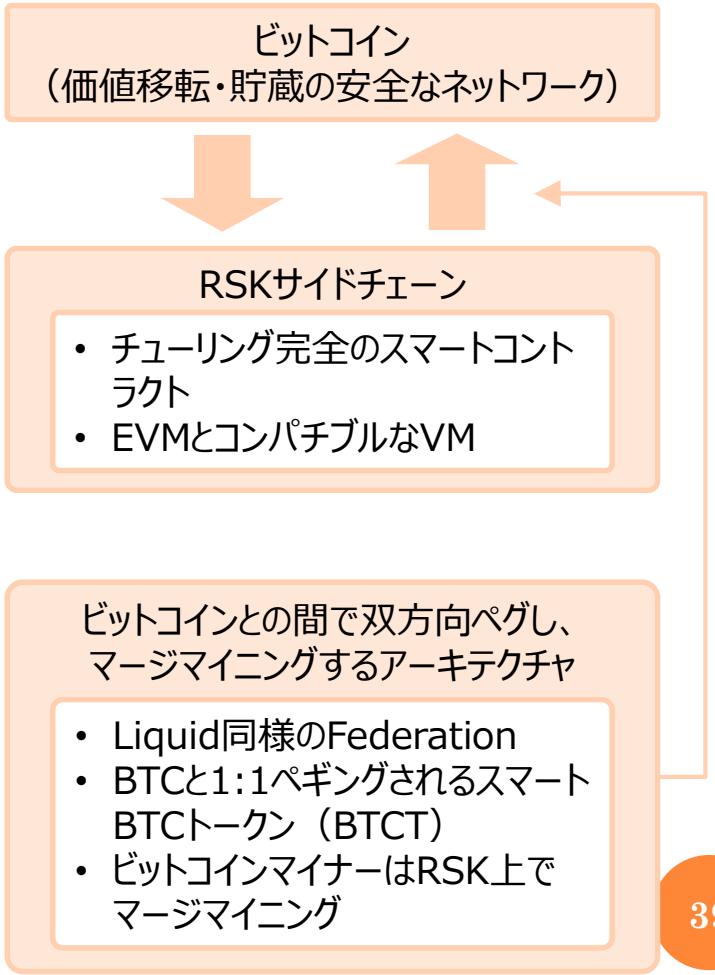
Release Candidate版(2018.3)に伴う主な機能拡張

- Liquidネットワークへペグインされるビットコイン管理にSegwitを用いて、トランザクションコスト削減。
- OP_CSVによるタイムロックを活用する事により、リカバリ手続きを簡素化。

→ 出典: https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/
→ 出典: https://medium.com/@ianedws/roadmap-to-bitcoin-developments-f7af59b6d122

前クールのトピックおさらい

- RSKサイドチェーンは、チューリング完全のスマートコントラクトをサポートするため、Ethereumの柔軟性をビットコインに導入。
  - RSKスマートコントラクトはSolidityでプログラミングされ、VMはEVMとコンパチブル。
  - Liquid同様にFederationシステムを利用。
    - BTCリリースがリクエストされると、BTCトランザクション候補がブリッジコントラクト運営に生成される。
    - 充分なRSKブロックが採掘され、RSK上でのconfirmationが充分行われるとFederatorにより署名。
    - 充分なFederationメンバーにより署名されると、Federatorによってトランザクションが BTCブロックチェーンネットワークへブロードキャストされる。
  - BTCと1:1ペギングされるスマートBTCトークンを利用。
  - ビットコインマイナーはRSK上でマージマイニング。
    - RSKのサイドチェーンを安全なものとするため、双方のブロックチェーンが同時にマイニングされる。
    - RSK上で動く全てのスマートコントラクトからフィーを受け取ることで、ビットコインマイナーが収益を増やせる。



→ 出典: https://medium.com/@ianedws/roadmap-to-bitcoin-developments-f7af59b6d122
→ 出典: https://news.bitcoin.com/bitcoin-ethereum-smart-contract-sidechain-rsk-launches/
→ 出典: http://www.rsk.co/

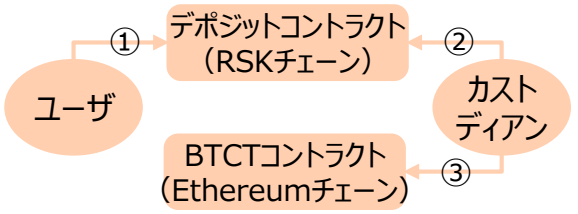
前クールのトピックおさらい

- RSKでは、カストディアンがRSKネットワーク～ビットコインメインネット間のビットコイン移動をトラッキングする仕掛けになっている。
  - カストディアンはEthereumチェーンにETH/ERC20でセキュリティデポジット。
  - この他、安全マージンをBTCの5%分RSKチェーンに置き、RSKチェーン上の不正ペナルティとする。
  - 右図のようにして、BTCをEthereumネットワークへ持っていこうとするのが、レイヤー1のスマートコントラクトによるアプローチ。
  - 一方で後述のCosmosなどは、レイヤー2としてアプローチするもの。

→ 出典：https://blog.kyber.network/bringing-bitcoin-to-ethereum-7bf29db88b9a

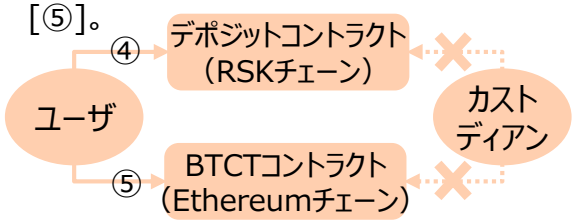
BTCトークン発行（BTC預入）

- ユーザーがRSKチェーン上のデポジットコントラクトへBTCをデポジットすると[①]、カストディアンがメッセージ（BTCがEthereum上にデポジットされた旨）に署名し、デポジットコントラクトへ提示[②]。
- カストディアンは併せてEthereum上のBTCTコントラクトに同額BTCTを発行[③]。



BTCトークン発行時のペナルティ

- カストディアンが署名しなければユーザーはRSKチェーン上で問いただしRSKチェーンへデポジットしたBTCを、カストディアンの不正ペナルティデポジットと併せて返金できる[④]。
- カストディアンが署名後にBTCT発行出来なければ、自ら署名メッセージ使いBTCT発行[⑤]。



前クールのトピックおさらい

- Drivechainは、マイナー投票により安全確保するサイドチェーン。
  - Drivechainの変更は「ハッシュレートエスクロー」「ブラインドマージマイニング」に二分される。
  - RSK同様、マージマイニングを用いてビットコインマイナーにより安全性を保つ仕組み。
    - Blind Merged Miningを開発中。
  - LiquidやRSKがfederatedモデル（セミトラストされたゲートキーパーのグループにより安全確保されるサイドチェーン）であるのに対して、drivechainはマイナーの投票により安全確保される点が特徴。
    - 監査人のFederationに依らずにSPV-Proofにマイナー投票を導入するモデル。
    - ロックされたビットコインのカストディをビットコインのマイナーに付与するものであり、マイナーに「いつロック解除するか」「それらをどこへ送るか」について投票させる。

ブラインド・マージマイニング

- マイナーに負荷を与えず、且つビットコインのプラグインとしてビットコインで報酬を与えたい。
- マイナーがサイドチェーンのフルノード運営者に報酬を与えることにより、マイナーとサイドチェーンフルノードを独立運営する動機に。

マイナー投票による安全確保

- 複数の監査人が橋渡しとしてチェーン間のやりとりを行うFederationモデルでは、結託リスク・トラスト必要性あり。
- マイナーを信頼できるブロックチェーン間の監査人として、マイナーの投票によりチェーン間のアセットやりとりを行う。

→ 出典：https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/
→ 出典：https://medium.com/@ianedws/roadmap-to-bitcoin-developments-f7af59b6d122
→ 出典：https://www.rsk.co/blog/sidechains-drivechains-and-rsk-2-way-peg-design
→ 出典：https://zoom-blc.com/drivechain

- プライバシー技術
  - 各種プライバシー技術の俯瞰・比較

各種プライバシー技術の俯瞰・比較

- 各種プライバシー技術について、アドレスリンク遮断、トランザクション数量機密化、ミキサー要否、Proofサイズ、トラストされたセットアップ要否などに着目して俯瞰。

タンブラー（攪拌）	CoinJoin	• グループ参加者が同数のコインをポットに入れて混ぜた上で同数のコインを戻すもの。 • 特定コンセンサスルール無しに多くの暗号通貨で機能し、比較的実装がシンプルで軽量 • 但し、ミキサーがオンラインであり且つミキサーがコインを盗まない/識別情報をロギングしないというトラストが必要なほか、匿名性が混合相手の数量により制約受ける点が課題。
	CoinShuffle++	• トラストされた第三者は不用となったものの、匿名性の制約やオンラインの必要性といった課題は残る。
	TumbleBit	• コインミキシングプロトコルであり、タンブラーを用いて単一のミキシングセッション中に全参加者から全参加者へのペイメントチャネルを作成して、皆が当初と異なるコインを、所有権の追跡無しに受け取ることが可能。タンブラーがユーザー同士をリンクできない。 • ミキシング用のファンドを利用可能にしておく必要があるといった課題が残る。
	ZeroLink	• TumbleBitと異なり中央サーバを用いて、トランザクションをリンク不可能な形でユーザーをリンクするもの。 • 単一のCoinJoinトランザクションを生成するため安価で済む。
Ring署名		• グループからのトランザクションを誰かを明かすことなく誰かが署名したことを証明できるもの。
	CryptoNote	• 似たようなアウトプット用いてRing署名トランザクションのインプットを形成する。 • ミキシングが自動で行われるためミキサー不用で、outputが新たなミキシングのinputになるため次第に匿名性が高まる。 • RingCTを実装するが、トランザクションサイズが大きくスケーラビリティが課題。
	RingCT	• Ring秘匿トランザクションとして、トランザクション数量も隠蔽可能。

→ 出典：https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/
→ 出典：https://zcoin.io/zcoins-privacy-technology-compares-competition/

各種プライバシー技術の俯瞰・比較

- 各種プライバシー技術について、アドレスリンク遮断、トランザクション数量機密化、ミキサー要否、Proofサイズ、トラストされたセットアップ要否などに着目して俯瞰。

ゼロ知識	Zerocoin/ Zcoin	• ミキサー不用なほか、上述したように他トランザクションを用いて不明瞭化するのではなく、ゼロ知識証明を用いてアドレス間のトランザクションリンクを完全遮断しながら監査可能性は保持する点がポイント。 • 具体的には、元のコインをburnして同等数量の新たなコインを元のトランザクション履歴を持たない形で生成するにあたり、元のコインをburnした証明としてゼロ知識証明を利用しており、参加者数やリングサイズに匿名性が制約受けない点が特徴とのこと。 • 但し、トラストされたセットアップが必要なほか、proofサイズが大きくなる点が課題。
	Zerocash/ Zcash	• 元のコインを変換して返すプロセスを必要無しにアドレス間のトランザクションリンクを完全遮断しながら、トランザクション数量も隠蔽し、proofサイズも小さく済む点が特徴。 • プライベートトランザクション生成に数分を要するほか、トラストされたマルチパーティセットアップが複雑な点、また監査可能性が提供されておらず偽造コイン検知困難な点、加えて比較的新しい暗号技術であるzkSNARKsを利用している点が課題とのこと。
	zkSTARKs	• zkSNARKsの課題解決のためトラストされたセットアップを必要としないようにするもの。 • 但し、それでもproofサイズが数百KBと大きい点は残るため、引き続き注視が必要。

→ 出典：https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/
→ 出典：https://zcoin.io/zcoins-privacy-technology-compares-competition/

- Bitcoin Cash
  - おさらい
  - Satoshi's Vision Conferenceトピック

前クールのトピックおさらい

- プロトコルアップグレードを2018年5月15日および2018年11月15日に計画。
  - デフォルトブロックサイズ上限を高める。
  - ブロック生成時間の短縮。
  - オペコードを再度有効にする。
  - 新しいBitcoin Cashアドレスフォーマットを実装する。
  - ブロック生成時間のバラツキ短縮や、二重消費耐性向上、DDA（難易度調整アルゴリズム）改善を実現。
  - Graphenを統合することによってブロック伝播を改善する。

デフォルトブロックサイズ上限を高める
- トランザクションオーダリングコンセンサスルールを撤廃し、正当なトランザクションオーダーに

ブロック生成時間の短縮
- より高速で小さなブロックに注力しながらユーザー体験を改善すべく、ブロック生成時間を現在の10分から1分や2分へ短縮

オペコードを再度有効化
- 新たにOP_GROUPおよびOP_DATASIGVERIFY向け実装を提供
- 2009年のビットコインローンチ後まもなく無効化されたオペコードを再度有効に

新Bitcoin Cashアドレスフォーマットを実装
- BTCが意図せずBCHウォレットへ送られてしまいにくくする

ブロック生成時間のバラツキ短縮など
- Bobtailの利用を検証

ブロック伝播を改善
- Graphenを統合

→ 出典：https://www.bitcoinunlimited.info/cash-development-plan
→ 出典：https://www.bitcoinabc.org/bitcoin-abc-medium-term-development

SATOSHI'S VISION CONFERENCEから見えたBITCOINCASHの歩み①

- OP_GROUPは、ビットコインキャッシュのブロックチェーン上でトークン発行（カラードコイン）を可能にするもの。
  - ビットコインにおけるカラードコイン発行方法として、「カウンターパーティのようにマルチシグスクリプト上に保持」および「オープンアセットプロトコルのようにOP_RETURNに記録」に続く第３の方法。
  - これは、ビットコインプロトコルに変更を加えてトークン発行を可能とするのが特徴。
  - ネイティブのレイヤー１トークンを、BCHで付与できるようにするものであり、実装に際しては、１Satoshiの量が１トークンにペグされないとされる。

→ 出典：https://btcnews.jp/1vt09itp15602/

＜ネイティブトークンが必要な理由＞
- レイヤー１トークンは、全ウォレットが機能を追加できる唯一の方法。
- ハードウェアウォレットによって完全サポートされるチャンスあり。
- SPVウォレットにとって検証が容易なため分散化できる。
- トークン発行やBurnにスクリプト言語を使える。

＜OPコードを使う理由＞
- Bitcoinトランザクションは余分な属性をアウトプットに含めるフィールドが不足している中、ハードフォークなしに可能な方法が、スクリプト中におくこと。
- これが完全なソリューションではないが、最小の変更ですむために採用した。

＜課題＞
- 交換業者がトークンを扱える必要。
- 先進ユーザー・発行者むけにAPIサービスやブロックエキスプローラが必要。
- 将来「フィアットトークン」が登場すると、マーチャントやユーザーはトークンとしてペイメントを受け取りたくなる可能性。

SATOSHI‘S VISION CONFERENCEから見えたBITCOINCASHの歩み②

- ゼロ確認ペイメントとは、複数ソースを介して、ゼロ確認トランザクションがBCHのMempool中にあると確認すると、ペイメント完了として、リターンが返却される前にトランザクション完了とするもの。
  - 一般的には二重支払いを防ぐために少なくとも１確認は必要とされる。
  - ゼロ確認ペイメントの場合は、交換業者やマーチャントが１回目のネットワーク確認が届く前にデジタル通貨を受け入れ、ブロックを待たずに即座に送金完了となる。
  - 今回、ネイティブでの「二重支払い耐性」として、「二重支払いリレー」が示された。

→ 出典：https://btcnews.jp/1vt09itp15602/

複数ソースを介して、ゼロ確認トランザクションがBCHのMempool中にあると確認

↓

ネイティブでの「二重支払い耐性」

＜二重支払いリレー＞
- ウォレットは二重支払いを検知するとアラート発行。
- アラートが無ければ、T秒後に、安全性が高まるとする。

↓

ペイメント完了とみなす
（交換業者やマーチャントが１回目のネットワーク確認が届く前にデジタル通貨を受け入れ）

↓

リターンが返却される前にトランザクション完了とする
（ブロックを待たずに即座に送金完了）

- その他トピック
  - Tether関連
  - Bitcoin Core 0.16.0リリース
  - Halong Mining、明示的AsicBoostを実装

ASIC耐性に関する議論　①

- Monero、ASIC対策でハードフォーク
  - Bitmainの他、Halong MiningなどもCryptoNightむけASICマシンを開発。
  - ハードフォークによりCryptoNight PoWハッシュアルゴリズムへの小改善を導入し、ASICマイニングハードウェア対策。
  - ハードフォーク前のMoneroブロックチェーンを用いるプロジェクトとして、Monero Classic、Monero-Classic、Monero 0、Monero Originalが誕生。
  - ハードフォークにはリプレイプロテクション無しのため、新ブロックチェーンでXMRを使うと、ハードフォーク前のブロックチェーン上のコインも意図せず使用される。
  - 双方のブロックチェーン上でコインを移動することにより、どのコインが同一ユーザーにより使われているかが判明し、Moneroのプライバシーを損なうため、片方のみを選択することが必要。
  - また、このように自身の保有するコインの判明したユーザーのコインとミキシングされることによって、他ユーザーの匿名性を損なうことも懸念。

→ 出典：https://bitcoinmagazine.com/articles/monero-just-hard-forked-and-it-resulted-four-new-projects/
→ 出典：https://www.coindesk.com/monero-community-holds-breath-as-contentious-hard-fork-activates/
→ 出典：https://monero0.org/
→ 出典：http://moneroclassic.org/
→ 出典：http://monero-classic.org/
→ 出典：https://github.com/XmanXU/monero
→ 出典：https://monerov.org/

ASIC耐性に関する議論　②

- ASIC耐性持続のためのハードフォーク是非が課題に

  - ASIC耐性持続を目的としてPoWアルゴリズムを頻繁に変更することはコストもかさみ、終わり無き戦いになる。開発者としては、ASICフレンドリーなアルゴリズムの様に、ASIC開発に対して公平で持続可能な環境構築を図るべき、という主張。

  - アルゴリズム変更によりASIC耐性を持続する方法は繰り返しハードフォークを行うことになり、コンセンサス形成負荷、バグ混入リスク、ハッシュパワー減耗などの点で持続性に疑問とのこと。

  - ASIC耐性を維持するためのハードフォークが持続可能でない場合にマイニングパワー集中化をもたらすかというと、多数の生産者参入によるASICのコモディティ化もあり得るため必ずしもそうとは限らないのでは、と。例えばBitcoinではマイニングの地理的分散やチップメーカー参入など分散傾向もある。

→ 出典：https://tokeneconomy.co/is-the-war-against-asics-worth-fighting-b12c6a714bed

ASIC耐性に関する議論　③

- Moneroのフォークを受けて、AntPoolはMonero Classicサポートを表明
  - https://media.weibo.cn/article?id=2309404225266690992678&jumpfrom=weibocom
- Bitmain、EthereumのEhHash向けASICとしてAntminer E3を800ドルで発売
  - https://shop.bitmain.com/product/detail?pid=00020180403174908564M8dMJKtz06B7
- EthereumはCasper移行を5ヶ月半後としASIC対策でハードフォーク意向無し
  - https://www.trustnodes.com/2018/04/06/ethereum-not-forking-asics-casper-coming-around-five-months
- EthereumもASIC耐性を持たせるべくEIP958提案がなされる
  - https://www.ethnews.com/new-eip-suggests-ethereum-hard-fork-for-asic-resistance
  - https://github.com/ethereum/EIPs/issues/958
- Moneroブロックチェーンの追跡可能性に関する指摘アップデートに対する反応
  - https://getmonero.org/2018/03/29/response-to-an-empirical-analysis-of-traceability.html
  - https://arxiv.org/pdf/1704.04299.pdf
- ビットコイン向け国産マイニングASICチップKAMIKAZE発表
  - https://prtimes.jp/main/html/rd/p/000000001.000033229.html
- マイニングチップ事業に参画したSumsungもGPUだけでなくASIC生産に取り掛かっていることを認めた
  - https://techcrunch.com/2018/01/31/samsung-confirms-asic-chips/
- Bitmain、ZcashなどのEquihash暗号通貨向けASIC（Antminer Z9 mini）発表
  - https://shop.bitmain.com/product/detail?pid=00020180503154806494uGcSyiu806FD
- Verge、51%攻撃受け250,000 verge盗難、ハードフォークへ
  - https://news.bitcoin.com/verge-is-forced-to-fork-after-suffering-a-51-attack/

TETHER関連

- TetherはUSDがTetherにより管理される口座へデポジットされると新規USDTトークンが発行され、逆にUSDが引き出されるとUSDTがburnされることとされ、20億USDTが流通している。
  - このUSDとUSDTの紐付けが本当になされ、USDT発行に対応したUSDデポジットを保有しているのかという点で疑惑の声があがっている。
- そんななかで、匿名の「Tether Report」文書が発表された。
  - Tetherの成長はマーケットコンディションに対応した新規発行を通じてのもの。
  - 調査期間中において、ビットコインの価格上昇の48.8%は、91回にわたるTether発行の二時間後に発生したもの。
  - Bitfinexの引き出し・デポジットの統計値は通常ではありえず、不正があればビットコインの価格は30-80%減少を来す可能性があるとしている。
- Tetherを巡るトピック
  - 監査法人フリードマンとの関係が打ち切られたとの報道。
  - 米規制当局CFTCから、BitfinexおよびTetherに対して召喚状・文書提出命令が発行。
  - BitMEXから、銀行による裏付けはありそうとのレポートがあったほか、プエルトリコNobleBankとの提携関係あり準備銀行として機能している可能性とのレポートも。
  - 3月にも、3億円分のUSDTを新規発行。

→ 出典：http://www.tetherreport.com/
→ 出典：https://www.trustnodes.com/2018/03/21/tether-starts-printing-300-million-freshly-minted
→ 出典：https://blog.bitmex.com/tether/
→ 出典：https://blog.bitmex.com/tether-addendum-new-financial-data-released-from-puerto-rico/

Bitcoin Core 0.16.0リリース

- Segwit ウォレットサポート
  - addresstype引数が追加され、legacy, p2sh-segwit(デフォルト）およびBech32アドレスをサポート。
- bc1で始まるBech32（BIP173）アドレスのフルサポート追加
  - BIP173アドレスへの送付、これらアドレスの生成が可能に。
- デフォルトで階層的決定性（HD）ウォレットに
  - GUIにおいてwalletrbfに拠らずデフォルトでRBFに。
  - Replace by feeは、unconfirmed トランザクションを、より高い手数料を払う別トランザクションバージョンに置き換えるもの。
  - なかなかブロックに入らないトランザクションを、手数料高く設定したトランザクションと置き換えてブロック取り込みスピードを上げるもの（BIP125）。

→ 出典: https://lists.linuxfoundation.org/pipermail/bitcoin-core-dev/2018-February/000052.html
→ 出典: https://btcnews.jp/4ae2jp7015197/

HALONG MINING、ビットコインマイニングハードウェア生産者として初めて明示的ASICBOOSTを実装

- DragonMintマイニングハードウェアはのAsicBoost実装を発表した。
  - Halong Mining社は、特許出願中の技術へのアクセスを可能とするBDPL（Blockchain Defensive Patent Lisence）に加盟したため、”version-rolling”によるAsicBoostを利用するライセンスを得ることができた。
  - これにより、DragonMintは従来比20%のエネルギー効率向上が見込まれる。

- 秘密裏に行うAsicBoost（マークル木を操作するタイプ。検知が難しいためCovert AsicBoostと呼ばれる）と異なり、明示的な方法によるAsicBoost（nVersionビット中の2ビットを用いる”version-rolling”タイプ。
  - ブロックヘッダーを見れば明示的なためOvert AsicBoostと呼ばれる）は、小さなブロックを作ったり、ビットコインプロトコルアップグレードに干渉するインセンティブを持たない。
  - Little Dragon Technology社が元の発明者から特許を得た以降、Halong Mining社は交渉を重ね、このほど特許保持者から特定条件下で特許利用をオープンとするアナウンスが3/1に行われたことを受け、今回の開示に至ったもの。

→ 出典: https://bitcoinmagazine.com/articles/halong-mining-first-bitcoin-mining-hardware-producer-implement-overt-asicboost/
→ 出典: https://halongmining.com/blog/2018/03/07/dragonmint-btc-miner-uses-version-rolling-asicboost/
→ 出典: https://blockchaindpl.org/
→ 出典: https://www.asicboost.com/single-post/2018/03/01/opening-asicboost-for-defensive-use/
→ 出典: https://blog.bitmex.com/graphical-illustration-of-a-bitcoin-block/

2. Ethereumエコシステムの動向

- スケーリング課題対応策の概観
- Casper（Casper FFG）
- Sharding
- State Channels
- Raiden・μRaiden
- サイドチェーン（POA Network、Parity Bridge）
- Plasma・Plasma Cash
- Truebit
- Cosmos
- 個別トピック

スケーリング課題対応策の概観

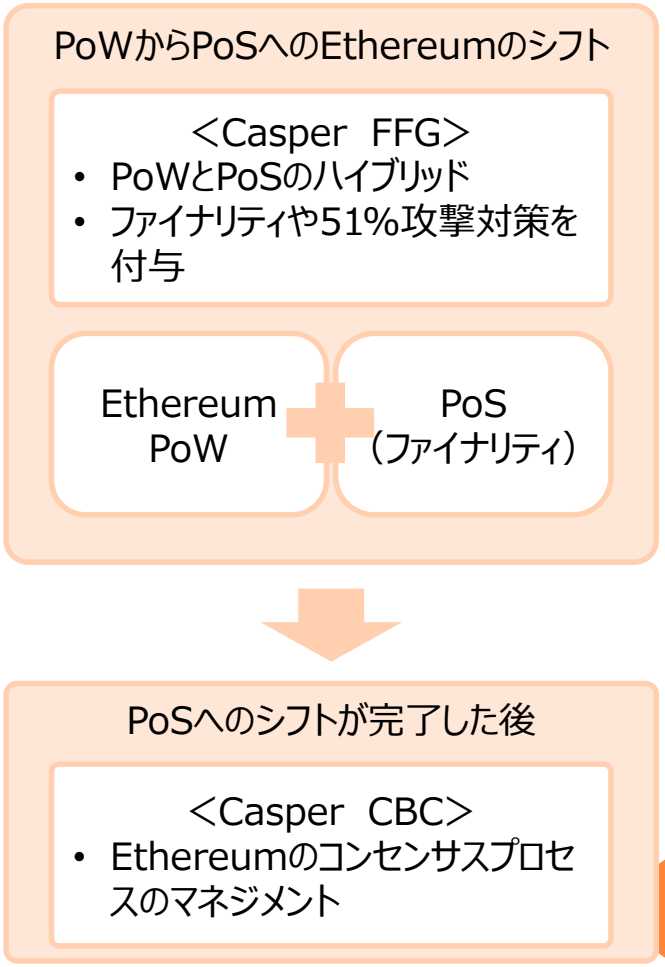
- Ethereumスケーリングソリューションを、オンチェーン／オフチェーンの二つに大別。
  - さらに、オフチェーンは、State ChannelおよびSidechainの２つに大別できる。
  - この他、スマートコントラクト計算をオフチェーンで行うTruebitなども。
  - Ethereumスケーリングソリューションサマリーシートがweb3により整理されている。
    - https://docs.google.com/spreadsheets/d/1BQ0bK_LhSQvxtvXryVoIcmxeKMuVJCq6oD0aS5_hpC8/htmlview#gid=0

オンチェーン Scaling		• 検証を並列的に計算してネット全体で検証効率化	• Sharding
オフチェーン Scaling	State Channel	• 二アドレス間で一対一のやりとりを直接行うチャネルを提供 • オフチェーンによるコミュニケーションを実施したうえで、最後の残高セツルメントをメインチェーンで行う	• μRaiden • Counterfactual
		課題：• チャネル利用中はEthereumデポジットおよびロックアップが必要 • そのほか、「DoS攻撃への脆弱性」「State Channel利用を前提としたアプリケーション開発」「全てのアプリケーションがチャネル化可能ではない」「マルチシグコントラクトへの依存」など	
	Sidechain	• メインチェーンと並列でメインチェーンと同じと限らないPoAやPoSコンセンサスメカニズムのチェーンを稼働 • 一時的にオフチェーンのやりとりを行った上で最終セツルメントをメインチェーンで行う	• Cosmos • Plasma • Parity • POA Network
		課題：• セツルメント完了にはルートチェーンに依存する • 「PoAではオーソリティをトラスト要」「ツールが不十分」「多対多トランザクションが可能だが資金移転がState Channelほど速くない」など	

→ 出典：https://medium.com/giveth/scalingnow-summit-transcript-ea5373be8523

CASPER ①
(CASPER THE FRIENDLY FINALITY GADGET:FFG)

- 既存のEthereum PoW上にPoSをオーバーレイする、PoWとPoSのハイブリッド。
  - CasperにはFFGとCBC（Correct-by-Construction）の二つがある。
  - FFGはPoWからPoSへのEthereumのシフトをマネジメントし、CBCはPoSへのシフトが完了した後のEthereumのコンセンサスプロセスのマネジメント。
  - ハードフォークを経て、まずPoS/PoWのハイブリッドシステムとして導入され、次いで時間をかけて徐々に完全なPoSシステムへと移行予定。
  - Casper FFGにより、Ethereumのセキュリティは PoW難易度からPoSファイナリティへシフトする。
  - PoW/PoSハイブリッドコンセンサスモデルへの移行に向けたEIP1011が発表されている。



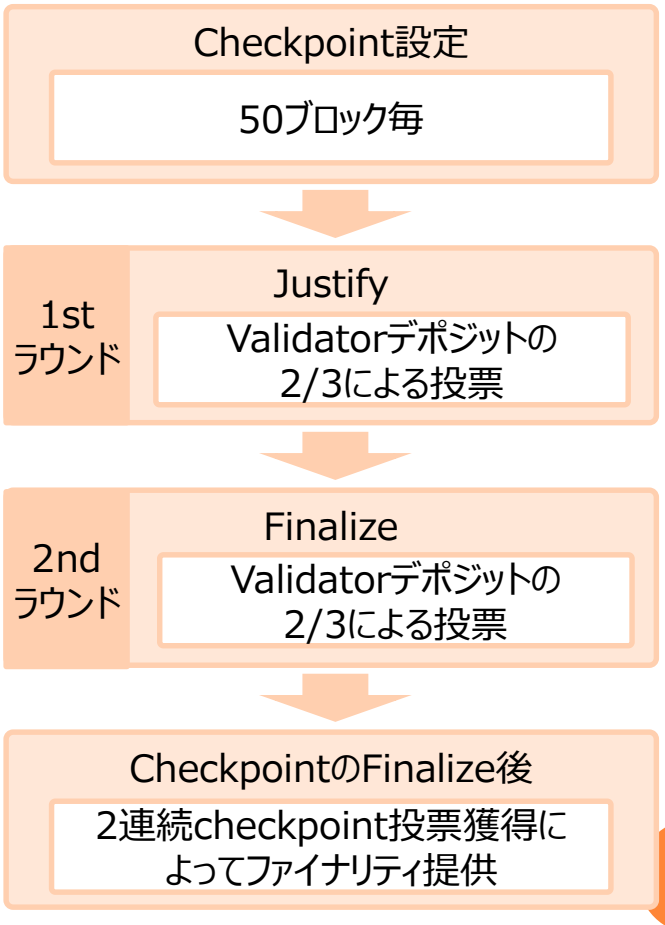
→ 出典: https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae
→ 出典: https://www.bitsonline.com/casper-testnet-released/

CASPER ②
(CASPER THE FRIENDLY FINALITY GADGET:FFG)

- Casper FFGでは、まずマイナーがPoWでブロック生成した上で（確率的ファイナリティに留まる）、次にバリデータがPoSで特定ブロック高ごとに検証を行ってファイナリティ提供。

  - Etherをデポジットすると公開鍵のように位置づけられメッセージへの署名に使われるValidation Codeが定まりValidatorになる。
  - Validatorプールに参加するとPoSコンセンサスプロセスに参加するためのメッセージを送付できる。
  - Validatorプール中のValidatorサイズはデポジット量に応じる。

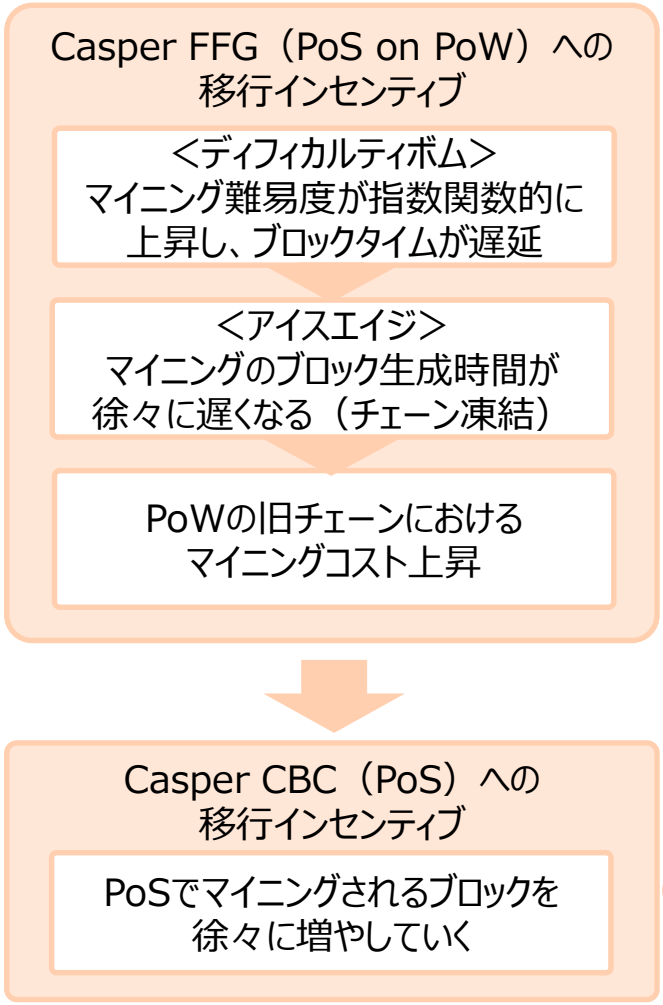
  - Validatorはファイナライズされると報酬を受け取れるが、同じブロック高の分岐で2つファイナライズがあると違反とみなし、ペナルティとしてデポジット減。
  - Validatorは２つの分岐に投票するとペナルティが課されるため、正統なチェーンに収斂していく動機付け。



→ 出典: https://github.com/ethereum/casper/blob/master/IMPLEMENTATION.md
→ 出典: http://individua1.net/casper-ffg-dynamic-validator-sets/

CASPER ③ (CASPER THE FRIENDLY FINALITY GADGET:FFG)

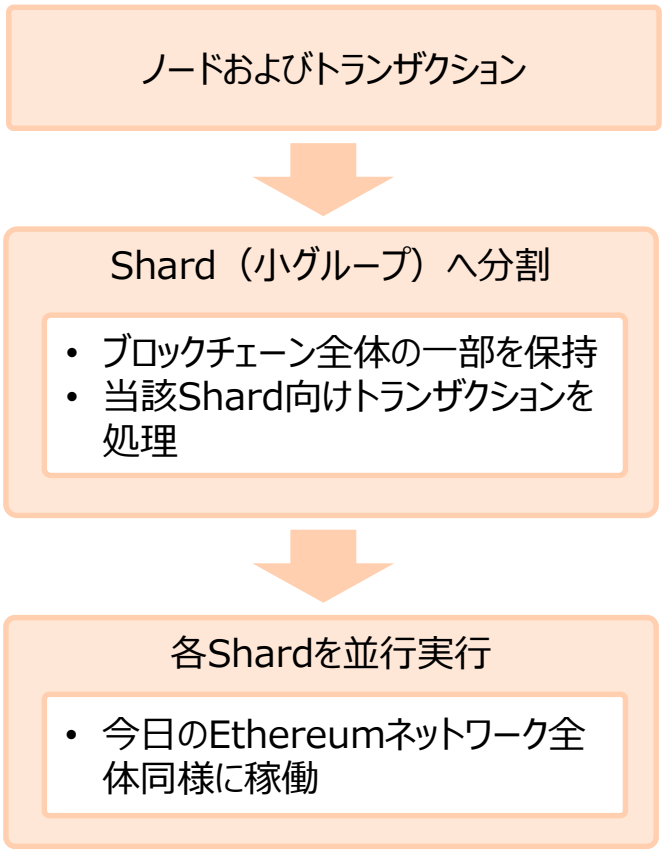
- ディフィカルティボムは、PoWからPoSへの移行を円滑に行うべく導入された、ディフィカルティ調整アルゴリズムによるインセンティブ機構。
  - いかにシステム全体が分裂なしに新しいチェーンへと移行できるようなインセンティブを与えられるか。
  - ブロック高に応じて、ディフィカルティが指数関数的に増加することによって、マイニングにかかる時間が徐々に延びる。
  - 旧チェーンでマイニングを続けても、徐々にマイニングコストが高まり、利益が生めなくなる仕組み。
  - CasperFFGについて、これまでのPoS提案の中で穏便であり評価しつつも、PoWによるチェーン収斂やセキュリティが不必要に希薄化すると懸念も。（nothing at stake問題など、コミュニティの想定よりも道のりは険しいとの見方）



→ 出典：http://blockchain.gunosy.io/entry/ethereum-difficulty-summary
→ 出典：https://ethereum-japan.net/ethereum/casper-ffg-testnet-release/
→ 出典：https://blog.bitmex.com/complete-guide-to-proof-of-stake-ethereums-latest-proposal-vitalik-buterin-interview/

SHARDING ①

- ノードおよびトランザクションをShardと呼ばれる小さなグループに分割した上で、それら全てを並行で実行し、今日のEthereumネットワーク全体同様に動くもの。
  - 各Shard内のノードは、ブロックチェーン全体の一部を保持するのみでよく、当該Shard向けトランザクションを処理するだけでよい。
  - Shardを横断するやりとりも可能だが、Confirmationに複雑で時間のかかる処理を必要とする。
  - ただし、Sharding実装にむけた具体的アプローチはまだ最終決定されておらず、またShardingがどれだけのスケーリング向上やデメリットをもたらしうるかが明らかになっていないのが課題。



→ 出典：https://medium.com/titan-digital-asset-group/scaling-ethereum-for-global-adoption-d0168fa66297

SHARDING ②

- Collationを提案する責任を分離してProposerで行うこととした。
  - 但し、その後、複雑性を避け、Collator/Proposer区別廃止し、Collator自身が提案する方向へ。
  - スケルトン(Minimal Sharding Protocol)が提案され、当面最小限の実装を行うのがよいと。

Shard	• 利用可能なCollationのチェーン。	ブロックチェーン
Collation	• CollationヘッダとCollation本体から成るデータユニット。 • Collatorに対して提案され、Proposer間のオープンオークションを通じてCollationツリーに含めてもらう。	ブロックに相当
Blob	• Collation内で区切られて配列されたデータ片。 • Collationに含めBlobを集合的に優先付けするのがProposerプール。	トランザクションに相当
Collationツリー	• 全shard向けに接続されたCollationのツリー。 • Collationツリーを伸ばすために提案されたCollationヘッダをProposalと呼ぶ。	ー
Proposer	• Collatorに対してCollationを提案する責任をもつSharding参加者。 • Blobを優先付けして、Collationとして組み立て。	ー
Collator	• Collationの可用性やチェーン接続に責任を持つ。Collation本体の可用性を判断したうえで、Proposerから最高額を支払う利用可能Collationを選択する。 • 全Shardのセキュリティに集合的に参加するCollatorの集まりをCollatorプールと呼ぶ。	マイナーに相当
Executor	• 所与のShardの正統なチェーンにおいて実行エンジンを走らせて、ステートルートの暗号経済的請求をポストする。 • これにより、軽量クライアントがノード実行無しにShardのステートルートを推察できる。	ー
SMC	• CollatorやProposerやCollationツリーを管理する、メインチェーン上のコントラクト(Sharding Management Contract)。	ー

→ 出典: http://ethresear.ch/t/sharding-phase-1-spec/1407
→ 出典: http://ethresear.ch/t/a-minimal-sharding-protocol-that-may-be-worthwhile-as-a-development-target-now/1650
→ 出典: https://medium.com/prysmatic-labs/ethereum-sharding-biweekly-development-update-1-prysmatic-labs-939ff0ed4b65

SHARDING関連コンテンツ

- Sharding phase 1 spec
  - http://ethresear.ch/t/sharding-phase-1-spec/1407
- Sharding Phase 1 の具体的な仕組みとセキュリティ課題
  - https://zoom-blc.com/sharding-phase-1
- Shardingの図解解説
  - https://docs.google.com/presentation/d/1mdmmgQlRFUvznq1jdmRwkwEyQB0YON5yAg4ArxtanE4/mobilepresent?slide=id.g359cce9869_12_3071
- Ethereum Shardingの大まかな説明と概念図
  - http://individua1.net/ethereum-sharding-overview/
- Shardingの部分的PoC開始
  - https://www.reddit.com/r/ethereum/comments/8g1q55/vitalik_teases_sharding_release_on_twitter/dy85pq0/
- Minimal Sharding Protocol におけるメインチェーン～shard間のクロスリンク
  - http://ethresear.ch/t/cross-links-between-main-chain-and-shards/1860

State Channels

- State Channelは、ペイメントに特化したペイメントチャネルをより汎用化し、トランザクションやステート更新をオフチェーンで行うもの。
  - 処理がチャネル内で行われるため、プライバシーやファイナリティ向上にも寄与する。
  - トランザクション開閉時のみパブリックになるためプライバシーが改善するほか、両者がステート更新に署名すればファイナリティと考えることが出来る。
  - Counterfactualは、EthereumベースDappでState Channelを実装する汎用版オープンフレームワーク。
  - Perunは、「ペイメントチャネル仮想化」「State Channelネットワーク」によるスケーリング・セキュリティ向上ソリューション。
    - 仮想ペイメントハブ。ハッシュロック用いてペイメントをルーティングする代わりにチャネルの仮想化するもの。仮想チャネルが構築できれば仲介無しにペイメント可能になるとのこと。
    - 「任意のスマートコントラクトをオフチェーンで実行可能」かつ「任意の仲介者数をサポートするチャネル」という二つの特徴備えたState Channelネットワーク。

→ 出典: https://counterfactual.com/
→ 出典: https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4
→ 出典: http://ethresear.ch/t/perun-virtual-payment-and-state-channel-networks/1685

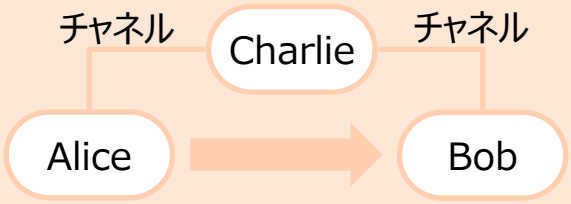
RAIDEN・マイクロRAIDEN

- Raiden Networkは、EtherやERC20トークン向けのLightning Networkにあたるオフチェーンスケーリングソリューション。
  - 単純なペイメントチャネルでは、支払先の各アドレスに対して新たにペイメントチャネル開設が必要となりコストがかさむことが課題となる。
  - Lightning同様にペイメントをネットワークを介してマルチホップでルーティングできるようにする。

- μRaidenは、所定の受け手に対する単方向ペイメントチャネル。
  - Raiden Network同様にState Channelを用いて、ペイウォール向けマイクロペイメントに特化。
  - Raiden Network（多対多双方向）と異なり、多対一の単一方向State Channelプロトコル。
  - ペイウォールの他、リクエスト払いのAPIなどDappによるマイクロペイメントリクエストへの応用に期待。

Raiden Network

- 多対多双方向の
  ペイメントチャネルプロトコル
- マルチホップでルーティング



μRaiden

- 多対一の単一方向の
  ペイメントチャネルプロトコル

→ 出典: https://medium.com/titan-digital-asset-group/scaling-ethereum-for-global-adoption-d0168fa66297
→ 出典: http://www.trustnodes.com/2017/12/01/ethereums-micro-raiden-launches
→ 出典: https://github.com/raiden-network/microraiden/blob/master/README.md

サイドチェーン（POA Network、Parity Bridge）①

- POA Networkは、バリデータによるPoA（Proof of Authority）を用いるサイドチェーン。
  - PoAの利点はマイニングがなく、代わりに、バリデータと呼ばれる事前選択されたオーソリティグループがブロックを生成する。
  - 高速かつスケーラブルかつコスト効率的ゆえに、Dappsなどがアイデアを安価・容易にテストできる。
  - PoAコンセンサスは中央集権の要素を含むコンソーシアムやプライベートチェーン向き。

- Parity Bridgeは、POA NetworkをEthereumと接続するもの。
  - サイドチェーン側がPoAやPoSであればレイテンシーは低いがボトルネックはメインチェーン側。
  - オーソリティは自身の評判をステークし、オーソリティの大多数が共謀することが無いとトラストすることが必要。

バリデータによるPoA

- 事前選択されたオーソリティグループがブロックを生成。
- バリデータ自身のアイデンティティをステークとする。
- ライセンスを付与されたバリデータのアイデンティティは第三者検証可。
- 公的評判維持で動機付けられ、それがネットワークの最大利益。
- 事前選定されたバリデータの圧倒的多数により、チェーンは有効に。

バリデータをトラストする必要あり

ファイナリティはメインチェーン

高速かつスケーラブルかつコスト効率的

コンソーシアムやプライベートチェーン向き

→ 出典：https://medium.com/giveth/scalingnow-summit-transcript-ea5373be8523
→ 出典：https://medium.com/@web3/investigating-short-term-scaling-solutions-for-ethereum-a5951fee8967

サイドチェーン（POA Network、Parity Bridge）②

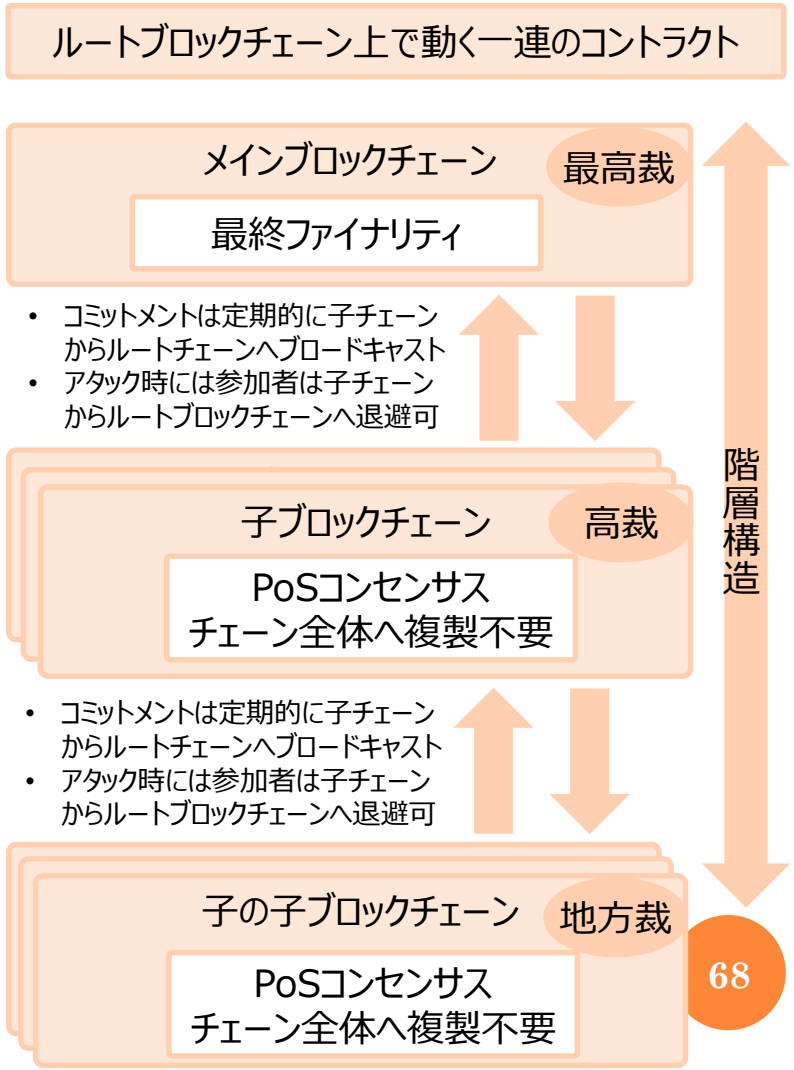
- Altcoin.ioは、サイドチェーンとPoAによって、スケーリングを改善する構想（Plasma DEX）。
  - アトミックスワップはトラストレスと共に相互運用性を提供する一方、オンチェーンのトランザクションconfirmationに時間を要し且つトランザクション手数料がかかりUXを損なう。そこでPlasmaのようにサイドチェーンのセカンドレイヤーへ。
  - Ethereum上のスマートコントラクトでデポジットをロックすると共にロック証明（デポジット証明）をトークンのサイドチェーンへ提供。トークンがスマートコントラクト中にロックされると、ユーザーがサイドチェーン上のトランザクションで利用可能に。
  - サイドチェーンのコンセンサスアルゴリズムとしてはTendermintを利用してTendermint Core上でデポジット管理などを行う。サイドチェーンはトランザクションを検証するTendermintノードにより構成される。その幾つかはAltcoin.ioによるオペレーターノード。
  - Verifierが全トランザクションを監視することにより、サイドチェーン上の二重利用防止。Verifierによる申し立てが無ければ、これらノードが署名したトランザクションが有効に。トランザクション手数料からVerifierへの報酬支払いにより、トランザクション有効性につき経済的インセンティブもたせる。
  - サイドチェーンがサポートするトランザクション種類は、Ethereum上のデポジット検証、メーカーおよびテイカーのオーダー、引き出しトランザクション（トークンのburn）。

→ 出典：https://blog.altcoin.io/plasma-dex-v1-launching-next-month-4cb5e5ea56f6

PLASMA・PLASMA CASH ①

- Plasmaは、Ethereum上の階層サイドチェーン。1ブロックチェーン上に多くのブロックチェーンをぶら下げることによって、秒あたり数十億トランザクションを目指す。

  - 子チェーンでPoSでコンセンサスし、失敗すればEthereumルートチェーンでセツルメント。
  - 最終ファイナリティはメインチェーン上で行われる。
  - アタック時には参加者は子チェーンからルートブロックチェーンへの退避が速やか且つ安価に可能。
  - メインチェーンのやりとりを最低限に留めながら、子チェーンのレベルで数千トランザクションのアプリケーションを実行するような複雑なオペレーションを処理することが可能となる。
  - 子チェーン上のオペレーションはEthereumブロックチェーン全体へ複製される必要が無いため、小額手数料で高速な実行が可能。



→ 出典：https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4
→ 出典：https://medium.com/chain-cloud-company-blog/plasma-in-10-minutes-c856da94e339

PLASMA・PLASMA CASH ②

- Plasmaでは、子チェーンはブロックチェーンの中味を公開せず、代わりにブロックの有効性を示すのに足りるブロックヘッダーのハッシュのみがルートチェーンへ提示される。
  - Ethereumなどルートブロックチェーン上で動く一連のコントラクトであり、ルートブロックチェーンはFraud proofと呼ばれるブロックの無効証明の仕組みを使ってステートの有効性を示す。
    - 子ブロックチェーンの全ステートはFraud Proofと呼ばれるスマートコントラクトロジックを介して、ステートの変移が有効化される。
  - ルートチェーン上Fraud proofがあればブロックはロールバックされてブロック生成者はペナルティを受ける。
    - それぞれの子ブロックチェーンは自身のトークンを持ちバリデータがFraud Proof Ruleに基づき不正保護を行う動機付けに使われる。

状態遷移とFraud Proof

Plasmaチェーンのブロックヘッダ情報をルートチェーンへ定期格納

状態遷移のコミット

不正確な状態遷移

Fraud Proofを用いてロールバック

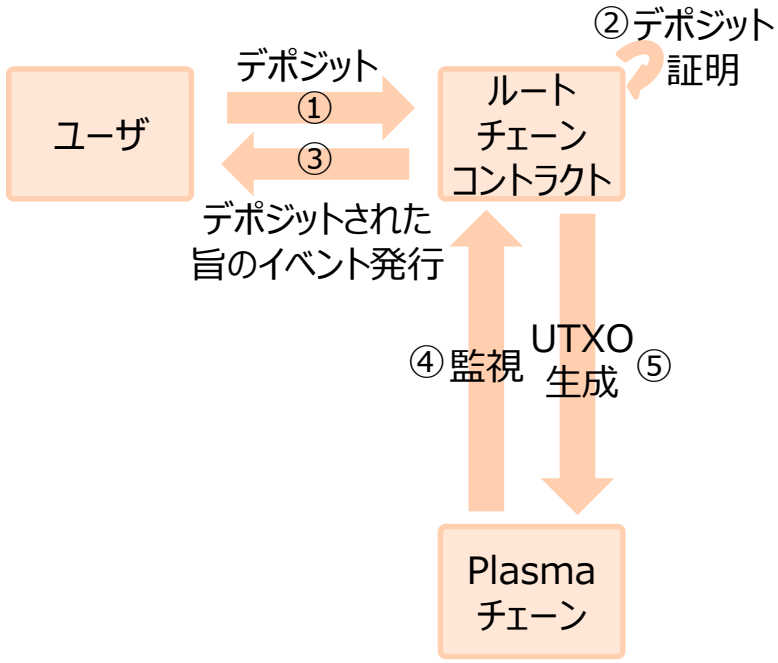
Fraud Proofに必要な情報が留保

ルートチェーンへ一斉引出

→ 出典: https://medium.com/chain-cloud-company-blog/plasma-in-10-minutes-c856da94e339
→ 出典: http://ethresear.ch/t/plasma-classic-compact-spec/1711
→ 出典: https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

PLASMA・PLASMA CASH ③

- Plasmaでは、ルートチェーンにアンカリングされたPlasmaチェーンを生成するが、このとき、ルートへデポジットするとPlasma内にUTXOが生成される一方で、ルートからデポジットを引き出すとこのUTXOが無くなる仕組み。
  - デポジットはアセットを送る[1]とルート上にデポジット証明が生成される[2]。
  - ルートチェーンコントラクトがそれを記録しデポジットされたとイベント発行[3]。
  - そしてイベントをプラズマチェーンが監視し[4]、そこにUTXO発行（ステートではなく）[5]。
  - デポジットトランザクションがPlasmaブロック内で確認できると支払いに使えるようになる仕組み。



→ 出典: http://ethresear.ch/t/plasma-classic-compact-spec/1711
→ 出典: https://speakerdeck.com/ymatsuwitter/plasma-overview-and-potential

PLASMA・PLASMA CASH ④

- Plasmaチェーン上の各トークンがユニークとなる識別子を付与することによって、Plasmaにおけるユーザーあたりのデータチェックを軽減するのが、Plasma Cash。
  - Plasmaでは、全ユーザーが、Plasmaブロック・各スマートコントラクトをダウンロードして検証要。
  - そこで、クライアントが処理する必要のあるデータ量を大きく削減すべく、履歴全体をダウンロードするのでなく、システム中で生成した自分のトークンを追跡するだけで済ます。
  - ユーザーがコントラクトへetherをデポジットとして交換業者へ送ることによりetherと同額のPlasma coinおよび、統合・分割不可能なユニークIDを生成。

トークン識別子の付与

- ネットワーク上のトークンにシリアルナンバーが振られている紙幣のイメージ。
- 各単一デポジットがユニークなコインIDに紐付く。
- トークンは分割・統合できない。

利点

- クライアントは自分のトークンをPlasmaチェーンで見ていればよく、個々のユーザ負担を増やさずにトランザクションスループットを改善できる。
- トランザクションの送付および確認という2フェーズを待たず、送付のみで確認フェーズが不要。

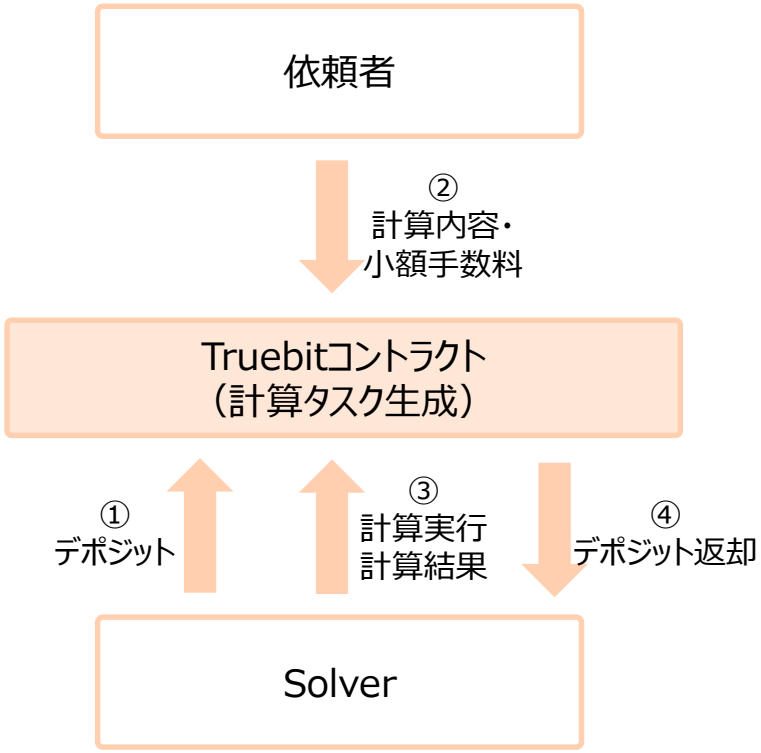
→ 出典: http://ethresear.ch/t/plasma-cash-plasma-with-much-less-per-user-data-checking/1298
→ 出典: https://karl.tech/plasma-cash-simple-spec/
→ 出典: https://www.coindesk.com/vitalik-reveals-new-idea-plasma-scaling-ethereum-event/
→ 出典: https://cointelegraph.com/news/buterin-presents-blockchain-scaling-solution-that-could-make-exchanges-hack-resistant
→ 出典: https://youtu.be/uyuA11PDDHE

PLASMA/PLASMA CASH関連コンテンツ

- Plasmaホワイトペーパー和訳版
  - https://github.com/shogochiai/plasma-whitepaper-jp/blob/master/Plasmaホワイトペーパー.pdf
- Plasmaの仕組み、デポジット、Fraud-proof、メリットと課題について
  - https://recruit.gmo.jp/engineer/jisedai/blog/plasma-blockchain/
- Quick comparison of blockchain scaling solutions（Statechannel、Sidechain、Plasma）
  - https://mobile.twitter.com/liamihorne/status/989302230065991680/photo/1
- Plasma MVP
  - https://docs.google.com/presentation/d/1RzextrcF7LJFt9pGEgEN3HyLFlQ_8kbl4nGAvsaAM4/edit#slide=id.g333c27f06c_0_4269
- Plasma MVPで知るPlasma
  - https://speakerdeck.com/ymatsuwitter/learning-plasma-from-plasma-mvp
- Plasma and the Internet of Money
  - https://blog.gridplus.io/plasma-and-the-internet-of-money-ccf7d5e8c3be
- Plasma & The Public Ethereum Chain - Joseph Poon (Ethereal Summit 2017)
  - https://youtu.be/oOQmnhQrq_U
- Scaling Ethereum with Plasma - Joseph Poon | Silicon Valley Ethereum Meetup
  - https://youtu.be/plf-kG8jt9c
- Plasmaのホワイトペーパーがオーディオブックに
  - https://soundcloud.com/user-337974466/plasma
- PlasmaからPlasma Cashへ。その仕組みとメリットと課題点
  - https://zoom-blc.com/what-is-plasma-cash
- Plasma Cash Simple Spec
  - https://karl.tech/plasma-cash-simple-spec/

TRUEBIT ①

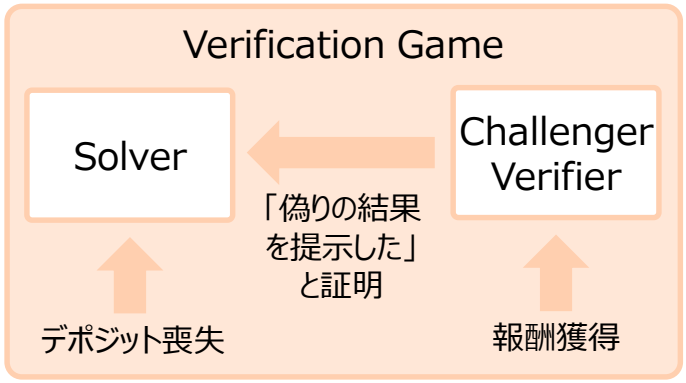
- Truebitは、スマートコントラクトにおける重たい複雑な計算をオフチェーンVMにオフロード。
  - Truebitコントラクトを通じて生成されるタスクを、クライアントがピックアップして実行。Solverに小額手数料を支払ってオフチェーンの計算を行ってもらう。（Truebitプロセスを待つレイテンシ有）
  - 基本的な流れとしては、まず最初にSolverがスマートコントラクト内にデポジットを支払う[1]。
  - 次に依頼者がSolverへ計算の内容説明を渡す[2]と、Solverが計算結果を返す[3]。
  - そしてもし計算結果が正しければデポジットが返却され[4]、Solverが適切に計算を行わなければデポジットを失う。



→ 出典: https://medium.com/truebit/truebit-the-marketplace-for-verifiable-computation-f51d1726798f
→ 出典: https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

TRUEBIT ②

- Truebitは、計算結果の真偽を告げる上で、Verification Gameと呼ばれる経済的メカニズムを用いている。
  - これはChallengerと呼ばれる他者に、Solverの働きをチェックするインセンティブを与える。
  - ChallengerがVerification Gameを通じて、「Solverが偽りの結果を提示した」と証明すれば、Challengerは報酬を得て、一方でSolverはデポジットを失うという結果となる流れ。
  - 三階層で構成され、コンピュテーション層、紛争解決層（VerificationGame）、インセンティブ層から成る。



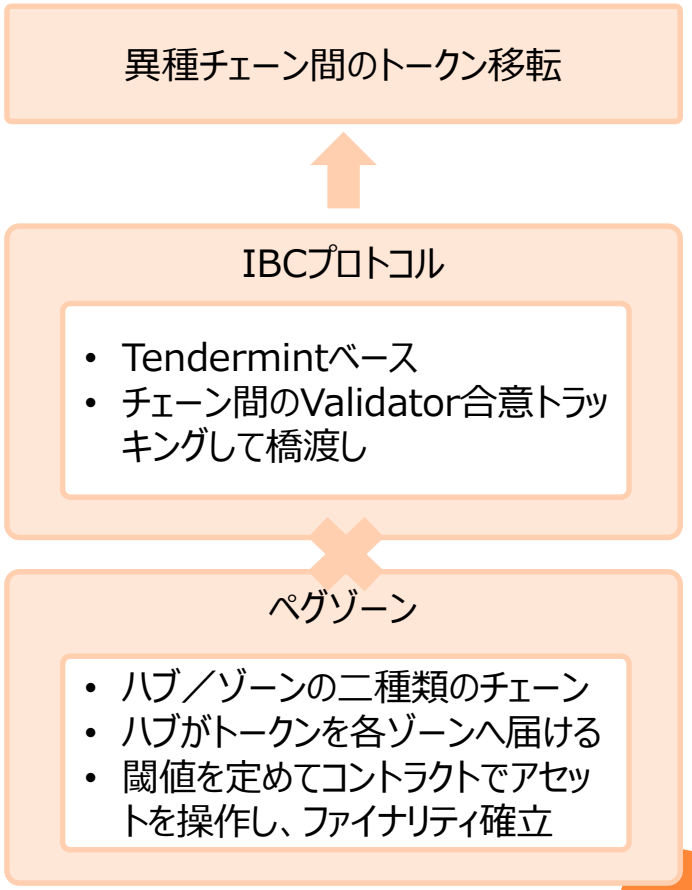
コンピュテーション層	• WebAssembly VMを用いたオフチェーンでのDApp向け計算をクライアント側へコードをダウンロードした上で行い、結果をコントラクトへ返却
紛争解決層	• SolverとVerifierによるVerificationゲーム • タイムアウト迄の時間、VerifierはSolverの解に対してチャレンジをかけることが出来る
インセンティブ層	• TRUトークンによる報酬・デポジット、トークンメカニズムによるマーケットプレイス運営といったクリプト経済デザイン

→ 出典：https://medium.com/truebit/truebit-the-marketplace-for-verifiable-computation-f51d1726798f
→ 出典：https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

COSMOS ①

※現況：最新UIがリリースされ、テストネットでライブとなっているが、2/28ローンチが延期されており、4月末時点で85%進捗の模様

- Cosmosは、異種チェーン間のトークン移転（インターブロックチェーンプロトコル）の仕組。
  - Tendermintをベースとしてチェーン間でValidatorの同意をトラッキングしてアセットを操作する「IBCプロトコル」と、ファイナリティ確立のために閾値を定めてスマートコントラクトでアセットを操作する「ペグゾーン」の仕組みの二つがポイント。
  - Tendermintを使い１ブロックで高速ファイナリティ。Ethermintでは秒間200トランザクション。
  - IBCプロトコル用いて２つのブロックチェーンを接続し、異なるブロックチェーン間を橋渡しすることで自由にトークンを移動できるクロスチェーンを実現することを目指す。
  - ハブとゾーンの二種類のブロックチェーンを持ち、ハブを中心としてBitcoinやEthereumがゾーンとして繋がっていれば、ハブがBitcoinトークンをEthereumへ届ける仕組み。



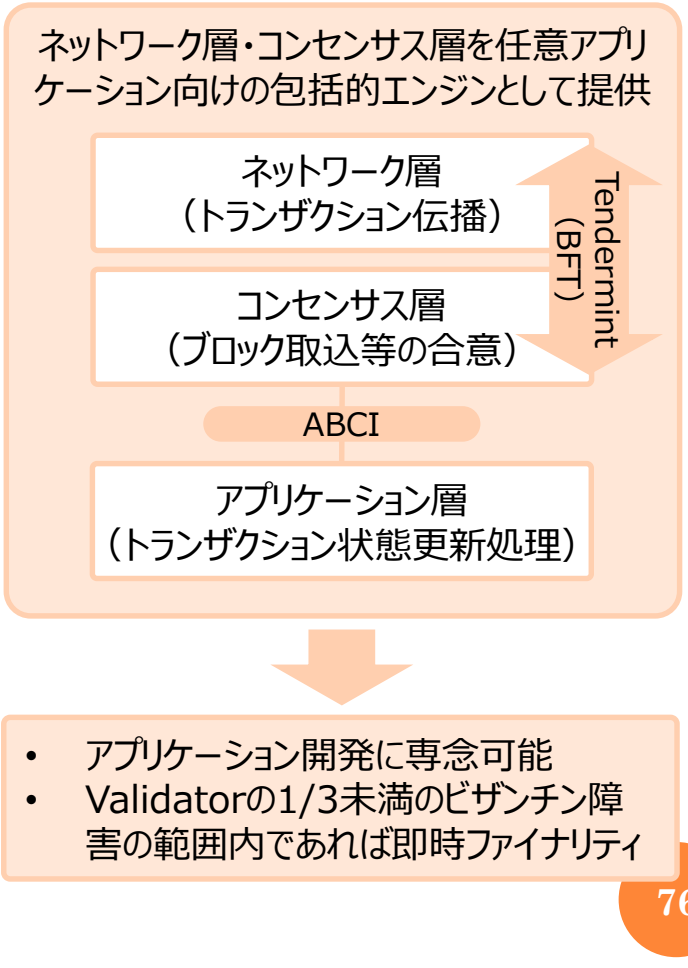
→ 出典：https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d
→ 出典：https://zoom-blc.com/what-is-cosmos

COSMOS ②

- Tendermintは、PoWにおけるスピードやスケーラビリティの課題に取り組むべく2014年に開発されたBFTコンセンサスアルゴリズム。

  - ブロックチェーンのアーキテクチャをネットワーク（トランザクション伝播）、コンセンサス（ブロック取り込み等の合意）、アプリケーション（トランザクション状態更新処理）の三階層に区分して考えると、Tendermintはこのうちネットワーク層・コンセンサス層の二つを任意のアプリケーション向けの包括的エンジンとして提供することによって、アプリケーション開発に専念できるようにするもの。

  - パフォーマンス面でも秒単位のブロック生成間隔で秒間数千トランザクションをハンドリングできる他、Validatorの1/3未満のビザンチン障害の範囲内であれば即時ファイナリティでありフォーク発生しないのが特徴。



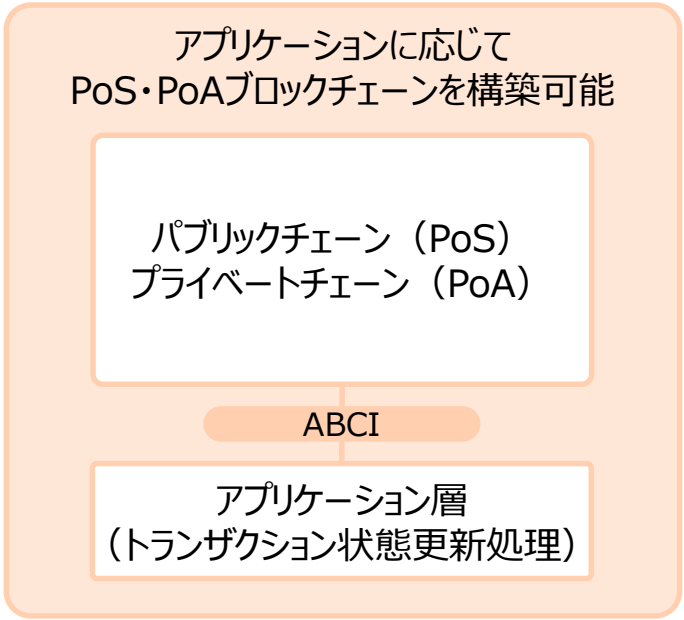
→ 出典：https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d
→ 出典：https://zoom-blc.com/what-is-tendermint

COSMOS ③

- Tendermintは、ABCI（Application Blockchain Interface）と呼ばれる仕組みを提供し、コンセンサスのロジックプロセスとアプリケーションのロジックプロセスを分割して、メッセージを送り合うことを可能としている。

  - Tendermint Core エンジンはABCIソケットプロトコル（任意のプログラミング言語にラップ可）によりアプリケーションと接続し、アプリケーションに応じこの上にパブリック（PoS）・プライベート（PoA）双方のブロックチェーンを構築できる。

  - ABCIはモジュール構成ゆえ、その上に既存ブロックチェーンコードベースをポート可能。例えば、EVMコードベースをTendermint上にプラグインしたものがEthermint。EthermintはEthereumのように動きながら、Tendermint の便益を享受可能。



＜ハードスプーン＞
- 既存チェーンからのステートを踏まえた新チェーンで、既存通貨残高を複製し新規通貨を鋳造
- Ethermintの場合は、Ethereumの残高を複製してEthrmint VMゾーンにペグづけし、フィートークンとして利用
- ブロックチェーン上のメタプロトコルであり、元のチェーンのトークンに由来したトークンを生成

→ 出典：https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d
→ 出典：https://zoom-blc.com/what-is-tendermint

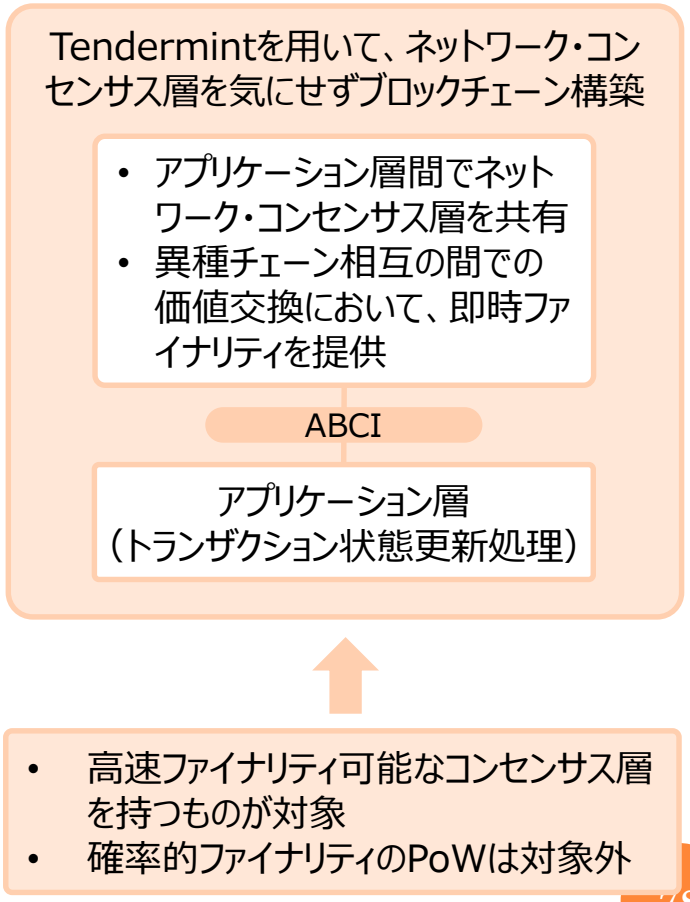
COSMOS ④

- IBC（Inter Blockchain Communication）は、Tendermintの特性を踏まえ、異種チェーン相互の間での価値交換において即時ファイナリティを提供する。

  - Tendermintを用いると、ネットワーク層・コンセンサス層を気にせずに高パフォーマンスのブロックチェーンを構築できるので、異なるアプリケーション層どうしで同じネットワーク層・コンセンサス層を共有でき、ひいては相互接続が可能。例えばパブリック～プライベートチェーン間でトークンを交換できる。

  - 但し、このとき対象となるのは高速ファイナリティ可能なコンセンサス層を持つものが対象であり、確率的ファイナリティとなるPoWは対象外。

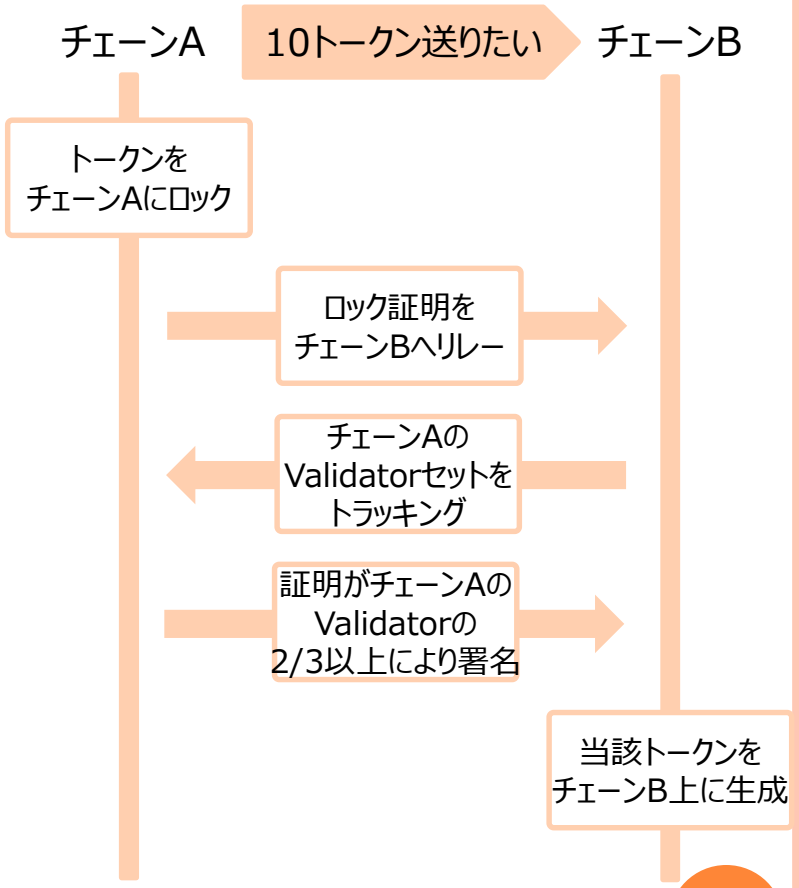
  - Cosmosは、このIBCを用いてブロックチェーンどうしのネットワークを構成しようとするもの。



→ 出典：https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d

Cosmos ⑤

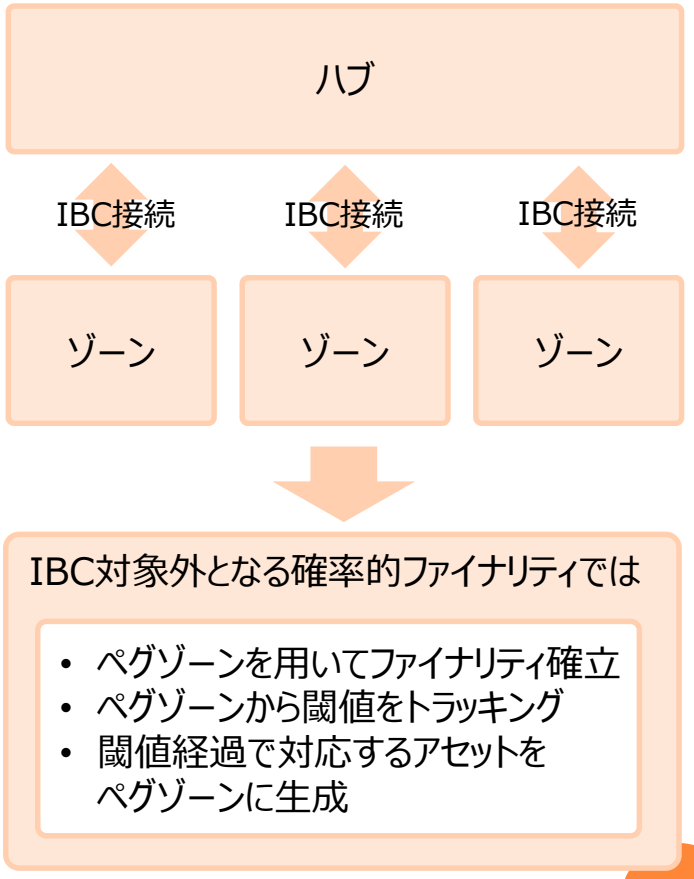
- IBCによるチェーン間トークン送付、トークンがロックされた証明をValidator多数が署名したことを以って、相手チェーンにトークン生成。
  - チェーンAからチェーンBへ10トークン送りたいとき、まずトークンがチェーンAにロックされ、このロックされた証明がチェーンBへリレーされる。
  - チェーンBはチェーンAのValidatorセットをトラッキングし、証明がチェーンAのValidatorの2/3以上により署名された場合に有効として、当該トークンがチェーンB上に生成される。
  - 但し、このときチェーンBに生成されたトークンは、チェーンA上にのみ実在するトークンそのものではなく、チェーンA上にトークンがロックされたことの証明に従って、チェーンA上の当該トークンをチェーンB上に表現したものである点に注意。



→ 出典：https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d

Cosmos ⑥

- IBC接続を用いてブロックチェーンネットワークを生成する上では、「接続数の多さ」「チェーン間の多重トラスト」が問題となるため、Cosmosでは「ゾーン」とそれを接続する「ハブ」というモジュール構成をとる。
  - 確率的ファイナリティのチェーンの場合は、ペグゾーンというプロキシチェーン（他のチェーンのステートをトラッキングするチェーン）を用いる。
  - ペグゾーン自身は高速ファイナリティ可能でIBC互換とし、橋渡しするチェーンにファイナリティを確立する役目。
  - このとき「当該ブロックの後に100ブロック追加されたときにファイナリティとみなす」といったファイナリティ閾値を定める。



→ 出典：https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d

クリプトエコノミクス　①

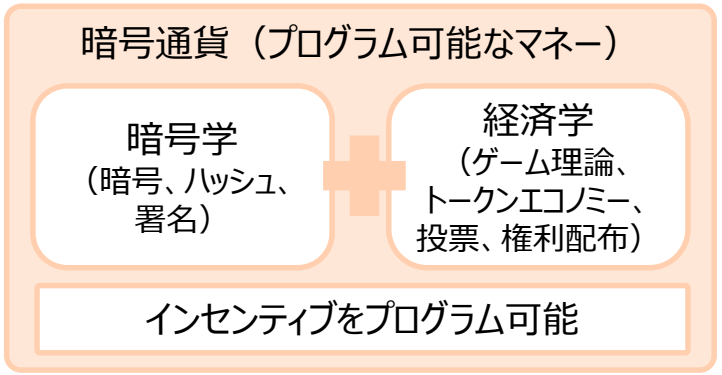
- 暗号学的経済インセンティブ・ペナルティを用いて、コンセンサスプロトコルを安全なものに。
  - セカンドレイヤーによる経済的メカニズムは、参加者が競争することで互いをチェックし合うインセンティブを与えるゲーム。
  - こうしたインセンティブゲームを通じて、State ChannelやPlasmaにおいてはトランザクションスループットを向上させ、Truebitにおいてはより多くの複雑な計算を実行することを可能に。
  - こうした経済メカニズム構築にあたっては、プログラム可能なブロックチェーンであることが大きく作用。
  - インタラクティブな経済的ゲームを設計する上では、制約の大きなスクリプト言語だけでは難しく、Ethereumがプログラム可能であるゆえに、仮想的・経済的メカニズムを実装できている。

Casper	Slasherと呼ばれる懲罰アルゴリズムが導入予定。 不正を行ったユーザーのStakeを没収することで、一定Stakeがあればリスクを負わず容易に不正ブロックを生成して二重消費を起こせてしまうNothing at Stake問題に対処。
Truebit	VerifierがSolverの誤りを証明させるインセンティブを与えることにより、Solverが真実を告げる確率向上。
Plasma	Fraud-proofや引き出しの管理に応用。
State Channel	互いに反論する機会をchallenge periodを通じて与えることによってチャネルの最終ステートを確定。

→ 出典: https://vitalik.ca/general/2018/03/28/plutocracy.html
→ 出典: https://github.com/jpantunes/awesome-cryptoeconomics/blob/master/readme.md
→ 出典: http://forum.cryptoeconomics.study/
→ 出典: https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

クリプトエコノミクス　②

- クリプトエコノミクスの主要トピックはゲーム理論、メカニズムデザイン、暗号学、コンセンサスメカニズム、ネットワーク効果、ガバナンス、セキュリティ、トークンエンジニアリングなど。
  - 独占ではなく協調といった、より良い結果をもたらすためのインセンティブを設計する。
  - そのためには、協調を動機付ける一方で、権力悪用・集中につながる動機を防ぐようなインセンティブ設計が望ましい。
  - よって、ブロックチェーンアプリの構築においては、正しいインセンティブ構造の設計が必要。



インセンティブ	オークション、投票、デリバティブ、罰金、配当
クリプト	ハッシュ関数、公開鍵暗号・デジタル署名、マークルツリー、不正証明、ゼロ知識証明、Pedersenコミットメント
デザインパターン	コンセンサス（PoW, PoS, PoA）、セカンドレイヤー（StateChannel, Plasma, Truebit、HTLC、アトミックスワップ）、Sharding、マイナーゲーム（セルフィッシュマイニング、バリデータのジレンマ）、Dappsデザインメカニズム

- 出典：http://forum.cryptoeconomics.study/
- 出典：https://vitalik.ca/general/2018/03/28/plutocracy.html
- 出典：https://github.com/jpantunes/awesome-cryptoeconomics/blob/master/readme.md
- 出典：https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

ETHEREUMコミュニティ内の論争　①

- 流出したEthereum資金を取り戻すための標準策定にむけた提案EIP867（Ethereum Recovery Proposals (ERPs) ）を巡る議論

  - EIPに提案されたStandadized Ethereum Recovery Proposals(ERPs)は、ブロックチェーン上の資産が予期せず失われた場合の復元ルールを予め決めておこうとするもの。

  - 不当にユーザー資産を没収することにつながりかねないことを危惧されている。

  - 日本の刑法161条の2には、「人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に行った者は、五年以下の懲役又は五十万円以下の罰金に処する」とされ、銀行預金残高記録やプリペイドカードの残高記録などが該当するとされる。

  - 可逆的なブロックチェーンとすることは、その判断に際して中央集権的な管理につながるため、非中央集権性とのジレンマに陥ることから、2016年のTheDAO事案に端を発した、ハッキングやエラーによるユーザー資産喪失時にブロックチェーンが修正されるべきかの問題に、昨今のコインチェック事案やBitGrail事案を受けて、改めて焦点が当たっている。

→ 出典：https://github.com/ethereum/EIPs/issues/866
→ 出典：https://medium.com/@pirapira/my-attitude-on-protocol-changes-affecting-particular-ethereum-accounts-13e26d1f37b4
→ 出典：https://jp.cointelegraph.com/news/ethereum-code-editor-resigns-over-legal-concerns-for-ledger-amendment-proposal
→ 出典：https://github.com/ethereum/EIPs/pull/867#issuecomment-365800936
→ 出典：https://github.com/ethereum/EIPs/pull/867#issuecomment-365800936
→ 出典：https://btcnews.jp/299d4fzv15068/

ETHEREUMコミュニティ内の論争　②

- EIP999に伴うEthereumハードフォーク論議
  - 昨秋のParityウォレット凍結解決のために提案されたEIP999。
  - 過半数がハードフォーク賛成するも、Parityはチェーン分断意向無しを表明。

- Upgradeable smart contracts in Ethereum
  - コード中にはバグが混在していた場合に改ざん困難性が速やかな復旧の支障となってきた（TheDAOやParityWallet等）ことを踏まえて、「アップグレード可能なスマートコントラクト」を設けよう、という提案。

→ 出典：http://eips.ethereum.org/EIPS/eip-999
→ 出典：https://paritytech.io/our-commitment-to-ethereum-and-a-decentralised-future/

→ 出典：http://www.zohaib.me/upgradeable-smart-contracts-in-ethereum/

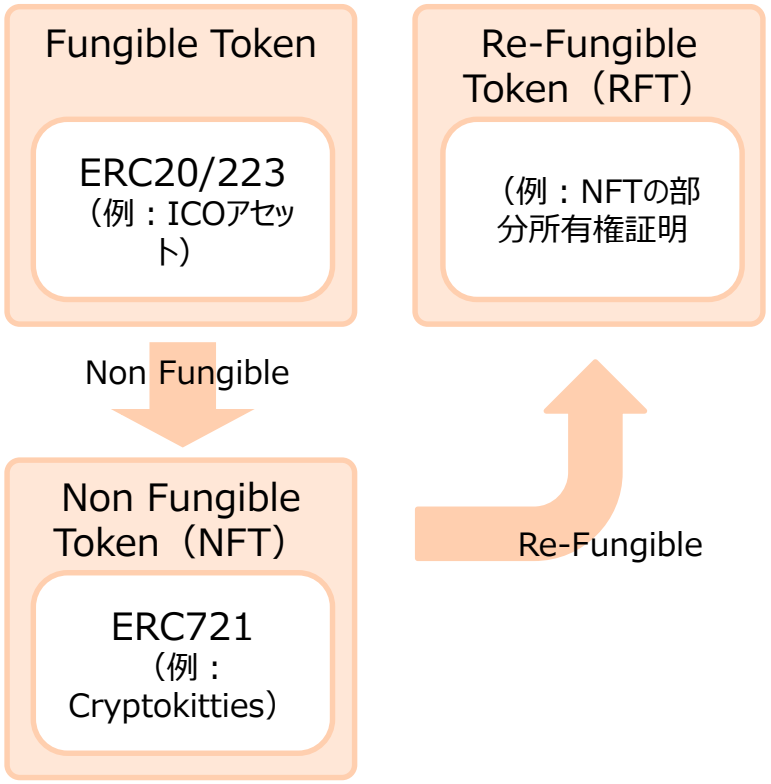
ETHEREUMへのエクリプス攻撃手法が論文に

- ブロックチェーンのネットワーク分断を図り、P2Pネットワークのコントロールを奪うエクリプス攻撃を、Ethereumネットワーク上で実行する方法に関する論文が示されたもの
  - 論文公開に先立ち、2018/1/9にこの攻撃についてEthereumへ開示されており、Geth v1.8.1にて解決済の事象。
  - BitcoinとEthereumの違いとして、Bitcoinにおけるエクリプス攻撃では、ノード接続を独占するために多くのIPアドレスコントロールが必要であり、攻撃者は大きなコストがかかる。これに対し、Ethereumでは僅か1-2台のマシンを用いて攻撃が可能な点がポイント。
    - この相違は、Bitcoinではノードがランダムに互いのコネクションを形成する「非構造ネットワーク」に依拠するのに対して、EthereumではKademliaと呼ばれる、ノードが他ノードと効率的に接続できるプロトコルに基づく「構造化ネットワーク」に依拠していることによる。そのため、いわば本攻撃は、ほとんどKademlia攻撃とも言えるもの。
    - 具体的には、EthereumのP2Pネットワーク中のノードは、公開鍵により識別される。ユーザーが無数のノードを実行できるようにしており、このとき異なる公開鍵を有するが、カギ生成アルゴリズムを用いると、攻撃者は無数のノードIDという識別子を高速で生成できてしまう。

→ 出典: https://bitcoinmagazine.com/articles/researchers-explore-eclipse-attacks-ethereum-blockchain/#1519922562
→ 出典: http://www.cs.bu.edu/~goldbe/projects/eclipseEth.pdf
→ 出典: http://ia.cr/2018/236

トークンのFUNGIBILITY

- トークンの表現力としては、ERC20/223のFungible Tokenが代表格で、最近はCryptokittiesが先鞭をつけたNon Fungible Token（ERC721）がトピックに。
  - Non Fungible Token(NFT)が再びFungibleなものになる「Re-Fungible Token(RFT)」とは、NFTのオーナーアドレスとしてERC20トークンを用いることによって、NFTを表す或る量のERC20トークンを保有するもの。
  - ERC20のインターフェースを通してトークン所有権を証明するのと同様に、NFTの”部分所有権”の証明が可能になる点がポイント。
  - ウォレットを使ってアドレスが或る量のRFTを保有しているかどうかをチェックしたり、元のNFTの”部分所有権”を検証したりできる。



→ 出典: https://medium.com/@billyrennekamp/re-fungible-token-rft-297003592769

STABLECOIN

- Stablecoinとは、市場価格のボラティリティを低く抑えるべく、特定資産とペグしたりスマートコントラクトでコントロールしたりすることを通じて価格安定を図るもの。
  - 例えばMakerによるDaiのように、他のトラストレスなアセットによりオンチェーンで裏付けられたStablecoinを作ることが考えられる。
  - この場合、裏付ける担保自身が、Decentralizedな暗号通貨通貨アセットであり、Daiではスマートコントラクト中の担保として保持されるETHにより裏付け。
  - この担保はスマートコントラクト中にトラストレスな形で保持されるため、ユーザは償還にあたりサードパーティを信頼する必要が無い。

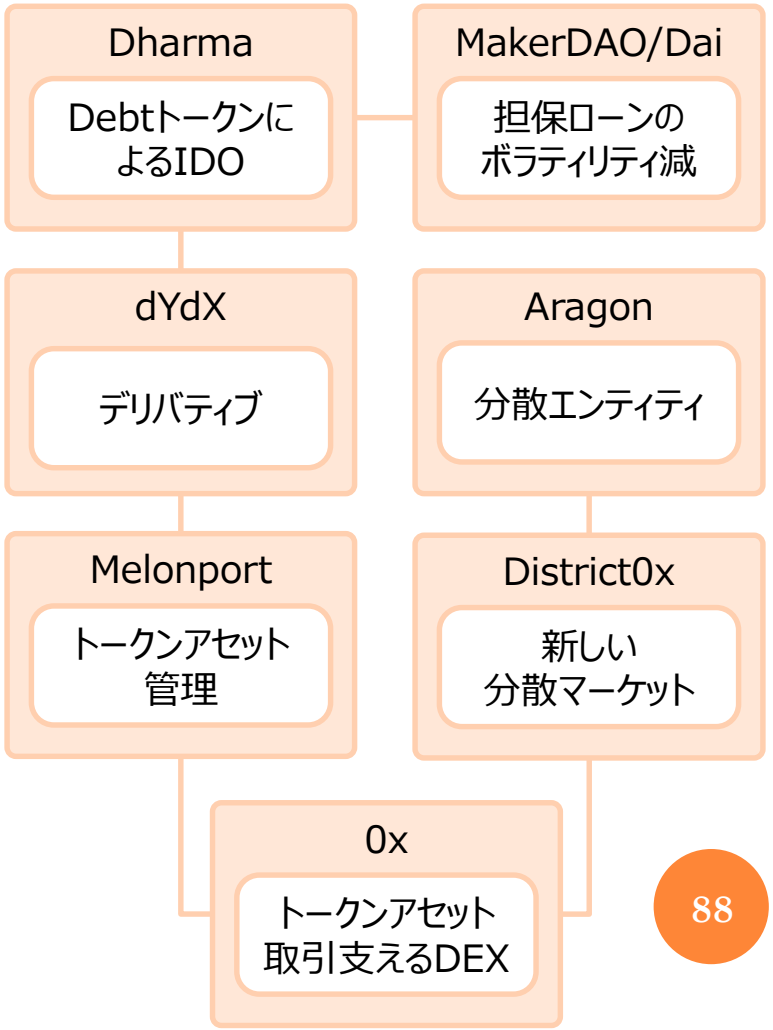
Tether	USDがTetherにより管理される口座へデポジットされると新規USDTトークン発行。逆にUSDが引き出されるとUSDTがburn
Dai	スマートコントラクト中の担保として保持されるETHにより裏付け
TrueUSD	エスクロー口座にてUSD担保
Basecoin	供給量をコントラクトでコントロール
Havven	Havven/nominのデュアルトークンエコシステムでトークン価格を安定させる
Abra	50種類の法定通貨とのリアルタイムスワップを通じたstablecoin技術による投資プラットフォームを発表

→ 出典: https://multicoin.capital/2018/01/17/an-overview-of-stablecoins/
→ 出典: https://www.trueusd.com/
→ 出典: http://www.getbasecoin.com/basecoin_explainer.pdf
→ 出典: https://havven.io/uploads/havven_whitepaper.pdf

分散金融システムと結びつく0x DAPPSコイン

- オープンな金融システム構築を目指すCoinbaseのグランドプランと、その元従業員が開発した0xプロトコルやdAppsによって、エコシステム形成が進んでいる。
  - 各種のdAppsが分散型金融商品を生み出し、ひいては自己統治を備える分散型金融業として結合していく未来が描かれてきている。
    - トークン化されたDebt商品をInitial Debt Offeringsとして提供するのがDharma。
    - これをデリバティブとして補完するのがdYdX。
    - 担保ローンに係る暗号通貨のボラティリティに対応するのがMakerのStablecoinであるDai。
    - 新しい分散マーケットを作るのがDistrict0x。
    - この上にマーケットを作る際のブロックチェーン上の管轄となるのがAragonの分散エンティティ。
    - これらトークン証券を最終的に投資ファンドとしてアセット管理するのがMelonport。
    - こうしたトークンアセット取引のマスアダプションを支えるのが0xのDEXプロトコルという位置づけ。

→ 出典：https://diar.co/volume-2-issue-13/



分散金融システムと結びつく0x DAPPSコイン

Bancor	• Bancorプロトコルは、暗号通貨コミュニティ向け流動性プロバイダー。 • 第1ステップとしてはEthereumネットワーク上のERC20トークンにフォーカスしている。 • トークンの流動性を確保するために、Bancorを準備通貨として用いて、スマートコントラクト内でBancor Reserve Ratioにより、トークン→Bancor或いはBancor→トークンの転換を仲介者無く可。 • 自動トークンコンバージョンをビルトインしたBancor Walletを発表。
Kyber Networks	• KyberはDEXプロトコル。分散レンディングのETHLendと統合を発表。
Dharma	• 0x上でのP2Pレンディングツール Dharma Plexを、アルファリリース。 • Dharma上に構築された債務relayer（借り手・貸し手をカストディ無しに接続することで流動性提供）であるBloqboardがテストネットローンチ。
Aragon	• 投票意思決定・組織中の持分表すトークン・透明性・個別パーミッション設定を提供するAragon Core、デジタル管轄域を構成するAragon Network、スマートコントラクトフレームを提供するAragon OS、の三つが主な構成要素。
Maker DAO	• 担保付債務ポジションCDPとDaiを発行するプロセスと、担保取戻し手数料とあわせDaiを返金するプロセスから成るので、アセットを担保にブローカーから借り、利子を付けて返すモーゲージローンと類似。
Gnosis	• 予測市場に必要なのは、公知イベント、網羅性ある結果選択肢、自動マーケットメーカ、イベント解決オラクルと公的検証可能性。 • 用途は、正確な情報を明らかにするインセンティブ提供、保険対象になる事象発生確率見積の他、「Futarchyなガバナンス」（プラスの効果を生むと見積る政策を法制化）。
aeternity	• state channel用いてオフチェーンで実行することによりスマートコントラクトをスケーラブルなものとし、信用のクラウドソーシングというブロックチェーンのパフォーマンスを引き出す。

- 出典: https://steemit.com/bancor/@bancor-network/bancor-s-new-product-roadmap-february-2018
- 出典: https://medium.com/@hichemfetoui/the-difference-between-token-relay-and-smart-token-in-bancor-protocol-97cbc729a99c
- 出典: https://blog.kyber.network/ethlend-integration-announcement-27e26a782fd0
- 出典: https://blog.dharma.io/introducing-dharma-plex-2b75eed2d45
- 出典: https://blog.bancor.network/hello-wallet-a635b5ff6c09
- 出典: https://blog.dharma.io/announcing-bloqboard-the-first-dharma-debt-relayer-58594041e123
- 出典: http://meetu.ps/e/F4TZl/m97z8/a
- 出典: https://blog.aeternity.com/how-smart-contracts-might-change-the-way-we-live-141f776a45cf

トークン分類フレーム

- トークンの性質に応じた分類フレームが数種類提案されている。

スイスFINMAの定義

ペイメントトークン	• 支払い手段として使われる
ユーティリティトークン	• アプリケーションやサービスへのデジタルアクセスを提供する目的とされる
証券トークン	• 証券規制に準拠するデジタルアセットで、従来型金融商品との交点に相当

Bravenewcoinの分類

既存のアセット	キャピタルアセット	エクイティ、債券、不動産収入	
	移転・消費可能アセット	コモディティ、貴金属	
	価値貯蔵アセット	現金、貴金属、アート	
クリプトアセット	汎用クリプトアセット（誰もが自由に使えるプログラム可能な価値）	ペイメントクリプトアセット	M2マネーサプライを捉えられる可能性のある汎用的マネーの形態。（Bitcoin等）
		プラットフォームクリプトアセット	P2P価値移転に限らず、高水準プログラミング機能を備える分散台帳（Ethereum等）
	プロトコルトークン（特定セグメントで価値貯蔵として移転・使用可能）	アプリケーショントークン	親チェーンにロックすることなく、その利用やマネタイズに関して用いられるDappsネイティブトークン（Gnosis等）
		サイドチェーン	親チェーン内に価値をロックすることで形成され、ペグ付けされた台帳へ送る（Gems等）

→ 出典：http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/
→ 出典：https://bravenewcoin.com/general-taxonomy-for-cryptographic-assets

証券トークン

- 証券トークンは、証券規制に準拠するデジタルアセットであり、デジタルアセット（トークン）と従来型金融商品の交点にあたるもの。
  - 「プログラム可能なオーナーシップ」と言える。
  - つまり、エクイティやデット、不動産といった、オーナーシップを持つアセットはどれもトークン化できる。
  - ユーティリティトークンと異なり、現実世界のアセットを裏付けに持つ点が特徴。
  - 企業や不動産のエクイティを裏付けに持つため、暗号通貨価値とは別に、目に見える・法定通貨で計測可能な価値を有する。

利点	• 投資トランザクションから仲介人を取り除くことによって、手数料低減・取引高速化・サービス自動化・市場操作回避などといった形で従来型金融商品への改善が可能 • 多数の参加者が小額エクイティを保有することを可能とすることによって、投資家や起業家による投資へのアクセスを民主化できる
欠点	• 仲介人を不要とする反面、仲介人の果たしてきた責任が買い手・売り手へ転嫁される • 例えば、ディールの引き受け・投資家の勧誘・規制遵守など • こうした機能を、多くの証券トークン発行者は従来型金融機関無しには成功裏に遂行できない可能性が指摘

Prometheum	https://www.prometheum.info/
Templum	https://www.tradetemplum.com/
Harbor	https://harbor.com/

→ 出典：https://medium.com/@apompliano/the-official-guide-to-tokenized-securities-44e8342bb24f
→ 出典：https://worldview.stratfor.com/article/security-tokens-where-digital-assets-meet-real-world

トークン関連トピック　①

- GasToken
  - https://gastoken.io/
  - EthereumのGasをトークン化することで、Gas価格が安価なうちにGasを蓄えておき、価格上昇時にリリースすることで差額で安価な手数料を享受できるという、アービトラージなERC20トークンとのこと。
  - Gas価格高騰対策として、GasBankingのようなことも可能に。

- ICOではないInitial Loan Procurements (ILPs)
  - https://www.careyolsen.com/briefings/goodbye-icos-hello-ilps
  - ILPは法的拘束力持つスマートコントラクトを使い負債者と債権者がローン契約。
  - 債権者の投資は企業業績と契約的に紐付き、業績をあげている限り年次リターンを得られるとのこと。
  - エストニアのBlockhiveとAgrelloが初のILP提供とのこと。

トークン関連トピック　②

- MyEtherWallet、一部DNSサーバーハイジャックに遭う
  - http://coinpost.jp/?p=23783
  - https://japan.zdnet.com/article/35118344/
  - MyEtherWalletサービス自体の問題ではなく、AmazonのDNSサーバーであるRoute53への経路上で通信ハイジャックされたことによるものであることに留意要。
  - ユーザーの通信がフィッシングサイトに誘導され、ウォレットの秘密鍵などが被害に遭ったもの。
  - こうしたDNSサーバーの被害を受けたケースとしては、2017年にEtherdeltaのケースがある。

- ERC20準拠のトークンコントラクトに、batchOverflow脆弱性問題
  - http://blockchain.gunosy.io/entry/erc20-token-Vulnerability
  - https://medium.com/@peckshield/alert-new-batchoverflow-bug-in-multiple-erc20-smart-contracts-cve-2018-10299-511067db6536
  - https://medium.com/@peckshield/integer-overflow-i-e-proxyoverflow-bug-found-in-multiple-erc20-smart-contracts-14fecfba2759
  - ERC20準拠処理ではない、独自拡張されたbatchTransfer関数で起きた脆弱性問題であるとのこと。
  - 当該関数を含まないERC20トークンであれば問題無し。
  - よって、こちらも、Ethereum自体の課題でもなければ、コントラクトトークンならびにERC20自体の課題でもないということ。
  - 今回の場合、算出処理におけるオーバーフローが発生し、特定アカウントのトークン量を膨大に増やすことでトークン価値の毀損に繋がる。
  - 算出処理であればzeppelin-solidityのセキュリティライブラリであるSafeMath.solなどのように、品質の担保されたコードを利用することが必要だという示唆。

DEX関連読み物

- Web3 Foundation: Decentralized Exchange Meetup, 24 JAN 18 - Berlin
  - https://youtu.be/hwfEH5XkBw8
- Decentralized Exchanges Workshop Outcomes
  - https://medium.com/@web3/decentralized-exchanges-workshop-outcomes-4753dbd86f2b
- DEX Projects Breakdown Spreadsheet
  - https://docs.google.com/spreadsheets/d/1H7_w7kazjFmXzeo6nU0TTRSpF9mvQI8dP1X3WFfIb_Q/htmlview
- Step-By-Step Guide to Radar Relay with Ledger
  - https://cryptospaceguides.com/radar-relay-guide/
- Upgrades to our Atomic Swap Wallet (and what to expect next)
  - https://blog.altcoin.io/upgrades-to-our-atomic-swap-wallet-and-what-to-expect-next-3d6b2a1f4ec6
- Governance in 0x Protocol
  - https://blog.0xproject.com/governance-in-0x-protocol-86779ae5809e
- Goodbye Centralisation. Hello Dex on Ocean Protocol.
  - https://medium.com/dex-sg/goodbye-centralisation-hello-dex-on-ocean-protocol-853a6915ad0d
- MIT Bitcoin Expoでの0xスライド
  - https://docs.google.com/presentation/d/1QoLokBKzLSfuXTrAi6lENqokS9KP5KP3UZzzjh0eAYs/mobilepresent?slide=id.p19
- 0xエコシステムのRelayerレポート
  - https://blog.0xproject.com/relayer-report-1-48263bbc745f
- 0x Relayerの用途、18種が挙げられている
  - https://blog.0xproject.com/18-ideas-for-0x-relayers-in-2018-80a1498b955f

3. Startup/Dapps系

3-1. プラットフォーム分野
3-2. ライフスタイル分野
3-3. シビックテック分野
3-4. 金融分野

オーバービュー

※今回紹介分から領域別に該当分を例示したもの」

マーケット	**教育** ODEM	**旅行** WindingTree	**不動産** imbrex	**スキル** skyllz	**エネルギー** ImpactPPA
サービス商流	**小額寄付** nanotip	**小額API** paypercall	**ゲーム** ETHEROBOTS		
情報流	**パーソナルデータ** VALID	**知財** COALA IP	**医療データ** LIFEX	**メディア** Y'alls	
組織運営	**DAOﾌﾟﾗｯﾄﾌｫｰﾑ** Aragon	**アイデンティティ** Civic	**投票** Agora	**バウチャー** Bounty0x	**ﾅﾚｯｼﾞｷｭﾚｰｼｮﾝ** Kauri
カネの流れ	**小額課金** LightningCharge	**貸付** ETHLend	**投資** 22xFund	**保険** Ethrisc	**デリバティブ** dYdX
カネ	**証券トークン** Harbor	**Stablecoin** TrueUSD	**ウォレット** Trust	**トレードDEX** IDEX	**カード** TenX
台帳	**リソース提供** Dfinity	**Statechannel** Counterfactual	**Dappsｻｲﾄﾞﾁｪｰﾝ** LoomNetwork	**Sharding** Zilliqa	

3-1) プラットフォーム分野
A) コンピューティングリソース

名称	サービス概略	URL
Dfinity	ブロックチェーン上でクラウドコンピューティングを組み合わせてホスティングすることで計算能力向上	→ https://dfinity.org/pdf-viewer/pdfs/viewer?file=../library/dfinity-consensus.pdf
Render Token	分散GPUレンダリングネットワーク・マーケットプレイス	→ https://www.rendertoken.com/
GasToken.io	Ethereumネットワーク上のGasをトークン化し、高いときにトークンをGasに充当するサービス	→ https://gastoken.io/
Arithmetica	数学計算むけ協働プラットフォーム	→ https://arithm3tica.github.io/project-info/
RightMesh	ワイヤレスメッシュネットワーク	→ https://www.rightmesh.io/
Hypernet	コンピューティングパワー接続	→ https://hypernetwork.io/

3-1) プラットフォーム分野
B) データ管理

名称	サービス概略	URL
VALID	ブロックチェーンベースのパーソナルデータ管理	→ https://valid.global/
COALA IP	コミュニティドリブンの知財ライセンシングプロトコル	→ https://www.coalaip.org/
Datachain	DMPにブロックチェーンを活用したデータ流通	→ https://datachain.jp/
Truset	Ethereum上でクリティカルなデータの収集・検証・共有	→ https://www.truset.com/
Thought Network	ブロックチェーンを用いてAIをデータに埋め込みネットワーク化	→ https://thought.live/

3-1) プラットフォーム分野
C) DAO

名称	サービス概略	URL
Aragon	分散組織ガバナンスプラットフォーム	→ https://aragon.one/
doGood	リーンスタートアップ向けソーシャルプラットフォーム	→ https://dogood.io/
DAOstack	分散ガバナンスの議論フォーラム	→ https://daostack.io/
SportsDAO	群衆知＆クリプトエコノミクスを応用してスポーツフランチャイズのインセンティブ改善（チームパフォーマンス向上に資する意思決定）	→ https://medium.com/@rzurrer/sportsdao-a-self-governing-meritocratic-decentralized-autonomous-organization-that-leverages-2dffac175b52
Kleros	仲裁クラウドソーシング結果をスマートコントラクトとして執行するサービス	→ https://kleros.io/
FOAM	コンセンサスドリブンの世界地図	→ https://foam.space/publicAssets/FOAM_Whitepaper_May2018.pdf
Wings	DAOプラットフォーム	→ https://www.wings.ai/

3-1) プラットフォーム分野
D) スマートコントラクト

名称	サービス概略	URL
witnet	スマートコントラクトを外部データソースと接続	→ https://witnet.io/#/
Chainspace	高速なスマートコントラクトプラットフォーム	→ http://chainspace.io/
witnet	スマートコントラクトと外部データの接続	→ https://witnet.io/#/

3-1) プラットフォーム分野
E) アイデンティティ

名称	サービス概略	URL
Civic	分散アイデンティティシステム	→ https://www.civic.com/
Alastria	Quorumベースのセルフソブリンアイデンティティシステム	→ https://alastria.io/index_en.html
Evernym	イリノイ州でパイロットを行っているデジタルアイデンティティシステム	→ https://www.evernym.com/
Sovrin	分散アイデンティティシステム	→ https://sovrin.org/
EDDITS	既存のデジタルアイデンティティをERC725アイデンティティに紐付け	→ https://eddits.io/
Leverj	ハードウェアウォレットサポート付き分散アイデンティティ	→ https://leverj.io/
DID AUTH	分散型個人ID	→ https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/draft-documents/did_auth_draft.md

3-1) プラットフォーム分野
F) BaaS

名称	サービス概略	URL
Counterfactual	汎用State Channelオープンフレームワーク	→ https://counterfactual.com/
Loom Network DAppChain	ゲーム・ソーシャルアプリ向けスケーリングを特徴とし、サイドチェーン上でDapp稼働するプラットフォーム	→ https://loomx.io/
Chimaera	ゲーム向けにオフチェーンでGame Channelsを実装しスケーリング	→ https://chimaera.io/
Zilliqa	Sharding利用しハイスループットを目指すプラットフォーム	→ https://www.zilliqa.com/
Perun Network	Ethereum上のペイメント&ステートチャネル	→ https://www.perun.network/ → https://eprint.iacr.org/2017/635
Hedera Hashgraph	新しい分散コンセンサスでスケーリングを目指すプラットフォーム	→ http://www.hederahashgraph.com/
DAGlabs	BlockDAGのプラットフォーム	→ https://www.daglabs.com/
bloXroute	スケーラブルなトラストレス・ブロックチェーン伝播ネットワーク	→ https://bloxroute.com/wp-content/uploads/2018/03/bloXroute-whitepaper.pdf
Algorand	スケーラブルなデジタル通貨高速ペイメントプラットフォーム	→ https://www.algorand.com/
Sirin	Dapps利用やコールドウォレット搭載のブロックチェーンスマホ	→ http://coinpost.jp/?p=24827

3-2) ライフスタイル分野
A)バウチャーコラボレーション

名称	サービス概略	URL
SureRemit	世界中へデジタルバウチャーを送付可能なプラットフォーム	→ https://sureremit.co/
Bounties Network	トークンベースの報奨金によるコラボレーション	→ https://bounties.network/
Bounty0x	タスク完遂と引き換えにトークンを受け取れる報奨金ハンター向け分散労働力・リワードモデルのプラットフォーム	→ https://bounty0x.io/

3-2) ライフスタイル分野
B)メディア

名称	サービス概略	URL
Current	マルチメディアストリーミングプラットフォーム	→ https://current.us/
Y'alls	Lightning Networkマイクロペイメントによる記事の読み書きサービスとしてメインネットローンチ	→ https://mainnet.yalls.org/
Lightning Publisher for WordPress	Lightning Chargeを用いてブログのプレビューを依頼した人へLNによる支払いを行うLapps	→ https://github.com/ElementsProject/wordpress-lightning-publisher/blob/master/README.md
Peepeth	分散型マイクロブログ	→ https://peepeth.com/welcome
Social X	コミュニティドリブンのソーシャルメディア	→ https://socialx.network/
ONG Social	分散ソーシャルネットワーク	→ https://ong.social/
モナバコ	質問者がモナコインを付けて質問できるQ&Aサービス	→ https://monabako.com/#/
Kauri	ConsenSysの技術ナレッジキュレーションインフラ	→ https://media.consensys.net/the-kauri-stack-bd8ba05a845c → https://kauri.io/
Gitcoin	ハードウェアからネットワークそしてデータ層へと進むオープンソースにおける、インセンティブを解決しようとするもの	→ https://medium.com/gitcoin/open-source-money-will-buidl-the-open-source-ecosystem-f4169def8748

3-2) ライフスタイル分野
B)流通・マーケットプレイス

名称	サービス概略	URL
BLOCKv	デジタルオブジェクトを地図やゲーム上にドロップ&シェア	→ https://blockv.io/documents/whitepaper.pdf
vAtomic	デジタルオブジェクト向けデリバリープラットフォーム	→ https://www.vatomic.io/
Filebazaar	Lightning Chargeを用いてデジタルファイルを売買するLapps	→ https://github.com/ElementsProject/filebazaar/blob/master/README.md
ODEM	分散教育マーケットプレイス	→ https://odem.io/
Winding Tree	分散型旅行流通	→ https://windingtree.com/
imbrex	不動産データマーケットプレイス	→ https://imbrex.io/
Skyllz	スキルのバリデーションプロトコル	→ https://skyllz.org/
Indorse	プロフェッショナルネットワーク	→ https://indorse.io/

3-2) ライフスタイル分野
C)マイクロペイメント

名称	サービス概略	URL
nanotip	Lightningインボイスを生成して少額寄付を受け付けるWebサーバ	→ https://github.com/ElementsProject/nanotip/blob/master/README.md
paypercall	HTTP APIむけにコールあたり課金	→ https://github.com/ElementsProject/paypercall/blob/master/README.md
nanopos	Lightning Charge用いたPOSシステム	→ https://github.com/ElementsProject/nanopos/blob/master/README.md
FTTT	Lightning インボイスをトリガーとしてアクション起動するアプレット開発を可能に	→ https://github.com/ElementsProject/ifpaytt/blob/master/README.md
Lightning Jukebox	YouTubeの歌・動画をマイクロペイメントでリクエスト	→ https://github.com/ElementsProject/lightning-jukebox/blob/master/README.md

3-2) ライフスタイル分野
D)ゲーム

名称	サービス概略	URL
ETHERBOTS	パーツを集めてロボットで戦うゲームDapps	→ https://etherbots.io/
CryptoCities	街の収集・トレードゲーム	→ https://cryptociti.es/
CryptoCup	ERC721トークンを用いたワールドカップ予想ゲーム	→ https://www.cryptocup.io/
EthernalGo	ブロックチェーン上での囲碁ゲーム	→ https://www.ethernalgo.com/#/
Ethmoji	ERC721トークンによるアバター生成	→ https://ethmoji.io/
Cryptocup	ワールドカップの予測ゲーム	→ https://cryptocup.io/landing
Game of blocks	戦略型ボードゲーム	→ https://www.gameofblocks.io/
くりぷ豚	ブタのキャラクターの収集・交配・売買ゲーム	→ https://prtimes.jp/main/html/rd/p/000000006.000021504.html

3-3) シビックテック分野
A) 医療

名称	サービス概略	URL
Medical Chain	Hyperledger Fabric用いて仮想通貨払いの遠隔医療	→ https://medicalchain.com/ja/
Healthureum	医療データの安全な管理むけサービス	→ http://www.healthureum.io/
LIFEX	トークン導入により研究者は医療ビッグデータを受け取り、トークン保持者が新規医療サービス享受のインセンティブとすることで医療費増加課題に取り組むサービス	→ https://lifex.bio/
Shivom	遺伝子データを研究むけに提供するユーザーへ報酬を与えるプラットフォーム	→ https://shivom.io/

3-3) シビックテック分野
B) 投票

名称	サービス概略	URL
Agora	デジタル民主主義むけ投票システム	→ https://agora.vote/ → https://agora.vote/Agora_Whitepaper_v0.1.pdf
Polys	Kaspersky Labによる投票プラットフォーム	→ https://polys.me/polys.me

3-3) シビックテック分野
C) エネルギー

名称	サービス概略	URL
ImpactPPA	分散エネルギープラットフォーム	→ http://impactppa.com/
Volt Markets	Ethereum上のP2Pエネルギー取引プラットフォーム	→ https://voltmarkets.com/
Energy Web Foundation	PoA且つシークレットトランザクション及びWebAssembly備えたEnergy Webのベータ版をテストネットローンチ	→ https://energyweb.org/2018/04/17/energy-web-foundation-unveils-major-blockchain-milestones-at-event-horizon/

3-4) 金融分野
A) トークントレード・DEX［1/2］

名称	サービス概略	URL
トークントレーダー	ERC20トークンを、取引所のトークンを預けずにエンドユーザ同士でトレードできるスマートコントラクトサービス	→ https://guide.blockchain.z.com/ja/docs/oss/token-trader/
クリプトカード	デジタルアセット流通プラットフォーム	→ http://www.consensus-base.com/info/cryptocards-2018-4-3/
ZooMeX	0xプロトコルを利用したDEXサービス	→ https://zoomex.fun/help → https://zoom-blc.com/what-is-zoomex
Gibraltar Blockchain Exchange	ブロックチェーンベースのトークン・デジタルアセット交換所	→ https://gbx.gi/
Amadeus Relay	Dapps向け0xリレイヤー	→ http://amadeusrelay.org/
Hodl Hodl	法定通貨とビットコインをエスクローを使って交換できるサービス	→ https://testnet.hodlhodl.com/
IDEX	ERC20トークンむけDEX	→ https://idex.market/eth/aura → https://idex.market/static/IDEX-Whitepaper-V0.7.5.pdf

3-4) 金融分野
A) トークントレード・DEX［2/2］

名称	サービス概略	URL
Tabby Pay	間違ったアドレスにetherを送付したときにキャンセル可能なエスクローコントラクト	→ https://tabby.io/
Block Collider	バリデータ無しにBTC/ETH間などのクロスチェーントランザクションを行うプロトコル	→ https://www.blockcollider.org/
Oasis Direct	インスタントDEXサービス	→ https://oasis.direct/
ALTTEX	DEXとクリプトメッセンジャーを備えたデジタルプラットフォーム	→ https://alttex.io/
BarterDEX	アトミックスワップによるDEX	→ https://komodoplatform.com/decentralized-exchange/
Commonwealth Crypto	交換業者のオーダーブックを用いてオフチェーン取引	→ https://www.commonwealthcrypto.com/
Ocean X	分散トレーディングプラットフォーム	→ https://theoceanx.com/

3-4) 金融分野
B) STABLECOIN

名称	サービス概略	URL
Saga	IMFのSDRにペグした低ボラティリティの暗号通貨	→ https://saga.org/
TrueUSD	エスクロー口座にてUSD担保するstablecoin	→ https://www.trueusd.com/
Basecoin	供給量をコントラクトでコントロールするstablecoin	→ http://www.getbasecoin.com/ → http://www.getbasecoin.com/basecoin_explainer.pdf
Havven	Havven/nominのデュアルトークンエコシステムでトークン価格を安定させるstablecoin	→ https://havven.io/ → https://havven.io/uploads/havven_whitepaper.pdf
Carbon	Hedera Hashgraghによる Stablecoin	→ https://www.carbon.money/
Digital Trade Coin	MITによるリザーブ通貨	→ https://tradecoin.mit.edu/mit-digital-tradecoin

3-4) 金融分野
C) 証券トークン

名称	サービス概略	URL
Harbor	証券トークンの発行・トレードむけプラットフォーム	→ https://harbor.com/
Prometheum	規制対応証券トークン	→ https://www.prometheum.info/
Templum	規制対応証券トークン	→ https://www.tradetemplum.com/
Harbor	規制対応証券トークン	→ https://harbor.com/
tZERO	Simple Agreements For Equity(SAFEs) 締結予定のトークンセール	→ https://www.tzero.com/
Polymath	証券トークンの発行プラットフォーム	→ https://www.polymath.network/

3-4) 金融分野
D) ウォレット

名称	サービス概略	URL
Trust	ERC20・ERC223トークン向けウォレット	→ https://trustwalletapp.com/
Eclair Wallet	Lightning Network向けAndroidウォレット	→ https://github.com/ACINQ/eclair-wallet
Atomicwallet	アトミックスワップをビルトインした軽量マルチアセットウォレット	→ https://atomicwallet.io/
Pigzbe	子供むけウォレットとゲーム感覚を組み合わせたファミリーむけプラットフォーム	→ https://www.pigzbe.com/

3-4) 金融分野
E) 投資

名称	サービス概略	URL
22xFund	スタートアップへのポートフォリオ投資トークン	→ https://www.22xfund.com/
Bnk to the future	オンライン投資プラットフォーム	→ https://bnktothefuture.com/
Circle Invest	リテール投資家むけ投資アプリケーション	→ https://www.circle.com/en/invest
Tradingene	トレーディングアルゴリズムのマーケットプレイス	→ https://tradingene.io/
Inpactor	CSR投資インセンティブを可視化するプラットフォーム	→ https://csr.inpactor.com/
icohub	ICO評価システム	→ https://www.hubtoken.org/images/icohub-one-pager.pdf
Pangea	ConsenSysによる不動産投資（シェアリングプロパティ）プラットフォーム	→ http://www.pangea.io/home → https://www.cnbc.com/2018/03/19/own-shares-of-brooklyn-building-with-tokens-blockchain-real-estate.html

3-4) 金融分野
F) デリバティブ、貸付、保険

名称	サービス概略	URL
dYdX	分散デリバティブ。空売りや買いのレバレッジをサポートする信用取引プロトコルを発表	→ https://medium.com/dydxderivatives/announcing-margin-trading-with-dydx-71e0485e85b0
Decentralized Derivatives Association	Ethereum mainnet上の分散型デリバティブコントラクト(DDA)	→ http://drct.decentralizedderivatives.org/
VariabL	トラストレスデリバティブ	→ https://variabl.io/
Sweetbridge	暗号アセット貸付サービス	→ https://sweetbridge.com/
Jibrel Network	投資家が金融アセットをトークン化して売却するレンディング	→ https://jibrel.network/
ETHLend	分散P2Pレンディング	→ https://ethlend.io/en/
Trusted Lending Circle	グループ内での貸付サービス	→ https://tlc.wetrust.io/
Bloom	分散型クレジットスコアリング	→ https://bloom.co/
Etherisc	非中央集権型保険をプエルトリコのハリケーン向けに開発	→ https://www.cryptoninjas.net/2018/04/24/etherisc-to-host-first-blockchain-based-hurricane-insurance-policy-in-puerto-rico/amp/

3-4) 金融分野
G) カード

名称	サービス概略	URL
TenX	暗号通貨をどこでも使えるようにするデビットカード	→ https://www.tenx.tech/
Monaco	複数の暗号通貨を使えるVISAデビットカード	→ https://mona.co/
COMIT	暗号学的にセキュアなオフチェーンでのマルチアセット即時トランザクションを行うネットワーク（クロスチェーン相互運用）	→ http://www.comit.network/

4. 規制関連の動向

- コインチェック事案続報
① 国・地域別の概況
② 規制・制度
③ 暗号通貨アダプション
④ ICO
⑤ 中央銀行・デジタル法定通貨

コインチェック事案続報 ①

日付	トピック	URL
1/26	事案発生、記者会見実施	→ http://corporate.coincheck.com/2018/01/26/29.html
1/29	関東財務局、コインチェックに対する行政処分を発表	→ http://kantou.mof.go.jp/rizai/pagekthp0130000001_00004.html
〃	金融庁、コインチェックに対する行政対応について記者説明を実施	→ https://bitpress.jp/news/market/entry-7620.html
〃	金融庁、全取引所を対象に仮想通貨システムを緊急調査	→ https://www.nikkei.com/article/DGXMZO26264470Z20C18A1000000/
2/2	金融庁、コインチェックに立ち入り検査	→ https://www3.nhk.or.jp/news/html/20180202/k10011312571000.html
2/7	対象NEMをDASHとの交換企てる動き	→ http://www.itmedia.co.jp/news/articles/1802/07/news086.html
〃	Binanceで長時間にわたりシステム障害でオフラインとなる状況発生	→ https://www.linkedin.com/pulse/binance-incident-recap-changpeng-zhao
2/8	金融庁、他の仮想通貨交換業者にも立入検査へ	→ https://www3.nhk.or.jp/news/html/20180208/k10011320101000.html
2/9	金融庁・警察庁・消費者庁、コインチェック事案で局長級連絡会議開催	→ http://www.fsa.go.jp/news/29/20180209.html
〃	コインチェック、2/13より日本円出金再開と発表	→ http://corporate.coincheck.com/2018/02/09/38.html

コインチェック事案続報 ②

日付	トピック	URL
2/10	金融庁、仮想通貨交換業者「みなし業者」営業に期限設定へ	→ https://this.kiji.is/334954609523557473
〃	金融庁、無登録の仮想通貨交換業者へ警告	→ https://www.nikkei.com/article/DGXMZO26791440Q8A210C1MM8000/
〃	警視庁、流出したNEMの一部を他暗号通貨と交換した日本人男性を聴取	→ http://news.tbs.co.jp/sp/newseye/tbs_newseye3289370.htm
〃	イタリアの仮想通貨交換業者BitGrailでトークンNano（Coinmarketcap24位。リブランド前の名称はRaiBlocks）が170億円相当不正流出	→ https://www.wsj.com/articles/cryptocurrency-worth-170-million-missing-from-italian-exchange-1518241679
2/13	コインチェック、金融庁へ業務改善報告を提出	→ http://corporate.coincheck.com/2018/02/13/39.html
〃	コインチェック、出金申請に基づく日本円の振込を開始。初日の出金総額は401億円	→ http://corporate.coincheck.com/2018/02/13/40.html
〃	コインチェック、記者会見を実施し、事業継続規模の意思を表明	→ http://coinpost.jp/?p=14334
2/14	金融庁、仮想通貨交換業「みなし業者」15社に集中立ち入り検査を通じて六月頃までに登録可否判断する方針	→ https://www.jiji.com/jc/article?k=2018021401319&g=eco

コインチェック事案続報 ③

日付	トピック	URL
3/11	Binance、3/7に受けたフィッシング攻撃のクラッカー逮捕に繋がる情報提供に25万ドルの報奨金	→ https://support.binance.com/hc/en-us/articles/360001615252-Binance-Hacker-Bounty
3/12	コインチェック、一部仮想通貨の出金、売却再開	→ http://corporate.coincheck.com/2018/03/12/48.html
〃	コインチェック、不正に送金されたNEMの保有者に対する補償について発表	→ http://corporate.coincheck.com/2018/03/12/47.html
3/18	NEM財団、コインチェックから流出したXEMの追跡用モザイクの送信を停止	→ https://medium.com/nemofficial/coincheck-hack-update-removal-of-mosaic-tagging-system-18b4157ff060
3/22	コインチェック含む交換業者７社、金融庁へ改善計画提出	→ http://corporate.coincheck.com/2018/03/22/49.html → https://www.sankeibiz.jp/business/news/180322/bse1803222206003-n1.htm
3/23	金融庁、Binanceに対して警告。一方でBinanceのマルタ拠点開設に対してマルタ首相は歓迎の意向	→ https://www.fsa.go.jp/policy/virtual_currency02/Binance_keikokushilyo.pdf → https://www.bloomberg.com/news/articles/2018-03-23/the-world-s-biggest-cryptocurrency-exchange-is-moving-to-Malta
3/29	ミスターエクスチェンジおよび東京ゲートウェイ、仮想通貨交換業の申請取り下げを発表	→ https://blog.mr.exchange/2018/03/29/news02/ → https://www.tokyogw.com/cont_info.php?id=18
〃	登録全16社加盟の日本仮想通貨交換業協会が発足	→ https://www.nikkei.com/article/DGKKZO28990400U8A400C1EE9000/

コインチェック事案続報 ④

日付	トピック	URL
4/2	金融庁、法改正視野に制度見直し議論へ	→ https://www.nikkei.com/article/DGXMZO28886310S8A400C1EE9000/
4/3	コインチェック支援要請にマネックスが買収案提示	→ https://r.nikkei.com/article/DGXMZO28923080T00C18A4MM0000
4/5	コインチェック、マネックスの出資受け入れる方針固める	→ https://www.nikkei.com/article/DGXMZO29027380V00C18A4MM0000/
〃	金融庁、コインチェックの業者登録容認へ	→ https://www.nikkei.com/article/DGXMZO29043790V00C18A4EE9000/
4/6	マネックス、コインチェックを完全子会社化と発表し共同記者会見	→ http://file.swcms.net/file/monexgroup/jp/news_release/auto_20180405405861/pdfFile.pdf → http://corporate.coincheck.com/2018/04/06/51.html → https://logmi.jp/277569
〃	金融庁、みなし登録業者三社へ行政処分発表	→ https://www.fsa.go.jp/policy/virtual_currency02/index.html
4/8	金融庁、登録業者に対する立ち入り検査実施へ	→ https://www.nikkei.com/article/DGXMZO29128870X00C18A4MM8000/

コインチェック事案続報 ⑤

日付	トピック	URL
4/16	コインチェック、新経営体制発足。併せて補償金の課税についても当局確認結果を発表	→ http://corporate.coincheck.com/2018/04/16/53.html → http://corporate.coincheck.com/2018/04/16/54.html
4/17	Kraken、日本居住者むけ仮想通貨交換業サービス廃止を発表	→ https://support.kraken.com/hc/ja/articles/360000570486
4/23	日本仮想通貨交換業協会、正式発足	→ http://jp.techcrunch.com/2018/04/23/launching-cryptocurrency-self-reguration-organization/ → https://bitpress.jp/news/market/entry-8612.html

①国・地域別の概況 – オーバービュー [1/3]

地域	国	トピック抜粋
日本		• 外為法改正案、仮想通貨の国際送金に報告義務　パブコメ募集も開始 • 金融庁、ICO規制を検討
北米	米国	• 米CFTC元委員長で現MITのGensler氏、ETHおよびXRPの証券性に言及 • Google、Twitter、Facebook、ICOや暗号通貨に関するプロモーションを禁止へ
〃	カナダ	• オンタリオ州規制当局、カナダ初のブロックチェーンETFを承認
欧州	フランス	• 仏AMF、ICOを合法的投資手段とする規制枠組を準備 • 小口の暗号通貨投資に係る税率低減検討
〃	ドイツ	• 独BaFin、ICOおよびトークン規制に関するステートメント発行
〃	イギリス	• 英FCA、暗号通貨は通貨やコモディティにあたらないが暗号通貨デリバティブは金融商品との見方 • 英政府、クリプトアセットタスクフォースをBoEやFCAと協働で設立
〃	スペイン	• ブロックチェーン関連企業やICO発行者の誘致へ向けた税制優遇を検討
〃	オランダ	• オランダ法廷、ビットコインを「移転可能な価値」との判断示す
〃	スイス	• スイス規制当局FINMA、ICOむけガイドライン発表 • Bitfinex、スイスZugへの移転を計画
〃	リヒテンシュタイン	• ブロックチェーンへの過度な規制は回避する方針と首相が表明
〃	マルタ	• 暗号通貨およびICOに関する規制枠組示す議案承認 • 香港Binance、Okexが拠点開設
〃	バミューダ	• 暗号通貨産業振興へむけて規制ドラフトを起案 • Binance、バミューダにグローバルコンプラセンター開設とあわせて15mドルの投資表明
〃	ロシア	• BRICSおよび欧州経済連合諸国による単一仮想通貨を構想 • ロシア～トルコ間の3000トンの小麦輸送でビットコイン決済
〃	ベラルーシ	• 暗号通貨を扱う新会計基準を採択し、暗号通貨フロンティアをサポートへ

①国・地域別の概況 – オーバービュー [2/3]

地域	国	トピック抜粋
アジア	中国	• 海外ネットワークを介した暗号通貨トレード禁止へ規制強化 • 中国人民銀行総裁、暗号通貨を決済手段として認めず • 中国投資協会、ブロックチェーンの投資・開発センター立ち上げへ
〃	韓国	• 規制当局、通常の暗号通貨トランザクションはサポートする旨を表明 • 昨秋からのICO禁止に関する緩和を検討
〃	台湾	• 既存AMLルールのもとにビットコイン規制へ
〃	タイ	• 金融当局、国内での暗号通貨利用を規制せず
〃	インドネシア	• 暗号通貨デジタルルピアの試行を計画
〃	フィリピン	• 暗号通貨事業者優遇地域の開発を検討
〃	カンボジア	• 米国による経済制裁の中で、ベネズエラ・トルコ・イランに続いて独自仮想通貨Entapay発行検討
〃	インド	• RBI、銀行が暗号通貨関連の個人・企業と取引することを禁止 • 中央銀行による暗号通貨禁止に対して交換業界から請願書
〃	シンガポール	• MAS、暗号通貨取引禁止の理由無しと表明
〃	豪州	• 豪州当局ASIC、既存ガイドラインをICO向けに拡張の意向示す • ブリスベン空港、空港内店舗でのBTC/ETH/DASHペイメント受付
中東	イスラエル	• 当局、ユーティリティトークンと証券トークンの定義。ビットコインは証券と扱わず
〃	イラン	• イラン中央銀行、暗号通貨取引を禁止 • 独自ローカル暗号通貨を実験的に開発
〃	UAE	• 規制当局SCA、投資家に対してICOへの警戒呼びかけ
〃	サウジアラビア	• サウジアラビア中央銀行、Rippleを用いたクロスボーダーペイメントのパイロット

①国・地域別の概況 – オーバービュー [3/3]

地域	国	トピック抜粋
アフリカ	南アフリカ	• 南アフリカ歳入庁（SARS）、暗号通貨に係る税金取扱方針を提示
南米	ベネズエラ	• 原油資産を裏付けとしたERC20トークンPetroを発行するICO • Petro用いてロシアから自動車部品購入、インドへPetro用いた原油購入にディスカウント提案 • 若者むけに暗号通貨銀行創設へ
〃	ブラジル	• ブラジル開発銀行、レアルをPublic Ethereum上でトークン化して透明性向上図る
〃	チリ	• 経済発展相、暗号通貨は重要なイノベーションであるとサポートを表明

※薄文字は前四半期

①国・地域別の概況 – 日本

規制・制度	• 麻生財務相、仮想通貨規制についてイノベーションと利用者保護のバランスを強調 • 外為法改正案、仮想通貨の国際送金に報告義務　パブコメ募集も開始
暗号通貨	• 東京金融取引所、ビットコイン先物を検討 • 三菱UFJ信託銀行、取引所破産に備え信託で全額保全へ • 三菱東京UFJ銀行、独自仮想通貨MUFGコインの発行へむけて取引所を開設へ • GMOインターネット、給与の一部を購入枠最大10万円をビットコインで受け取れる制度 • テックビューロ、仮想通貨で給与上乗せ3割相当分 • メルカリ、子会社メルペイを通じて仮想通貨取引業登録申請へ • ヤマダ電機、ビットコイン決済導入 • LINE、持株会社設立し暗号通貨提供へ • DMM、金沢にマイニングファーム • ヤフー、登録業者ビットアルゴに資本参加し仮想通貨交換業に参入 • 筑波大学・落合陽一氏がReadyforでビットコイン寄付受付開始 • 企業会計基準委員会ASBJ、仮想通貨の会計処理に関する取扱を決定 • 財務省、3000万超相当の仮想通貨による海外送金を当局報告とするルール整備へ
ICO	• 金融庁、ICO規制を検討 • SBIホールディングス、ICOにより500億円調達すると発表
中央銀行	• 日銀総裁、今のビットコインは支払・決済手段というより投機対象のため「金融政策に障害は無い」との見方 • 日銀FinTechセンター長、法定デジタル通貨について「技術的には可能だが検討段階にはない」とコメント

①国・地域別の概況 – 米国

規制・制度	• 米SECとCFTCが暗号通貨関連の詐欺的行為の取締へむけて共同声明 • 米CFTC、Pump&Dumpスキームへの注意喚起 • 米ワイオミング州、Utility Tokenに証券性無しとの法案 • 米サウスカロライナ州、クラウドマイニングは証券契約にあたるとの判断示す • 米SEC委員長、トークンの利用可否により証券となるとの見方示す • 米CFTC元委員長で現MITのGensler氏、ETHおよびXRPの証券性に言及
暗号通貨	• CMEおよびCBOE、ビットコイン先物をローンチ • PayPal、仮想通貨トランザクションシステムで特許 • Square、BitLicence取得へむけ準備中 • ダウジョーンズ、プレミアコンテンツアクセスにBATペイメントを試行すべくBraveと提携 • ソロス氏、暗号通貨投資を準備 • Nasdaq、規制市場における暗号通貨交換業者になることを志向している旨を表明 • ジョージア州、ビットコインなどの暗号通貨による税金支払を認める法案 • Wisconsin州、暗号通貨による政治献金ガイドライン受け入れ検討 • Arizona州、暗号通貨購入時に納税トランザクションが州へ直接送信される法案 • CoinbaseはSEC登録を目指す • Goldman Sachs出資のCircle、Poloniexを4億ドルで買収
ICO	• Google、Twitter、Facebook、ICOや暗号通貨に関するプロモーションを禁止へ • 米SEC、三件のICO案件の取引を停止処分 • 米SEC、tZEROを含むICOに関して召喚状発行し調査開始 • ルイジアナ州Lafayette、Berkeleyに続きデジタル通貨発行しICO
中央銀行	• セントルイスFRB、中央銀行が支払形態として暗号通貨を適用する場合のコントロール構造に関するレポート発表

①国・地域別の概況 – カナダ

規制・制度	• ー
暗号通貨	• オンタリオ州規制当局、カナダ初のブロックチェーンETFを承認 • トロント証券取引所、暗号通貨の価格ベンチマーク情報提供など仲買サービス立ち上げ • カナダBMO、デビットカードを用いた暗号通貨購入を禁止
ICO	• ー
中央銀行	• ー

①国・地域別の概況 – フランス

規制・制度	• 仏AMF、暗号通貨デリバティブに免許制導入 • 仏AMF、ICOを合法的投資手段とする規制枠組を準備 • 小口の暗号通貨投資に係る税率低減検討
暗号通貨	• 仏当局AMF、暗号通貨デリバティブの広告を禁止
ICO	• ブロックチェーンを用いた非上場株式取引を許可へ • 規制当局AMFがICO規制フレームワーク検討にむけUNICORN立ち上げ
中央銀行	• フランス中央銀行、ビットコイン投資は自己責任と警告 • 中央銀行、金融機関に暗号通貨関連ビジネスに関与しないよう求める

①国・地域別の概況 – ドイツ

規制・制度	• 仏独で三月のG20サミットへ向けて暗号通貨規制の合同提案を検討
暗号通貨	• 証券取引所SWB、カナダTMXに続き子会社で暗号通貨取引アプリ • ドイツ国民観光局、ビットコイン受け入れへ
ICO	• 独BaFin、ICO実施者の義務を明確化 • 独BaFin、ICOおよびトークン規制に関するステートメント発行
中央銀行	• ー

①国・地域別の概況 – イギリス

規制・制度	• 英FCA、Coinbaseにe-moneyライセンス発行 • 英FCA、暗号通貨は通貨やコモディティにあたらないが暗号通貨デリバティブは金融商品との見方 • 中国Huobi、ロンドン進出を発表
暗号通貨	• Barclays、暗号通貨トレーディングデスク設置を検討 • 英政府、クリプトアセットタスクフォースをBoEやFCAと協働で設立
ICO	• ー
中央銀行	• BoE、商業銀行からの預金引き出しなど不安定化の懸念からデジタル通貨発行計画をキャンセル • BoE、RGTS刷新へむけてClearmaticsやR3とPoCへ • BoE、DLT上でのプライバシーについてChainとPoC実施へ

①国・地域別の概況 – スペイン

規制・制度	• ー
暗号通貨	• ー
ICO	• ブロックチェーン関連企業やICO発行者の誘致へ向けた税制優遇を検討
中央銀行	• ー

①国・地域別の概況 – オランダ

規制・制度	• オランダ法廷、ビットコインを「移転可能な価値」との判断示す
暗号通貨	• Rabobank、オンラインバンキングに暗号通貨ウォレット追加を検討
ICO	• ー
中央銀行	• ー

①国・地域別の概況 – スイス

規制・制度	• Bitfinex、スイスZugへの移転を計画
暗号通貨	• –
ICO	• スイス規制当局FINMA、ICOむけガイドライン発表
中央銀行	• スイス国立銀行頭取、暗号通貨は通貨より投資に近いとの認識

①国・地域別の概況 – リヒテンシュタイン

規制・制度	• ブロックチェーンをサポートする規制を今夏目処に予定 • ブロックチェーンへの過度な規制は回避する方針と首相が表明
暗号通貨	• Bank Frick、投資家むけに暗号通貨投資サービス提供
ICO	• –
中央銀行	• –

①国・地域別の概況 – マルタ

規制・制度	• 暗号通貨およびICOに関する規制枠組示す議案承認
暗号通貨	• 香港OKexもBinanceに続いて欧州マルタに拠点開設
ICO	• FSA、ICOトークンがいつ証券になるかに関する試行を提案
中央銀行	• ー

①国・地域別の概況 – バミューダ

規制・制度	• 暗号通貨産業振興へむけて規制ドラフトを起案
暗号通貨	• Binance、バミューダにグローバルコンプラセンター開設とあわせて15mドルの投資表明
ICO	• ICOを受け入れる方向で規制を検討へ
中央銀行	• ー

①国・地域別の概況 – ロシア

規制・制度	• ロシア中央銀行、暗号通貨投資への警告 • 暗号通貨のマイニング禁止を検討 • 暗号通貨およびICO規制法案を提出 • 電子金融資産に関する新法案を提出 • ICOへのライセンス導入 • 暗号通貨合法化へ • 通信省副大臣、政府独自プラットフォームの必要性主張 • ICO向け規制を発表 • 600,000ルーブル以上の暗号通貨取引に為替規制適用を検討 • 下院の金融市場委員長、クリプトルーブル発行を来年を待たずに行う意向を示す
暗号通貨	• ロシア～トルコ間の3000トンの小麦輸送でビットコイン決済 • カリーニングラードのホテルがW杯期間中の支払いでビットコイン受け入れ • ガスプロムバンクが仮想通貨取引を試行 • Sberbank、ルーブルでビットコイン購入できる交換業Sberkoin開設
ICO	• ベネズエラによるPetro立ち上げサポートを表明
中央銀行	• BRICSおよび欧州経済連合諸国による単一仮想通貨を構想 • ロシア中央銀行、EAEU向けペイメントネットワークをEthereumベースのMasterchain上にデプロイする考えを表明 • ロシア中央銀行、ブロックチェーン上に預金者の統合登録簿を作成 • ロシア中銀、国内送金SPFSにEthereum利用適用検討

①国・地域別の概況 – ベラルーシ

規制・制度	• 暗号通貨合法化を含む経済特区法案を承認
暗号通貨	• 暗号通貨を扱う新会計基準を採択。エストニア、リヒテンシュタイン、スイス、シンガポール、マルタに続いて暗号通貨フロンティアをサポートへ
ICO	• ビットコインの取引・マイニングおよびICOの合法化、5年間の非課税を表明
中央銀行	• ー

①国・地域別の概況 – 中国

規制・制度	• 中国人民銀行、ビットコインマイニング業者の電力利用への規制可能性について言及 • 当局、マイニング活動も停止へ。Bitmainもスイスに子会社設立 • 海外ネットワークを介した暗号通貨トレード禁止へ規制強化 • 香港SFC、交換業者やICO発行者へ警告 • 淘宝網、ICO関連サービスラインナップを禁止へ
暗号通貨	• 中国人民銀行総裁、暗号通貨を決済手段として認めず、”DCEP(digital currency electronic payment)”検討 • Bitmain、ブロックチェーンを活用した民間中央銀行の設立を構想 • 中国CoinEx、USDTのクレジットデフォルトスワップ取扱開始 • 香港Bitfinex、JPYおよびGBPとの間のペアを追加する旨を発表 • 香港Bitfinex傘下のEthfinex、Daiをサポート開始すると発表 • 香港Ethfinexは集中型ExchangeとDEXを繋いでハイブリッドを目指す。Dai/USDTペア取扱はその第一歩とのこと • 香港FSTBマネロンリスクレポート、ビットコインそのものに特段の金融犯罪関係は無いとした一方、匿名取引には潜在的マネロンリスクを指摘
ICO	• ー
中央銀行	• 中国社会科学院、各国中央銀行は国際決済で仮想通貨を検討すべきと進言 • 中国投資協会、ブロックチェーンの投資・開発センター立ち上げへ • PBoC、中央銀行発行デジタル通貨へむけた計画を強調 • PBoC、ブロックチェーンの追跡可能性やスマートコントラクトを賞賛の一方でスケーラビリティのボトルネックを解消すべく絶対的な非中央分散を諦めるべきと主張

①国・地域別の概況 – 韓国

規制・制度	• ビットコインの先物・デリバティブ取引を禁止 • 取引所の自主規制を制定 • 匿名アカウント作成禁止および当局による取引所閉鎖も可能とする規制強化へ • 大手取引所へ警察・税務当局が急襲。取引禁止準備も • 暗号通貨取引を禁止しない旨を表明 • 当局が、取引所むけ口座提供銀行６行の検査 • 取引実名制を導入 • 規制当局、通常の暗号通貨トランザクションはサポートする旨を表明 • ６月までに課税枠組発表へ • 韓国財務相、暗号通貨は代替支払手段として法定通貨の脅威になると発言
暗号通貨	• Samsung、ASICチップおよびマイニング機器製造を開始 • Kakao、2018年中に暗号通貨の取り込みを計画 • Bithumb、レストランでのペイメントに使えるキオスク端末サービスを立ち上げ予定 • ソウル市、独自暗号通貨を検討
ICO	• 昨秋からのICO禁止に関する緩和を検討
中央銀行	• ー

①国・地域別の概況 – 台湾

規制・制度	• シンガポールにならった規制を検討 • 既存AMLルールのもとにビットコイン規制へ
暗号通貨	• 遠東航空、暗号通貨による支払を受け入れへ • 鴻海精密工業、仮想通貨の商業銀行設立を計画 • Foxconn、暗号通貨を支払い手数料無く扱い、トークンをサポートしトークンに変換可能な携帯電話を開発へ
ICO	• ー
中央銀行	• 中央銀行がビットコインAML規制を提案

①国・地域別の概況 – タイ

規制・制度	• 金融当局、国内での暗号通貨利用を規制せず • 仮想通貨規制の枠組を3月中公表 • 規制当局、暗号通貨キャピタルゲイン課税見直しを否定
暗号通貨	• ー
ICO	• ICO規制へ
中央銀行	• ー

①国・地域別の概況 – インドネシア

規制・制度	• ビットコインおよび他の暗号通貨を禁止へ
暗号通貨	• –
ICO	• –
中央銀行	• 中央銀行、暗号通貨によるペイメントは非合法との声明を発行し、売買・取引を行わないよう警告 • 暗号通貨デジタルルピアの試行を計画

①国・地域別の概況 – フィリピン

規制・制度	• SEC、クラウドマイニングを証券にあたるとの見方示す • 暗号通貨事業者優遇地域の開発を検討
暗号通貨	• –
ICO	• 暗号通貨の取引およびICOの規制を検討
中央銀行	• –

①国・地域別の概況 – カンボジア

規制・制度	• ー
暗号通貨	• カンボジア、米国による経済制裁の中で、ベネズエラ・トルコ・イランに続いて独自仮想通貨Entapay発行検討と発表
ICO	• ー
中央銀行	• chaintope、カンボジア国立銀行及びカンボジア企業と仮想通貨開発を開始

①国・地域別の概況 – インド

規制・制度	• 税務当局が取引所の検査を実施 • 財務省が仮想通貨投資について注意するよう声明を発表 • 銀行口座からの暗号通貨購入を禁止 • RBI、銀行が暗号通貨関連の個人・企業と取引することを禁止 • 中央銀行による暗号通貨禁止に対して交換業界から請願書
暗号通貨	• インド財務相、暗号通貨を決済通貨として利用する可能性を排除する姿勢を発表
ICO	• ー
中央銀行	• インド準備銀行、ビットコイン等の暗号通貨に関するリスクを警告

①国・地域別の概況 – シンガポール

規制・制度	• MAS、暗号通貨投資に注意喚起 • MAS、暗号通貨取引禁止の理由無しと表明
暗号通貨	• –
ICO	• –
中央銀行	• MAS、Project Ubin フェーズ2を発表 • MAS、国際ペイメントにおけるブロックチェーン利用を表明

①国・地域別の概況 – 豪州

規制・制度	• デジタル通貨交換業者にAML/CMF義務付けへ • 交換業者にAUSTRAC登録義務づけ
暗号通貨	• ブリスベン空港、空港内店舗でのBTC/ETH/DASHペイメント受付
ICO	• 豪州当局ASIC、既存ガイドラインをICO向けに拡張の意向示す
中央銀行	• オーストラリア準備銀行、e-AUDに関するスピーチ

①国・地域別の概況 – イスラエル

規制・制度	• 暗号通貨を課税対象とする旨を表明 • 当局、ユーティリティトークンと証券トークンの定義。ビットコインは証券と扱わず
暗号通貨	• –
ICO	• –
中央銀行	• ブラックマーケット抑制にむけて暗号通貨導入を検討

①国・地域別の概況 – イラン

規制・制度	• イラン中央銀行、暗号通貨取引を禁止
暗号通貨	• ー
ICO	• 独自ローカル暗号通貨を実験的に開発
中央銀行	• イラン中央銀行、暗号通貨取引を禁止

①国・地域別の概況 – UAE

規制・制度	• 規制当局SCA、投資家に対してICOへの警戒呼びかけ
暗号通貨	• –
ICO	• –
中央銀行	• サウジアラビアと合同でデジタル通貨を検討

①国・地域別の概況 – サウジアラビア

規制・制度	• –
暗号通貨	• –
ICO	• –
中央銀行	• UAEと合同でデジタル通貨を検討 • サウジアラビア中央銀行、Rippleを用いたクロスボーダーペイメントのパイロット

①国・地域別の概況 – 南アフリカ

規制・制度	• ー
暗号通貨	• 南アフリカ歳入庁（SARS）、暗号通貨に係る税金取扱方針を提示
ICO	• ー
中央銀行	• 南ア中央銀行、Ethereumベースの銀行間決済 • 南アSARB、Quorumを用いた銀行間送金のパイロットをConsenSysと協業で実施

①国・地域別の概況 – ベネズエラ

規制・制度	• ー
暗号通貨	• 市民動員による暗号通貨マイニング支援プログラム開始
ICO	• 原油資産を裏付けとしたERC20トークンPetroを発行するICO • OPECへ公式にPetroを提案へ • Petro用いてロシアから自動車部品購入 • インドへPetro用いた原油購入に30%ディスカウント提案
中央銀行	• 若者むけに暗号通貨銀行創設へ

①国・地域別の概況 – ブラジル

規制・制度	• ファンドによる仮想通貨投資を規制
暗号通貨	• –
ICO	• –
中央銀行	• ブラジル開発銀行、レアルをPublic Ethereum上でトークン化して透明性向上図る

①国・地域別の概況 – チリ

規制・制度	• チリCEF、暗号通貨を経済安定化への脅威と捉えていない旨を表明 • 経済発展相、暗号通貨は重要なイノベーションであるとサポートを表明
暗号通貨	• –
ICO	• –
中央銀行	• –

※薄文字は前四半期

②規制・制度 – 日本

名称	サービス概略	URL
日本	金融庁が金融行政方針にて仮想通貨に言及	→ http://www.fsa.go.jp/news/29/2017StrategicPoint.pdf
日本	国税庁が仮想通貨に関する所得の計算方法を発表	→ http://www.nta.go.jp/shiraberu/zeiho-kaishaku/joho-zeikaishaku/shotoku/shinkoku/171127/01.pdf
日本	企業会計基準委員会が「資金決済法における仮想通貨の会計処理等に関する当面の取扱い（案）」を公表	→ https://bitpress.jp/news/market/entry-7001.html → https://www.asb.or.jp/jp/accounting_standards/exposure_draft/y2017/2017-1206.html
日本	日銀総裁、今のビットコインは支払・決済手段というより投機対象のため「金融政策に障害は無い」との見方	→ http://www.boj.or.jp/announcements/press/kaiken_2017/kk1712c.pdf
日本	麻生財務相、仮想通貨規制についてイノベーションと利用者保護のバランスを強調	→ http://jp.mobile.reuters.com/article/amp/idJPL4N1P7131

②規制・制度 – 日本

名称	サービス概略	URL
日本	金融庁、ICO規制を検討	→ http://www.sankei.com/economy/news/180227/ecn1802270005-n1.html
日本	外為法改正案、仮想通貨の国際送金に報告義務　パブコメ募集も開始	→ https://btcnews.jp/2wgjtds915685/

②規制・制度 – 北米 [1/7]

名称	サービス概略	URL
米国	米商品先物取引委員会（CFTC）が取引所むけ信用取引ルールを提案	→ http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister121517.pdf
米国	米SECとCFTCが暗号通貨関連の詐欺的行為の取締へむけて共同声明	→ https://www.sec.gov/news/public-statement/joint-statement-sec-and-cftc-enforcement-directors → http://www.cftc.gov/PressRoom/PressReleases/mcdonaldstatement011918#PrRoWMBL
米国	米国SECおよびCFTCが米議会で公聴会	→ https://youtu.be/Ld9hcKgf7GI
米国	米CFTC、Pump&Dumpスキームへの注意喚起	→ http://www.cftc.gov/PressRoom/PressReleases/pr7697-18 → http://www.cftc.gov/idc/groups/public/@customerprotection/documents/file/customeradvisory_pumpdump0218.pdf
米国	米サイバーセキュリティ担当大統領補佐官、米政府によるビットコイン規制は近日行われることは無いと表明	→ https://www.newsbtc.com/2018/02/16/munich-security-conference-u-s-govt-nowhere-close-to-regulating-bitcoin/

②規制・制度 – 北米 [2/7]

- 米議会で公聴会。CFTCジャンカルロ委員長の発言が注目集める
  - ジャンカルロ委員長が公聴会冒頭で、「若い世代の仮想通貨への熱意に敬意を示し、思慮深い規制対応をすべき」と述べたほか、質疑応答の中で「ビットコインが無ければブロックチェーンも無かった」と回答し、またHODLの意味を解説したことも注目を集めた。
  - 主な論点は以下のとおり。
    - ほとんどユーティリティトークンは証券であるゆえ、ほとんどのICOが証券販売にあたる。
    - トークン販売プラットフォームとしてのexchangeはSEC登録されていないため取引所ではない。
    - SEC登録済のICOは無く、またSECが暗号通貨関連アセットを承認していないことに投資家は用心すべき。
    - ICOプラットフォームやマーケットエージェント達は、無登録証券販売に関与しないよう注意すべき。
  - 出所：
    - https://www.ethnews.com/seven-takeaways-from-the-sec-and-cftcs-testimony-on-virtual-currency
    - https://youtu.be/Ld9hcKgf7GI
    - https://jp.cointelegraph.com/news/sec-and-cftc-hearing-more-legitimate-icos-or-if-there-was-no-bitcoin-there-would-be-no-blockchain
    - https://news.bitcoin.com/bitcoins-new-rock-star-j-christopher-giancarlo/
    - https://hackernoon.com/top-10-points-made-by-the-sec-and-cftc-congress-testimony-on-cryptocurrencies-f4c71712624c
    - https://www.banking.senate.gov/public/_cache/files/a5e72ac6-4f8a-473f-9c9c-e2894573d57d/BF62433A09A9B95A269A29E1FF13D2BA.clayton-testimony-2-6-18.pdf
    - https://www.banking.senate.gov/public/_cache/files/d6c0f0b6-757d-4916-80fd-a43315228060/A2A6C1D8DDBB7AD33EBE63254D80E9E3.giancarlo-testimony-2-6-18b.pdf

②規制・制度 – 北米 [3/7]

名称	サービス概略	URL
米国	米SEC、暗号通貨の価格操作に係る通報に報奨金	→ http://www.globalcryptopress.com/2018/02/us-sec-is-hunting-down-pump-dump-groups.html
米国	米FinCEN、「ICOトークン販売者は資金送金者に該当し、送金業者登録およびAML/KYC関連法律準拠させる方針」との見解示すとともに、「ICOについても性質に応じて証券性あればSEC、コモディティ性あればCFTCの規制に準じる」との見解	→ https://coincenter.org/link/fincen-raises-major-licensing-problem-for-icos-in-new-letter-to-congress → https://www.coindesk.com/fincen-money-transmitter-rules-apply-ico-developers-exchanges/
米国	米SEC、証券法で定義される証券（利益共有契約や投資契約など）にあたるデジタルアセットを扱い、証券法の適用されるExchangeを運営するプラットフォームは証券取引所として登録必要との表明	→ https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading

②規制・制度 – 北米 [4/7]

名称	サービス概略	URL
米国	Bittrexは米SECのルールに準拠したレビュープロセスで証券に該当しないものとしてデジタルトークン提供に臨んでいる旨を表明	→ https://www.ccn.com/crypto-exchange-bittrex-compliant-secs-ico-rules/ → https://support.bittrex.com/hc/en-us/articles/360001525152-Bittrex-statement-on-the-SEC-s-online-trading-platforms-announcement-
米国	米ワイオミング州、Utility Tokenに証券性無しとの法案	→ https://www.coindesk.com/wyoming-utility-token-bill-heads-governor-approval/ → https://bitcoinmagazine.com/articles/wyoming-blockchain-bill-rockets-ahead-signing/
米国	米CFTC長官、「暗号通貨コミュニティは自己規制団体を発足させ、管轄の横通しに時間を要するに規制当局とのギャップを埋めてはどうかと」の見解を、コモディティを管轄する当局意見として発表	→ https://www.coindesk.com/crypto-industry-should-self-regulate-says-cftc-commissioner/ → https://dcebrief.com/cftc-commissioner-says-crypto-community-should-create-oversight-body/

②規制・制度 – 北米 [5/7]

名称	サービス概略	URL
米国	暗号通貨およびICO市場に関する米国公聴会	→ https://www.c-span.org/video/?442556-1/hearing-focuses-cryptocurrency-markets&live → https://youtu.be/-CCqCsmCDdw
米国	米SEC、ICOについて知っておくべきことを開示	→ https://www.sec.gov/ICO
米国	米サウスカロライナ州、クラウドマイニングは証券契約にあたるとの判断示す	→ https://news.bitcoin.com/south-carolina-declares-cloud-mining-contracts-securities/ → https://blog.genesis-mining.com/the-importance-of-collaboration
米国	米財務省、外国資産管理局によるSDNリストに暗号通貨アドレス追加の可能性	→ https://news.bitcoin.com/u-s-treasury-plans-to-add-cryptocurrency-addresses-to-the-sdn-list/
米国	米SEC、暗号通貨関連ヘッジファンドへの検査を近日実施へ	→ https://www.wsj.com/articles/crypto-focused-hedge-funds-on-secs-radar-1521757104

②規制・制度 – 北米 [6/7]

名称	サービス概略	URL
米国	CLOUD Actがアメリカで成立、プライバシー保護懸念高まる	→ https://btcnews.jp/27uh8xgv15592/
米国	米SEC委員長、トークンの利用可否により証券となるとの見方示す	→ https://coincenter.org/entry/sec-s-clayton-use-of-a-token-can-evolve-toward-or-away-from-being-a-security → https://www.coindesk.com/sec-chief-not-icos-bad/
米国	NY検察当局、仮想通貨交換業者へ質問状（取引ポリシー、内部統制、プライバシー・AML、顧客資産保護リスク等）	→ https://ag.ny.gov/press-release/ag-schneiderman-launches-inquiry-cryptocurrency-exchanges
米国	米大手VC、米SECに対して暗号通貨やブロックチェーンの発展に向けた規制免除の必要性を主張、ETHを証券と位置づけるべきでないとの考え示す	→ https://www.ethnews.com/andreessen-horowitz-union-square-ventures-reportedly-seek-regulatory-exemptions-for-blockchain-cryptocurrency-development-in-sec-meeting

②規制・制度 – 北米 [7/7]

- 米SEC委員長、トークンの利用可否により証券となるとの見方示す
  - トークンが同じく証券として規制されるものではなく、販売後の利用によって経済的にリアリティを帯びるかどうか。
  - ランドリートークンを洗濯のために持っているなら証券ではないが、未開発であり将来利用あるいは売却のために買うようなら証券にあたる。

  - 出所：
    - https://coincenter.org/entry/sec-s-clayton-use-of-a-token-can-evolve-toward-or-away-from-being-a-security
    - https://www.coindesk.com/sec-chief-not-icos-bad/

②規制・制度 – 北米 [6/7]

名称	サービス概略	URL
米国	米CFTC元委員長で現MITのGensler氏、ETHおよびXRPの証券性に言及	→ https://www.nytimes.com/2018/04/22/technology/gensler-mit-blockchain.html → https://coinchoice.net/eth-and-xrp-regarded-as-securities/
米国	Coincenter、Etherの価値は財団ではなく開発者やユーザーに依拠したものであり、有用な非中央集権トークンは証券とみなされるべきでない旨を主張	→ https://coincenter.org/entry/no-ether-is-not-a-security
米国	米SEC委員長、下院歳出委員会に先立つヒアリングでビットコインは証券ではないとし、SECとCFTCで分けて考える方向を示した模様	→ https://coincenter.org/link/sec-chairman-clayton-bitcoin-is-not-a-security

②規制・制度 – 南米

名称	サービス概略	URL
ブラジル	ファンドによる仮想通貨投資を規制	→ https://web.fisco.jp/FiscoPFApl/SelectedNewsDetailWeb?nwsId=00107700201801150 15&nwsType=00107700
チリ	チリCEF、暗号通貨を経済安定化への脅威と捉えていない旨を表明	→ https://www.newsbtc.com/2018/04/11/financial-stability-board-chile-says-cryptocurrencies-no-threat/
チリ	経済発展相、暗号通貨は重要なイノベーションであるとサポートを表明	→ https://news.bitcoin.com/chilean-minister-supports-cryptocurrencies-after-court-sided-with-exchanges-against-banks/

②規制・制度 – 欧州　フランス

名称	サービス概略	URL
フランス	ブロックチェーンを用いた非上場株式取引を許可へ	→ https://distributed.com/news/france-opens-doors-unlisted-securities-trading-through-blockchains/
フランス	規制当局AMFがICO規制フレームワーク検討にむけUNICORN立ち上げ	→ https://www.coindesk.com/french-regulator-launches-unicorn-ico-support-project/
フランス	フランス中央銀行、ビットコイン投資は自己責任と警告	→ http://www.independent.co.uk/news/business/news/bitcoin-latest-updates-france-central-bank-currency-cryptocurrency-digital-francois-villeroy-de-a8086186.html

②規制・制度 – 欧州　フランス

名称	サービス概略	URL
フランス	中央銀行、金融機関に暗号通貨関連ビジネスに関与しないよう求める	→ https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf
フランス	仏AMF、暗号通貨デリバティブに免許制導入	→ http://www.amf-france.org/en_US/Actualites/Communiques-de-presse/AMF/annee-2018?docId=workspace%3A%2F%2FSpacesStore%2Fa225bf1d-de35-4f58-89e3-f03cb7e9e551
フランス	仏AMF、ICOを合法的投資手段とする規制枠組を準備	→ https://www.reuters.com/article/us-france-cryptocurrencies/france-to-create-legal-framework-for-cryptocurrency-offerings-idUSKBN1GY0YE
フランス	小口の暗号通貨投資に係る税率低減検討	→ http://www.lemonde.fr/argent/article/2018/04/26/le-conseil-d-etat-change-la-fiscalite-sur-les-gains-generes-par-les-bitcoins_5291137_1657007.html

②規制・制度 – 欧州　ドイツ

名称	サービス概略	URL
フランス・ドイツ	三月のG20サミットへ向けて暗号通貨規制の合同提案を検討	→ https://www.reuters.com/article/us-global-bitcoin-france-germany/france-germany-to-make-joint-bitcoin-regulation-proposal-at-g20-summit-idUSKBN1F728X
ドイツ	独BaFin、ICO実施者の義務を明確化	→ https://jp.cointelegraph.com/news/german-regulator-clarifies-obligations-for-ico-operators-following-increased-interest
ドイツ	独BaFin、ICOおよびトークン規制に関するステートメント発行	→ https://www.lw.com/thoughtLeadership/bafin-publishes-statement-on-ico-and-token-regulation

②規制・制度 – 欧州　イギリス

名称	サービス概略	URL
イギリス	英FCA、Coinbaseにe-moneyライセンス発行	→ https://www.coindesk.com/coinbase-receives-e-money-license-from-u-k-financial-regulator/
イギリス	英FCA、暗号通貨は通貨やコモディティにあたらないが暗号通貨デリバティブは金融商品との見方	→ https://www.fca.org.uk/news/statements/cryptocurrency-derivatives
イギリス	中国Huobi、ロンドン進出を発表	→ https://cryptobriefing.com/huobi-plans-london-move/

②規制・制度 – 欧州　スイス

名称	サービス概略	URL
スイス	スイス国立銀行頭取、暗号通貨は通貨より投資に近いとの認識	→ https://www.reuters.com/article/us-swiss-snb/snbs-jordan-sees-crypto-currencies-as-more-of-investment-than-currency-idUSKBN1DN1ZM
スイス	スイス規制当局FINMA、ICOむけガイドライン発表	→ https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/
スイス	Bitfinex、スイスZugへの移転を計画	→ https://bitcoinmagazine.com/articles/cryptocurrency-exchange-bitfinex-plans-move-switzerland/

②規制・制度 – 欧州　EU

名称	サービス概略	URL
ECB	ドラギ総裁、暗号通貨の与えるインパクトと限定的との認識	→ https://www.reuters.com/article/us-ecb-bitcoin-draghi/digital-currencies-no-threat-to-ecb-yet-draghi-idUSKBN1DK208
35ヶ国および欧州委員会	FATFへ暗号通貨に関する標準の見直しを要請、G20でFATFからAML対策の提示の見込み	→ http://cryptoventures.io/2018/02/28/35-countries-eu-and-fatf-agree-to-revise-global-cryptocurrency-standards/
欧州委員会	ブロックチェーン含めたFinTechの包括的規制枠組み整備へ	→ https://jp.cointelegraph.com/news/european-commission-to-release-bloc-wide-blockchain-framework-says-draft-document
EBA	暗号通貨への過度な規制は金融革新の流れを抑制するため望ましくない旨の表明	→ https://news.bitcoin.com/excessive-crypto-regulation-not-optimal-eu-banking-authority-says/
欧州委員会	ブロックチェーンパートナーシップ締結し、ブロックチェーンで連盟設立	→ https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership
欧州議会	欧州理事会による暗号通貨規制強化にむけた合意に関して投票行い賛成多数	→ http://www.europarl.europa.eu/news/en/press-room/20180411IPR01527/anti-money-laundering-meps-vote-to-shed-light-on-the-true-owners-of-companies

②規制・制度 – 欧州　その他

名称	サービス概略	URL
ブルガリア	取引所の銀行口座を閉鎖	→ https://sofiaglobe.com/2017/12/08/bitcoin-bulgarian-banks-terminate-accounts-of-cryptocurrency-exchanges/
ベラルーシ	暗号通貨合法化を含む経済特区法案を承認	→ https://cointelegraph.com/news/belarusian-president-alexander-lukashenko-to-sign-decree-legalizing-Cryptocurrencies
ベラルーシ	ビットコインの取引・マイニングおよびICOの合法化、5年間の非課税を表明	→ https://news.bitcoin.com/belarus-legalizes-cryptocurrencies-icos-tax-free/
バルト三国	分散台帳を用いた地域資本市場開発への協業に関するMOU締結	→ https://www.rahandusministeerium.ee/sites/default/files/news-related-files/mou_panbaltic.pdf

②規制・制度 – 欧州　その他

名称	サービス概略	URL
オーストリア	暗号通貨およびICOへの規制を計画	→ https://www.coindesk.com/austria-cryptocurrency-regulation-icos-gold-derivatives/
オランダ	オランダ法廷、ビットコインを「移転可能な価値」との判断示す	→ https://cointelegraph.com/news/dutch-court-finds-bitcoin-a-legitimate-transferable-value
ベラルーシ	暗号通貨を扱う新会計基準を採択。エストニア、リヒテンシュタイン、スイス、シンガポール、マルタに続いて暗号通貨フロンティアをサポートへ	→ https://news.bitcoin.com/belarus-adopts-crypto-accounting-standard/

②規制・制度 – 欧州　その他

名称	サービス概略	URL
バミューダ	ICOを受け入れる方向で規制を検討へ	→ https://www.coindesk.com/bermuda-drafting-ico-friendly-legislation-to-draw-crypto-businesses/
リヒテンシュタイン	ブロックチェーンをサポートする規制を今夏目処に予定	→ https://cointelegraph.com/news/liechtenstein-to-support-blockchain-with-new-regulations
リヒテンシュタイン	ブロックチェーンへの過度な規制は回避する方針と首相が表明	→ https://www.coindesk.com/liechtenstein-to-avoid-excessive-blockchain-regulation-says-prime-minister/
バミューダ	暗号通貨産業振興へむけて規制ドラフトを起案	→ http://bernews.com/2018/04/ico-initial-coin-offering-legislation-tabled/
マルタ	FSA、ICOトークンがいつ証券になるかに関する試行を提案	→ https://www.mfsa.com.mt/pages/readfile.aspx?f=/Files/Announcements/Consultation/2018/20180413_FITest.pdf → https://www.mfsa.com.mt/pages/readfile.aspx?f=/files/Announcements/Consultation/2017/20171130_DiscussionPaperVCs.pdf

②規制・制度 – 欧州　その他

名称	サービス概略	URL
マルタ	暗号通貨およびICOに関する規制枠組示す議案承認	→ https://ohiobitcoin.com/maltas-cabinet-approves-cryptocurrency-bill/
バミューダ	Binance、バミューダにグローバルコンプラセンター開設とあわせて15mドルの投資表明	→ https://www.coindesk.com/binance-bermuda-ink-15-million-crypto-investment-agreement/

②規制・制度 – ロシア

名称	サービス概略	URL
ロシア	情報技術・通信相がビットコインの合法化を否定	→ http://tass.com/economy/976510
ロシア	大統領が暗号通貨およびICO向け立法準備を指示	→ https://www.ethnews.com/putin-instructs-government-to-prepare-legislation-on-token-offerings-Cryptocurrency
ロシア	ロシア中央銀行、暗号通貨投資への警告	→ http://tass.com/economy/977847
ロシア	暗号通貨のマイニング禁止を検討	→ https://www.ethnews.com/russia-weighing-ban-on-cryptocurrency-mining
ロシア	暗号通貨およびICO規制法案を提出	→ https://www.ccn.com/russia-reveal-bitcoin-ico-draft-regulation-bill-next-week/
ロシア	電子金融資産に関する新法案を提出	→ http://cryptorussian.blogspot.com/2018/01/blog-post_28.html

②規制・制度 – ロシア

名称	サービス概略	URL
ロシア	ICOへのライセンス導入	→ https://jp.cointelegraph.com/news/russia-ministry-of-communications-requires-ico-issuers-to-have-17-mln-nominal-capital/
ロシア	暗号通貨合法化へ	→ https://www.ccn.com/russia-legalizing-cryptocurrency-markets-july-2018/
ロシア	通信省副大臣、政府独自プラットフォームの必要性主張	→ https://jp.cointelegraph.com/news/russian-vice-minister-government-needs-blockchain-platform-focused-on-stability
ロシア	ICO向け規制を発表	→ https://rucrypto.com/ico/rossiya-podgotavlivaet-strogie-pravila-v-otnoshenii-ico.html
ロシア	600,000ルーブル以上の暗号通貨取引に為替規制適用を検討	→ https://forklog.com/rossijskoe-pravitelstvo-namereno-vzyat-obmen-kriptovalyut-pod-kontrol/
ロシア	下院の金融市場委員長、クリプトルーブル発行を来年を待たずに行う意向を示す	→ http://tass.ru/ekonomika/5141851

②規制・制度 – 中国

名称	サービス概略	URL
中国	中国人民銀行、ビットコインマイニング業者の電力利用への規制可能性について言及	→ https://www.reuters.com/article/us-markets-bitcoin-china-mining/china-central-bank-can-tell-local-governments-to-regulate-bitcoin-miners-power-use-source-idUSKBN1ES0TD
中国	当局、マイニング活動も停止へ。Bitmainもスイスに子会社設立	→ http://jp.wsj.com/articles/SB12417666850591433362304583630302583260698 → https://www.coindesk.com/bitmain-expands-to-switzerland-as-china-cools-to-bitcoin-miners/
中国	OKCoin、韓国NHN Entertainmentと提携して韓国で取引所開設へ	→ https://www.ccn.com/okcoin-formerly-largest-cryptocurrency-exchange-china-launch-south-korea/

②規制・制度 – 中国

名称	サービス概略	URL
中国	海外ネットワークを介した暗号通貨トレード禁止へ規制強化	→ http://www.scmp.com/business/banking-finance/article/2132009/china-stamp-out-cryptocurrency-trading-completely-ban → http://m.thepaper.cn/newsDetail_forward_1983173
中国	香港SFC、交換業者やICO発行者へ警告	→ https://www.ethnews.com/hong-kong-sfc-issues-letters-to-exchanges-and-ico-issuers-in-cryptocurrency-crac
中国	淘宝網、ICO関連サービスラインナップを禁止へ	→ https://rule.taobao.com/detail-7969.htm?spm=a2177.7231193.0.0.7d9017eaIUYMET&tag=self
中国	香港FSTBマネロンリスクレポート、ビットコインそのものに特段の金融犯罪関係は無いとした一方、匿名取引には潜在的マネロンリスクを指摘	→ http://news.8btc.com/hong-kong-report-grade-bitcoin-as-low-risk-in-financial-crime

②規制・制度 – 台湾

名称	サービス概略	URL
台湾	シンガポールにならった規制を検討	→ https://www.ethnews.com/taiwan-to-use-singapore-as-model-for-digital-asset-regulation
台湾	中央銀行がビットコインAML規制を提案	→ https://www.coindesk.com/taiwan-central-bank-proposes-money-laundering-rules-for-bitcoin/
台湾	既存AMLルールのもとにビットコイン規制へ	→ https://www.moj.gov.tw/dl-31999-2161ed4e21114a42a65ba413dc68a8d9.html

②規制・制度 – 韓国

名称	サービス概略	URL
韓国	ビットコインの先物・デリバティブ取引を禁止	→ https://www.coindesk.com/report-bitcoin-derivatives-banned-south-korean-government/
韓国	取引所の自主規制を制定	→ https://ethereum-japan.net/news/korea-is-drawing-up-bitcoin-regulations/ → https://themerkle.com/south-korea-to-permit-crypto-exchanges-under-6-conditions/
韓国	匿名アカウント作成禁止および当局による取引所閉鎖も可能とする規制強化へ	→ https://www.reuters.com/article/uk-southkorea-bitcoin/south-korea-to-impose-new-curbs-on-cryptocurrency-trading-idUSKBN1EM05K

②規制・制度 – 韓国

名称	サービス概略	URL
韓国	大手取引所へ警察・税務当局が急襲。取引禁止準備も	→ https://www.reuters.com/article/uk-southkorea-bitcoin/south-koreas-major-cryptocurreny-exchanges-raided-by-police-tax-authorities-idUSKBN1F002A → https://www.reuters.com/article/us-southkorea-bitcoin-law/south-koreas-justice-minister-says-preparing-a-bill-to-ban-cryptocurrency-trading-idUSKBN1F00B7
韓国	暗号通貨取引を禁止しない旨を表明	→ https://www.ccn.com/south-korea-govt-confirms-no-cryptocurrency-trading-ban-market-optimistic/
韓国	当局が、取引所むけ口座提供銀行６行の検査	→ http://bitguru.co.uk/south-korean-banks-face-inspection-for-accounts-linked-to-cryptocurrency/

②規制・制度 – 韓国

名称	サービス概略	URL
韓国	取引実名制を導入	→ https://coinchoice.net/crypto-currency-funds-clean-guidelines/
韓国	規制当局、通常の暗号通貨トランザクションはサポートする旨を表明	→ http://m.yna.co.kr/mob2/en/contents_en.jsp?cid=AEN20180220006500320&input=rss&site=02000000000&mobile
韓国	昨秋からのICO禁止に関する緩和を検討	→ https://www.ccn.com/south-korea-regulators-considering-reversal-ico-ban-report/
韓国	６月までに課税枠組発表へ	→ http://coinpost.jp/?p=20036
韓国	韓国財務相、暗号通貨は代替支払手段として法定通貨の脅威になると発言	→ https://themerkle.com/cryptocurrency-has-potential-to-threaten-fiat-south-koreas-finance-minister/

②規制・制度 – アジア域　タイ

名称	サービス概略	URL
タイ	ICO規制へ	→ https://news.bitcoin.com/thailand-taking-steps-to-regulate-icos/
タイ	金融当局、国内での暗号通貨利用を規制せず	→ https://news.bitcoin.com/thailand-regulators-stop-cryptocurrency-use-regulate/
タイ	仮想通貨規制の枠組を3月中公表	→ https://www.bangkokpost.com/business/news/1427642/cabinet-oks-digital-asset-draft-decrees
タイ	規制当局、暗号通貨キャピタルゲイン課税見直しを否定	→ https://themerkle.com/thai-regulators-reject-request-to-revamp-cryptocurrency-taxation-guidelines/

②規制・制度 – アジア域　マレーシア

名称	サービス概略	URL
マレーシア	暗号通貨向け規制フレームワークを検討	→ https://www.reuters.com/article/uk-malaysia-cenbank-cryptocurrency/malaysia-says-working-on-regulatory-framework-for-crypto-currencies-idUSKBN1DM0DQ
マレーシア	中銀が取引所むけ規制ドラフトを発表	→ http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4575&lang=en

②規制・制度 – アジア域　インドネシア

名称	サービス概略	URL
インドネシア	ビットコインおよび他の暗号通貨を禁止へ	→ https://themerkle.com/indonesia-will-officially-ban-bitcoin-and-other-cryptocurrencies/
インドネシア	中央銀行、暗号通貨によるペイメントは非合法との声明を発行し、売買・取引を行わないよう警告	→ http://www.bi.go.id/en/ruang-media/siaran-pers/Pages/sp_200418.aspx

②規制・制度 – アジア域　フィリピン

名称	サービス概略	URL
フィリピン	暗号通貨の取引およびICOの規制を検討	→ http://www.manilatimes.net/regulators-eye-wider-virtual-currency-use/364344/
フィリピン	SEC、クラウドマイニングを証券にあたるとの見方示す	→ http://www.sec.gov.ph/advisory-on-cloud-mining-contracts/
フィリピン	暗号通貨事業者優遇地域の開発を検討	→ https://bitsonline.com/philippines-creates-special-economic-zone-crypto-businesses/

②規制・制度 – アジア域 インド

名称	サービス概略	URL
インド	税務当局が取引所の検査を実施	→ https://timesofindia.indiatimes.com/business/india-business/income-tax-lens-on-bitcoin-exchanges-across-six-cities/articleshow/62060918.cms
インド	財務省が仮想通貨投資について注意するよう声明を発表	→ http://www.pib.nic.in/PressReleseDetail.aspx?PRID=1514568
インド	インド準備銀行、ビットコイン等の暗号通貨に関するリスクを警告	→ https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR15304814BE14A3414FD490B47B0B1BF79DDC.PDF
インド	政府によるビットコイン規制は困難との見方	→ https://news.bitcoin.com/india-cant-regulate-bitcoin-says-official/
インド	銀行口座からの暗号通貨購入を禁止	→ https://www.ccn.com/india-bans-banks-from-processing-cryptocurrency-purchases/
インド	RBI、銀行が暗号通貨関連の個人・企業と取引することを禁止	→ https://m.rbi.org.in//Scripts/BS_PressReleaseDisplay.aspx?prid=43574
インド	中央銀行による暗号通貨禁止に対して交換業界から請願書	→ https://www.ccn.com/delhi-high-court-issues-notice-to-rbi-union-of-india-and-gst-council-in-coinrecoils-petition/

②規制・制度 – アジア域　シンガポール

名称	サービス概略	URL
シンガポール	シンガポールMAS、暗号通貨投資に注意喚起	→ http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-cautions-against-investments-in-cryptocurrencies.aspx
シンガポール	MAS、暗号通貨取引禁止の理由無しと表明	→ http://www.mas.gov.sg/News-and-Publications/Parliamentary-Replies/2018/Reply-to-Parliamentary-Question-on-banning-the-trading-of-bitcoin-currency-or-cryptocurrency.aspx

②規制・制度 – アジア域　豪州

名称	サービス概略	URL
豪州	デジタル通貨交換業者にAML/CMF義務付けへ	→ http://www.austrac.gov.au/news/digital-currency-exchange-providers-register-online-austrac
豪州	交換業者にAUSTRAC登録義務づけ	→ http://www.abc.net.au/news/2018-04-11/cryptocurrencies-subject-to-anti-money-laundering-and-terrorism/9640642
豪州	豪州当局ASIC、既存ガイドラインをICO向けに拡張の意向示す	→ http://download.asic.gov.au/media/4711013/speech-john-price-icos-and-cryptocurrency-26-april-2018.pdf

②規制・制度 – 中東

名称	サービス概略	URL
UAE	規制当局SCA、投資家に対してICOへの警戒呼びかけ	→ http://www.sca.gov.ae/English/News/Pages/Articles/2018/2018-2-4.aspx
イスラエル	暗号通貨を課税対象とする旨を表明	→ https://cryptovest.com/news/its-confirmed-israel-will-treat-cryptos-as-property-for-tax-purposes/
イスラエル	当局、ユーティリティトークンと証券トークンの定義。ビットコインは証券と扱わず	→ https://www.coindesk.com/israel-regulators-utility-tokens-not-securities/ → https://taxes.gov.il/incometax/documents/hozrim/hoz_07_2018_acc.docx.pdf → https://news.bitcoin.com/israel-declares-bitcoin-is-not-a-security/
イラン	イラン中央銀行、暗号通貨取引を禁止	→ https://www.reuters.com/article/us-crypto-currencies-iran/iran-central-bank-bans-cryptocurrency-dealings-idUSKBN1HT0YN

②規制・制度 – アフリカ

名称	サービス概略	URL
モロッコ	暗号通貨利用に罰則ありと規制当局が警告	→ http://www.oc.gov.ma/portal/sites/default/files/actualites/communiqu%C3%A9%20monnaies%20virtuelles.pdf
ジンバブエ	中銀がビットコイン取引を違法と認識	→ https://cointelegraph.com/news/zimbabwean-central-bank-considers-bitcoin-illegal

②規制・制度 – 国際協調

名称	サービス概略	URL
IMF	暗号通貨に関する国際協調が必要と表明	→ https://www.bloomberg.com/news/articles/2018-01-18/imf-calls-for-global-talks-on-digital-fx-as-bitcoin-whipsaws
IMF	IMF専務理事、暗号通貨の安全性確保へ国際協力呼びかけ	→ https://jp.reuters.com/article/imf-head-on-crypto-currency-idJPKCN1GP27Z
金融安定理事会	「現時点で世界金融の安定を脅かす存在でなく技術的発展を見守るべき」として、G20におけるクリプトアセットへの規制強化呼びかけを否定	→ http://coinpost.jp/?p=18385 → http://www.fsb.org/wp-content/uploads/P180318.pdf
G20	クリプトアセットへの言及を行い閉幕	→ https://back-g20.argentina.gob.ar/sites/default/files/media/communique_g20.pdf → http://www.mof.go.jp/international_policy/convention/g20/180320.htm
IMF	政策立案にあたってはオープンマインドでクリエイティブな取組が身を結べるようにすべきと表明	→ https://blogs.imf.org/2018/04/16/an-even-handed-approach-to-crypto-assets/

②規制・制度 – 国際協調

- G20、クリプトアセットへの言及を行い閉幕
  - クリプトアセットを支える技術的イノベーションに効率性や金融包摂を改善するポテンシャルがあると認識しつつも、消費者・投資家保護や税金、マネロンの課題が取りざたされている。
  - クリプトアセットはソブリン通貨としての基本属性を満たすものではないが、ある時点で金融安定に影響をもたらす可能性がある。
  - FATFスタンダードをクリプトアセットへ適用。
  - クリプトアセットおよびそのリスクモニタリングを継続することを国際的標準化団体に求める。
  - 七月までに規制のリコメンドを提示。

  - 出所：
    - https://back-g20.argentina.gob.ar/sites/default/files/media/communique_g20.pdf
    - http://www.mof.go.jp/international_policy/convention/g20/180320.htm

③暗号通貨アダプション – 米国

名称	サービス概略	URL
米国	CME（シカゴマーカンタイル取引所）、ビットコイン先物をローンチ	→ http://www.cmegroup.com/media-room/press-releases/2017/12/01/cme_group_self-certifiesbitcoinfuturestolaunchdec18.html
米国	CBOE（シカゴオプション取引所）、ビットコイン先物をにローンチ	→ http://ir.cboe.com/~/media/Files/C/CBOE-IR-V2/press-release/2017/cboe-plans-december-10-launch-of-bitcoin-futures-trading.pdf
米国	Nasdaq、ビットコイン先物を2018年前半にローンチと発表	→ https://www.wsj.com/articles/nasdaq-plans-to-launch-bitcoin-futures-in-first-half-2018-1511968313
米国	ビットコインETF、米SEC懸念により提案取り下げ	→ https://www.cnbc.com/2018/01/08/fund-managers-say-bitcoin-etf-proposals-withdrawn-due-to-sec-concern.html

③暗号通貨アダプション – 米国

名称	サービス概略	URL
米国	インターコンチネンタル取引所（ICE）、Blockstreamと提携して暗号通貨データフィードを立ち上げ	→ https://blockstream.com/2018/01/18/ice-blockstream-deliver-consolidated-trading-data-service.html
米国	JP Morgan ChaseのJamie Dimon CEO、ビットコインを詐欺と称したことを「後悔」と表明	→ https://www.ft.com/content/e04e359a-e9e9-3f8e-8e2f-3f4373e5efb0
米国	Goldman、暗号通貨トレーディングデスク設置へ	→ https://www.bloomberg.co.jp/news/articles/2017-12-21/P1BYMQ6S972A01
米国	Goldman、暗号通貨はサブサハラアフリカのような通貨が価値を失った地域で代替通貨となる可能性ありとレポート	→ https://www.bloomberg.com/news/articles/2018-01-10/goldman-says-viability-of-crypto-is-highest-in-developing-world
米国	VISAのCEO、ビットコインはペイメントシステムではなく法定通貨以外のトランザクションはプロセシングするつもりが無い旨を表明	→ https://www.cnbc.com/2018/01/17/visa-will-not-process-bitcoin-transactions-says-ceo-alfred-kelly.html
米国	MoneyGram、XRP用いたペイメントのパイロット開発へ提携	→ http://ir.moneygram.com/releasedetail.cfm?releaseid=1054088

③暗号通貨アダプション – 米国（FINTECH系）

名称	サービス概略	URL
米国	株式トレードアプリRobinhood、手数料ゼロの暗号通貨売買サービスをロールアウト	→ http://blog.robinhood.com/news/2018/2/21/robinhood-crypto-trading-is-here
米国	PayPal、仮想通貨トランザクションシステムで特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180060860.PGNR.&OS=dn/20180060860&RS=DN/20180060860
米国	Square、BitLicence取得へむけ準備中	→ https://www.coindesk.com/cash-app-bitcoin-wyoming-bitlicense/
米国	ダウジョーンズグループ、プレミアコンテンツアクセスにBATを用いたペイメントを試行すべくBraveと提携	→ https://basicattentiontoken.org/dow-jones/

③暗号通貨アダプション – 米国（金融機関・ファンド）

名称	サービス概略	URL
米国	BofAおよびJP Morgan、暗号通貨購入目的のクレジットカード利用を中止	→ https://www.coindesk.com/report-bank-america-jp-morgan-ban-credit-crypto-purchases/
米国	MasterCard、ビットコインを条件付で受け入れ	→ https://crypto-lines.com/2018/03/19/mastercard-accepting-cryptocurrencies/
米国	ソロス氏、暗号通貨投資を準備	→ https://www.bloomberg.com/news/articles/2018-04-06/george-soros-prepares-to-trade-cryptocurrencies-as-prices-Plunge
米国	ロックフェラー系VCのVenrock、Coinfundと提携	→ https://blog.coinfund.io/venrock-and-coinfund-teams-announce-strategic-partnership-eb1277dd4658
米国	Nasdaq、規制市場における暗号通貨交換業者になることを志向している旨を表明	→ https://www.cnbc.com/2018/04/25/nasdaq-is-open-to-becoming-cryptocurrency-exchange-ceo-says.html
米国	Nasdaq、Geminiとの協業を発表	→ https://cointelegraph.com/news/winklevoss-crypto-exchange-partners-with-nasdaq-to-fight-market-manipulation-in-industry-first
米国	Goldman Sachs、ビットコイントレーディングオペレーションをウォール街に開設	→ https://www.nytimes.com/2018/05/02/technology/bitcoin-goldman-sachs.html

③暗号通貨アダプション – 米国(各州)

名称	サービス概略	URL
米国	アリゾナ州、ビットコインによる納税法案が前進中	→ https://legiscan.com/AZ/bill/SB1091/2018
米国	ジョージア州、ビットコインなどの暗号通貨による税金支払を認める法案	→ https://www.ccn.com/georgia-bill-would-allow-residents-to-make-bitcoin-tax-payments/
米国	Wisconsin州、暗号通貨による政治献金ガイドライン受け入れ検討	→ https://news.bitcoin.com/wisconsin-mulls-guidelines-for-campaign-contributions-in-bitcoin/
米国	Arizona州、暗号通貨購入時に納税トランザクションが州へ直接送信される法案	→ https://www.ccn.com/breaking-news-arizona-overhauls-blockchain-bill-to-focus-on-payments/
米国	California州、株券の発行・移転をブロックチェーンで行う法案	→ http://sd18.senate.ca.gov/news/4182018-hertzberg-presents-blockchain-bill-senate-banking-committee → https://legiscan.com/CA/text/SB838/id/1787257

③暗号通貨アダプション – 米国（交換業者）

名称	サービス概略	URL
米国	Coinbase、Coinbase Commerceボタンを追加できるマーチャント向けプラグインをローンチ	→ https://tokeneconomy.co/token-economy-35-the-failure-of-the-old-world-corporation-35ac2312eced
米国	Coinbase、適格投資家向けにCoinbase Index Fundを組成	→ https://blog.coinbase.com/announcing-coinbase-index-fund-3925fbf548db
米国	Coinbase、オープンソースに貢献するプロトコルチームを開設	→ https://blog.coinbase.com/introducing-the-coinbase-protocol-team-3bc1e9a63614
米国	Coinbase、Earn.comの買収を検討	→ https://www.coindesk.com/coinbase-talks-buy-one-bitcoins-best-funded-startups/
米国	Coinbase、ERC20サポートを発表	→ https://blog.coinbase.com/adding-erc20-support-to-coinbase-fe9cba6782b
米国	CoinbaseはSEC登録を目指す	→ https://www.wsj.com/articles/cryptocurrency-firm-coinbase-in-talks-to-become-sec-regulated-brokerage-1523043315

③暗号通貨アダプション – 米国(交換業者)

名称	サービス概略	URL
米国	Bitrex、USDTとTrueUSDのペア取引を開始へ	→ https://mobile.twitter.com/bittrexexchange/status/979419926917275651
米国	Goldman Sachs出資のCircle、Poloniexを4億ドルで買収	→ https://blog.circle.com/2018/02/26/circle-acquires-poloniex/
米国	Digital Currency Group、米Silvergate銀行へ112億円投資	→ https://jp.cointelegraph.com/news/crypto-vc-firm-digital-currency-group-invests-114-mln-in-pro-crypto-silvergate-bank
米国	Abra、20種類の暗号通貨をウォレット取扱対象に追加すると共に、50種類の法定通貨とのリアルタイムスワップを通じたstablecoin技術による投資プラットフォームを発表	→ https://www.abra.com/blog/decentralized-investment-platform/
米国	Gemini、機関投資家向けにブロックトレーディング導入	→ https://gemini.com/blog/introducing-gemini-block-trading/

③暗号通貨アダプション – 米国

- Abra、20種類の暗号通貨をウォレット取扱対象に追加すると共に、50種類の法定通貨とのリアルタイムスワップを通じたstablecoin技術による投資プラットフォームを発表
  - マルチシグのスマートコントラクトを用いて、Bitcoin/Litecoinベースのstablecoinを生成する投資プラットフォームを開発。
  - USD/EUR/JPYなどのstablecoinを用いて多額のトランザクションを実施してきており、今回これを他の暗号通貨を含むstablecoinへと拡張することによって、ユーザーが物理的な通貨保有無しに、暗号通貨や法定通貨への投資エキスポージャーを付与するとしている。
  - Bitcoin/LitecoinのP2SHスクリプト上のマルチシグコントラクトがUSDベースのゴールドETF投資契約をシミュレート。
  - ゴールドの契約であれば、ゴールドの価格が上昇すればユーザーはUSDを得て、ゴールドの価格が下落すればUSDを失うが、同様のことをUSDの代わりにBitcoin/Litecoinを用いて、AbraがP2SHスクリプトへのカウンターパーティとして行う。
  - これらスクリプト上でカウンターパーティリスクをヘッジするマーケットメイクオペレーションを実施。
  - これまでにこのオペレーションを通じて法定通貨・Bitcoin ・etherのカウンターパーティリスク管理を行ってきている。
  - 現在P2SHスクリプトはAbraを相手とする2of2マルチシグだが、本年中に他の法的管轄を第三署名とするOracle機能を追加予定。

  - 出所：
    - https://news.bitcoin.com/abra-mobile-app-adds-20-new-cryptocurrencies-and-stablecoin-technology/
    - https://www.abra.com/blog/decentralized-investment-platform/

③暗号通貨アダプション – カナダ

名称	サービス概略	URL
カナダ	オンタリオ州規制当局、カナダ初のブロックチェーンETFを承認	→ https://www.theglobeandmail.com/globe-investor/funds-and-etfs/etfs/osc-approves-canadas-first-blockchain-etf/article37828183/
カナダ	トロント証券取引所、暗号通貨の価格ベンチマーク情報提供など仲買サービス立ち上げへ	→ https://bitcoinmagazine.com/articles/tmx-launch-worlds-first-stock-exchange-cryptocurrency-brokerage-service/
カナダ	カナダBMO、デビットカードを用いた暗号通貨購入を禁止	→ https://www.coindesk.com/bank-of-montreal-expands-crypto-purchase-ban/

※薄文字は前四半期

③暗号通貨アダプション – 日本

名称	サービス概略	URL
日本	東京金融取引所、ビットコイン先物を検討	→ https://www.bloomberg.com/news/articles/2017-12-05/tokyo-financial-exchange-takes-first-step-toward-bitcoin-futures → https://www.nikkei.com/article/DGXMZO25376900V00C18A1EA4000/
日本	三菱UFJ信託銀行、取引所破産に備え信託で全額保全へ	→ https://www.nikkei.com/article/DGXMZO25047970V21C17A2MM8000/
日本	三菱東京UFJ銀行、1MUFGコインをほぼ1円へ価格誘導する独自仮想通貨MUFGコインの発行へむけて取引所を2018年度開設へ	→ https://mainichi.jp/articles/20180114/ddm/001/020/146000c
日本	SBIホールディングス、中国Huobiグループと提携	→ http://www.sbigroup.co.jp/news/2017/1207_10908.html
日本	SBI BITS、nChainとパートナーシップ締結	→ http://www.sbibits.com/download/Press_Release_SBI%20Group_nChain_strategic_partnership_JP.pdf

③暗号通貨アダプション – 日本

名称	サービス概略	URL
日本	GMOインターネット、給与の一部を購入枠最大10万円をビットコインで受け取れる制度を導入	→ https://prtimes.jp/main/html/rd/p/000002271.000000136.html
日本	テックビューロ、仮想通貨で給与上乗せ3割相当分	→ https://www.nikkei.com/article/DGXMZO25098530W7A221C1EE9000/
日本	DMM.com、仮想通貨のマイニングマシン研究開発チーム新設	→ https://dmm-corp.com/press/press-release/20963
日本	LINE、ビットコイン等の仮想通貨決済導入を検討中	→ https://www.bloomberg.co.jp/news/articles/2018-01-09/P2A5386JTSE901
日本	フィスコ、仮想通貨ヘッジファンド立ち上げへ	→ http://www.fisco.co.jp/uploads/20180110_fisco_pr.pdf
日本	メルカリ、子会社メルペイを通じて仮想通貨取引業登録申請へ	→ http://itpro.nikkeibp.co.jp/atcl/news/17/011002935/
日本	freee、仮想通貨の確定申告をサポート	→ https://headlines.yahoo.co.jp/hl?a=20180111-35113010-cnetj-sci
日本	ヤマダ電機、ビットコイン決済導入	→ https://www.nikkei.com/article/DGXMZO26134650V20C18A1TJ2000/

③暗号通貨アダプション – 日本

名称	サービス概略	URL
日本	LINE、持株会社設立し暗号通貨提供へ	→ https://www.bloomberg.co.jp/news/articles/2018-01-30/P3CVL96K50YG01
日本	DMM、金沢にマイニングファーム	→ https://www.houdoukyoku.jp/posts/25880
日本	GMOインターネットのZ.com Cloud Mining、8月開始にむけて3/1より事前申込開始	→ https://cloudmining.z.com/ja/
日本	GMO、3月分のマイニング事業収益を開示	→ https://www.gmo.jp/news/article/?id=6001 → https://www.gmo.jp/news/article/?id=5967
日本	ヤフー、登録業者ビットアルゴに資本参加し仮想通貨交換業に参入	→ https://www.nikkei.com/article/DGXMZO28495990T20C18A3I00000/
日本	筑波大学・落合陽一氏がReadyforでビットコイン寄付受付開始	→ https://readyfor.jp/projects/ochyaigogo2
日本	仮想通貨・ブロックチェーン企業限定 合同企業説明会が開催	→ https://withb.co.jp/lp/jobfair01/

③暗号通貨アダプション – 日本

名称	サービス概略	URL
日本	OmiseとOmiseGOが韓国 新韓カードとMoU締結	→ https://www.omise.co/omise-and-omisego-sign-mou-with-shinhancard-to-explore-opportunities-for-fintech-and-blockchain-initiatives
日本	Omise、取引所開設へ。PoSステークする取引量をもつべく、流動性提供	→ https://blog.omisego.network/strategy-vol-02-89a4d8476eed
日本	新電力会社の熊本電力、マイニング事業参入	→ https://prtimes.jp/main/html/rd/p/000000012.000024573.html
日本	SBIホールディングス、Huobiグループとの資本・業務提携取り止めを発表	→ http://www.sbigroup.co.jp/news/2018/0309_11020.html
日本	SBIホールディングス、コールドウォレットを手がける台湾CoolBitXへの出資を発表	→ http://www.sbigroup.co.jp/news/2018/0302_11009.html
日本	SBIホールディングス系モーニングスター、Coindeskと業務提携	→ http://www.sbigroup.co.jp/news/2018/0223_10999.html
日本	bitbank.cc、「仮想通貨を貸して増やす」サービス開始	→ https://bitbank.cc/blog/bitbank-lending-launch-announce/

③暗号通貨アダプション – 日本

名称	サービス概略	URL
日本	企業会計基準委員会ASBJ、仮想通貨の会計処理に関する取扱を決定	→ https://www.asb.or.jp/jp/accounting_standards/practical_solution/y2018/2018-0314.html
日本	企業会計基準委員会ASBJ、4月のASAF会議向けに仮想通貨に関するペーパーを提出	→ https://www.asb.or.jp/jp/ifrs/asaf/y2018/2018-0416/2018-0315.html
日本	財務省、3000万超相当の仮想通貨による海外送金を当局報告とするルール整備へ	→ https://www.nikkei.com/article/DGXMZO29013240U8A400C1EE8000/

③暗号通貨アダプション – 韓国

名称	サービス概略	URL
韓国	Samsung、ASICチップおよびマイニング機器製造を開始	→ https://www.newsbtc.com/2018/01/30/samsung-south-koreas-largest-company-manufacturing-asic-chips-bitcoin-mining/
韓国	Kakao、2018年中に暗号通貨の取り込みを計画	→ https://www.ccn.com/south-koreas-kakao-integrate-cryptocurrency-12000-merchants-millions-users/
韓国	Bithumb、レストランでのペイメントに使えるキオスク端末サービスを立ち上げ予定	→ https://news.bitcoin.com/bithumb-launching-kiosks-restaurants-food-orders-crypto-payments-korea/
韓国	ソウル市、独自暗号通貨を検討	→ https://cointelegraph.com/news/seoul-mayor-aims-to-launch-capitals-own-crypto-establish-better-environment-for-blockchain-startups

③暗号通貨アダプション – 中国

名称	サービス概略	URL
中国	中国人民銀行総裁、暗号通貨を決済手段として認めず、”DCEP(digital currency electronic payment)”検討	→ https://jp.reuters.com/article/china-parliament-pboc-0309-idJPKCN1GL272 → https://bitsonline.com/china-digital-currency-dcep/
中国	Bitmain、ブロックチェーンを活用した民間中央銀行の設立を構想	→ https://btcnews.jp/15tnvomj15383/
中国	中国CoinEx、USDTのクレジットデフォルトスワップ取扱開始	→ https://www.coinex.com/cds
中国	香港Bitfinex、JPYおよびGBPとの間のペアを追加する旨を発表	→ http://blog.bitfinex.com/announcements/fiat-trading-pair-additions/
中国	香港Bitfinex傘下のEthfinex、Daiをサポート開始すると発表	→ https://blog.ethfinex.com/announcing-dai-integration-da1484ed86f
中国	香港Ethfinexは集中型ExchangeとDEXを繋いでハイブリッドを目指す。Dai/USDTペア取扱はその第一歩とのこと	→ https://blog.ethfinex.com/announcing-dai-integration-da1484ed86f
中国	香港OKexもBinanceに続いて欧州マルタに拠点開設	→ https://news.bitcoin.com/malta-succeeds-in-attracting-another-cryptocurrency-exchange-okex/

③暗号通貨アダプション – 台湾

名称	サービス概略	URL
台湾	遠東航空、暗号通貨による支払を受け入れへ	→ http://news.8btc.com/china-far-eastern-air-transport-announce-to-accept-cryptocurrency-payment
台湾	鴻海精密工業、仮想通貨の商業銀行設立を計画	→ http://www.quick.co.jp/6/article/14306
台湾	Foxconn、暗号通貨を支払い手数料無く扱い、トークンをサポートしトークンに変換可能な携帯電話を開発へ	→ https://www.newsbtc.com/2018/04/05/sirin-labs-hires-foxconn-to-manufacture-worlds-first-blockchain-phone/

③暗号通貨アダプション – アジア太平洋域

名称	サービス概略	URL
インド	インド財務相、暗号通貨を決済通貨として利用する可能性を排除する姿勢を発表	→ https://qz.com/1195316/budget-2018-busts-bitcoin-arun-jaitley-has-just-killed-indias-cryptocurrency-party/
カンボジア	カンボジア、米国による経済制裁の中で、ベネズエラ・トルコ・イランに続いて独自仮想通貨Entapay発行検討と発表	→ https://jp.cointelegraph.com/news/inspired-by-venezuelan-petro-cambodia-may-issue-a-national-cryptocurrency → https://www.prnewswire.com/news-releases/cambodia-may-issue-its-legal-cryptocurrency-following-venezuela-300607358.html
豪州	ブリスベン空港、空港内店舗でのBTC/ETH/DASHペイメント受付	→ http://bitguru.co.uk/brisbane-airport-to-accept-cryptocurrency-payments/

③暗号通貨アダプション – 中東・アフリカ域

名称	サービス概略	URL
エジプト	エジプト政府、市民のコンピュータをMoneroマイニングにリダイレクト	→ https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/
南アフリカ	南アフリカ歳入庁（SARS）、暗号通貨に係る税金取扱方針を提示	→ http://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-of-cryptocurrencies-.aspx

③暗号通貨アダプション – ロシア

名称	サービス概略	URL
ロシア	ロシア～トルコ間の3000トンの小麦輸送でビットコイン決済	→ https://news.bitcoin.com/3000-metric-tons-of-wheat-was-recently-traded-for-bitcoin/
ロシア	ベネズエラによるPetro立ち上げサポートを表明	→ https://www.coindesk.com/report-russians-helped-venezuela-launch-petro/
ロシア	カリーニングラードのホテルがW杯期間中の支払いでビットコイン受け入れ	→ https://news.bitcoin.com/russian-hotels-to-surprise-world-cup-fans-with-bitcoin-payments/
ロシア	ガスプロムバンクが仮想通貨取引を試行	→ https://bitpress.jp/column/fisco/entry-8439.html
ロシア	特許発行手続きへのブロックチェーン利用をサポートへ	→ https://rns.online/it-and-media/Minkomsvyaz-podderzhalo-vnedrenie-blokcheina-v-protseduru-oformleniya-patentov-2018-04-02/
ロシア	Sberbank、ルーブルでビットコイン購入できる交換業Sberkoin開設	→ https://steemit.com/crypto/@samdman/the-crypto-exchanger-sberkoin-was-opened-in-moscow

③暗号通貨アダプション – 欧州（金融機関）

名称	サービス概略	URL
イギリス	Barclays、機関投資家向けに暗号通貨トレーディングデスク	→ https://theicojournal.com/source-barclays-commissions-cryptocurrency-trading-desk-reaching-out-to-hedge-funds-institutional-investors/
イギリス	Barclays、暗号通貨トレーディングデスク設置を検討	→ https://www.bloomberg.com/news/articles/2018-04-16/barclays-is-said-to-be-sounding-out-clients-about-trading-Crypto
ドイツ	証券取引所SWB、カナダTMXに続き子会社で暗号通貨取引アプリ	→ https://www.bisonapp.de/
オランダ	Rabobank、オンラインバンキングに暗号通貨ウォレット追加を検討	→ https://bitcoinmagazine.com/articles/major-dutch-bank-considering-cryptocurrency-wallet-its-customers/
リヒテンシュタイン	Bank Frick、投資家むけに暗号通貨投資サービス提供	→ https://www.coindesk.com/liechtenstein-bank-opens-up-cryptocurrency-investment-for-clients/

③暗号通貨アダプション – 欧州（行政府）

名称	サービス概略	URL
EU	Europol、欧州域内の犯罪収益の4%が暗号通貨を使いロンダリングされていると発表	→ https://www.newsbtc.com/2018/02/13/europol-estimates-cryptocurrencies-account-for-4-of-illicitly-trafficked-cash-in-europe/
イギリス	英政府、クリプトアセットタスクフォースをBoEやFCAと協働で設立	→ https://www.gov.uk/government/news/fintech-sector-strategy-launched-at-international-fintech-conference
ドイツ	ドイツ国民観光局、ビットコイン受け入れへ	→ http://cryptocurrencymagazine.com/german-national-tourism-board-accept-bitcoin → https://news.bitcoin.com/germanys-tourism-board-accepts-bitcoin-payments/
スペイン	ブロックチェーン関連企業やICO発行者の誘致へ向けた税制優遇を検討	→ https://www.ccn.com/spains-government-prepares-lure-blockchain-firms-ico-issuers/

※薄文字は前四半期

④ICO – 米国

名称	サービス概略	URL
米国	SEC、カナダのPlexCorpsをICOにまつわるスキャムで告訴し1500万ドル没収	→ https://www.sec.gov/news/press-release/2017-219
米国	SEC、MuncheeのICO停止	→ https://www.sec.gov/litigation/admin/2017/33-10445.pdf → https://www.sec.gov/news/press-release/2017-227 → https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11
米国	北米証券監督者協会、暗号通貨およびICOに関して声明発表	→ https://www.sec.gov/news/public-statement/statement-clayton-stein-piwowar-010418 → http://www.nasaa.org/44073/nasaa-reminds-investors-approach-cryptocurrencies-initial-coin-offerings-cryptocurrency-related-investment-products-caution/
米国	米国金融業規制機構（FINRA）、スキャムへの注意喚起を発表	→ http://www.finra.org/investors/alerts/dont-fall-cryptocurrency-related-stock-scams

④ICO – 米国

名称	サービス概略	URL
米国	Google、六月から暗号通貨およびICOの広告禁止へ	→ https://support.google.com/adwordspolicy/answer/7648803?hl=en
米国	Twitter、ICOおよびほぼ全ての暗号通貨交換業者の広告を禁止へ	→ https://www.cnbc.com/2018/03/26/twitter-bans-cryptocurrency-advertising-joining-other-tech-giants-in-crackdown.html
米国	Facebook、ICOや暗号通貨に関するプロモーションを禁止するポリシーを制定	→ https://www.zerohedge.com/news/2018-01-30/facebook-bans-bitcoin-ico-ads
米国	米SEC、AriseBankのICOをスキャムとして停止	→ https://www.sec.gov/news/press-release/2018-8
米国	米SEC、三件のICO案件の取引を停止処分	→ https://www.sec.gov/news/press-release/2018-20
米国	米SEC、tZEROを含むICOに関して召喚状発行し調査開始	→ http://jp.wsj.com/articles/SB12346302927663484593304584073882534179484
米国	PraetorianGroup、不動産投資ICOを証券公開としてSEC申請	→ http://www.praetoriangroup.io/ → https://www.sec.gov/Archives/edgar/data/1721980/000137647418000045/pr_s1.htm

④ICO – 米国

名称	サービス概略	URL
米国	tZERO、トークントレーディングシステムの動画公開	→ https://www.tzero.com/#demo-videos
米国	米国、大統領令にてベネズエラ政府により発行されたあらゆるデジタルコインに関するあらゆるトランザクションを禁止	→ https://www.whitehouse.gov/presidential-actions/executive-order-taking-additional-steps-address-situation-venezuela/
米国	ルイジアナ州Lafayette、Berkeleyに続きデジタル通貨発行しICO	→ http://www.theadvocate.com/acadiana/news/article_3698996a-3e9b-11e8-a53c-17d7ea1c02d4.html

④ICO – 南米

名称	サービス概略	URL
ベネズエラ	原油資産を裏付けとしたERC20トークンPetroを発行するICOを通じて50億ドルの調達を目指す	→ http://www.elpetro.gob.ve/Whitepaper_Petro_en.pdf
ベネズエラ	Petroは8240万単位が利用可能に	→ https://www.telesurtv.net/english/news/Venezuela-82.4M-Units-of-Petro-Cryptocurrency-Available-20180220-0004.html
ベネズエラ	中国格付け機関Dagong Global Credit Rating、ベネズエラPetroについてレポート	→ http://en.dagongcredit.com/index.php?m=content&c=index&a=show&catid=20&id=4950
ベネズエラ	OPECへ公式にPetroを提案へ。一方で裏付資産が無いとの指摘も	→ https://www.trustnodes.com/2018/02/07/venezuela-officially-propose-crypto-backed-petro-opec
ベネズエラ	市民動員による暗号通貨マイニング支援プログラム開始	→ https://btcnews.jp/f9a4hqf715480/
ベネズエラ	Petro用いてロシアから自動車部品購入	→ https://news.bitcoin.com/venezuela-to-use-the-petro-to-buy-auto-parts-from-russia/
ベネズエラ	インドへPetro用いた原油購入に30%ディスカウント提案	→ http://www.business-standard.com/article/markets/venezuela-offers-india-30-discount-on-crude-but-with-cryptocurrency-rider-118042900018_1.html

④ICO – 日本

名称	サービス概略	URL
日本	SBIホールディングス、ICOにより500億円調達すると発表	→ https://www.nikkan.co.jp/articles/view/00461959

④ICO – 米国以外

名称	サービス概略	URL
中東	ベネズエラに続いてトルコ・イランも政府発行暗号通貨を計画	→ https://cointelegraph.com/news/turkey-iran-to-release-state-backed-cryptocurrencies-on-heels-of-venezuelas-petro
イラン	独自ローカル暗号通貨を実験的に開発	→ https://www.reuters.com/article/uk-crypto-currency-iran/iran-cryptocurrency-project-on-track-despite-cenbank-ban-minister-says-idUSKBN1HZ0O6
アジア太平洋	マーシャル諸島、独自仮想通貨ソブリン発行しICOへ	→ https://jp.cointelegraph.com/news/marshall-islands-plans-to-launch-national-cryptocurrency-and-ico-govt-officials-report
欧州	仏当局AMF、暗号通貨デリバティブの広告を禁止	→ https://www.trustnodes.com/2018/02/22/french-fca-bans-crypto-derivatives-advertising
ロシア	Telegram、ICOで1800億円を調達	→ https://news.bitcoin.com/telegrams-ico-has-raised-1-7-billion-but-not-everyone-is-impressed/

⑤中央銀行 – 日本

名称	サービス概略	URL
日本	日銀FinTechセンター長、法定デジタル通貨について「技術的には可能だが検討段階にはない」とコメント	→ https://www.bloomberg.co.jp/news/articles/2018-01-28/P35GIW6TTDS001

⑤中央銀行 – 中国

名称	サービス概略	URL
中国	中国社会科学院、各国中央銀行は国際決済で仮想通貨を検討すべきと進言	→ https://jp.reuters.com/article/china-crytocurrency-cenbank-idJPKBN1FR18P
中国	中国投資協会、ブロックチェーンの投資・開発センター立ち上げへ	→ https://www.ethnews.com/govt-affiliated-investment-association-in-china-to-launch-blockchain-center
中国	PBoC、中央銀行発行デジタル通貨へむけた計画を強調	→ https://www.ethnews.com/amp/pboc-deputy-governor-highlights-digital-currency-at-party-conference#click=https://t.co/P5OEiiq6sd
中国	PBoC、ブロックチェーンの追跡可能性やスマートコントラクトを賞賛の一方でスケーラビリティのボトルネックを解消すべく絶対的な非中央分散を諦めるべきと主張	→ http://m.yicai.com/news/5418853.html

⑤中央銀行 – 米国

名称	サービス概略	URL
米国	セントルイスFRB、中央銀行が支払形態として暗号通貨を適用する場合のコントロール構造に関するレポート発表	→ https://research.stlouisfed.org/publications/review/2018/02/13/the-case-for-central-bank-electronic-money-and-the-non-case-for-central-bank-Cryptocurrencies
米国	セントルイスFRB、ビットコインは三つの点で通常の通貨と似ている旨の整理	→ https://www.stlouisfed.org/open-vault/2018/april/three-ways-bitcoin-regular-currency

※薄文字は前四半期

⑤中央銀行 – 欧州（イギリス）

名称	サービス概略	URL
イギリス	The Bank of England総裁、中央銀行デジタルマネーへの問題意識を表明	→ https://www.reuters.com/article/uk-britain-boe-carney-bitcoin/bank-of-englands-carney-bitcoin-is-not-a-financial-stability-problem-idUSKBN1EE1ZO
イギリス	The Bank of England、ポンドとリンクした暗号通貨の導入可能性を検討中	→ http://www.telegraph.co.uk/news/2017/12/30/bank-england-plots-bitcoin-style-digital-currency/
イギリス	The Bank of England、商業銀行からの預金引き出しなど不安定化の懸念からデジタル通貨発行計画をキャンセル	→ https://themerkle.com/bank-of-england-cancels-plans-to-issue-a-digital-currency/
イギリス	BoE、RGTS刷新へむけてClearmaticsやR3とPoCへ	→ https://www.bankofengland.co.uk/-/media/boe/files/payments/rtgs-renewal-proof-of-concept.pdf
イギリス	BoE、DLT上でのプライバシーについてChainとPoC実施へ	→ https://www.bankofengland.co.uk/-/media/boe/files/fintech/chain.pdf

⑤中央銀行 – ロシア

名称	サービス概略	URL
ロシア	BRICSおよび欧州経済連合諸国による単一仮想通貨を構想	→ https://www.rt.com/business/414444-brics-eeu-joint-cryptocurrency/
ロシア	ハッカーによるSWIFTのメッセージシステム攻撃によりロシア中央銀行から600万ドル不正送金	→ https://jp.reuters.com/article/russia-cyber-swift-idJPKCN1G00I5
ロシア	ロシア中央銀行、EAEU向けペイメントネットワークをEthereumベースのMasterchain上にデプロイする考えを表明	→ https://www.ethnews.com/russian-central-bank-pitches-ethereum-platform-to-support-eaeu-payments-network
ロシア	ロシア中央銀行、ブロックチェーン上に預金者の統合登録簿を作成	→ http://cryptorussian.blogspot.com/2018/03/blog-post_19.html
ロシア	ロシア中銀、国内送金SPFSにEthereum利用適用検討	→ https://bitcoinist.com/russia-may-use-ethereum-blockchain-swift-payments/

⑤中央銀行 – アジア・太平洋域

名称	サービス概略	URL
シンガポール	MAS、Project Ubin フェーズ2を発表	→ http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20Phase%202%20Reimagining%20RTGS.pdf → https://bitsonblocks.net/2017/11/14/mas-just-released-corda-for-central-banks-so-what/ → https://github.com/project-ubin/ubin-quorum/blob/master/README.md
カンボジア	chaintope、カンボジア国立銀行及びカンボジア企業と仮想通貨開発を開始	→ https://prtimes.jp/main/html/rd/p/000000002.000030542.html
オーストラリア	オーストラリア準備銀行、e-AUDに関するスピーチ	→ https://www.rba.gov.au/speeches/2017/sp-gov-2017-12-13.html
インドネシア	暗号通貨デジタルルピアの試行を計画	→ https://www.ethnews.com/bank-indonesia-plans-state-issued-cryptocurrency-trial
シンガポール	MAS、国際ペイメントにおけるブロックチェーン利用を表明	→ http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2018/Crypto-Tokens-The-Good-The-Bad-and-The-Ugly.aspx

⑤中央銀行 – 中東

名称	サービス概略	URL
サウジアラビアとUAE	合同でデジタル通貨を検討	→ http://m.gdnonline.com/details.html?id=298264
イスラエル	ブラックマーケット抑制にむけて暗号通貨導入を検討	→ https://cointelegraph.com/news/israel-government-considering-national-cryptocurrency
南アフリカ	南ア中央銀行、Ethereumベースの銀行間決済	→ https://www.ccn.com/south-africas-central-bank-plots-ethereum-based-blockchain-pilot/
イラン	イラン中央銀行、暗号通貨取引を禁止	→ https://www.reuters.com/article/us-crypto-currencies-iran/iran-central-bank-bans-cryptocurrency-dealings-idUSKBN1HT0YN
サウジアラビア	サウジアラビア中央銀行、Rippleを用いたクロスボーダーペイメントのパイロット	→ https://ripple.com/insights/ripple-and-saudi-arabian-monetary-authority-offer-pilot-program-for-saudi-banks/
南アフリカ	南アSARB、Quorumを用いた銀行間送金のパイロットをConsenSysと協業で実施	→ https://www.ethnews.com/south-african-reserve-banks-fintech-programme-to-pilot-quorum-for-interbank-transfers

⑤中央銀行 – 南米

名称	サービス概略	URL
ウルグアイ	法定デジタル通貨の試験運用開始	→ https://www.nikkei.com/article/DGXMZO23403080T11C17A1EE9000/
ブラジル	ブラジル開発銀行、レアルをPublic Ethereum上でトークン化して透明性向上図る	→ https://www.trustnodes.com/2018/03/06/brazilian-state-bank-tokenize-brazilian-real-ethereums-public-blockchain
ベネズエラ	若者むけに暗号通貨銀行創設へ	→ https://www.telesurtv.net/english/news/Venezuela-to-Create-Digital-Cryptocurrency-Bank-for-Youth-20180503-0026.html

⑤中央銀行 – 国際協調

名称	サービス概略	URL
BIS	BIS、中央銀行発行デジタル通貨に関するレポートを発表し、慎重な検討を進めるべきと示唆	→ https://www.bis.org/cpmi/publ/d174.pdf
IBM	IBM、中央銀行発行デジタルマネーに向けて20行へアプローチ	→ https://www.coindesk.com/ibm-evolution-big-blue-finally-getting-serious-cryptocurrency/

5. Enterprise/Government系

5-1. プラットフォーム分野
5-2. ライフスタイル分野
5-3. サプライチェーン分野
5-4. シビックテック分野
5-5. 金融分野

5-1) プラットフォーム分野
ブロックチェーンプラットフォーム開発の進展

名称	サービス概略	URL
mijin	「mijin v.2 (Catapult)」オープンソース化プロジェクトを開始	→ http://mijin.io/ja/catapult
mijin	mijin v.1、Azure Marketplaceに採用	→ http://mijin.io/ja/1640.html
Digital Asset	エンタープライズスマートコントラクト開発プログラムをオープン	→ https://cdn2.hubspot.net/hubfs/2704830/Press%20Releases/PRESS%20Release%20-%20Digital%20Asset%20Developer%20Ecosystem.pdf
Lisk	Lisk Core 1.0.0をベータリリース	→ https://blog.lisk.io/lisk-core-1-0-0-open-beta-released-intensified-testing-reddit-ama-announcement-Cea7297415cd

5-1) プラットフォーム分野
中国勢によるBaaSプラットフォーム開発の加速

名称	サービス概略	URL
中国テンセント	BaaSとしてTrustSQL開発中	→ https://trustsql.qq.com/chain_oss/index_gw.html
中国Baidu	BaaSとしてBaidu Blockchain Open Platformローンチ	→ https://chain.baidu.com/
中国JD	サプライチェーントラッキングや課税などのアプリケーション開発向けBaaSプラットフォーム開発へ	→ https://www.coindesk.com/e-commerce-giant-jd-to-launch-blockchain-as-a-service-platform/
中国紙幣ブロックチェーン研究所	BaaSプラットフォームBROP（Blockchain Registry Open Platform）発表	→ http://www.zcblockchain.com/m.index.html → http://www.zcblockchain.com/images/whitepaper.pdf
中国Huawei	Hyperledger Fabric上にBlockchain Serviceプラットフォーム開発	→ https://www.huaweicloud.com/product/bcs.html → https://static.huaweicloud.com//upload/files/pdf/20180411/20180411144924_27164.pdf
中国Xunlei（迅雷）	dapps開発むけプラットフォームThunderChain開発	→ https://www.coindesk.com/xunlei-launches-blockchain-platform-amid-ongoing-ico-lawsuits/

5-1) プラットフォーム分野
テクノロジー大手も開発着手

名称	サービス概略	URL
Oracle	BaaSとしてOracle Blockchain Cloud Service ローンチ	→ https://www.oracle.com/cloud/blockchain/index.html
AWS	Ethereum（パブリック/プライベート）およびHyperledger Fabricむけデプロイ用テンプレート提供へ	→ https://aws.amazon.com/about-aws/whats-new/2018/04/introducing-aws-blockchain-templates/
Google	クラウドビジネスサポート向けにブロックチェーン関連技術を検討	→ https://www.bloomberg.com/news/articles/2018-03-21/google-is-said-to-work-on-its-own-blockchain-related-Technology
LINE	トークンエコノミー活かしたdapps開発促進へ独自ブロックチェーン	→ http://coinpost.jp/?p=23509
SAP社（前クール紹介済み）	”SAP Leonardo Blockchain Early Access”発表	→ http://cloud.watch.impress.co.jp/docs/column/infostand/1085120.html

5-1) プラットフォーム分野
大手による特許戦略も進む

名称	サービス概略	URL
Intel	Bitcoinマイニングハードウェアアクセラレータで特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180089642.PGNR.&OS=dn/20180089642&RS=DN/20180089642
IBM	テストタスクをマイナーに割り当て、タスク完了の報酬を暗号通貨で渡すもの特許。 ハードウェア集約的になった自動ソフトウエアテストのリソースコスト削減図る	→ http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=9,934,138.PN.&OS=pn/9,934,138&RS=PN/9,934,138

5) Enterprise/Government系

5-1) プラットフォーム分野

IETF、「The Decentralized Internet Infrastructure Research Group (DINRG)」を立ち上げ

- 取組背景
  - 当初インターネットは分散システムとして設計されたが、時を経る中で、中央集権的な会計・管理に基づくビジネスモデルにより、中央集権・階層的なものとなった。
  - 昨今の分散システム技術の進化に伴い、IoTのようなユースケースも現れ始めている。
  - 或いは、分散ネームサービス（Ethereum Name Serviceなど）、アイデンティティ管理（OneNameなど）、分散ストレージ（IPFSなど）、DApps（Blockstackなど）といった関連技術なども進化を遂げつつある。
  - こうしたシステムをインターネット技術の見地から調査し、IRTFやIETFの専門家と、分散システムコミュニティとを繋ぐことに取り組む上では、このタイミングが好機という考え。

- 取組内容
  - 分散インフラサービスである、トラスト管理やアイデンティティ管理、名前解決、オーナーシップ管理などに取り組む。
  - 具体的には、「ユースケースおよびこれを分散的方法で実装するための必要要件の調査」「スケーラビリティ・パフォーマンス・セキュリティなどインターネットレベルでのデプロイへのソリューションの討議・評価」「技術的ソリューションやベストプラクティスの開発」「スケーラビリティイシューを特定するツールや指標の開発」「IETFが将来的に取り組むべきテーマの特定」など。

- 取組上の課題
  - 「グローバルスケールな分散インフラサービスを実現する上でのスケーラビリティ」「分散コミュニケーションにおけるトラスト管理」「検証可能な情報開示と両立するプライバシー」「ユースケースへの適用可能性」「インターネット基盤サービスにフォーカスした特定シナリオむけコンセンサスアルゴリズム」など。

→ 出典：https://datatracker.ietf.org/rg/dinrg/about/

5-2) ライフスタイル分野
A)ロイヤリティ・流通

名称	サービス概略	URL
シンガポール航空	ブロックチェーンベースのロイヤルティウォレットをローンチへ	→ https://www.singaporeair.com/en_UK/sg/media-centre/press-release/article/?q=en_UK/2018/January-March/ne0518-180205
ドバイ	観光業むけB2Bマーケットプレイス開発を計画	→ http://www.arabianbusiness.com/travel-hospitality/390892-dubai-plans-to-create-blockchain-marketplace-for-Tourism

5-2) ライフスタイル分野
B)ペイメント

名称	サービス概略	URL
Amazon	ストリーミングデータ売買分野での特許。暗号通貨トランザクションをリアルタイムで受信	→ http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=9,947,033.PN.&OS=pn/9,947,033&RS=PN/9,947,033
Walmart	ペイメント情報の安全管理へ向けた特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180108010.PGNR.&OS=dn/20180108010&RS=DN/20180108010
Walmart	認証されてない他者からのアクセス不可とする特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180107977.PGNR.&OS=dn/20180107977&RS=DN/20180107977

5-2) ライフスタイル分野
C)アイデンティティ

名称	サービス概略	URL
カナダ・オランダ	エアラインセキュリティ・透明性向上へブロックチェーンIDシステムKnown Traveler Digital Identityのパイロット試行	→ https://nrc-cnrc.explorecatena.com/en/ → http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf → http://www.tokenverse.com/news/canada-looks-to-blockchain-for-airline-security-government-transparency/
Omise	タイ政府とデジタルアイデンティティに向けたMOU締結	→ https://www.ethnews.com/omise-signs-mou-to-participate-in-official-thai-digital-id-project

5-2) ライフスタイル分野
D)通信キャリア

名称	サービス概略	URL
Carrier Blockchain Study Group	通信キャリア業界むけブロックチェーンコンソーシアム	→ https://www.softbank.jp/en/corp/group/sbm/news/press/2018/20180223_01/
ソフトバンク	ブロックチェーン活用した送金・決済で海外通信大手と通信連合	→ https://www.nikkei.com/article/DGXMZO27625350S8A300C1X30000/ → https://iotnews.jp/archives/67847

5-2) ライフスタイル分野
E)クルマ

名称	サービス概略	URL
ポルシェ	自動運転への活用めざし車両にEthereumブロックチェーン搭載へ	→ https://www.trustnodes.com/2018/02/27/porsche-launches-ethereum-based-blockchain-pilot-smartify-cars
ダイムラーAG	優良ドライバーむけインセンティブmobiCOIN発行	→ https://blog.daimler.com/2018/02/12/mobicoin-testphase/
Ford	自動車間通信への暗号通貨利用で特許	→ https://news.bitcoin.com/ford-cryptocurrency-inter-vehicle-communication-system/
Ford	交通渋滞解消にトークン利用システムを開発、特許を取得へ	→ https://coinchoice.net/eliminate-traffic-congestion-token/
Audi	流通ネットワークにおけるブロックチェーン利用を検討	→ https://cointelegraph.com/news/audi-is-exploring-blockchain-for-its-distributional-network
BMWやBosch、Ford、GM、ルノー等	Mobility Open Blockchain Initiative（MOBI）立ち上げを発表	→ https://docs.wixstatic.com/ugd/bd1fb8_4e16d895b37e4b2a9d4dafdbb82cef2a.pdf → https://www.dlt.mobi/

5-2) ライフスタイル分野
F)エネルギー

名称	サービス概略	URL
中部電力	Lightning Networkを用いて、Nayutaおよびインフォテリアと電気自動車の充電支払実験	→ http://www.chuden.co.jp/corporate/publicity/pub_release/press/3267230_21432.html → http://jp.techcrunch.com/2018/03/01/nayuta-lightning-network/
東京電力	ブロックチェーンベースのスマートエネルギーを目指すElectifyとMoU締結	→ https://medium.com/electrifyasia/befriending-goliath-599a2363a413
関西電力	PowerLedgerとP2P再生可能エネルギー取引を日本で取り組むべく提携	→ http://www.kepco.co.jp/corporate/pr/2018/0424_1j.html
環境省	ブロックチェーン技術を活用した再エネCO2削減価値創出モデル事業	→ https://prtimes.jp/main/html/rd/p/000000033.000016392.html
チリ	エネルギーセクターの価格・コスト・キャパシティなど各種統計記録にパブリックEthereum活用	→ https://www.cne.cl/prensa/prensa-2018/04-abril-2018/ministra-jimenez-lanza-tecnologia-blockchain-en-datos-del-sector-energetico/
Wien Energie	コモディティトレードへの応用	→ https://www.usnews.com/news/technology/articles/2018-02-07/wien-energie-to-introduce-blockchain-based-energy-Products
英BP	内部トークンを試行	→ https://www.coindesk.com/energy-giant-bp-says-tested-internal-tokens/

5-2) ライフスタイル分野
G)認定

名称	サービス概略	URL
Sony Global Educations	Hyperledger Fabric用いて資格認定システム	→ https://www.hyperledger.org/wp-content/uploads/2017/12/Hyperledger_CaseStudy_Sony.pdf
ソニー	ソニーピクチャーエンタテインメントとデジタル権利管理への特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180115416.PGNR.&OS=dn/20180115416&RS=DN/20180115416
百度	ブロックチェーンベースの写真権利保護プラットフォームをローンチ	→ https://image.baidu.com/eco/index?tn=wise&page=0
中国ファーウェイ	ブロックチェーンによる知財保護システムの特許	→ https://jp.cointelegraph.com/news/huaweis-patent-for-blockchain-based-system-to-protect-intellectual-property-Unveiled
ロシアのアナウンサー	トークン発行を発表。芸能人の著作権管理、保護ブロックチェーン	→ https://ttrcoin.com/olga-buzova-zapustit-kriptovalyutu-buzcoin.3122/

5-2) ライフスタイル分野
H)ゲーム・メディア

名称	サービス概略	URL
中国Tencent	モンスターハンティングゲーム“一起来捉妖”を公開	→ https://qz.com/1260192/tencents-blockchain-game-merges-cryptokitties-and-pokemon-go/ → http://zhuoyao.qq.com/gicp/news/172/6424344.html
西日本新聞	Steemitのアカウント開設	→ https://steemit.com/introduceyourself/@westjapandaily/japanese-newspaper-joined-steemit → https://www.nishinippon.co.jp/nnp/news_release/article/397370
電通	ブロックチェーンの技術活用へ向け社内横断組織設立	→ http://www.dentsu.co.jp/news/sp/release/2018/0228-009477.html
Warner Music 等	JAAK社による分散型音楽権利データベースKORDのパイロットに参加	→ https://www.musicbusinessworldwide.com/global-music-rights-database-pilot-launched-with-top-music-companies/

5-3) サプライチェーン分野
A)コンソーシアム

名称	サービス概略	URL
Bita	GEの輸送部門、FedEx・UPSに続いて運輸ブロックチェーンコンソーシアムに加盟	→ http://www.getransportation.com/ge-transportation-joins-blockchain-transport-alliance-seeks-advance-exploration-technology
Kuehne + Nagel	海運大手とAccenture、海運ドキュメントのコンソーシアム	→ https://newsroom.accenture.com/news/industry-consortium-successfully-tests-blockchain-solution-developed-by-accenture-that-could-revolutionize-ocean-shipping.htm

5-3) サプライチェーン分野
B)スマートロジスティクス

名称	サービス概略	URL
Samsung	スマートロジスティックプラットフォームへブロックチェーンおよびAIを統合	→ https://www.ethnews.com/samsung-adds-ai-and-blockchain-to-smart-logistics-platform-cello
Samsung	グローバル輸送管理にブロックチェーン	→ https://www.bloomberg.com/news/articles/2018-04-15/samsung-jumps-on-blockchain-bandwagon-to-manage-its-supply-Chain
Walmart	ブロックチェーンにコンディションや位置情報を記録するSmarter Packageの配送トラッキングへ向けて特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180061162.PGNR.&OS=dn/20180061162&RS=DN/20180061162
米Postal Service	デジタルトラストアーキテクチャへの応用で特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch- → adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180083771.PGNR.&OS=dn/20180083771&RS=DN/20180083771
セゾン情報システムズ	ブロックチェーン利用した宅配ボックスを「カエルパルコ」利用者むけにテスト運用開始	→ http://home.saison.co.jp/company/news/pdf/2018/pr180419_01_7ms4ep7p.pdf

5-3) サプライチェーン分野
C)貴金属

名称	サービス概略	URL
BMW	コバルト調達のトラッキングに向けて英Circular社と提携	→ https://walletinvestor.com/magazine/bmw-has-announced-another-blockchain-related-partnership/ → https://www.reuters.com/article/us-mining-bmw-blockchain/uk-firm-pilots-using-blockchain-to-help-bmw-source-ethical-cobalt-idUSKBN1GH2UP
IBM	ダイヤモンドのサプライチェーンにおける採掘から店頭までの来歴証明を行うTrustchain	→ https://www.trustchainjewelry.com/ → http://newsroom.ibm.com/announcements?item=122899
コンゴ	コバルトのサプライチェーンにおける児童労働を抑止にむけてトラッキング	→ https://www.reuters.com/article/us-mining-blockchain-cobalt/blockchain-to-track-congos-cobalt-from-mine-to-mobile-idUSKBN1FM0Y2

5-3) サプライチェーン分野
D)食品

名称	サービス概略	URL
スターバックス	コーヒー豆のトレーサビリティのパイロット実施	→ https://news.starbucks.com/news/starbucks-to-pilot-bean-to-cup-traceability
アリババ	豪州でfood trust frameworkパイロット実施	→ https://www.coindesk.com/alibaba-advances-blockchain-food-fraud-platform-to-pilot-phase/
アリババ	ロジスティック関連会社、サプライチェーン不正防止へブロックチェーン活用	→ http://news.8btc.com/alibabas-logistics-affiliate-uses-blockchain-to-detect-fraud-in-the-supply-chain-of-imported-goods
中国EC大手 JD.com	豪州からの牛肉輸入トレーサビリティにブロックチェーン活用	→ https://corporate.jd.com/whatIsNewDetail?contentCode=fol%2BdxdvCjV%2BLtmLHiuklg%3D%3D&pagePath=inTheNews

5-3) サプライチェーン分野
E)医薬品

名称	サービス概略	URL
DHL	Accentureと、医薬品物流トラッキングへの活用としてシリアルナンバー管理	→ https://cointelegraph.com/news/dhl-accenture-reveal-blockchain-prototype-to-tackle-pharmaceutical-tampering → http://cargo-news.co.jp/cargo-news-main/881
スイスポスト	医薬品などの温度に敏感な品物の輸送における温度モニタリングへの応用検討	→ https://www.ccn.com/swiss-post-taps-modum-blockchain-for-temperature-monitoring-of-shipments/
インド	偽薬防止へブロックチェーン利用	→ https://factordaily.com/niti-aayog-blockchain-for-drugs-in-india/
Intel	二重投薬による伝染病防止へJonson & Jonson等と製薬会社から家庭までの医薬品サプライチェーントラッキング	→ https://www.bloomberg.com/news/articles/2018-04-30/can-blockchain-fix-the-opioid-epidemic-intel-wants-to-find-out

5-3) サプライチェーン分野
F)IoT

名称	サービス概略	URL
Trusted IoT Alliance	テストネットをローンチ	→ https://blog.trusted-iot.org/the-launch-of-the-trusted-iot-alliance-testnet-5a40b75963bd → https://blog.trusted-iot.org/the-trusted-iot-alliance-architecture-50ab2b45edcc
Nokia	スマートシティ向けIoTセンシングサービス	→ https://onestore.nokia.com/asset/201997/NOKIA_Sensing-as-a-service_Solution-paper_EN.pdf
Cisco	グループチャットへのブロックチェーン利用で特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180091489.PGNR.&OS=dn/20180091489&RS=DN/20180091489
IBM	IoTデバイスのスマートコントラクト向けPoWで特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180115425.PGNR.&OS=dn/20180115425&RS=DN/20180115425

5-4) シビックテック分野
A) ICO

名称	サービス概略	URL
カリフォルニア州Berkeley	規制準拠の債券発行によるICO検討	→ https://www.trustnodes.com/2018/02/09/berkeley-plans-launch-ico-token-backed-bonds → https://www.coindesk.com/us-city-plans-to-sell-tokenized-bonds-in-initial-community-offering/
ソウル市	独自暗号通貨S-Coinを検討	→ https://www.coindesk.com/south-koreas-capital-is-planning-to-launch-its-own-cryptocurrency/ → https://www.technologyreview.jp/nl/the-city-of-seoul-dreams-of-its-own-government-backed-cryptocurrency/

5-4) シビックテック分野
B) 不動産・土地

名称	サービス概略	URL
Vermond州	米国初のEthereumブロックチェーン上での不動産取引（土地売買）をウクライナPropy社（ウクライナ政府と連携し昨秋にウクライナで実践済）と協働で成功	→ https://www.zerohedge.com/news/2018-03-08/first-us-real-estate-transaction-blockchain-completed-whats-next → https://ethereum-japan.net/news/ethereum-based-startup-propy-signs-ukraine-government/
スウェーデン土地所有権管理機関	ブロックチェーンによる不動産取引	→ https://jp.cointelegraph.com/news/swedish-government-land-registry-soon-to-conduct-first-blockchain-property-Transaction
積水ハウス	不動産契約実行システムを2018年夏稼働へ	→ https://jp.reuters.com/article/sekisui-house-blockchain-idJPKCN1GL0WD
OpenLaw	豪州法律事務所と協働で不動産のエンドツーエンド移転をEthereumのERC721トークン用いて実施	→ https://media.consensys.net/the-purchase-and-sale-of-real-property-on-ethereum-55bdc289a7b5 → https://youtu.be/nFTGd-nZjNg

5-4) シビックテック分野
C) 投票

名称	サービス概略	URL
ロシア	大統領選の出口調査データ監視にブロックチェーン利用	→ https://jp.cointelegraph.com/news/russia-blockchain-will-be-used-to-protect-2018-presidential-exit-poll-data
シエラレオネ	大統領選投票結果監視にブロックチェーン利用し、結果公表するも、公的にはブロックチェーンの役割を否定	→ https://bitsonline.com/sierra-leone-blockchain-vote/ → https://techcrunch.com/2018/03/19/sierra-leone-government-denies-the-role-of-blockchain-in-its-recent-election/
米ウェストバージニア州	ブロックチェーンによるモバイル投票を試行へ	→ http://www.govtech.com/biz/West-Virginia-Becomes-First-State-to-Test-Mobile-Voting-by-Blockchain-in-a-Federal-Election.html
Kaspersky	Ethereumによる投票検証プラットフォームをローンチ	→ http://www.itp.net/mobile/616954-kaspersky-lab-launches-blockchain-based-voting-platform

5-4) シビックテック分野
D) アイデンティティ

名称	サービス概略	URL
イリノイ州	ブロックチェーンによるアイデンティティおよび公共アセット管理インフラへの応用可能性	→ https://www.ethnews.com/illinois-taskforce-advocates-government-blockchain-infrastructure
テキサス州オースティン	ホームレス向けアイデンティティでブロックチェーン試行	→ https://techcrunch.com/2018/04/14/austin-is-piloting-blockchain-to-improve-homeless-services/
カナダ政府とオランダ政府	エアライン向けにKnown Traveler Digital Identity (KTDI) システムをブロックチェーンと生体認証を組み合わせプロトタイプ実施へ	→ https://www.ethnews.com/canada-and-netherlands-pilot-airline-passenger-biometric-identity-solution-with
World Identity Network (WIN)	児童売買対策むけソリューションをConsenSysと開発へ	→ https://www.benzinga.com/pressreleases/18/03/n11355810/building-blockchain-based-identity-systems-to-combat-child-trafficking
Coca-Cola	Bitfuryと協働でブロックチェーンベースの労働者登録簿	→ https://www.ethnews.com/coca-cola-us-state-department-consider-blockchain-for-labor-registry

5-4) シビックテック分野
E)ブロックチェーン法案

名称	サービス概略	URL
テネシー州	ブロックチェーンやスマートコントラクト用いた電子トランザクション法案通過	→ https://cointelegraph.com/news/v tennessee-passes-bill-recognizing-blockchain-smart-contracts-for-electronic-Transactions
アリゾナ州	企業によるブロックチェーン上でのデータ共有が合法化で法的拘束力	→ https://www.coindesk.com/arizon as-governor-signs-latest-blockchain-bill-into-law/ → https://btcnews.jp/26jtu33m1576 6/
ワイオミング州	ブロックチェーン推進５法案通過	→ https://media.consensys.net/wyo ming-passes-5-pro-blockchain-laws-points-the-way-in-digital-asset-regulation-6fae9e07d129

5-4) シビックテック分野
F)国連

名称	サービス概略	URL
国連WFP	国際送金にEthereumベースのペイメントシステム	→ https://www.ccn.com/banks-begone-uns-world-food-programme-builds-ethereum-blockchain-money-transfers/
国連WFP	ParityのPoA network上で食糧援助決済・報告サマリー・モニタリング	→ http://paritytech.io/fighting-hunger-with-blockchain/ → http://innovation.wfp.org/project/building-blocks
国連WFP	チュニジアの学校給食トラッキングにEthereum利用へ	→ https://www.ethnews.com/un-wfp-is-leveraging-blockchain-technology-to-track-school-lunches
UNICEF	シリアの子供たちむけにEthereumマイニングを促すゲームGame Changersをローンチ	→ https://www.chaingers.io/en/index.html → https://coinjournal.net/unicef-launches-innovative-project-calling-gamers-mine-ethereum-syrian-children/
Unicef豪州	CoinhiveでMoneroマイニング	→ https://www.zdnet.com/article/unicef-australia-turns-to-cryptocurrency-mining-for-fundraising/

5-4) シビックテック分野
G)データ管理

名称	サービス概略	URL
NASA	宇宙空間におけるコミュニケーションのための回復力あるネットワークへのEthereum活用にむけた研究に着手	→ https://www.nasa.gov/sites/default/files/atoms/files/strg_ecf17_wei_quad.pdf → https://discover.coinsquare.io/digital-currency/nasa-research-blockchain-in-space/ → https://sensorweb.nasa.gov/Bitcoin%20Blockchains%20and%20Distributed%20Satellite%20Management%20Control%209-15-17v12.pdf
UAE	2021ブロックチェーン戦略を策定。文書管理などの政府業務活用	→ http://www.mediaoffice.ae/en/media-center/news/11/4/2018/uae-blockchain-strategy.aspx
ロシア	IPChain協会が特許データを格納するパイロット開発へ向けてキルギス政府と合意	→ http://tass.ru/ekonomika/5120173
インド	DNAデータ管理へブロックチェーン利用	→ https://qz.com/1244824/andhra-pradesh-is-using-blockchain-to-collect-dna-data-of-50-million-citizens/
メキシコ	入札のトラッキングへの適用を試行	→ https://www.coindesk.com/mexico-tests-blockchain-track-public-contract-bids/
Caltech	細胞生物学者の研究結果共有にブロックチェーン利用	→ https://blockexplorer.com/news/caltech-uses-blockchain-tech-to-share-cell-biology-research-with-public/
ドバイ	法人登記への活用へ「Dubai Blockchain Business Registry Project」立ち上げ	→ http://www.arabianbusiness.com/technology/395613-dubais-ded-launches-blockchain-based-commercial-business-registry

5-5) 金融分野
金融機関 – 日本(1/3)

※薄文字は前四半期

名称	サービス概略	URL
BTMU、SMBC、みずほ	三メガバンクがデジタル通貨統一へ協議会	→ http://mw.nikkei.com/sp/#!/article/DGXMZO22838390X21C17A0EA4000/
東京三菱UFJ銀行	貿易情報連携基盤のシンガポールNational Trade Platformとの接続実証実験を開始	→ https://japan.zdnet.com/article/35111529/
内外為替一元化コンソーシアム	RCクラウド2.0をIIJと構築完了	→ http://www.sbigroup.co.jp/news/2017/1206_10906.html
損保ホールディングス	BitFuryと戦略的パートナーシップ締結	→ https://prtimes.jp/main/html/rd/p/000000002.000028720.html
SBIホールディングス	ブロックチェーン活用でカード業界と連携	→ http://www.sbigroup.co.jp/news/2017/1227_10934.html
JCB	異種ブロックチェーン間の相互運用の仕組みをカレンシーポートと共同研究へ	→ https://www.nikkei.com/article/DGXMZO25513360Q8A110C1EE9000/ → http://www.global.jcb/ja/press/000000000162579.html

5-5) 金融分野
金融機関 – 日本(2/3)

名称	サービス概略	URL
GMO	オープンソース第3弾として、地域ポイントの発行・運用ができる「地域トークン」を公開	→ https://www.gmo.jp/news/article/?id=5770
飛騨信用組合	電子地域通貨さるぼぼコインを高山市で導入	→ https://www.nikkei.com/article/DGXLASFL16HFL_W7A111C1000000/
東京短資	デジタルガレージと機関投資家向けシステム開発	→ https://www.nikkei.com/article/DGXMZO23693590Q7A121C1TJ2000/
ソフトバンク	金融機関向けの個人情報管理	→ https://www.nikkei.com/article/DGXMZO24856490Q7A221C1EE9000/
マネーフォワード	「MF ブロックチェーン・仮想通貨ラボ」設立	→ http://jp.techcrunch.com/2017/12/29/moneyfoward-blockchain/
日本マイクロソフト	ブロックチェーンの金融システム提供（送金・為替）	→ https://www.nikkei.com/article/DGXMZO25787400X10C18A1EAF000/
IIJ	デジタル通貨の取引・決済を行なう金融サービス事業に参入	→ https://www.iij.ad.jp/news/pressrelease/2018/0125.html

5-5) 金融分野
金融機関 – 日本(3/3)

名称	サービス概略	URL
ジャパンネット銀行	mijinとHyperledger Fabricを連携させて契約締結管理	→ http://mijin.io/ja/1367.html → http://pr.fujitsu.com/jp/news/2018/02/6.html
SBI Ripple Asia	分散台帳技術等を活用した証券コンソーシアムを発表	→ http://www.sbigroup.co.jp/news/2018/0130_10962.html
楽天	「楽天コイン」構想を発表	→ https://www.nikkei.com/article/DGXMZO27458100X20C18A2TI1000/
内外為替一元化コンソーシアム	スマホ向け送金アプリMoney Tap提供	→ http://www.sbigroup.co.jp/news/2018/0307_11012.html
りそな銀行	デジタルガレージと弁護士ドットコムと協働で、ローン業務にelementsベースのスマートコントラクトを使う実証実験	→ http://jp.techcrunch.com/2018/03/12/dg-bengo4-risona-try-elements/
三メガ	有価証券売買情報連携をブロックチェーンにリプレイスする実証実験を日本ユニシスと実施へ	→ https://www.nikkei.com/article/DGXMZO28768100Z20C18A3000000/
SBI Ripple Asia	RippleとSBI Ripple Asia主導の証券コンソーシアム発足	→ http://www.sbigroup.co.jp/news/2018/0419_11063.html
MUFG	MUFGコイン、レジ無し店舗実験開始	→ https://jp.reuters.com/article/mitsubishiufj-mufgcoin-idJPKBN1HT117

5-5) 金融分野

金融機関 – 海外銀行業界　北米

※薄文字は前四半期

名称	サービス概略	URL
BofA	ハイブリッドブロックチェーンをはじめ特許申請	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=0&f=S&l=50&TERM1=%22block+chain%22&FIELD1=&co1=AND&TERM2=%22Bank+of+America+corporation%22&FIELD2=&d=PG01
BofA	企業顧客むけ暗号通貨の取引所特許	→ http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=9,836,790.PN.&OS=pn/9,836,790&RS=PN/9,836,790

5-5) 金融分野
金融機関 – 海外銀行業界　北米

名称	サービス概略	URL
BofA	データ共有むけ内部台帳としての特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180103042.PGNR.&OS=dn/20180103042&RS=DN/20180103042
Western Union	Rippleを用いた送金をテスト	→ https://www.bloomberg.com/news/articles/2018-02-13/western-union-says-it-s-testing-transactions-with-ripple
Quorum	JP Morganからスピンオフへ	→ https://www.nytimes.com/reuters/2018/03/22/technology/22reuters-blockchain-jpmorgan.html
カナダTD Bank	デジタルアセットトラッキングにパブリックチェーン利用へ	→ https://www.coindesk.com/td-bank-considers-public-blockchain-for-asset-tracking/
JP Morgan	銀行間P2P決済の特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180121911.PGNR.&OS=dn/20180121911&RS=DN/20180121911

5-5) 金融分野
金融機関 – 海外銀行業界　欧州

名称	サービス概略	URL
UBS	ブロックチェーンベースのバリデーションで特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netahtml/PTO/search-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20170344988.PGNR.&OS=dn/20170344988&RS=DN/20170344988
UBS他	EthereumによるMiFID II対応プロセス	→ http://www.ibtimes.co.uk/ubs-barclays-credit-suisse-thomson-reuters-explore-ethereum-based-mifid-ii-solution-1651014
Prudential	中小企業むけトレードプラットフォーム	→ http://www.starhub.com/about-us/newsroom/2017/november/prudential-and-starhub-to-launch-blockchain-based-digital-trade-.html
クレディスイスなど	ブロックチェーンを住宅ローン証券むけ検証試験完了	→ https://www.bloomberg.co.jp/news/articles/2018-01-19/P2SIJD6KLVRB01
スペインBBVA	Waveと共同で欧州ー南米間の国際トレードトランザクション	→ https://www.bbva.com/en/bbva-and-wave-carry-first-blockchain-based-international-trade-transaction-europe-and-latin-america/
INGとSociete Generale	ブロックチェーントレードプラットフォームEasy Trading Connect (ETC) を用いて大豆の輸送	→ https://www.ethnews.com/ing-societe-generale-transact-first-blockchain-based-agric-commodity-trade
ロシアSberbank	Hyperledger Fabricによる銀行間決済	→ https://www.cryptocoinsnews.com/russias-biggest-bank-pilots-money-transfer-ibm-blockchain/

5-5) 金融分野
金融機関 – 海外銀行業界　欧州

名称	サービス概略	URL
Santander	xCurrent用いたグローバルペイメントアプリをローンチ	→ https://ripple.com/insights/santander-launches-first-mobile-app-for-global-payments-using-ripples-xcurrent/
ABN Amro Clearing Bank	エスクロー口座の代替手段としてブロックチェーンを介した口座サービスを開発	→ https://www.abnamro.com/en/newsroom/press-releases/2018/abn-amro-clearing-bank-develops-alternative-for-escrow-accounts.html
ING	R3などとトレードファイナンスをテスト	→ https://www.ing.com/Newsroom/All-news/Another-blockchain-milestone-in-trade-finance-.htm
UBS	IBMのBataviaプラットフォームを用いてクロスボーダートレード	→ https://www.coindesk.com/ubs-backed-blockchain-platform-completes-live-trade-transactions/
BBVA	コーポレートローン実施にあたりネゴシエーションプロセスをプライベートチェーン、完了契約登録をEthereumパブリックチェーンで	→ https://www.bbva.com/en/bbva-indra-deliver-worlds-first-blockchain-supported-corporate-loan/
ING	Zero-knowledge Range Proofを数字以外のデータ形式（名前・住所・位置情報など）に拡張したZero-knowledge set membershipプロトコルを計画	→ https://www.coindesk.com/banking-giant-ing-quietly-becoming-serious-blockchain-innovator/

5-5) 金融分野
金融機関 – 海外銀行業界　中国

名称	サービス概略	URL
香港HKMAおよびシンガポールMAS	Hong Kong Trade Finance Platform (HKTFP) 構想へ20以上の銀行が参加表明	→ https://www.coindesk.com/over-20-banks-join-singapore-hong-kong-blockchain-trade-network/
Standard Charterd	印AxisBank、UAE RAKBANK、RippleNetによるクロスボーダーペイメント	→ https://ripple.com/insights/ripple-powered-instant-payment-services-now-live-axis-bank-rakbank-standard-chartered/
Bank of China	スケーリングに向けた特許申請	→ https://www.coindesk.com/bank-of-china-thinks-it-has-a-solution-to-the-blockchain-scaling-issue/ → http://itech.ifeng.com/44885519/news.shtml?srctag=pc2m&back
HSBC	分散台帳上でのトレードファイナンスへ準備すすむ	→ https://www.gtreview.com/news/fintech/hsbc-ready-live-trade-finance-transactions-blockchain/
Standard Chartered	クロスボーダーペイメントへのRippleNet利用国を拡大	→ https://www.finextra.com/newsarticle/32048/standard-chartered-to-extend-use-of-ripplenet-to-more-countries

5-5) 金融分野
金融機関 – 海外銀行業界　アジア・中東

名称	サービス概略	URL
豪州 Commonwealth Bank	ブロックチェーンによる債券を2018年発行へ	→ http://www.zdnet.com/article/commonwealth-bank-to-deliver-world-first-issuance-of-a-bond-on-the-blockchain/
韓国Shinhan銀行	引出時のみの手数料でデポジット時には手数料無料のvaultサービスを試験中	→ http://cryptogeeks.com/bitcoin-1-shinhan-bank-approx-2nd-3rd-largest-bank-korea-test-phase-build-cryptocurrency-vaultwallet
State bank of India	スマートコントラクトベースのKYCをベータローンチ予定	→ https://www.coindesk.com/state-bank-of-india-to-roll-out-smart-contracts-and-blockchain-kyc/
Ripple	日韓の銀行間でパイロット実施	→ https://ripple.com/insights/top-korean-banks-work-japan-bank-consortium-modernize-cross-border-payments/

5-5) 金融分野
金融機関 – 海外銀行業界　アジア・中東

名称	サービス概略	URL
インドCity Union Bank	SWIFTハッキングで2億円流出	→ https://www.reuters.com/article/us-city-union-bank-swift/indias-city-union-bank-ceo-says-suffered-cyber-hack-via-swift-system-idUSKCN1G20AF
インドICICI銀行	国内外トレードファイナンスプラットフォーム試行に250社が参画	→ https://www.icicibank.com/managed-assets/docs/about-us/2018/blockchain-platform-for-trade-finance.pdf
タイ	14の銀行がコンソーシアムを組成し信用保証状のデジタル化をHyperledger Fabricで実施へ	→ https://www.coindesk.com/14-thai-banks-back-blockchain-platform-digitize-contracts/
マレーシア	9銀行でトレードファイナンスシステム構築へ	→ https://www.coindesk.com/9-malaysian-banks-team-up-for-trade-finance-blockchain-apps/
エミレーツNBD	小切手ブロックチェーン	→ https://www.bankingtech.com/2018/04/emirates-nbd-goes-blockchain-for-its-cheque-chain/
ニュージーランド ANZ	IBMと保険向けデータ移転におけるペイメントリコンサイル透明化ソリューションのPoC	→ https://www.ccn.com/anz-ibm-develop-a-blockchain-insurance-solution-in-new-zealand/

5-5) 金融分野
金融機関 – 海外証券業界　北米

名称	サービス概略	URL
Nasdaq	アセットオーナシップをブロックチェーンに格納する特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20170330174.PGNR.&OS=dn/20170330174&RS=DN/20170330174
Nasdaq	南アフリカのCSD向けにブロックチェーンベースの投票システムを提供	→ https://globenewswire.com/news-release/2017/11/22/1204914/0/en/Nasdaq-to-Deliver-Blockchain-e-Voting-Solution-to-Strate.html
JP Morgan	Goldman Sachs、BNP Paribas、Citiなど11金融機関、Axoniの分散台帳を用いてエクイティスワップのパイロット実施	→ https://www.prnewswire.com/news-releases/multi-firm-blockchain-implementation-for-equity-swaps-completes-second-phase-300559102.html

5-5) 金融分野
金融機関 – 海外証券業界　北米

名称	サービス概略	URL
CME Group	全参加者のコンセンサス無しにブロックチェーンプロトコル変更を可能とする特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=14&f=G&l=50&d=PG01&s1=blockchain&p=1&OS=blockchain&RS=blockchain
ノーザントラスト	プライベートエクイティのファンドデータのリアルタイム監査サービスをPwCとHyperledger Fabric上で開発	→ https://m.northerntrust.com/news-financial-statement/press-release?c=e2c653df01fd5f65cd9b42445ed7d5ef
DTCC	ブロックチェーン導入プロジェクトが棚上げ	→ https://www.reuters.com/article/us-banks-fintech-blockchain/wall-street-rethinks-blockchain-projects-as-euphoria-meets-reality-idUSKBN1H32GO
JP Morgan	債券発行プロセス改善へNational Bank of Canadaなどと提携し試行	→ https://www.coindesk.com/jpmorgan-trial-puts-debt-issuance-on-a-blockchain/
カナダ証券取引所	Ethereumによる証券トークンオファリング（STO）を計画	→ https://thecse.com/en/about/publications/cse-news/cse-unveils-canadas-first-platform-for-clearing-and-settling-securities

5-5) 金融分野
金融機関 – 海外証券業界　欧州

名称	サービス概略	URL
CSD Working Groupコンソーシアム	分散台帳ベースの投票システム開発推進	→ https://www.coindesk.com/csd-consortium-reveals-requirements-for-first-project/
仏ファンド運用会社TOBAM	ビットコイン連動投資信託を開設	→ http://www.tobam.fr/tobam-launches-first-bitcoin-mutual-fund-in-europe/
伊Intesa Sanpaolo	Ethereumベースのデリバティブを検討	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075540
NivauraとLucDeco	初めてのEthereum建て社債発行	→ https://style.nikkei.com/article/DGXLASFL28HQY_Y7A121C1000000
ロシアNSD	暗号通貨むけデポジトリ検討	→ https://www.ethnews.com/russia-designing-national-cryptocurrency-depository

5-5) 金融分野
金融機関 – 海外証券業界　欧州

名称	サービス概略	URL
Credit Suisse と ING	Corda上で証券レンディングアプリを使ったライブトランザクション	→ https://www.r3.com/blog/2018/03/01/credit-suisse-and-ing-execute-first-live-transaction-using-hqlax-securities-lending-app-on-r3s-corda-blockchain-platform/
英Marex Solutions	Nivauraと協働でブロックチェーンで初めてとなる仕組み債をパブリック版Ethereum上で組成	→ http://www.marexspectron.com/about-us/news/2018/03/worlds-first-blockchain-based-structured-product
ドイツ取引所 Borseグループ	クロスボーダー証券決済に Hyperledger Fabric利用	→ https://www.hyperledger.org/wp-content/uploads/2018/03/Hyperledger_CaseStudy_DeutscheBorse_FINAL.pdf
BNP Paribas	ブロックチェーン導入プロジェクトが棚上げ	→ https://www.reuters.com/article/us-banks-fintech-blockchain/wall-street-rethinks-blockchain-projects-as-euphoria-meets-reality-idUSKBN1H32GO

5-5) 金融分野
金融機関 – 海外証券業界　中国・アジア

名称	サービス概略	URL
深セン証券取引所	ブロックチェーンベースのクレジットレポーティングネットワークをリリース	→ http://news.8btc.com/shenzhen-stock-exchange-release-blockchain-based-credit-reporting-network
豪州ASX	ポストトレードシステムをDigital Asset プラットフォームによるリプレイスへ	→ http://hub.digitalasset.com/market-announcements/asx-gives-digital-assets-technology-green-light-to-replace-chess
香港HKEX	豪州ASXに続きブロックチェーンによるエクイティ決済システム検討	→ https://www.coindesk.com/hong-kong-stock-exchange-looks-to-asx-for-blockchain-equity-settlement/
豪州ASX	Digital Assetと構築中のセツルメントシステムを2020年までに本番稼働見込みと発表	→ http://www.afr.com/technology/asx-blockchain-to-go-live-at-end-of-2020-20180427-h0zcgx

5-5) 金融分野
金融機関 – 保険業界

名称	サービス概略	URL
三井住友海上	保険申込書類の確認業務へmiyabi用いた実証実験	→ https://bitflyer.com/pub/bitFlyer-begins-proof-of-concept-tests-using-private-blockchain-miyabi-for-insurance-application-verification-processes-ja.pdf
医療保険 United Health	医療提供者データ管理共有を他４社と実施	→ https://www.businesswire.com/news/home/20180402005181/en/Humana-MultiPlan-Optum-Quest-Diagnostics-UnitedHealthcare-Launch
保険大手ブローカーMarsh	IBMと保険証明提供プラットフォーム構築へ	→ https://www.businesswire.com/news/home/20180416005918/en/Marsh-Collaborates-IBM-ACORD-ISN-Apply-Blockchain
Cognizant	インドの生命保険14社と業界横断データ共有	→ https://investors.cognizant.com/2018-04-16-Leading-Indian-Life-Insurers-Partner-with-Cognizant-to-Develop-Industry-Wide-Blockchain-Solution-for-Secure-Data-Sharing-and-Improved-Customer-Experience,1

5-5) 金融分野
金融機関 – カード業界

名称	サービス概略	URL
Amex	リワードプログラムむけデータベースで特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html
Amex	RippleNet加入	→ https://ripple.com/insights/american-express-joins-ripplenet-giving-visibility-and-speed-to-global-commercial-payments/
Visa	クロスボーダーB2Bペイメントとして Visa B2B Connect platform を2018年半ばにローンチへ	→ https://usa.visa.com/visa-everywhere/innovation/visa-b2b-connect.html
Visa	マスターカードとアメックスに続きブロックチェーンで国際間B2B決済	→ https://apptimes.net/archives/9449
Visa Europe	カードイシュアのWaveCrestへサービス停止	→ https://www.ethnews.com/visa-cuts-cords-on-cryptocurrency-cards
MasterCard	インスタントペイメントの特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20170323294.PGNR.&OS=dn/20170323294&RS=DN/20170323294

5-5) 金融分野
金融機関 – カード業界

名称	サービス概略	URL
UCカード	SBIホールディングスおよびOrbと地域通貨「UC台場コイン（仮称）」実証実験	→ http://www.sbigroup.co.jp/news/2018/0306_11011.html
Amex	ブロックチェーンベースのペイメントネットワークで特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180075453.PGNR.&OS=dn/20180075453&RS=DN/20180075453
MasterCard	偽物防止へ向けたアイデンティティ保護へ向けた特許	→ http://pdfaiw.uspto.gov/.aiw?PageNum=0&docid=20180101684&IDKey=883F5BF2B7E6&HomeUrl=http%3A%2F%2Fappft.uspto.gov%2Fnetacgi%2Fnph-Parser%3FSect1%3DPTO2%2526Sect2%3DHITOFF%2526u%3D%25252Fnetahtml
MasterCard	新ノードを速やかにブロックチェーンネットワークへ追加する方法で特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180115413.PGNR.&OS=dn/20180115413&RS=DN/20180115413
SWIFT	Hyperledger Fabricによる34行でのノストロ調整の実証実験完了	→ https://www.swift.com/news-events/press-releases/swift-completes-landmark-dlt-poc
Omise	ブロックチェーンベースのAML/KYCソリューション提案	→ https://www2.abaconline.org/assets/2018/2_Tokyo_Japan/8_AGFSCB/AGFSCB_38009/AGFSCB_38009A/Meeting02-Paper03A_Hasegawa_Second_Draft.pdf

6.参考資料リンク集

① イベント
② ブックマーク集
③ Lightning関連データ
④ ブロックチェーン関連リソースデータ
⑤ 通貨関連リソースデータ
⑥ Dapps関連データ
⑦ 個別トピックデータ
⑧ ドキュメンタリー
⑨ カリキュラム
⑩ ユースケースリスト
⑪ レポート

イベント ①

日付	タイトル	URL
1/24-26 @Stanford	Blockchain Protocol Analysis and Security Engineering 2018（BPASE 2018）	→ https://cyber.stanford.edu/bpase18
2/7 @Tokyo	第5回 日銀FinTechフォーラム	→ https://www.boj.or.jp/announcements/release_2018/rel180214a.htm/
2/16-18 @Denver	ETHDenver	→ https://ethdenver.com/
3/2 @Berlin	Blockstack Berlin2018	→ https://blockstack.org/berlin2018 → https://www.youtube.com/channel/UC3J2iHnyt2JtOvtGVf_jpHQ
3/2 @Curacao	The 5th Workshop on Bitcoin and Blockchain Research	→ https://fc18.ifca.ai/bitcoin/schedule.html

イベント ②

日付	タイトル	URL
3/5-3/6 @Barcelona	Giveth ScalingNOW	→ http://scalingnow.giveth.io/ → https://www.youtube.com/playlist?list=PL4Artm1rmCWGksgoRe6HF5d9eklC01IcC → https://docs.google.com/document/d/1AAdN1J1oWxYmlWhOTRPMQ4WLzL-JSUmTyG9vYpyKNk0/edit → https://medium.com/@web3/scalingnow-day-2-summary-dapp-developers-deliberating-sensible-scaling-solutions-83740e0eaec5
3/7 @Tokyo	Cordacon	→ https://www.r3.com/cordacon/
3/7-3/8 @Washington	DC Blockchain Summit	→ https://youtu.be/RyZiqSx52Nk → https://youtu.be/5Txf2bVwp84 → https://www.youtube.com/channel/UChwEyC2QsQCztk2qGzm1b6Q

イベント ③

日付	タイトル	URL
3/8-3/10 @Paris	EthCC - Ethereum Community Conference	→ https://docs.google.com/spreadsheets/d/1t3CdiKlTiozbFkFwBVbNQ1Qc9s9ipDSRJPwGsHd0Yvw/htmlview → https://www.reddit.com/r/ethereum/comments/83mz5q/all_videos_from_ethcc_18_in_paris/
3/9-3/18 @Austin	SXSW	→ https://www.sxsw.com/ → https://schedule.sxsw.com/2018/events/PP99517
3/17-3/18 @Boston	MIT Bitcoin Expo 2018	→ http://mitbitcoinexpo.org/ → https://youtu.be/ZmVzRmBVzWk → https://youtu.be/1wdPLsdHmvY → https://www.youtube.com/watch?v=i-0NUqIVVV4
3/17-3/18 @Boston	MIT Bitcoin Expo 2018	→ http://mitbitcoinexpo.org/
3/21 @Taipei	Ethereum All-Star Tech Talk - Taipei Ethereum Meetup	→ https://youtu.be/ilsjZAtUUvQ → https://ethertw.github.io/tickets/

イベント ④

日付	タイトル	URL
3/23-3/25 @Tokyo	Satoshi's Vision	→ https://www.satoshisvisionconference.com/agenda.html → https://www.youtube.com/playlist?list=PLpd9yRMC7Ebl40OAmLUI8Zev9Ixekxv6s
3/28 @Tokyo	Ethereum Japan Community Meetup #1	→ https://ethereumjapan.peatix.com/ → https://note.mu/ico_post/n/n71c9837059d7
3/29 @Tokyo	Ethereum Community Fund Launch Event	→ https://youtu.be/aaMmdxlHDyA → https://youtu.be/-l1T9UQ0UEQ
4/3-4/4 @Seoul	Deconomy2018	→ https://threadreaderapp.com/thread/981069924255739904.html → https://youtu.be/WaWcJPSs9Yw → http://coinpost.jp/?p=20493 → https://www.youtube.com/channel/UC_HZkGAEXMobMwRtz_3SlFw

イベント ⑤

日付	タイトル	URL
4/10 @Tokyo	「仮想通貨交換業等に関する研究会」（第１回）	→ https://www.fsa.go.jp/news/30/singi/20180410-2.html
4/13 @Tokyo	Hi-Ether Meetup - Block #2	→ http://y-nakajo.hatenablog.com/entry/2018/04/16/092538
4/17 @Tokyo	Ethereum Japan Community Meetup #2	→ https://ethereumjapan-2.peatix.com/
4/26 @Tokyo	Plasma勉強会#1	→ https://speakerdeck.com/amachino/plasma-woli-jie-surutamefalse-ethereum-protocol-falsekihon → https://speakerdeck.com/osuke/isariamusukeringufalsebei-jing-togai-yao → https://speakerdeck.com/ymatsuwitter/plasma-overview-and-potential → http://blockchain.gunosy.io/entry/sidechain-plasma-plasma-mvp → https://speakerdeck.com/shogochiai/plasmafalsezhi-yue-tohuan-he

イベント ⑥

日付	タイトル	URL
4/27 @Tokyo	「仮想通貨交換業等に関する研究会」（第２回）	→ https://www.fsa.go.jp/news/30/singi/20180427.html
4/29-5/3 @Tel Aviv	Eurocrypto2018	→ https://eurocrypt.iacr.org/2018/program.html
5/3-5/5 @Tronto	EDCON: COMMUNITY ETHEREUM DEVELOPMENT CONFERENCE	→ https://edcon.io/ → https://youtu.be/vlLFQqfgOPk

ブックマーク集

- Crypto Canon / a16zによる暗号通貨関連リンク集
  - http://a16z.com/2018/02/10/crypto-readings-resources/
- 暗号通貨ツールリンク
  - http://individua1.net/cryptocurrency-tools/
- Lightning Network関連のリンク集 / Lightning Resources
  - http://lnroute.com/
  - http://dev.lightning.community/resources/
- Lightning Network Megathread
  - https://www.reddit.com/r/Bitcoin/comments/7pwna9/lightning_network_megathread/
- Cryptoeconomics関連
  - https://github.com/snario/awesome-cryptoeconomics/blob/master/README.md
- State Channels関連
  - https://github.com/machinomy/awesome-state-channels/blob/master/readme.md

LIGHTNING関連データ

- Lightning Network Search and Analysis Engine
  - https://1ml.com/#search
- Lnd Explorer
  - https://graph.lndexplorer.com/
- Lightning Network Search and Analysis Engine
  - https://1ml.com/#search
- Directory of different lightning sites
  - https://www.robtex.com/lightning/
- Lnmainnetの様子
  - https://lnmainnet.gaben.win/
- Mainnet lightning network stores
  - http://lightningnetworkstores.com/
- Lightning App Directory
  - http://dev.lightning.community/lapps/
- Lightning Networkの時系列統計
  - https://bitcoinvisuals.com/lightning/

ブロックチェーン関連リソースデータ

- Unspent Transaction Output Set
  - http://statoshi.info/dashboard/db/unspent-transaction-output-set
- Mempool-based fee estimator
  - https://whatthefee.io/
- Bitcoin Fee estimation matrix
  - https://whatthefee.io/
- transactionfee.info
  - https://transactionfee.info/
- Blockchair
  - https://blockchair.com/bitcoin/blocks
  - https://blockchair.com/bitcoin-cash/blocks
- Block'tivity
  - https://blocktivity.info/
- TX Highway
  - https://txhighway.com/
- AsicBoost.dance Block Explorer
  - https://asicboost.dance/

通貨関連データ

- Global Cryptocurrency Charts - Total Crypto Market Cap and Volume
  - https://coincheckup.com/global
- Bitcoin Futures Quotes
  - http://www.cmegroup.com/trading/equity-index/us-index/bitcoin.html
- ビットコインNVTレシオ
  - http://charts.woobull.com/bitcoin-nvt-ratio/
- Digital Currency Groupのポートフォリオ
  - http://dcg.co/portfolio/
- JCBA、会員取扱仮想通貨一覧をアップデート
  - https://cryptocurrency-association.org/list/
- Dominance Chart
  - http://individua1.net/dominance-chart/

DAPPS関連データ

- State of the DApps
  - https://www.stateofthedapps.com/
- DappRadar.com
  - https://dappradar.com/
- Dapps Info
  - https://dappsinfo.net/
- Dapp Insight
  - https://dappinsight.com/
- Dapp Board
  - http://dappboard.com/app

地域関連事情データ

- Cryptovalley Directory
  - http://cryptovalley.directory/index.html
- 欧州オーストリアのプレイヤー鳥瞰マップ
  - https://www.bitcoinnews.ch/8272/bitcoin-oesterreich/
- 5分でわかるロシアのブロックチェーン概況
  - https://drive.google.com/file/d/1FrL-9pstjS7iE3a8GkLKz5c9IdgdoGbQ/view
- Berlin Blockchain Guide
  - https://medium.com/innogy-innovation-hub/berlin-blockchain-guide-2ea1cda1367e
- A mapping of the Belgium Blockchain ecosystem
  - https://cryptospace.be/

個別トピックデータ

- トークン関連
  - Elementus
    - https://elementus.io/visualization-token-fest
- ICO関連
  - The Token Sale Explosion Visualized, January 2014 - March 2018
    - https://www.youtube.com/watch?v=rIMKNkF6d28
  - PwC Global ICO Compass - Treatment of ICOs worldwide
    - https://www.pwc.ch/en/industry-sectors/financial-services/fs-regulations/ico.html
- DEX関連
  - DEX Resource List
    - https://github.com/distribuyed/index/blob/master/README.md
  - DEX Tracker
    - https://etherscan.io/stat/dextracker
- GOX関連
  - This script watch for the MTGox Cold Wallet addresses
    - http://gaelb.alwaysdata.net/MTgox_watch_CW/index.html

ドキュメンタリー

- マジック・マネー:ビットコイン革命
  - https://youtu.be/qTiI2itIPO4
- Bitcoin:Beyond the Bubble
  - https://satoricoin.jp/en/
  - https://youtu.be/r1cP5KGgbgU

カリキュラム

- CryptoZombies、Dapps開発をゲームで学ぶレッスンサービス
  - https://cryptozombies.io/jp/

- Oxford Blockchain Strategy Programme
  - https://www.getsmarter.com/courses/uk/oxford-blockchain-strategy-programme

ユースケースリスト

- ヘルスケア関連プロジェクトリスト
  - https://github.com/acoravos/healthcare-blockchains/blob/master/README.md

- 政府系における利用ケース一覧
  - https://airtable.com/shreIXQjzluCxam37/tbl7qVDFKKiEcFFrc

レポート(米国の見方)

- 米NIST（国立標準技術研究所）によるブロックチェーン技術に対する概観レポート
  - https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf
- 米国議会JOINT ECONOMIC REPORT（第9章 暗号通貨とブロックチェーン）
  - https://www.congress.gov/115/crpt/hrpt596/CRPT-115hrpt596.pdf
- JP Morganによる暗号通貨に関するレポート
  - https://t.co/idlLsmW4YY

レポート(各国の規制事情)

- Cryptocurrency Regulation in 2018: Where the World Stands Right Now
  - https://bitcoinmagazine.com/articles/cryptocurrency-regulation-2018-where-world-stands-right-now/#1517514315
- Token regulation paper
  - http://bundesblock.de/wp-content/uploads/2018/02/180209_Statement-Token-Regulation_blockchain-bundesverband.pdf
- A snapshot of current crypto regulations of all G20 member states
  - https://medium.com/@Torquecapital/a-snapshot-of-current-crypto-regulations-of-all-g20-member-states-3b5f80ffac81
- Making Sense of the World's Cryptocurrency Rules（世界の暗号通貨むけ規制マップ）
  - https://www.bloomberg.com/news/articles/2018-03-19/is-this-legal-making-sense-of-the-world-s-cryptocurrency-rules
  - https://www.bloomberg.co.jp/news/articles/2018-03-20/P5VM4N6KLVR501

レポート(ICO関連)

- 2017 Token Sales / ICOs in Review
  - https://www.smithandcrown.com/2017-year-review-part/
  - https://www.smithandcrown.com/2017-token-sales-review-part-ii/
  - https://www.smithandcrown.com/2017-token-sales-review-part-iv-geography-token-sales/
- Introducing the Private ICO (PICO)
  - https://medium.com/harborhq/introducing-the-private-ico-pico-3e8b782924c1
- スイスFINMAのICOラウンドテーブル資料
  - https://cdn.crowdfundinsider.com/wp-content/uploads/2018/03/Switzerland-FINMA-ICO-Presentation-Veranstaltung.pdf
- 昨年11月に発足した多摩大学ルール形成戦略研究所（ICOビジネス研究グループ）より、ICOルール形成の提言
  - https://www.tama.ac.jp/crs/2018_ico_en.pdf
- クリプトアセット13種の分析レポート
  - https://messari.io/research.html

レポート(地域事情)

- BitMEX過去レポート（Mining incentives, part 2: Why is China dominant in Bitcoin mining?）
  - https://blog.bitmex.com/mining-incentives-part-2-why-is-china-dominant-in-bitcoin-mining/
  - 中国マイニング成長は電気代の安さだけが注目されるが、その背景として大量電力消費するアルミニウム向け過剰設備があったこと、そしてその電力を都市部へ供給するにも超高圧送電設備が普及していなかったゆえ、四川省などの地方でマイニングが普及したという視点で分析されている。

- ビットコインとシャリアに関するレポート（2017年4月付。blossomによる）
  - https://blossomfinance.com/is-bitcoin-halal-shariah-analysis-of-bitcoin-cryptocurrency-and-blockchain
  - 暗号通貨利用者は関連リスクを考慮するようにと。
  - コモディティや投資商品として扱うよりも、暗号通貨ネットワークが従来のシステムと比べて利点を提供できる場合にペイメントシステムとして用いることを想定している模様。

レポート(中央銀行)

- Central bank digital currencies（BIS）
  - https://www.bis.org/cpmi/publ/d174.pdf
  - http://www.boj.or.jp/announcements/release_2018/data/rel180315a.pdf

- Project Stella：日本銀行・欧州中央銀行による分散型台帳技術に関する共同調査報告書（第2フェーズ）
  - http://www.boj.or.jp/announcements/release_2018/rel180327a.htm/

レポート(マネロン・セキュリティ)

- Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services
  - https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering
- BLOCKCHAIN KYC/AML UTILITIES FOR INTERNATIONAL PAYMENTS
  - https://www.r3.com/research/
- Ledger Receive Address Attack
  - https://www.docdroid.net/Jug5LX3/ledger-receive-address-attack.pdf
  - http://kaatcrypto.com/ledgernanowarning
- Cryptocurrency Security Standard
  - https://cryptoconsortium.github.io/CCSS/
- 分散台帳技術のセキュリティ要件:　銀行口座振替処理への適用
  - https://www.imes.boj.or.jp/research/papers/japanese/kk37-1-4.pdf
- 欧州のデータ保護規制（GDPR）とブロックチェーン
  - https://www.eugdpr.org/key-changes.html
  - https://www.eugdpr.org/gdpr-faqs.html

レポート(LN・DEX・DAPPS)

- Lightning Networkに関するUX レポート。（Eclairなど既存ウォレット比較など）
  - https://patestevao.gitbooks.io/lightning-network-ux-research/content/
- State of Decentralized Exchanges, 2018
  - https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79
- ブロックチェーン（dApps）ゲームまとめ
  - http://www.kiyosui.com/entry/blockchaingame-matome
- State of the DApps: 5 Observations From Usage Data (April 2018)
  - https://medium.com/@mccannatron/state-of-the-dapps-5-observations-from-usage-data-april-2018-a3e9da01bc22

7.論文リスト

2017 4Qの関連論文リスト(1/13)

タイトル	URL
Atomic **Cross-Chain** Swaps	→ https://arxiv.org/abs/1801.09515
A Delay-Tolerant Payment Scheme Based on the **Ethereum** Blockchain	→ https://arxiv.org/abs/1801.10295
Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains	→ https://arxiv.org/abs/1801.10228
When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through **Bitcoin Transactions Analysis**	→ https://arxiv.org/pdf/1801.07501.pdf
On the Preliminary Investigation of **Selfish Mining** Strategy with Multiple Selfish Miners	→ https://arxiv.org/abs/1802.02218
ModelChain: Decentralized Privacy-Preserving **Healthcare** Predictive Modeling Framework on Private Blockchain Networks	→ https://arxiv.org/abs/1802.01746
But Why does it Work? A Rational Protocol Design Treatment of **Bitcoin**	→ https://eprint.iacr.org/2018/138

2017 4Qの関連論文リスト(2/13)

タイトル	URL
Chainspace: a sharded **smart contracts** platform	→ https://blog.acolyer.org/2018/02/08/chainspace-a-sharded-smart-contracts-platform/
ForkBase: An Efficient Storage Engine for **Blockchain** and Forkable Applications	→ https://arxiv.org/abs/1802.04949
A Blockchain Based Liability Attribution Framework for Autonomous Vehicles	→ https://arxiv.org/abs/1802.05050
On the Feasibility of **Decentralized Derivatives Markets**	→ https://arxiv.org/abs/1802.04915
Smart Contract-Based **Access Control for the Internet of Things**	→ https://arxiv.org/abs/1802.04410
A first look at the usability of **bitcoin key management**	→ https://arxiv.org/abs/1802.04351
The **DCS** Theorem	→ https://arxiv.org/abs/1801.04335
Simple **Schnorr Multi-Signatures** with Applications to Bitcoin	→ https://eprint.iacr.org/2018/068

2017 4Qの関連論文リスト(3/13)

タイトル	URL
Analysis of the **XRP Ledger** Consensus Protocol	→ https://arxiv.org/pdf/1802.07242.pdf
Blockchain: Data Malls, Coin Economies and **Keyless Payments**	→ https://arxiv.org/abs/1802.07422
A Survey on the **Security of Blockchain** Systems	→ https://arxiv.org/abs/1802.06993
Quantum-Assisted Blockchain	→ https://arxiv.org/abs/1802.06763
Toward **Open Data Blockchain Analytics**: A Bitcoin Perspective	→ https://arxiv.org/abs/1802.07523
CASPaxos: **Replicated State Machines** without logs	→ https://arxiv.org/abs/1802.07000
Green **Mining**: toward a less energetic impact of cryptocurrencies	→ https://eprint.iacr.org/2018/197
SoK: unraveling **Bitcoin smart contracts**	→ https://eprint.iacr.org/2018/192

2017 4Qの関連論文リスト(4/13)

タイトル	URL
Can **Bitcoin** be used as a **hedge** against the Swedish market?	→ https://su.diva-portal.org/smash/get/diva2:1183765/FULLTEXT01.pdf
Low-Resource **Eclipse Attacks** on **Ethereum**'s Peer-to-Peer Network	→ http://www.cs.bu.edu/~goldbe/projects/eclipseEth.pdf
Decentralization in **Bitcoin and Ethereum** Networks	→ http://fc18.ifca.ai/preproceedings/75.pdf
Paralysis Proofs: Safe Access-Structure Updates for **Cryptocurrencies** and More	→ https://fc18.ifca.ai/bitcoin/papers/bitcoin18-final20.pdf
The **Blockchain Consensus** Layer and BFT	→ http://bulletin.eatcs.org/index.php/beatcs/article/download/506/495

2017 4Qの関連論文リスト(5/13)

タイトル	URL
Trustless Machine Learning Contracts; Evaluating and Exchanging **Machine Learning** Models on the **Ethereum** Blockchain	→ https://arxiv.org/abs/1802.10185
Transparent **Voting** Platform Based on Permissioned Blockchain	→ https://arxiv.org/abs/1802.10134
Fundamental Values of Cryptocurrencies and Blockchain Technology	→ https://arxiv.org/abs/1802.10117
Tool Demonstration: FSolidM for Designing **Secure Ethereum Smart Contracts**	→ https://arxiv.org/abs/1802.09949
CCP: Conflicts Check Protocol for **Bitcoin Block Security**	→ https://arxiv.org/abs/1802.09860
Valuation, Liquidity Price, and Stability of **Cryptocurrencies**	→ https://arxiv.org/abs/1802.09959
A Semantic Framework for the **Security Analysis of Ethereum smart contracts**	→ https://arxiv.org/abs/1802.08660
Finding The Greedy, Prodigal, and Suicidal **Contracts** at Scale	→ https://arxiv.org/pdf/1802.06038.pdf

2017 4Qの関連論文リスト(6/13)

タイトル	URL
How to Squeeze a Crowd: Reducing Bandwidth in **Mixing Cryptocurrencies**	→ https://isi.jhu.edu/~mgreen/mixing.pdf
Are **cryptocurrencies** connected to forex? A quantile cross-spectral approach	→ https://www.econstor.eu/bitstream/10419/174884/1/Baumohl%20%282018%29.pdf
zkLedger: **Privacy-Preserving Auditing** for Distributed Ledgers	→ https://eprint.iacr.org/2018/241
The Limit of Blockchains: Infeasibility of a **Smart** Obama-Trump **Contract**	→ http://ia.cr/2018/252
Low-Resource **Eclipse Attacks** on **Ethereum**'s Peer-to-Peer Network	→ http://ia.cr/2018/236
A New Approach to Deanonymization of Unreachable **Bitcoin Nodes**	→ http://ia.cr/2018/243
Stake-Bleeding Attacks on **Proof-of-Stake** Blockchains	→ https://eprint.iacr.org/2018/248

2017 4Qの関連論文リスト(7/13)

タイトル	URL
A Framework for **Blockchain-Based Applications**	→ https://arxiv.org/abs/1803.00892
Ouroboros Praos: An adaptively-secure, semi-synchronous **proof-of-stake** blockchain	→ https://eprint.iacr.org/2017/573.pdf
Bitcoin as a Transaction Ledger: A Composable Treatment	→ https://eprint.iacr.org/2017/149.pdf
Initial Coin Offerings: The Top 25 Jurisdictions and Their Comparative **Regulatory** Responses	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3117224
Initial Coin Offerings and the Value of Crypto Tokens	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137213
Why Preventing a **Cryptocurrency Exchange** Heist Isn't Good Enough	→ http://www0.cs.ucl.ac.uk/staff/P.McCorry/preventing-cryptocurrency-exchange.pdf

2017 4Qの関連論文リスト(8/13)

タイトル	URL
Finding The Greedy, Prodigal, and Suicidal **Contracts** at Scale	→ https://arxiv.org/pdf/1802.06038.pdf
SoK: Uncentralisable Ledgers and their Impact on **Voting Systems**	→ https://arxiv.org/pdf/1801.08064.pdf
IcoRating: A Deep-Learning System for **Scam ICO Identification**	→ https://arxiv.org/abs/1803.03670
Distributed **Data Vending** on Blockchain	→ https://arxiv.org/abs/1803.05871
SHARVOT: secret SHARe-based **VOTing on the blockchain**	→ https://arxiv.org/abs/1803.04861
NECTAR: **Non-Interactive Smart Contract** Protocol using Blockchain Technology	→ https://arxiv.org/abs/1803.04860
CIoTA: Collaborative IoT Anomaly Detection via **Blockchain**	→ https://arxiv.org/abs/1803.03807
Chimeric Ledgers: Translating and Unifying **UTXO-based and Account-based Cryptocurrencies**	→ https://eprint.iacr.org/2018/262
Vault: Fast Bootstrapping for **Cryptocurrencies**	→ https://eprint.iacr.org/2018/269

2017 4Qの関連論文リスト(9/13)

タイトル	URL
MathCoin: A **Blockchain Proposal** that Helps Verify Mathematical Theorems In Public	→ https://eprint.iacr.org/2018/271
Database Perspectives on **Blockchains**	→ https://arxiv.org/abs/1803.06015
BitML: a calculus for **Bitcoin smart contracts**	→ https://eprint.iacr.org/2018/122.pdf
Committing to Quantum Resistance: A Slow Defence for **Bitcoin** against a Fast **Quantum Computing Attack**	→ https://eprint.iacr.org/2018/213.pdf
A Quantitative Analysis of the Impact of Arbitrary **Blockchain Content on Bitcoin**	→ https://fc18.ifca.ai/preproceedings/6.pdf
Anonymous Post-Quantum **Cryptocash**	→ https://fc18.ifca.ai/preproceedings/16.pdf
Improving **Bitcoin's Resilience** to Churn	→ https://arxiv.org/abs/1803.06559
Are **Bitcoin** Bubbles Predictable? Combining a Generalized Metcalfe's Law and the LPPLS Model	→ https://arxiv.org/abs/1803.05663

2017 4Qの関連論文リスト(10/13)

タイトル	URL
Beyond Godel (Craig Wright)	→ https://coingeek.com/app/uploads/2018/03/SSRN-id3147440.pdf
Bitcoin: A Total **Turing Machine** (Craig Wright)	→ https://files.acrobat.com/a/preview/981caa5a-fb13-459d-907b-2ab2476511b9
Bitcoin: Seir-C **Propagation Models of Block** and Transaction Dissemination (Craig S Wright)	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3151940
ZebraLancer: Private and Anonymous **Crowdsourcing System atop Open Blockchain**	→ https://arxiv.org/abs/1803.01256
Towards More Reliable **Bitcoin Timestamps**	→ https://arxiv.org/abs/1803.09028

2017 4Qの関連論文リスト(11/13)

タイトル	URL
Making **Bitcoin Legal**	→ http://www.cl.cam.ac.uk/~rja14/Papers/making-bitcoin-legal.pdf
Developing a K-ary malware using **Blockchain**	→ https://arxiv.org/abs/1804.01488
On the Economic Significance of Ransomware Campaigns: **A Bitcoin Transactions Perspective**	→ https://arxiv.org/abs/1804.01341
Blockchain-based TLS Notary Service	→ https://arxiv.org/abs/1804.00875
Chain of Trust: Can Trusted Hardware Help **Scaling Blockchains**?	→ https://arxiv.org/abs/1804.00399
An (Institutional) Investor's Take on **Cryptoassets**	→ https://s3.eu-west-2.amazonaws.com/john-pfeffer/An+Investor's+Take+on+Cryptoassets+v6.pdf
Subchains: A Technique to **Scale Bitcoin** and Improve the User Experience	→ https://www.bitcoinunlimited.info/resources/subchains.pdf

2017 4Qの関連論文リスト(12/13)

タイトル	URL
Digital Trade Coin (DTC): Towards a more **stable digital currency**	→ https://hardjono.mit.edu/sites/default/files/documents/Digital-Trade-Coin.pdf
Ransomware Payments in the **Bitcoin Ecosystem**	→ https://arxiv.org/abs/1804.04080
An Equilibrium **Valuation of Bitcoin** and Decentralized Network Assets	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3142022
Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant **Smart Contract Execution**	→ https://arxiv.org/abs/1804.05141
Monero **Ring Attack**: Recreating Zero Mixin Transaction Effect	→ https://eprint.iacr.org/2018/348
BeatCoin: **Leaking Private Keys** from Air-Gapped Cryptocurrency Wallets	→ https://arxiv.org/abs/1804.08714
Adapting Blockchain Technology for Scientific Computing	→ https://arxiv.org/abs/1804.08230

2017 4Qの関連論文リスト(13/13)

タイトル	URL
Thunderella: Blockchains with Optimistic **Instant Confirmation**	→ https://eprint.iacr.org/2017/913
But Why Does it Work? A Rational **Protocol Design Treatment of Bitcoin**	→ https://eprint.iacr.org/2018/138.pdf
Ouroboros Praos: An adaptively-secure, semi-synchronous **proof-of-stake blockchain**	→ https://eprint.iacr.org/2017/573.pdf
Quantum Blockchain using entanglement in time	→ https://arxiv.org/abs/1804.05979
Agreement with Satoshi – On the Formalization of **Nakamoto Consensus**	→ https://eprint.iacr.org/2018/400
Fun with **Bitcoin smart contracts**	→ https://eprint.iacr.org/2018/398
Ouroboros Genesis: Composable **Proof-of-Stake Blockchains** with Dynamic Availabilit	→ https://eprint.iacr.org/2018/378
Post-Quantum One-Time Linkable **Ring Signature** and Application to **Ring Confidential Transactions** in Blockchain (Lattice RingCT v1.0)	→ https://eprint.iacr.org/2018/379
On and Off-Blockchain Enforcement Of **Smart Contracts**	→ https://arxiv.org/abs/1805.00626
Enforceable Data Sharing Agreements Using **Smart Contracts**	→ https://arxiv.org/abs/1804.10645
How Value is Created in **Tokenized Assets**	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3146191

お役に立てば嬉しいです

- **BTCアドレス**

  12EBgvVeVdY7iaRUgSbyg9ZJRtbtVynimE

→おしまい