Bitcoin & Blockchain概況

2018.02 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）：**今回

第12回の臨時構成

- 第一部：通常編成で各分野の動向トピック
  - コインチェック事案をトピックスとして冒頭で紹介
- 第二部：ユースケースまとめ（金融以外）

Table of Contents

- 今回は、2017年11月～2018年1月の動きを中心に整理

トピックス：コインチェック関連

トピックス：コインチェック関連

- コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日に保有者への自己資金による補償方針を発表

  - 発生した事象の概要と経緯
  - 現時点で想定される原因
  - NEM側の動き
  - 暗号通貨利用者が留意すべきこと（一般論として）
  - 今後について

注：本記載内容は、2018年1月30日時点の公知情報に基づき、確からしいと考えられる内容をまとめたものに過ぎません。

コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日には保有者への自己資金による補償方針を発表。（1/9）

注：本記載内容は、2018年1月30日時点の公知情報に基づいて、同日時点において確からしいと考えられる内容をまとめたものに過ぎません。直近の情報は各自で確認ください。

- 発生した事象の概要と経緯
  - **コインチェックが保有するほぼ全てのNEMが不正に外部へ送金**された（事象の発生は1/26の02:57頃）。
    - 該当する5.2億XEMは、NEMのプレマイン発行量およそ90億XEMのうち約6%にあたる。
    - JPY換算では580億円相当。BTC換算では約5万BTC相当。
    - ちなみに、2013年のマウントゴックスはBTC換算で約70万BTCと今回のコインチェック事案の10倍以上であったが、JPY換算では約370億円相当。
    - 2016年のBitfinexは約12万BTCで約80億円相当。BTC換算で見ると今回のコインチェック事案は両事案より小さなケースとなる。
  - コインチェックとしては、1/26の11:25に事態を検知し（自動アラートシステムによるものとのこと）、関係監督官庁および国内外取引所への連絡などを行った上で、同日23:30頃より記者会見。
  - 暗号通貨の価格面のみをマスコミが過剰に煽る形（利用者自身で必要となる資産保護などリテラシー向上に資するものではない）で牽引された相場上昇もあり、580億円相当という、国内過去最大（JPYベース）の金額規模の被害額となったことから、特に日本国内においては、消費者が被害を受けた経済事件として報道されることになり、ここまで煽ってきた主体が掌を返してネガティブキャンペーンを始めることによって、暗号通貨への不信感が再び高まることが懸念される。
  - NEM資産の動きはブロックチェーン上に記録されており、explorerで確認する中では、00:02に10XEMの送金が行われたのを皮切りに、**1/26の00:04頃から00:09にかけて、５回にわたり1.0億XEMずつが不正送金された模様**。いずれも送金元は同一のアドレスであることから、1つの秘密鍵が漏洩するだけで、取引所保有のほぼ全てのNEM資産送金が可能だった可能性。

コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日には保有者への自己資金による補償方針を発表。(2/9)

注:本記載内容は、2018年1月30日時点の公知情報に基づいて、同日時点において確からしいと考えられる内容をまとめたものに過ぎません。直近の情報は各自で確認ください。

- 現時点で想定される原因
  - 取引所側がNEM資産について、**コールドウォレット（インターネットと切断されたオフライン環境）およびマルチシグ（秘密鍵を複数に分割しm人のうちn人の署名を必要とするもの）が不使用**だった点を突かれた攻撃の可能性。
    - よって、**NEM自体のセキュリティに問題があったのではない模様。**
    - 上述のように１つのアドレスに大量保管されていた理由、取引所の秘密鍵が漏洩した経緯、いつからどのように危険な状態になっていたのか、その状態に至る外的・内的要因の有無などは明らかにされていないため、これから本格的な原因調査および再発防止にむけた技術面・オペレーション面・人的リソース面など複合的な対応を講じる必要があると思われる。
  - 記者会見で一部メディアがマルチシグに過剰反応していたが、取引所システムの刷新負荷や鍵管理リスクを考慮すると、カバー取引に必要な額を差し引いても、NEM推奨マルチシグコントラクトの不使用よりも**コールドウォレット不使用**（全額ホットウォレット）であった点のほうが大きな要因と思われる。（なお、コインチェックのサイトでは、「コールドウォレットによるビットコインの管理」とされている）。
    - コールドウォレットという完全オフライン運用を実現する上で、技術的な課題や人材確保の課題などがあったにせよ、別の手段として秘密鍵を紙にエキスポートして金庫に管理しておくペーパーウォレットという簡易な選択肢もあったのではという意見もある。
    - 2018年1月からテレビCM開始など、ユーザ拡大を進めてきた中で本事態が発生したが、セキュリティ面の対応がユーザ拡大に間に合っていなかった可能性もある。

コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日には保有者への自己資金による補償方針を発表。(3/9)

注:本記載内容は、2018年1月30日時点の公知情報に基づいて、同日時点において確からしいと考えられる内容をまとめたものに過ぎません。直近の情報は各自で確認ください。

- NEM側の動き
  - NEM Foundationは、本件に伴って当該トランザクションを巻き戻すことにあたる**ハードフォークを行わない**ことを言明している。
  - また、NEM側で、流出資金の自動追尾に向けて、**当該XEMアセットへの自動タグ付けシステム**を準備中ともされる。
    - NEM Foundationメンバー外でも日本の個人エンジニアが協力するなどして、攻撃者のウォレット（NEMの通貨そのものに対してではない）にブロックチェーン上でマーキングするための取り組みが進められている。
    - この場合、NEMのMosaicによってブロックチェーン上にマーキングされたウォレットを持つ攻撃者アカウントはこれを外すことが出来ないため売却できない抑止力となることが期待される。
  - 1/28時点において、コインチェックの**当該NEM資産は全てのアカウントがブロックチェーン上**にあり、攻撃者は当該資産を取引所あるいはNEMコミュニティメンバーの個人アカウントへ送金することもされていないとのこと。

コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日には保有者への自己資金による補償方針を発表。（4/9）

注：本記載内容は、2018年1月30日時点の公知情報に基づいて、同日時点において確からしいと考えられる内容をまとめたものに過ぎません。直近の情報は各自で確認ください。

- 暗号通貨利用者が留意すべきこと（一般論として）
  - 今回コインチェックから補償対象として示されたNEM保有者が約26万人だったことから、日本における暗号通貨投資ユーザが（他の暗号通貨各種を合算した値として）約100万人ほど存在すると仮定すると、日本の人口のおよそ1%に相当する。
  - また、不正送金されたコインチェック単体のNEM預り高が580億円相当だったことから、他の暗号通貨を合算した値として数千億円以上の規模の投資規模となっていることが想定され、**現時点の日本の暗号通貨投資マーケットは草の根まで含めてかなりの規模**になっている。
  - 不正送金被害に遭った取引所が、当該資産に対して補償を行うことが今回は可能だったのは、タイミング（仮想通貨高騰直後で取引所に利益の蓄積があった）やコインチェック固有事情（古くから参入していることによる自己保有暗号通貨資産の値上がり益、月間取引高1兆円とも言われる巨額の取引を支える販売所サービスによるスプレッドなど）など複数要因がたまたま重なって返金可能だったという僥倖に過ぎず、これが当たり前だと勘違いして**「取引所に資産を保管しておいても大丈夫」と思うべきではない**。
  - トレード上の必要性や雑所得となる税制などから法定通貨に転換しないまま暗号通貨として留めおきたい場合であったとしても、**暗号通貨資産は取引所に保管するのではなく、自身の保有するウォレットに保管する**ことが重要。

コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日には保有者への自己資金による補償方針を発表。（5/9）

注：本記載内容は、2018年1月30日時点の公知情報に基づいて、同日時点において確からしいと考えられる内容をまとめたものに過ぎません。直近の情報は各自で確認ください。

- 暗号通貨利用者が留意すべきこと（一般論として）　（続き）
  - 今回の件を契機として、**自身のウォレットで管理する習慣**を利用者ひとりひとりが当たり前にするべき。
    - あわせて、現在のウォレットの機能・使いやすさ・セキュリティは一般ユーザにはマッチしていないために普及が進んでないことも提供者側は今後考慮して、サービス・プロダクトを開発していく必要。
  - 暗号通貨のアセット管理方法として、**ビットコインと比べてアルトコインには安定したウォレットが少ないことにアルトコイン投資時には留意すべき**だが、NEMの場合、NEM対応（NEMが利用している署名アルゴリズムEd25519に対応）のハードウェアウォレットとして、例えば**NEM NanoWalletと統合されたTrezor**がある。
    - なお、TrezorやLedger Walletなどのハードウェアウォレット購入時は、悪意あるソフトウェア混入のリスクを避けるため、**必ず販売元公式サイトから購入すべき**とされる。
  - 利用者としては、「**自身の資産保護を取引所に委ねるのではなく、取引所に「多額」の暗号通貨を保管したままにすること自体が危険であること**」や「**自分が信じて利用している対象をきちんと理解しないまま利用するには何事もリスクが伴うこと**」を改めて認識するべき。

コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日には保有者への自己資金による補償方針を発表。(6/9)

注:本記載内容は、2018年1月30日時点の公知情報に基づいて、同日時点において確からしいと考えられる内容をまとめたものに過ぎません。直近の情報は各自で確認ください。

- 今後について
  - 補償方針に関して、1/28、コインチェックから**NEM保有者およそ26万人に対して日本円でコインチェックウォレットへ返金する旨の発表**が行われた。
    - 対象資産総額は5.23億XEMであり、補償金額は88.549円（売買停止から補償方針発表時までの加重平均価格）に保有数を乗じたもの。
    - **補償時期や手続き方法は検討中**とし、返金原資（約463億円に相当）は**自己資本により実施**するとのこと。
      （意思決定の速さ、全額自己資本可能な資本力に加えて、対象となるNEM保有者の多さから透けてみえる日本の仮想通貨人口の多さがインパクトのある発表であった）
    - 事態発覚から約36時間、記者会見から約24時間という、きわめて短期間で補償方針が示されたことにより、納税資金がコインチェックに預けたままとなり納税資金を用意できず困窮に陥る利用者が大量発生するといった問題は回避できる可能性が出てきた。
  - とはいえ、補償期日など含めて未確定の要素もあるためまだ安心はできない他、補償が**納税に与える影響**（NEMでなく日本円による補償のため、利確を先延ばししていた保有者までもが強制的に利確として扱われる可能性）も要注視。

コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日には保有者への自己資金による補償方針を発表。（7/9）

注：本記載内容は、2018年1月30日時点の公知情報に基づいて、同日時点において確からしいと考えられる内容をまとめたものに過ぎません。直近の情報は各自で確認ください。

- 今後について（続き）
  - コインチェックにおいては、返金にむけた利用者対応手続きの具体化・準備、関係省庁対応、原因究明・当該アセットの追跡、関係省庁対応などで引き続きやるべきことが山積みと思われるが、加えて、本格対応としての技術面（今回の原因とされるホットウォレットやマルチシグコントラクト対応）・業務オペレーション面（危険な状態に至らしめたプロセスの再発防止）・人的リソース面（技術者の確保・体制増強、加えて、今回は該当しないとしても内部犯行を発生させないためのデューデリジェンスなど）含めた総合的対策が急務となると思われる。

  - 他の取引所については、**金融庁が国内取引所各社へシステム再点検を求める注意文書を送付**した他、**業界団体JCBAも会員へ緊急点検を要請**しており、業界横断によるセキュリティ基準策定も必要。

コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日には保有者への自己資金による補償方針を発表。(9/9)

注：本記載内容は、2018年1月30日時点の公知情報に基づいて、同日時点において確からしいと考えられる内容をまとめたものに過ぎません。直近の情報は各自で確認ください。

- 今後について（続き）
  - 1/29付けで、**関東財務局がコインチェックへの行政処分**を発表。下記内容の業務改善命令にあたり、2/13迄に書面で報告するよう求めている。
    - 本事案の事実関係及び原因の究明
    - 顧客への適切な対応
    - システムリスク管理態勢にかかる経営管理態勢の強化及び責任の所在の明確化
    - 実効性あるシステムリスク管理態勢の構築及び再発防止策の策定等
  - 同じく1/29に**金融庁で行政対応に関する記者説明**が行われ、その中では、「発生原因」「顧客対応・今後の予定」「拡大防止策」および「財務・資金繰りの影響」について報告を求めたとしている。また、他の取引所についても安全対策に関して緊急調査を行うとのこと。
  - 中期的には、(1)一般ユーザへの暗号通貨普及が想定以上進んでいることか今回明らかになったことを受けて、ユーザビリティ・機能・セキュリティ（耐タンパ性など）を考慮したウォレットの開発・提供を進める必要がある。(2)また、取引所のカウンターパーティリスク軽減のために、分散型取引所（DEX）の技術開発の推進ならびにユーザビリティ向上（現在の分散型取引所は従来型の集中取引所と比べて高いリテラシーが前提となっているため）が必要。

トピックス

コインチェック、約5.2億XEMの不審な移動があるとしてアルトコイン売買を停止した後、翌日には保有者への自己資金による補償方針を発表。(8/8)

- 出典：http://corporate.coincheck.com/2018/01/26/29.html
- 出典：http://corporate.coincheck.com/2018/01/28/30.html
- 出典：http://explorer.ournem.com/#/s_account?account=NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG
- 出典：http://chain.nem.ninja/#/account/NC3BI3DNMR2PGEOOMP2NKXQGSAKMS7GYRKVA5CSZ/0
- 出典：https://btcnews.jp/4qcnoudq14806/
- 出典：https://cryptonews.com/news/coincheck-hacked-more-than-500-million-xem-stolen-1093.htm
- 出典：https://logmi.jp/260622
- 出典：https://logmi.jp/260631
- 出典：https://logmi.jp/260644
- 出典：https://logmi.jp/260658
- 出典：https://blog.trezor.io/announcement-trezor-integration-nanowallet-nem-xem-cryptocurrency-feature-803e7ffbf023
- 出典：http://itpro.nikkeibp.co.jp/atcl/news/17/012703040/
- 出典：https://ethereum-japan.net/ethereum/coincheck-nem-hacking-analysis/
- 出典：https://medium.com/nemofficial/coincheck-hack-interview-with-nem-foundation-vp-jeff-mcdonald-alex-tinsman-from-inside-nem-8d678babb19a
- 出典：http://techwave.jp/archives/bccc-reports-the-case-of-coincheck-outflow-nem.html
- 出典：https://www.nikkei.com/article/DGXMZO26264470Z20C18A1000000/
- 出典：https://bitpress.jp/news/market/entry-7620.html
- 出典：http://kantou.mof.go.jp/rizai/pagekthp0130000001_00004.html

1. Bitcoinエコシステムの動向

- ビットコインエコシステムにおける主なニュース
- ビットコイン技術トピックの解説
- Scaling Bitcoin２０１７のトピック概観
- その他のトピックニュース

1) Bitcoinエコシステムの動向

- ビットコインエコシステムにおける主なニュース
  - Bitcoin Goldハードフォーク
  - Segwit2x、ハードフォーク計画中止
  - Tetherを巡りハッキングおよびBitfinexとの協調の疑惑がとりざたされる
  - Bitcoin Cashに係る開発・テスト協定が発表
  - BitPay、年間10億ドルのビットコイン決済を扱う中で送金手数料高騰に伴いBitcoin Cash採用へ
  - Lightning、複数実装間のペイメントを試行
  - RSK、テストネットへベータローンチ
  - Bitfury、アドレス・クラスタリングのホワイトペーパー発表
  - c-lightning向け補完パッケージLightning Charge、Elements Projectへ導入

Bitcoin Goldハードフォーク

- 491406ブロック時点でビットコインからフォーク。
  - 日本時間11/13am3:00にローンチ。
  - **SHA256ではなく、Zcashと同じくEquihashを使用してPoW**することで、**ASICによるマイニング集中を避ける**と主張。
  - Segwit2xと異なり、**コミュニティ（開発リソース、ハッシュレート）の分裂は無し。**
- BitcoinGoldの取り出しスキャムサイトで300万ドル被害
  - この種の**ハードフォークコインの取り出しツールは、秘密鍵盗み取りに要注意。**

→ 出典: https://btcgpu.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf
→ 出典: http://doublehash.me/bitcoin-gold-fork/
→ 出典: https://blog.coinbase.com/timeline-and-support-bitcoin-segwit2x-and-bitcoin-gold-eda72525efd
→ 出典: http://www.jpbitcoinblog.info/entry/20171024/1508781425
→ 出典: https://ethereum-japan.net/bitcoin/bitcoin-gold-price-analysis/
→ 出典: https://web.archive.org/web/20171113184358/https://mybtgwallet.com/

SEGWIT2X、ハードフォーク計画中止

- **コミュニティ内の十分なコンセンサスが得られず**ハードフォーク計画中止を宣言した
- Segwit2xハードフォークは、アクティベートせず
  - btc1と呼ばれるSegwit2xノードはビットコインブロックから分岐しSegwit2xブロックチェーンおよびB2Xを生成するようプログラムされていたものの、**btc1コードベースにバグや仕様の周知不足**があり、フォークポイント（494,784 block）を迎えてもSegwit2xブロックはマイニングされず。

- 出典: https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html
- 出典: http://www.ibtimes.com/segwit2x-dies-bitcoin-fork-averted-2612274
- 出典: https://medium.com/@spair/segwit2x-should-be-canceled-b7399c767d34
- 出典: https://bitcoinmagazine.com/articles/now-segwit2x-hard-fork-has-really-failed-activate/
- 出典: https://ethereum-japan.net/bitcoin/segwit2x-hardfork-had-failed-due-to-off-by-one-error/

TETHERを巡りハッキングおよびBITFINEXとの協調の疑惑がとりざたされる（1/2）

- Tetherは**1米ドルにペグ付けされたstable coinをUSDTとして発行**しており、**取引所などによりBitfinexやPoloniexなどの取引所間で米ドルを送金する代用品**として利用されている。
- このうち3100百万ドル相当のUSDTがハッキングにより不正に引き出された。
- TetherはOmni上で動いており、Omni Coreソフトウェアの新バージョンをリリース。
- Tetherを巡っては、「Bitfinexと同一人物がコーディネートしているため同一エンティティである」「USDTトークンを裏付け無しに乱造している」「USDTトークンがBitfinexでのBTC価格引き上げなどの市場調査に使われた可能性がある」といった、Bitfinexとの間での共謀関係も取りざたされている。

→ 出典: https://elementus.io/blog/tether-hack/
→ 出典: http://www.trustnodes.com/2017/11/21/tether-allegedly-hacked-30-million-hardforks-blacklist
→ 出典: https://tether.to/tether-critical-announcement/
→ 出典: https://tether.to/update-on-security-incident/
→ 出典: https://btcnews.jp/vl4errmi13772/
→ 出典: https://tokeneconomy.co/24-to-tether-or-not-to-tether-3765b2c51846

TETHERを巡りハッキングおよびBITFINEXとの協調の疑惑がとりざたされる（2/2）

- Factomは2015年3月に、TetherおよびCoinapultと提携している。
  - これら提携におけるFactomの役割は何だろうかということで、公開質問を挙げている。

- Tetherについては、以下の4点。
  - まだ提携関係が続いているのかどうか。
  - **Tetherが一定量のUSDを、発行されたUSDTと1対1で管理された下で保有することを検証できるか**どうか。
  - TetherとBitfinexが直接USDTを発行して、自身でBTCを購入しCoinbase上で売却して（代理口座を用いて）USDのCoinbaseを緩やかに破綻に追い込んでいないと検証できるかどうか。
  - TetherとBitfinexが顧客請求に対して正確な量のBTCを保有していると検証できるかどうか。

→ 出典：https://hackernoon.com/open-questions-for-factom-53e4eeaafdb

BITCOIN CASHに係る開発・テスト協定が発表（1/2）

- Bitcoin Cashクライアントソフトウェアの開発チーム７社（Bitcoin ABC、Bitcoin Unlimited、nChain、Bitcrust、Bitprim、ElectrumX、Parity）がロンドンで会合を持った。
  - 会合の目的は、**中期的な開発プライオリティの討議**であり、Bitcoin Cashを大きくスケールさせ、高速で低手数料でグローバルなP2P電子キャッシュシステムとするためのビジョンを全参加者で共有できたとしている。
  - Bitcoin UnlimitedおよびBitcoinABCの発表に挙げられているポイントは以下のとおり。

- 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。
  - アップグレード３ヶ月前の2018年2月15日迄に、アップグレードに含める機能およびコードを最終化。
- **デフォルトブロックサイズ上限**を高める。
  - その最初のステップとして、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へ移行する。
- **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**。

→ 出典：https://www.bitcoinunlimited.info/cash-development-plan
→ 出典：https://www.bitcoinabc.org/bitcoin-abc-medium-term-development
→ 出典：http://www.tottemoyasashiibitcoin.net/entry/2017/11/30/125755
→ 出典：https://btcnews.jp/1d1hbpbz13926/

Bitcoin Cashに係る開発・テスト協定が発表(2/2)

- オペコードを再度有効にする。
  - 新たにOP_GROUPおよびOP_DATASIGVERIFY向け実装を提供するとともに、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とし、Representative tokenやバイナリコントラクトなどの機能を利用できるようにする。
- **新しいBitcoin Cashアドレスフォーマット**を実装する。
  - BTCが意図せずBCHウォレットへ送られてしまうことを難しくする。
- **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。
  - ユーザー体験向上に寄与するべく、**Bobtailの利用**を検証する。
- **Graphen**を統合することによって**ブロック伝播を改善**する。
  - 同時に、Graphenの実装を単純化すべくブロック内のトランザクションオーダリング要件を取り除くことのメリデメを検証する。

→ 出典：https://www.bitcoinunlimited.info/cash-development-plan
→ 出典：https://www.bitcoinabc.org/bitcoin-abc-medium-term-development
→ 出典：http://www.tottemoyasashiibitcoin.net/entry/2017/11/30/125755
→ 出典：https://btcnews.jp/1d1hbpbz13926/

BitPay、年間10億ドルのビットコイン決済を扱う中で送金手数料高騰に伴いBitcoin Cash採用へ

- BitPayのビットコイン決済は2016年と比べて一年間で300%以上成長して10億ドル規模に。
  - そうした成長に対応していくべく、**ビットコイン以外のブロックチェーン上でのペイメントもサポート**していくとした。
  - ユーザからは、**高速なトランザクション確定や、ペイメントのプライバシー等の要求**が寄せられている。
  - 今年9月から既にウォレット上でのBCHのサポートを追加しているが、**BCHによるペイメントプロセシングへの要求**が増えている。

- BCHは**トランザクション確定が高速**なほか、**マイナー手数料が安価**（12/15時点でキロバイトあたり手数料がBCHは0.021ドル、BTCは60.82ドル）な点が特徴。

- そうした環境を受け、**BCHによるペイメントオプションのサポートを開始**予定。
  - **インボイスにデフォルトでBCHペイメントを含める**ようにし、支払い時に従来どおりBTCとあわせてBCHを使うことを選択できるようになる。
  - 他の暗号通貨についても、ハッシュパワーやセキュリティ、支払い利便性、普及率、市場価値などを要素として採用を判断していく。

→ 出典: https://blog.bitpay.com/bitpay-growth-2017/
→ 出典: https://blog.bitpay.com/multiple-blockchains/

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。

- 二つのサンプルケース
  - １つ目のサンプルケースは、eclairアプリケーションを用いた**Starblocksコーヒーショップ**を用いて、lndのLightningアプリケーションを使って顧客がビットコインで支払い、それがc-lightningを通してルーティングされるというもの。
  - ２つ目のサンプルケースは、eclairからlndによる**記事マイクロペイメントであるYalls.orgへペイメント**を行い、c-lightningを通してルーティングされるというもの。

- レイヤー2ソリューションにとっての2018年
  - まだMainnet上でのベータ版リリース時期は示されていないが、先日ラトビアで行われたBaltic Honeybadger Bitcoin Conference にて、Lightning LabsのElizabeth Stark CEOは**2018年がレイヤー２ソリューションにとって広く使われるための準備期間にしたい**と述べている。

→ 出典: https://medium.com/@lightning_network/lightning-protocol-1-0-compatibility-achieved-f9d22b7b19c4
→ 出典: https://coinjournal.net/bitcoins-lightning-network-version-1-rc-mainnet-beta-implementations-way/
→ 出典: http://individual.net/lightning-network-successful-cross-implementation-test-on-bitcoin-mainnet/
→ 出典: https://starblocks.acinq.co/#/

RSK、テストネットへベータローンチ

- 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Merge Mining**によりビットコインマイニングとあわせて行われる。
- ビットコインのハッシュパワーの６割を占めるマイナーが、**RSKのMerge Miningプラグインを導入**。さらに３割も後に続く見込みとされる。
- RSKにより、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すことが可能となる。
- ベータローンチのコードネームはBamboo。

- RSK、**ビットコイン誕生日にあわせGenesis ブロックをマイニング**し、**メインネットのベータ版**ローンチ
  - http://www.rsk.co/
  - https://news.bitcoin.com/rsk-mines-genesis-block-bitcoin-ethereum-like-smart-contract-platform/
  - https://docs.google.com/forms/d/e/1FAIpQLSfoG_qF5wPY27tqcYnFbzNv4uwwDq6JeBe5no_zoYvKH62mBA/viewform

→ 出典: https://news.bitcoin.com/bitcoin-ethereum-smart-contract-sidechain-rsk-launches/

BITFURY、アドレス・クラスタリングのホワイトペーパー発表

- **ブロックチェーンデータの関連ビットコインアドレスを分析**することを通じて、単一ユーザーに属するアドレスを決定する。
- 関連アドレスをリンクするクラスタリングにより、**捜査当局が単一主体と紐付ける**ことが可能に。
- 従来の方法では、ブロックチェーンの情報を用いてクラスタリングモデルを構築し、それをオフチェーンデータと検証するものだったが、Bitfuryはモデル構築段階で双方のデータを用いることにより、分析結果の正確性を向上。

→ 出典：https://medium.com/@BitFuryGroup/the-bitfury-group-unveils-solution-for-analyzing-related-bitcoin-addresses-8eba57f4c7f9
→ 出典：http://bitfury.com/content/5-white-papers-research/clustering_whitepaper.pdf

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。
  - Elements ProjectでリリースされているJavaScriptやPHPライブラリでアクセス可能なREST APIを通じてc-lightningの機能を利用できるようにしている。
  - c-lightningはLightningのスペックを実装するために設計されたものであり、クレジットカード会社や既存のオンラインペイメントシステムと統合するには手間がかかるものであり、Lightningによるペイメント普及にはそれらを容易にすることが必要。
  - **Lightning Chargeは、Lightning上にアプリを構築しやすくするべく**、Blocksreamと活動している個人開発者のNadav Ivgiにより設計されたもの。
  - 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。

- Blockstream Storeでは**ビットコインメインネット上のLightningペイメント**を用いて、ステッカーやTシャツを購入可能（ただし、**Lightning Networkはテスト段階の技術であることに注意**）。
  - Blockstream StoreはWordPressおよびWooCommerce上に構築され、WooCommerce Lightning Gateway（同じくElements Projectで利用可能な、Lightning Changeに基づきLightningペイメントを受けるためのプラグイン）を通じてLightning ChargeおよびC-lightningに接続。

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

1) Bitcoinエコシステムの動向

- ビットコイン技術トピックの解説
  - 技術トレンド全体像
  - ブロック伝播に関するもの
  - Lightning Network／アトミックスワップ／ペイメントチャネルに関するもの
  - プライバシーに関するもの
  - 双方向ペグ／サイドチェーンに関するもの
  - 署名／証明／スクリプトに関するもの
  - コンセンサスルール変更

- ビットコイン技術トピックの解説
  - 技術トレンド全体像
    - Segwit対応
    - セカンドレイヤーソリューション
    - プライバシー技術
    - サイドチェーン
    - Shnorr署名
  - ブロック伝播に関するもの
  - Lightning Network／アトミックスワップ／ペイメントチャネルに関するもの
  - プライバシーに関するもの
  - 双方向ペグ／サイドチェーンに関するもの
  - 署名／証明／スクリプトに関するもの
  - コンセンサスルール変更

2018年注目のビットコイン技術トレンド(1/3)

- 2017年はビットコイン価格上昇が注目されたが、技術面ではまだスタートしたばかり。
  - 2018年の注目トピックは**「Segwitおよび新しいアドレス体系」「Lightning Networkのメインネットへのロールアウト」「TumbleBitおよびZeroLinkを通じたプライバシー向上」「サイドチェーンの適用」「Shnorr署名」**。

- Segwitの適用率は未だ低いままだが、2018年はSegwitトランザクションの送信・受入に対応したBitcoin Coreインタフェースが可能となる見込み。
  - Bitcoin Core 0.16が5月に予定されており、そこでは新しいアドレス体系Bech32が導入予定。
  - 現在Segwit向けに使われているP2SHフォーマットからコインを使うには、トランザクション中のRedeemスクリプトを明かす必要があるが、ネイティブSegwitアウトプットにおいてはこれは不必要であり、Segwitトランザクションの受け手は低コストでこれらのコインを使うことが出来る。
  - 加えて、CoinbaseもSegwitへのアップグレードを計画しており、ネットワーク渋滞緩和の可能性。

- 中期的なスケーラビリティにおいて**セカンドレイヤーソリューション**は重要であり、中でも少額トランザクションにおいてLNへの期待は大きい。
  - 2017年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を確保**した他、10月にはデスクトップウォレットアプリを提示。
  - 2018年は開発者に加えユーザーにも適用が広まることが期待される。

→ 出典: https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/

2018年注目のビットコイン技術トレンド(2/3)

- プライバシー技術として、**TumbleBit**および**ZeroLink**のメインネットへのデプロイも間近とされる。
  - TumbleBitは、**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。**
  - また**タンブラーがユーザー同士をリンクすることもできない。**
  - NTumbleBitとして初めて実装された後、StratisによるBreezeWalletへ実装された（2017年12月にベータ版）。
  - 一方ZeroLinkは、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**であり、単一のCoinJoinトランザクションを生成するため安価で済む。2017年12月に100ユーザーの参加によるテストを行ったことを発表。

→ 出典：https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/

2018年注目のビットコイン技術トレンド(3/3)

- **サイドチェーンは、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。
  - **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**だが、2018年には1.0版がリリース予定。
  - もう一つの注目サイドチェーンは**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**することが出来る。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。
  - あと一つの注目サイドチェーンは**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、**drivechainはマイナーの投票により安全確保される**点が特徴。

- **Shnorr署名**は**複数の署名を単一の署名へと集約が可能**なため、**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でき、スケーラビリティ向上**にも寄与（トランザクションあたり平均25%の節約）。
  - **Scriptless Scriptsを用いるスマートコントラクト**等も可能となる。

→ 出典：https://bitcoinmagazine.com/articles/keep-eye-out-these-bitcoins-tech-trends-2018/

- ビットコイン技術トピックの解説
  - 技術トレンド全体像
  - ブロック伝播に関するもの
    - ビットコインのブロック伝搬とCompact Block Relay
    - Bitcoin Cashにおけるテラバイトブロック
    - Bitcoin Cash関連のトピックニュース
  - Lightning Network／アトミックスワップ／ペイメントチャネルに関するもの
  - プライバシーに関するもの
  - 双方向ペグ／サイドチェーンに関するもの
  - 署名／証明／スクリプトに関するもの
  - コンセンサスルール変更

ビットコインのブロック伝搬とCOMPACT BLOCK RELAY

- 通常、ブロックのリレー時には**トランザクション授受が二回**行われる（**トランザクションのブロードキャスト時**と**マイニングブロックのリレー時**）。
- Compact Block Relayでは、**通常のブロックリレーよりも帯域使用量を減らしてリレー**を行う。
- 1MBのブロックをリレーするのではなく、ブロックヘッダや短略トランザクションID、特定トランザクションのみをリレーしてデータ容量をコンパクトに収めた上で、リレー後にそれらデータからブロックを再構築してチェーンに繋ぐ方法をとる。

→ 出典：http://blockchain.gunosy.io/entry/network-and-blockrelay

Bitcoin Cashにおけるテラバイトブロック

- テラバイトブロックが技術・経済両面で実現可能であることを示すもの。
- 地球上の全人類が１日あたり50トランザクションの処理を、0.1セント以下のコストで可能。
  - ハードウェアコスト低減や、ソフトウェアのブレークスルーを前提とせず、既存技術の組合せのみ。
- 秒あたり数トランザクションが上限であるBitcoin Coreに対して、**Bitcoin Cashによるテラバイトブロック生成の場合には秒あたり700万トランザクション**が可能。
  - これは、100億人が１日あたり55トランザクション発行するパフォーマンスに相当。
- コスト面でも、マイニングリグに関するコストは健全な非中央集権市場（現在のビットコインマイニングよりも分散した数百の独立マイナーを想定）を可能とするだけの低さに収まるとする。
- スケーリング面では、トランザクション伝播、トランザクションバリデーション、ブロックのブロードキャストの三段階での検証につき言及している。

→ 出典：http://blog.vermorel.com/journal/2017/12/17/terabyte-blocks-for-bitcoin-cash.html

BITCOIN CASH関連のトピックニュース

- Bitcoin Cash、難易度調整アルゴリズム(DAA)含むハードフォーク完了し、Bitcoin Clasic誕生
  - http://www.trustnodes.com/2017/11/13/bitcoin-cash-successfully-hardforks
  - https://www.bitcoinabc.org/november
  - http://bitcoinclashic.org/
  - https://btcnews.jp/4aatxnj813648/
- Bitcoin Unlimited主催の**”Satoshi’s Vision Conference”**、3/23-25に東京で開催
  - https://satoshisvisionconference.com/
- Bitcoin Unlimited Cash、1.2.0.0リリースノート公開
  - https://github.com/BitcoinUnlimited/BitcoinUnlimited/blob/BitcoinCash/doc/release-notes/release-notes-bucash1.2.0.0.md

- ビットコイン技術トピックの解説
  - 技術トレンド全体像
  - ブロック伝播に関するもの
  - Lightning Network／アトミックスワップ／ペイメントチャネルに関するもの
    - Lightning Networkと取引所の統合
    - ペイメントチャネル間の資金移動を可能にするChannel Factory
    - アトミックスワップを巡る2017年のトピック振り返り
    - Counterpartyとクロスチェーンアトミックスワップ
    - スクリプトレス・スクリプトによるアトミックスワップ
  - プライバシーに関するもの
  - 双方向ペグ／サイドチェーンに関するもの
  - 署名／証明／スクリプトに関するもの
  - コンセンサスルール変更

LIGHTNING関連のトピック

- Lightning Lab、**Litecoin/Bitcoinのクロスチェーンアトミックスワップ**を発表
  - https://blog.lightning.engineering/announcement/2017/11/16/ln-swap.html
  - http://coffeetimes.hatenadiary.jp/entry/2017/11/17/145437
  - https://bitcoinmagazine.com/articles/atomic-swaps-how-the-lightning-network-extends-to-altcoins-1484157052/
  - https://btcnews.jp/4auzpr8n13788/

LIGHTNING NETWORKと取引所の統合 （1/2）

- Lightning Networkがビットコインのスケーラビリティに貢献できる主要領域は、**ユーザーと取引所間のトランザクションを高速かつ安価にする**ところ。
  - ビットコインの現在の**オンチェーン取引量に占める大部分は取引所が絡む**ものであるため、これらのうち**幾分かをLightningのペイメントチャネルへ移すことにより皆にとって手数料を安価に**できるほか、高速な取引所の実現は流動性を高めビットコイン生態系における価格決定をより効率的なものとできる。
- 現時点で利用できるLightning Networkのトランザクションの機能を用いて、二つのタイプの提案（1. **取引所-取引所**、2. **取引所-ユーザ**）を行う。
  - 前者（**取引所-取引所**）のタイプの場合、**取引所は互いにチャネルを開設**し、**取引所間におけるユーザー資金移動スピード**を高め安全なものとできる。
  - 一方で後者（**取引所-ユーザ**）のタイプの場合、**ユーザーは最低限の手数料で高速で資金をデポジットしたり引き出したり**できるほか、**ユーザーが取引所間の資金移動を低い摩擦および高いプライバシーのもとに行う**ことが可能となる。
- 取引所-取引所へのLN適用による取引所にとってのメリット・デメリット
  - メリットは、ユーザーへの資金移動を高いセキュリティで可能となること。
  - デメリットとしてはトレーダーがトランザクション詳細を取引所に開示必要となる点。
  - 例えば、受取先取引所の名前や、受取先取引所のアカウントIDを、送り元取引所に開示要。

→ 出典：https://docs.google.com/document/d/1r38-_IgtfOkhJh4QbN7l6bl7Rol05qS-i7BjM3AjKOQ

LIGHTNING NETWORKと取引所の統合 （2/2）

- この場合、取引所は互いにLightningのペイメントチャネルを開設し、取引所のウェブサイトにユーザがほかの取引所上のアカウントへ直接資金移動できるインタフェースを追加する。
  - 取引所間でアカウント名の標準が整備されることにより、情報特定をLightningトランザクションへ付随するペイロードに含めることができる。
  - さらに、取引所はこれをトレーディングAPIの中で自動的に起動できるようにして、アービトラージを追求できるようにする可能性も。
- **取引所-ユーザ**へのLN適用により、**トレーダーは取引所内外の資金移動を高速で行うことが可能。**
  - また取引所のコントロール下におく残高を小さく保てるため、取引所でセキュリティ違反が起きたときにもリスク低減可能。
  - 一方でユーザーが自身のLightningペイメントチャネルに責任を持つ必要があるためユーザーにとって煩雑となるデメリットあり。
- この場合は、取引所が一つまたは複数のパブリックにアクセス可能なLightningノードを運営するため、これらノードが取引所のウォレットバックエンドと統合され、Lightningペイメントを通じてデポジット・引き出された資金をすぐに利用可能。

→ 出典：https://docs.google.com/document/d/1r38-_IgtfOkhJh4QbN7l6bl7Rol05qS-i7BjM3AjKOQ

ペイメントチャネル間の資金移動を可能にする CHANNEL FACTORY （1/2）

- Lightning Networkの課題
  - **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の提供するソリューション
  - **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。
  - **ファ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。
  - **マルチパーティチャネル内でのチャネル開閉時にはブロックチェーンに戻ることが無い**ので、**オンチェーントランザクション手数料無しに何度もチャネル開閉できる**ことがポイント。

- Channel Factoryのアーキテクチャ
  - ブロックチェーン、マルチパーティチャネル、マイクロペイメントチャネルという三層構造。
  - マルチパーティチャネルはチャネルファクトリーとも呼ばれ、通常のマイクロペイメントチャネル同様にタイムロックや罰則が実装される。

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

ペイメントチャネル間の資金移動を可能にする CHANNEL FACTORY （2/2）

- Channel Factoryのトランザクション処理プロセス
  - マルチパーティチャネルへのファンディングトランザクションをフックトランザクションと呼び、参加者のファンドをマルチシグの共有所有としてロックする。
  - ロックされたファンドをインプットとして、二者間チャネルへ渡すファンディングトランザクションをアロケーションと呼び、各トランザクションをリプレイスする。
  - あるノードがマルチパーティチャネルをクローズすると決めると、その決定をブロードキャストし、受信したノードは子チャネルの更新を停止し、持分の合計をブロードキャストする。
  - ブロードキャストをもとに各ノードがセツルメントトランザクションを生成・署名してブロードキャストする（トータル持分を偽るとセツルメントトランザクションは無効化）。

- 期待効果
  - **ブロックチェーンに現れるのはフックトランザクションとセツルメントトランザクションの二つのみ**であり、ブロックチェーン容量を節約して、不必要な情報を隠蔽できる。
  - シュノア署名を用いて署名集約することにより、単一の公開鍵・単一の署名にまとめることができる。
  - マルチシグアウトプットを一つの公開鍵によって生成して、対応する署名を一つの署名にまとめることができるので、署名集約を通じて更なるブロックチェーン容量の節約ができる点がポイント。

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

アトミックスワップを巡る2017年のトピック振り返り

- 9月に**Decred-Litecoin間**のオンチェーンアトミックスワップが発表された。
- 10月には**Bitcoin-Ethereum間**のオンチェーンアトミックスワップが発表された。
  - Decred-Litecoin間のケースと異なり、**異なるブロックチェーン間のスワップ**であり、より複雑な実装が必要とされ、さらに前進した。
  - 主要ブロックチェーン間の**オンチェーンスワップ**は、**トレード中もトレーダーのアセットが安全に保たれることを示した**意味で重要なマイルストーンとなった。
  - **オンチェーンスワップの場合、完了まで2～3分**を要するため、**即時で済み手数料も要しないオフチェーンスワップが次のマイルストーン**となった。
  - DEXが安全にトランザクションを履行する上でも、価格変動に左右されないために即時スワップが必要となる。
- 11月、**Bitcoin-Litecoin間**の**オフチェーンアトミックスワップ**がLightning Labsから発表された。
  - **HTLCでなくLightning Networkを介して**行われたもの。
  - 次のマイルストーンは、EthereumブロックチェーンからBitcoinへのアトミックスワップであり、Raiden Networkで実現されると想定。
- トークンのよってたつ**ブロックチェーンに依らず、どのトークン同士でも**アトミックスワップが**即時・安全かつ最低限の手数料で実現**されることがゴールとなる。

→ 出典：https://blog.altcoin.io/the-evolution-of-atomic-swaps-e33ad3af8818

COUNTERPARTYとクロスチェーンアトミックスワップ

- **オンチェーンアトミックスワップ**は必ずしも集中型取引所より高速・安価にアセットやトークンの取引するものではなく、そのメリットはむしろ**トラストレスに取引可能な点**にある。
- ある種の**トラストレスなエスクロー**としてブロックチェーンを用いることにより（ある秘密が分かればそこから使うことができる、誰にもコントロールされないアドレスにアセットを送る）、**第三者を介する必要なくデジタルアセットを交換できる。**
- Counterpartyアセット間のビットコインブロックチェーン上の取引だけでなく、**異なるブロックチェーン間で例えばCounterpartyのSATOSHICARDとEthereumのCryptokittyをトレードすることも可能。**
- クロスチェーンアトミックスワップの要件は、**双方のチェーンが秘密のハッシュ値を検証でき**（同じハッシュ関数をサポート）、**払い戻しのタイムアウト条項を含める**ことのみ。
- あとは、**それぞれのブロックチェーンが安定的**であり、大きなreorgの発生が起きにくいことが必要。

→ 出典：https://blog.indiesquare.me/counterparty-and-cross-chain-token-atomic-swaps-947b6b0011c1

スクリプトレス・スクリプトによるアトミックスワップ（1/2）

- **通常のアトミックスワップ**
  - 通常のオンチェーンアトミックスワップの場合、**参加者双方のみが知る秘密を明かすことを条件にコインを使えるようにする**ことによってオンチェーンでスワップを行うが、**契約条件はトランザクション中のscriptPubKey中**に埋め込まれる。
  - ネットワークの**全ノードがコントラクトを実行**するため、**計算リソースを消費**する他、プライバシー上も問題。
  - また、マルチシグやタイムロック等のスマートコントラクトが複雑になれば、**実装の異なるソフトウェアがコントラクト詳細をわずかでも異なる解釈をしてネットワークコンセンサスが難しくなる可能性**もある。

- **Scriptless Scripts**
  - **署名集約を可能とするシュノア署名**（**差分の計算**も可能）を用いて、**アトミックスワップ**。
  - 例えば、二者で**差分**「７」を合意しておき、一方が「１００」をブロードキャストすると、他方のみが秘密の数字「９３」を知ることができる。
  - **有効な署名のパーツを「アダプタ署名」**とし、公開を合意した署名の秘密を明かすことにより、**アダプタだけが有効署名を生成できるような「ある種の約束ごと」**として機能させることが出来る。

→ 出典：https://download.wpsoftware.net/bitcoin/wizardry/mw-slides/2017-03-mit-bitcoin-expo/slides.pdf
→ 出典：https://bitcoinmagazine.com/articles/scriptless-scripts-how-bitcoin-can-support-smart-contracts-without-smart-contracts/
→ 出典：https://joinmarket.me/blog/blog/flipping-the-scriptless-script-on-schnorr/

スクリプトレス・スクリプトによるアトミックスワップ（2/2）

- Scriptless Scriptsの例示（ストリーミングでアーティストの曲を聴きたいケース）
  1. 通常のビットコイントランザクションで、リスナーからアーティストへの送金トランザクションを生成し、**双方がシュノア署名の片割れを提供して１つのシュノア署名を作る。**
  2. アーティストは、自分のシュノア署名の片割れ８０００、曲の署名７０００の**差分１０００を「アダプタ署名」として**リスナーへ渡す。
  3. リスナーは、受け取ったアダプタ署名１０００が「アーティストのシュノア署名の片割れ」と「曲の署名」の差分であることを**ゼロ知識証明**を用いることで、どちらの署名にもアクセスせず検証可。
  4. リスナーは、アダプタ署名を検証した後、自分のシュノア署名の片割れをアーティストに渡す。
  5. アーティストは、リスナーのシュノア署名の片割れと自分のシュノア署名の片割れを使って完全な署名を生成し、ビットコインネットワーク上でブロードキャスト（リスナーからアーティストへの送金トランザクション）すると共に、自分の**シュノア署名の片割れ８０００を皆に明かす。**
  6. リスナーは、アーティストのシュノア署名の片割れ８０００を使ってアダプタ署名１０００と**引き算を行うと、曲の署名７０００が分かる**ので、曲を聴くことが出来る。
- 特徴
  - ビットコインセツルメントトランザクション以外のコントラクトはブロックチェーンに記録されないので、**コントラクトに関わるデータは当事者以外に知られることが無い。**
  - ビットコインのブロックチェーンからスマートコントラクトを切り出しつつ、セキュリティも強化できる。

→ 出典：https://download.wpsoftware.net/bitcoin/wizardry/mw-slides/2017-03-mit-bitcoin-expo/slides.pdf
→ 出典：https://bitcoinmagazine.com/articles/scriptless-scripts-how-bitcoin-can-support-smart-contracts-without-smart-contracts/
→ 出典：https://joinmarket.me/blog/blog/flipping-the-scriptless-script-on-schnorr/

- ビットコイン技術トピックの解説
  - 技術トレンド全体像
  - ブロック伝播に関するもの
  - Lightning Network／アトミックスワップ／ペイメントチャネルに関するもの
  - プライバシーに関するもの
  - 双方向ペグ／サイドチェーンに関するもの
  - 署名／証明／スクリプトに関するもの
  - コンセンサスルール変更

プライバシー関連のトピックニュース

- Confidential Transaction、通常トランザクションの16倍あったサイズを3倍へ抑えるアップデート発表
  - https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-November/015283.html
  - https://www.reddit.com/r/Bitcoin/comments/7d5zbc/finally_real_privacy_for_bitcoin_transactions/
- MimbleWimbleの実装であるgrinがテストネットへローンチ
  - https://themerkle.com/mimblewimble-launches-first-of-many-testnets/
  - https://github.com/mimblewimble/grin/blob/master/doc/build.md
- 複数参加者間のスクリプトのプライバシー向上を図るためのTaprootコンセプトをBlockstreamを離れたGregory Maxwellが発表
  - https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html
  - http://techmedia-think.hatenablog.com/entry/2018/01/27/163755

- ビットコイン技術トピックの解説
  - 技術トレンド全体像
  - ブロック伝播に関するもの
  - Lightning Network／アトミックスワップ／ペイメントチャネルに関するもの
  - プライバシーに関するもの
  - 双方向ペグ／サイドチェーンに関するもの
    - 双方向ペグの概要
    - Drivechainの概要
    - トラストレスなサイドチェーン実現に必要なコンパクト証明を提供するNIPoPoW（PoWの非対話証明）
  - 署名／証明／スクリプトに関するもの
  - コンセンサスルール変更

双方向ペグの概要 （1/4）

- **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**される。
  - 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**。
  - 相手のブロックチェーンに決済ファイナリティの無い場合、双方向ペグのセキュリティモデルは、財産管理人（カストディアン）グループによる「いつビットコインのロック解除を行うか」「ロック解除したビットコインをどこへ送るか」に関する投票（デジタル署名やハッシュパワー（PoW）や暗号通貨持分（PoS）等によるもの）と同等。

- 双方向ペグの設計にはいくつかの提案がされており、**sidechain**や**drivechain**、**マルチシグカストディ、およびハイブリッド版**などがある。

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

双方向ペグの概要 （2/4）

- 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。

- 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**を行うもの。
  - 公証認定を複数の国・場所に分散することにより単一カストディモデルより分散されるものの、なおも**コントロールの集中性が残る**。

- サイドチェーンによる双方向ペグ
  - **サードパーティーの関与を減らす**ため、**コンセンサスによるバリデーション**を行う。
  - 各ブロックチェーンが相手のコンセンサスシステムを理解し、相手方のブロックチェーンにおいて**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。
  - 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**（ビットコインブロックチェーン側で、**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**）や、オペコード追加にソフトフォークが必要となる点がある。

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

双方向ペグの概要 （3/4）

- **Entangledブロックチェーン**による双方向ペグ
  - **双方のブロックチェーンをもつれさせる**ことによって決済ファイナリティの無さを補完するもの。
  - 第一チェーン中の**トランザクションロックの取消**に伴って第二チェーンの**トランザクションロックを取消**。
  - ブロックチェーンをもつれさせる方法としては、例えば**第二チェーンのトランザクションを第一チェーンのトランザクション内に埋め込むものがある**（例: CounterpartyにおけるOP_RETURNペイロード）。
  - 或いは、第二チェーンのブロックを第一チェーンのトランザクション内の**コミットメントによってアンカリング**するもの。
  - 前者の方法の場合は第二チェーンにSPV-Proofを検証させる。
  - 残る問題としては、第二チェーンのトランザクションを埋め込むときに**第二チェーンのユーザー全員が双方のチェーンのトランザクションを検証する必要**がある。

- **Drivechain**による双方向ペグ
  - 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。
  - マイナーがビットコインブロックチェーンを用いて投票を行い、正直なマイナーが多く参加するほどに安全なものになる仕組み。

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

双方向ペグの概要 （4/4）

- **ハイブリッドモデル**による双方向ペグ
  - ここまで挙げたモデルは対称的なものであり、相手方チェーンのコインのロック解除に使われた方法はビットコインのロック解除にも使われる。
  - だが第一チェーンと第二チェーンは本質的に異なるものであり、第一チェーンは新たにネイティブトークンを発行するが第二チェーンはそうでは無い。
  - ハイブリッドモデルでは、**それぞれのチェーンでロック解除に異なる方法を用いて双方向ペグ**を行うものであり、例えば第一チェーンでdrivechainを用いて第二チェーンでサイドチェーンを用いるなど。

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

DRIVECHAINの概要

- 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**。
  - Proof of Burnではメインチェーンからサイドチェーンへビットコインを送ることは出来るが、サイドチェーンからメインチェーンへビットコインを戻すことができないため、双方向のやりとり可能なサイドチェーンが必要。
  - 双方向ペグを行うにあたり、**Liquidサイドチェーン**は**マルチシグで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モデルであり、P2Pでなく**監査人が結託するリスク**がある（**監査人を信頼する必要**もある）ため、**drivechainでは監査人のFederationに依らずにSPV-Proofにマイナー投票を導入するモデル**。
- drivechainでは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。
  - メインチェーンへ戻すときに、サイドチェーンから送られてくるどのメッセージが正しいかメイン側で判断。
  - サイドチェーンのブロックヘッダに記録されたトランザクションIDがメインチェーンのCoinbaseトランザクションに記録されたものと一致するかを確認し、マイナーの投票（Coinbaseコミットメント）で**51%以上の賛成が得られると当該トランザクションIDを有効としてメインチェーンへ記録**。
  - マイナーが**メインチェーンとサイドチェーンで同時にマイニングを行うMerged Mining**にあたり、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るべく、Blind Merged Mining（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インセンティブとする）を開発中。

→ 出典：https://zoom-blc.com/drivechain
→ 出典：https://zoom-blc.com/sidechain

トラストレスなサイドチェーン実現に必要なコンパクト証明を提供するNIPoPoW（PoWの非対話証明） 1/2

- 中央集中のFederatedではなく、**トラストレスなサイドチェーン**の実現に向けた証明ソリューション。
- トラストレスなサイドチェーンはシンプルではあるが、**SPV証明に依存し、実現が難しい**とされる。
  - コインをサイドチェーンへ送り、再びビットコインのメインチェーンへ戻すために、**資金を持っていることを示す証明を添付することが必要**。
  - 証明が無いと、コインをビットコインのメインチェーンへ戻すときに実態以上のコインを受け取れる。
  - 但し、証明をビットコインに組み込む上では、盗難を回避できることに加えて、ネットワークを送信できるだけ小さいことが必要。
  - コンパクトSPV証明が提案されたことがあるが、攻撃に弱くサイドチェーン上でコインを盗まれる危険があった。
- NIPoPoWは、PoWベースの既存暗号通貨へ適用可能な証明であり、攻撃への耐性を有することに加えて、線形的に成長するチェーン全体を検証する必要のある従来型ブロックチェーンクライアントと異なり、NIPoPoWベースのクライアントはブロックチェーン長に対して**対数的なリソース消費で済むだけを検証する**点がポイント。
  - 効率的なトランザクション検証のためのSPVクライアントを構築するほか、効率的にサイドチェーン証明を構築するという、二つの問題を解決する。

→ 出典：https://eprint.iacr.org/2017/963.pdf
→ 出典：https://www.coindesk.com/sidechains-breakthrough-almost-everyone-bitcoin-missed/

トラストレスなサイドチェーン実現に必要なコンパクト証明を提供するNIPoPoW（PoWの非対話証明） 2/2

- 多くのアルトコインが登場してビットコインのドミナンスが低下する中で、効率的なマルチブロックチェーンクライアントが求められている。
- また、論理トランザクションが複数のブロックチェーンへ伝播するクロスチェーンアプリケーション開発にも有効。
  - 今日でもビットコインとetherのトレードといったシンプルなクロスチェーントランザクションは可能だが、さらに進めて、或る暗号通貨のブロックチェーンに別の暗号通貨のクライアントを埋込むことを可能に。
  - このコンセプトは当初、難しいアップグレードプロセスを回避するために考えられたサイドチェーンであり、実験的オペコードのような新機能を持つ新しいブロックチェーンを、オリジナル側となるビットコインのデポジットで裏付けるもの。
  - アップグレードや実験の仕組みとしてサイドチェーンを使うことはビットコインのエコシステムでスケーラビリティを実現するために歓迎された。
  - また、サイドチェーンはビットコインネットワークの負荷をオフロードするための仕組み（コインをサイドチェーンへ移してその後に再び戻す）として使うことも出来る。
- このように、NIPoPoWのソリューションにより、相互運用性とスケーラビリティという、次世代のブロックチェーンに求められる重要要素に貢献が見込まれる。

→ 出典：https://eprint.iacr.org/2017/963.pdf
→ 出典：https://www.coindesk.com/sidechains-breakthrough-almost-everyone-bitcoin-missed/

- ビットコイン技術トピックの解説
  - 技術トレンド全体像
  - ブロック伝播に関するもの
  - Lightning Network／アトミックスワップ／ペイメントチャネルに関するもの
  - プライバシーに関するもの
  - 双方向ペグ／サイドチェーンに関するもの
  - 署名／証明／スクリプトに関するもの
    - MAST - Merklized Abstract Syntax Tree
    - 範囲証明サイズを小さくおさめるBulletproof
    - シュノア署名ベースのマルチシグによるスケーラビリティ・プライバシー向上の提案
  - コンセンサスルール変更

MAST – Merklized Abstract Syntax Tree

- ビットコインスクリプトの抱える課題
  - ビットコインプロトコルではスクリプトがTrueを返さないとコインを使えず、秘密鍵による署名を求めるといった制約を課していて、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ため、**スクリプトの未使用部分を含める必要性を無くそう**と言うもの。
- MASTの提供するソリューション
  - 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である**「抽象構文木（AST）」**と、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とするのに使われている**「マークル木」**の組み合わせ。
  - **抽象構文木（AST）でスクリプトをパーツに分割**し、**マークル木を用いてスクリプト全体無しに、それに属する個別パーツであることを検証可能**とすることにより、**使わないスクリプトをリプレイス**する。
  - 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解した上で、それらをもとにマークル木を作り、このマークルルートが制約事項を一意に識別する。
- MASTがもたらす価値
  - **制約事項を抽象構文木（AST）で分割**して出来た子スクリプトがそれぞれTrueを返して**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やプライバシー向上**や大きなコントラクトを可能とできるのがポイント。

→ 出典：https://bitcointechtalk.com/what-is-a-bitcoin-merklized-abstract-syntax-tree-mast-33fdf2da5e2f

範囲証明サイズを小さくおさめるBULLETPROOF（1/2）

- **コミットされた値がある範囲内にあると示す範囲証明**を効率的に可能。
  - 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**）。

- Confidential Transactionで使われる範囲証明（nに比例）サイズを大きく改善。
  - 範囲証明のサイズはnに線形なので、範囲証明のサイズがConfidential Transactionの大部分を占めている（二つのアウトプットを持つConfidential Transactionのサイズは5.5KBだがこのうち5.3KBを範囲証明が占める）。
  - 証明の生成・検証時間はビット長nに比例するため、処理時間短縮に寄与。

- 範囲証明の集約もサポート。
  - 複数参加者によるConfidential Transactionを単体の小さな証明にまとめる証明集約が可能。

→ 出典：https://eprint.iacr.org/2017/1066.pdf
→ 出典：https://joinmarket.me/blog/blog/bulletpoints-on-bulletproofs/

範囲証明サイズを小さくおさめるBULLETPROOF (2/2)

- Confidential Transactionの場合
  - 金額へのコミットメントを使うことによって衆人環視から隠蔽。
  - 各CTの有効性についてゼロ知識証明を含めることによって、トランザクションインプット合計値がアウトプット合計値より大きいことをチェックできるようにしている。
  - 但し、正しくセットアップされたことを皆がトラストすることが必要（trusted setup）。

- Bulletproofの場合
  - 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**。
  - そこで**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**する。
  - 秘密のコミットされた値を持つ複数参加者が、小さなサイズの範囲証明を生成するMPCプロトコル（複数参加者計算）を提供する。
  - Confidential Transactionはトランザクション中のインプット額・アウトプット額をPedersen Commitment内に隠蔽。
  - Confidential Transactionで値を検証可能とするため、各トランザクションにゼロ知識証明を含める。
  - Confidential Transaction中のゼロ知識証明では、コミットされたインプット合計がアウトプット合計より大きく、且つアウトプット全てが範囲内にあることを証明。

→ 出典: https://eprint.iacr.org/2017/1066.pdf
→ 出典: https://joinmarket.me/blog/blog/bulletpoints-on-bulletproofs/

シュノア署名ベースのマルチシグによるスケーラビリティ・プライバシー向上の提案

- 既存の**Bellare-Nevenマルチシグが3ラウンドのコミュニケーション**であるのに対して**2ラウンドで済む効率性（予備的コミットメントフェーズを無くす）**、且つシュノア署名と同じ鍵・署名長が特徴。

- また、署名者たちの個々の公開鍵から算出される集約公開鍵に対応する**結合署名で検証する「鍵集約（キーアグリゲーション）」**ができる点がポイント。

- n-of-nタイプのマルチシグにおいて皆が**個々の公開鍵を明かすことなしに、秘密裏に集約鍵を計算**して、オリジナルの鍵として公開する。

- このマルチシグにより、ビットコインの**パフォーマンス（コンパクト）およびユーザープライバシーの改善**に資すると述べられている。

→ 出典：https://eprint.iacr.org/2018/068.pdf

- ビットコイン技術トピックの解説
  - 技術トレンド全体像
  - ブロック伝播に関するもの
  - Lightning Network／アトミックスワップ／ペイメントチャネルに関するもの
  - プライバシーに関するもの
  - 双方向ペグ／サイドチェーンに関するもの
  - 署名／証明／スクリプトに関するもの
  - コンセンサスルール変更
    - ビットコインにおける19回のコンセンサスルール変更の系譜

ビットコインにおける19回のコンセンサスルール変更の系譜 （1/3）

- チェーン分岐とは、共通の祖先を持つ二つの別のチェーンへと分岐したものであり、ソフトフォークとハードフォークとそれ以外に拠る。
- **ハードフォークは、ブロック有効性に関するコンセンサスルールの「緩和」**であり、従来の 無効とされたブロックを有効とみなす等。新しいHFチェーンをフォローするため既存ノードは**アップグレードが必要**。
- **ソフトフォークは、ブロック有効性に関するコンセンサスルールの「厳格化」**であり、従来有効とされたブロックを無効とみなす等。新しいSFチェーンをフォローするため既存ノードは必ずしも**アップグレードする必要は無い**。
- これらの用語は2012/4に生まれ、BIP98およびBIP123で正式化された。
- 次ページに、ビットコインコンセンサスフォークのリストを示す。

→ 出典：https://blog.bitmex.com/bitcoins-consensus-forks/

ビットコインにおける19回のコンセンサスルール変更の系譜 （2/3）

時期	Ver/BIP	概要
2010/07/28	バージョン0.3.5	OP_RETURN無効化。誰もがビットコインを使えるバグフィックス。SF。
2010/07/31	バージョン0.3.6	OP_VERおよびOP_VERIFの無効化（SF）。OP_NOP追加（HF）。
2010/08/01	バージョン0.3.7	scriptSigおよびscriptPubKeyの評価。
2010/08/15	バージョン0.3.10	アウトプットバリューオーバーフローのバグフィックス（SF）およびOP_CAT無効化（SF）。
2010/09/12	—	1MBブロックサイズ制限追加（SF）。 MAX_BLOCK_SIZE=1000000のコミットは2010/07/19の0.3.2 rc1にてリリースされた。 1MBルール適用のコミットは2010/09/07にて。 この後2010/09/20にSatoshiがこのアクティベーションロジックを削除したが1MB制限は残った。
2012/03/15	BIP30	同一txidを持つトランザクションは古いものが消費されてない限り無効とする（SF）。
2012/04/01	BIP16	P2SH。PublicKeyHashの代わりにScriptHashへ送付するトランザクションを可能にする（SF）。

→ 出典：https://blog.bitmex.com/bitcoins-consensus-forks/

ビットコインにおける19回のコンセンサスルール変更の系譜 （3/3）

時期	Ver/BIP	概要
2013/03/24	BIP34	Coinbaseトランザクションにブロック高を含めることを必要にする（SF）。
2013/03/11	バージョン0.8.0	Berkeley DBからLevel DBへの移行（HF）
2013/03/18	バージョン0.8.1	一時的SF
2013/05/15 2013/08/16	BIP50	10000BDBロックリミットルールに違反するブロック生成。
2015/07/04	BIP66	厳格なDER署名（SF）。
2015/12/14	BIP65	CLTV（CheckLockTimeVerify）で特定時刻までロック可能に。ビットコインで初めての新しい関数（SF）。
2016/07/04	BIP68、BIP112、BIP113	相対ロックタイム導入（SF）。
2016/07/23	BIP91	SegWitアップグレードに向けたシグナリングを行う一時的SF。
2017/08/01	BIP148	SegWitアップグレードに向けたシグナリングを行う一時的SF
2017/08/24	BIP141、143、BIP147	SegWitアップグレード（SF）。

→ 出典：https://blog.bitmex.com/bitcoins-consensus-forks/

- Scaling Bitcoin2017のトピック概観

SCALING BITCOIN2017のトピック概観(1/12)

- Ethereum Devcon3とScaling Bitcoin2017
  - 11月の第1週、EthereumとBitcoinという、代表的な暗号通貨・ブロックチェーンにおける国際会議が開催された。
  - 前者が11/1-4、後者が11/4-5と日程が一部重複したものの、今後の暗号通貨・ブロックチェーンの動向を見定める上で重要なトピックが集中的に発表される機会であったので、ここに全体のトピックについて整理する。
  - 全体的な基調として、**Devconは商業利用中心であり内容もプラットフォームから開発ツール、個別プロダクトの紹介まで**というものだったのに対して、**Scalingはアカデミックな基調であり、内容は論文の紹介が中心**であり、二者の雰囲気は大きく異なるものだったといえる。

- Scaling Bitcoin2017全体の所感
  - 昨年のMilanが正にフンジビリティ一色といっても過言でないほど、TumbleBitやWimblemimble等で席捲したのに対して、**スケーリングテーマ等の幅広いテーマが扱われたことが、2017年のScaling Bitcoinの特徴**といえる。
  - 主要スポンサー、登壇者にBlockstream関係者が出身者を含め見られなかったことも、雰囲気を昨年と大きく違うものにしている。
  - 登壇者のみならず、オーガナイザーにもBlockstream関係メンバーが見られず、昨年までのさながらBlockstream主催イベントという空気感がなかった他、参加者にもごくわずかのBlockstream社員が見られる程度であった様子。

SCALING BITCOIN2017のトピック概観(2/12)

- テーマの概観
  - **スケーリング**に関するテーマとして、**FlyClient（SPVを拡張した超軽量クライアント）**や**Graphene（ブロック伝播をCompactBlockの10%に削減）**、**Bobtail（ブロック生成時間のバラつき縮小）**、**Microchain（スマホによるフルノード）**、**BlockDAG（DAG構造）**。この他、**ギガブロックによるテストネットの実験結果**が発表された。
  - **プライバシーやフンジビリティ**に関するテーマとしては、**Bolt（プライベートなペイメントチャネル）**、**ValueShuffle（CoinJoin＋Confidential Transaction）**、**DLC（ブロックチェーンへパブリッシュされないインチャネルコントラクト）**。
  - **クロスチェーンアトミックスワップトレード（XCAT）**に関する発表として、Rogerとの賭けを題材とした**エスクローに拠らないXCAT**、**アダプタ署名によるXCAT**の２つが発表されたことは、今年ならではの特徴。
  - 上記のほか、ユニークなテーマとして、**短波ラジオを使ったビットコイントランザクションブロードキャスト**について、Nick Szaboから発表された。

SCALING BITCOIN2017のトピック概観(3/12)

- スケーリングに関するテーマを概観する。
  - スケーリングに関するテーマとして、FlyClient（SPVを拡張した超軽量クライアント）やGraphene（ブロック伝播をCompactBlockの10%に削減）、Bobtail（ブロック生成時間のバラつき縮小）、Microchain（スマホによるフルノード）、BlockDAG（DAG構造）。
  - この他、ギガブロックによるテストネットの実験結果が発表された。これらの背景と概要をみてみる。

  - 150GBあるブロックチェーンをモバイルクライアントで検証することは現実的でないことから、トランザクションのハッシュツリーをマークルツリーとして保有しているブロックヘッダのみを検証している。
  - これらが、**SPV（simple payment verification）クライアントだが、その場合も全ブロックヘッダ**分として、2GBが必要。そこで、そこで、全ブロックヘッダを必要とせず、**SPVクライアントをMerkle Mountain Rangeで拡張する超軽量クライアントを考えたのが、FlyClient**である。
  - Merkle Mountain Rangesは、マークルツリーの考え方を更に拡張し、各クライアントがチェーンのヘッダを格納するだけでよくすることによって、ブロックがチェーンの一部であると示すマークルプルーフのみを使って「あるトランザクションが含まれること」を証明するもの。
  - さらに、**証明者と検証者のやりとりを必要としない**、**非対話型PoW（non-interactive proofs of PoW ： NiPoPoW）**を用いている。

SCALING BITCOIN2017のトピック概観（4/12）

- スケーリングに関するテーマを概観する。（続き）
  - P2Pネットワークにおけるブロック情報の伝播プロセスにおいて、**ブロックサイズが小さいほど早く伝播することができる他、チェーンの分岐に伴うOrphanの発生を抑止**することができる。
  - そこで、**より高速なブロック伝播を行う**ことを目指したのが、**Graphene**である。
  - **BloomフィルタとIBLTを併用**することによって、従来比で10分の１で伝播を行うことができるようにしている。

  - **ブロック生成間隔にはバラつき**があり、80%のブロックが１分～24分を要しているが、こうしたバラつきが**ダブルスペンドやセルフィッシュマイニングの要因**となっている。
  - そこで、**生成間隔のバラつきを低減**させようというのが、**Bobtail**である。

  - スケーラビリティ向上策としては、レイヤー２技術の他、レイヤー１ではブロックサイズ拡大に焦点があたっているが、**スマホでフルノードを実行させることを可能とする**ことで、スケーラビリティ向上を目指すのが、**Microchain**である。
  - Microchainでは、少数の大きなチェーンを持つのではなく、多数の小さなチェーンを持つようにしている。

SCALING BITCOIN2017のトピック概観（5/12）

- スケーリングに関するテーマを概観する。（続き）
  - トランザクションの格納をチェーン状の**ブロック構造とするのではなく、有向非巡回グラフ（Directed Acyclic Grapgh）型の「もつれ」状のブロック構造**とするのが、**BlockDAG**である。**単一チェーンではなく全グラフ情報を保持**するため、**安全性やスケーリングでメリット**がある可能性がある一方、フォーク発生は日常的なものとして認める、一つのパラダイムシフトとして捉えられている。
  - マイナーは同じTXを選択することを避けるようにインセンティブが働くため、BlockDAGプロトコルを実装する上では、インセンティブが重要となる。

  - 今後のトランザクション増加を展望した際、40億人が1日1回決済すると仮定すると、5万TPSを処理することが必要とされる。
  - そこで、通常サイズの1MBの1000倍にあたる1GBのブロックを処理できるテスト環境で、2000TPSのペースでトランザクションを発生させた実験結果が発表された。
  - 100TPSでMempoolがボトルネックとなった他、その後は500TPSでブロック伝播時間がボトルネックになったため、スケーリングに向けては、Mempool改善のほか、Xtreme Thinblockのようなブロック伝播の改善が必要となる。

SCALING BITCOIN2017のトピック概観(6/12)

- このうち、ブロック伝播を改善する「Graphene」について詳しくみてみる。
  - オンチェーンスケーリングの方法としては、ブロックサイズを大きくするものがある。
  - 代替案として、ブロックチェーン上方の圧縮を行うものがある。
  - これは、ブロック自体は大きくとも、構築に必要なリソースを少なくて済ますものである。

  - Grapheneは、ブロック伝播を10%に削減するものであり、Bitcoin Unlimitedによって提案されているXtreme Thinblocksに基づいている。
  - 17.5KBのXtreme Thinblockを、Compact Blockにより10KBにエンコードでき、Grapheneを使うことで更に2.6KBへエンコードすることが可能。

  - まず、Xtreme Thinblockについてみる。
  - Xtreme Thinblockは、BUIP010としてBitcoin Unlimited向けに提案されていたもの。BitcoinノードはUnconfirmトランザクションのリストをメモリ中に保持する。新しいブロックがマイニングされると、そのトランザクションがノード間をリレーされる。ビットコインネットワークのスケーリングのためには、高速で帯域を消費しない方法が必要。
  - Thin Blockはトランザクションを再度送付することを避けるための技術。ブロックの再生成にあたり、それを全てダウンロードするのではなく、リクエスト者のメモリプール中に存在するトランザクションを使うことによって、ブロックリレーをスピードアップすべく設計されたものである。
  - 今回扱うXtreme Thinblockでは、通常のThinblockとは異なり、Bloomフィルタを用いて伝達サイズを削減する。

SCALING BITCOIN2017のトピック概観(7/12)

- このうち、ブロック伝播を改善する「Graphene」について詳しくみてみる。
  - 次に、Bloomフィルタについてみてみる。
  - これは、ある要素が集合に含まれているかどうかを判定するために使われ、非常に早く動作し空間効率の良い確率的データ構造である。
  - 「確率的」というのは、含まれないものを含まれるとしてしまう偽陽性の誤検出はありえるが、含まれるものを含まれないとしてしまう偽陰性の誤検出は無い、という意味をいう。
  - このBloomフィルタによって、SPVウォレットは、自分のアドレスに関連するトランザクションデータのみを部分的にダウンロードすることが可能になった。

  - ・Grapheneは、このBloomフィルタとIBLTを組み合わせ、トランザクションを正確にマッピングすることによって、１つのIPパケットにフィットさせている。

SCALING BITCOIN2017のトピック概観（8/12）

- このうち、ブロック伝播を改善する「Graphene」について詳しくみてみる。
  - 最後に、IBLT（可逆的なBloom探索テーブル）について見てみる。
  - IBLTは、セットリコンサイルデータ構造であり、プールを用いてネットワーク上のオーバヘッドを軽減するものである。
  - ブロック中の全てのトランザクションが高い確率で既にネットワークへ伝播されているとしたら、ブロックの全トランザクションを送る必要はない、という考えに基づく。
  - IBLTを用いると、データセットをリコンサイルすることができて、ブロック内の全トランザクションを送付するかわりに各ピアはそれらトランザクションデータをより小さなIBLTへ圧縮する。

  - このように、Grapheneでは、BloomフィルタとIBLT、両者を組み合わせることによって、トランザクションIDのリストを送付することなしに、小さなBloomフィルタおよびIBLTを、Compact BlocksやXtreme Thinblocksといった従来のブロック伝播プロトコルの10%のサイズで運ぶことが可能としている。

SCALING BITCOIN2017のトピック概観（9/12）

- 次に、プライバシー・フンジビリティに関するテーマを概観する。
  - プライバシーやフンジビリティに関するテーマとしては、Bolt（プライベートなペイメントチャネル）、ValueShuffle（CoinJoin＋Confidential Transaction）、DLC（ブロックチェーンへパブリッシュされないインチャネルコントラクト）が発表された。
  - これらの背景と概要をみてみる。

  - ビットコインはアドレスリンクされる可能性があるため、**フレッシュアドレスの混合リストを用いるCoinJoin**や、**P2PミキシングプロトコルDiceMix**などが開発されてきた。
  - **ミキシング以外のプライバシー提供手段**としては、**Confidential Transaction**や、**ステルスアドレス**、**署名アグリゲーション（署名集約）**がある。
  - **ValueShuffle**は、**Confidential TransactionをCoinJoinに応用**しようというもの。

  - ペイメントチャネルは、デポジットを少額償却して最後に精算する、二者間の少額支払経路であるが、同じチャネルにおける支払いはリンク可能のため、送金者を特定される可能性がある。そこで、**プライベートなペイメントチャネルを考えるのがBolt**である（※LightningNetworkの共通仕様とは関係ない）。
  - **TumbleBitではハブが裏切ると送信者が特定**される他、同様に**LightningNetworkでもチャネル上の全参加者が裏切ると送信者を特定**されるのに対して、このBoltでは完全プライベートを実現できるとしている。

SCALING BITCOIN2017のトピック概観（10/12）

- 次に、プライバシー・フンジビリティに関するテーマを概観する。（続き）
  - **ペイメントチャネルを使った送金**において、**コンカレンシーとプライバシーの間にはトレードオフ**があるため、それぞれに対応するプロトコルが必要となる。
  - **Fulgor**は**コンカレンシーを捨てプライバシーを実現**するものであり、条件付ペイメントであるマルチホップHTLC （Hash Time Lock Contracts）を、非対話ゼロ知識（NIZK）と呼ばれるブロックと併用することでプライバシーを担保する。
  - 一方、**Rayo**は、グローバルなトランザクション識別子を導入することで、**トランザクションのデッドロックを回避**し、**少なくとも１つのペイメントを終結**させることによって、**コンカレンシーを解決**。

  - 2-of-2マルチシグの場合、当事者間のコンフリクト発生時にデポジットがデッドロックしてしまうため、調停者を交えた2-of-3マルチシグが好ましいとされるが、この**調停者（オラクル）に権力集中して贈収賄の発生リスク**がある。
  - そのため、**オラクルはコントラクトの内容を知らないほうが好ましい**とされる。
  - **Discreet Log Contract**は、**シュノア署名を用いたスマートコントラクト**を使い、**オラクルの不正を解決**するもの。
  - オラクルの署名が秘密鍵の一部になるものの、オラクルはコントラクトを参照できず、どの秘密鍵の一部になるかを分からないように出来る。

SCALING BITCOIN2017のトピック概観（11/12）

- また、クロスチェーンアトミックスワップトレード（XCAT）に関する発表について、背景と概要をみてみる。

  - **オンチェーンにおけるスマートコントラクト**は、スクリプト言語を用いて記述され、全ノードによってダウンロードされ構文解析されるため、**スクリプトの詳細は可視化され、プライバシーは損なわれる。**
  - **スマートコントラクトの実行によってのみ有効なデジタル署名を生成**できるのが、**スクリプトレススクリプト**である。
  - アトミックスワップの実装を、**アダプタ署名を用いたスクリプトレススクリプト**として考えることができる。
  - **アダプタ署名**とは、異なる楕円曲線を採用するチェーン間で横断して機能するものであり、プロトコルをマスキングして通常のマルチシグのようにみえる他、**リンク不可能かつ否認可能**である点が特徴。

  - ハードフォーク実施に先立つRogerとの賭けを題材としたエスクローに拠らないXCATを実装する上で、トランザクション展性がある場合、双方がアトミックトレードに署名する前はブロックチェーン上へデポジットすべきでないため、複雑な実装となる。

SCALING BITCOIN2017のトピック概観（12/12）

- 最後に、短波ラジオを使ったビットコイントランザクションブロードキャストについて、背景と概要をみてみる。

  - 2017年4月、スイスETH Zurichによってインターネット BGP基盤の脆弱性に関する問題点が提起された。
  - ISPがBGPを使ってビットコイントラフィックの乗っ取りを行うことが可能とするもの。
  - このように、**インターネットのみにトラフィックを依存することは、検閲耐性の観点からも、ビットコインの安定的存続にとってリスク**となる。
  - 同様の文脈から、人工衛星を用いてブロードキャストを行うBlockstream Satelliteが本年8月に発表された。
  - 今回発表されたのは、**大気のさらに上層に存在する電離層（無線電波を反射）を用いて、インターネットを迂回したブロードキャスト**を行うもの。

- その他のトピックニュース

その他のトピックニュース

- ビットコイン、誕生9年目を迎える
  - https://www.reddit.com/r/Bitcoin/comments/7nt9fc/9_years_ago_block_0_was_mined_happy_birthday/
  - https://blockchair.com/bitcoin/block/0
  - https://blockchain.info/block-index/14849/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
- The Baltic Honeybadger、ラトビアのリガで開催
  - https://bh2017.hodlhodl.com/
  - https://youtu.be/DHc81OL_hk4

その他のトピックニュース

- NiceHash、ビットコインウォレットのハッキングで7800万ドル被害
  - https://ethereum-japan.net/news/bitcoin-was-stolen-from-nicehash/
- 独Envion、再生可能エネルギーを用いたマイニングユニットを開発
  - https://medium.com/@envion/the-worlds-most-cost-efficient-self-expanding-mining-infrastructure-9f8add8b6159
  - http://techon.nikkeibp.co.jp/atcl/news/16/112409952/
- ビットコイン開発者によるマイニングハードウェアDragonmint開発
  - https://bitcoinmagazine.com/articles/bitcoin-developer-about-take-mining-hardware-industry/
  - https://halongmining.com/shop/

その他のトピックニュース

- Intel、ウォレットソフトウェアへのSGX技術統合にむけLedgerと提携
  - https://www.coindesk.com/intel-ledger-partner-cryptocurrency-storage-integration/
- 主要ブラウザで初めて仮想通貨マイニングスクリプトをブロックする機能を内蔵した「Opera 50 Beta RC」ベータ版をリリース
  - https://japan.cnet.com/article/35112437/
- Steve Wozniak氏、ビットコインをゴールド以上のものと評価
  - https://bitcoinmagazine.com/articles/money2020-wozniak-thinks-bitcoin-better-gold/
- Peter Thiel氏、人々はビットコインを過小評価していると発言
  - https://www.cnbc.com/2017/10/26/bitcoin-underestimated-peter-thiel-says.html

2. Ethereumエコシステムの動向

- Devcon3の全体トピック概観
- Ethereumの次世代ロードマップ
- Ethereumエコシステムにおける主なニュース
- Ethereum技術トピックの解説

- Devcon3の全体トピック概観

DEVCON3の全体トピック概観（1/4）

- 新しいムーブメント
  - 新しいアセットクラス（実行可能な金融商品）
  - 新しいシステムクラス（トラスト不要）
  - 新しい社会組織（暗号ベースのトラストやパートナーシップ）
  - こうした新しいグローバルムーブメントを支えるのがブロックチェーン
  - そのためのエコシステムが成長しつつあるのがみて取れた

- 新しいムーブメントを支える「クリプトエコノミクス」
  - 暗号通貨の開発により、暗号学（暗号化、ハッシュ、署名）および経済学（ゲーム理論、トークンエコノミー、投票、権利配布）を活用した「プログラム可能なマネー」を手にした
  - マネーをプログラム可能であれば、インセンティブもプログラム可能
  - さらには、インセンティブをプログラム可能。であれば、それによる人々の行動もプログラム可能
  - クリプトエコノミクスによって、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ことができる。
  - 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を設計することが必要

DEVCON3の全体トピック概観 (2/4)

- 現在ブロックチェーンやスマートコントラクトが抱える技術的な課題
  - ブロックチェーンのトリレンマ（分散化、スケーラビリティ、セキュリティ）
  - スマートコントラクトの課題は、スケーラビリティ（分散化に影響を与えずにトランザクションを多く処理したい）、プライバシー（機密データを安全に取り扱いたい）、コレクトネス（スマートコントラクトを如何に考えたとおり動かすか）
  - スケーラビリティ向上にむけては、BitcoinNGのようなオンチェーンによる対処の他に、Lightning NetworkやRaiden、或いはTeechanやTeechainのようなオフチェーンによる対処が考えられている

DEVCON3の全体トピック概観 (3/4)

- Ethereumの全体アーキテクチャに関するトピック
  - Byzantiumハードフォークは、Ethereumにとり最大のアップグレードであったが、10/16にスムーズに行われ、リング署名やZK-SNARKsといった強力なプライバシー機能が実装された
  - 現在Vitalikは、チーフサイエンティストとして、他15人のリサーチャーと共に、PoS・スケーラビリティソリューション・Sharding・プライバシーソリューションに従事
  - Shardingは、ブロックチェーンステートを複数のユニバースに分割するもの。Ethereum2.0構想では「1ブロックチェーン2システム」を掲げて、メインシャード（安全重視で保守的な運営）および他のユニバースから成るシャード（実験的取組を素早く実装）の２層構造
  - Casperは、デポジットベースでBFTスタイルのPoS。バリデータがEtherをデポジットして、ファイナライズしたと考えるブロックへ投票。ルール違反のバリデータはペナルティとしてデポジットを没収。ただし開発にはなお時間がかかる見込みで、実装時期は明示されなかった
  - Prasmaは、ブロックチェーンを複数階層のツリー構造をとるもの。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。
  - μRAIDENは、オフチェーンのペイメントチャネルネットワーク
  - eWASMは、Webブラウザ上でEthereumを動かすもの
  - ステートレスクライアントは、クライアントのネットワーク同期を効率化して早めるもの

DEVCON3の全体トピック概観（4/4）

- 個別のスケーラビリティソリューション
  - Thunderellaは、ランダムに参加者から選ばれたグループがコンセンサス責任を負うもの。コンセンサス参加者を減らして且つコーディネーターを置くことでスピードを向上させる
  - TrueBitは、Ethereumネットワークの計算に係るオフチェーンプロセシングを通じてスケーラビリティを向上させるもの。オフチェーンでの計算結果について合意をとることによって、実行をわずかな数のノードのみで済ませる。
  - CITAは、Ethereumクライアントをマイクロサービスのセットとして分割し、これを並列同期実行させることによってスケーラビリティを高める。

- 個別プロダクト
  - Cryptoletは、Microsoftが提案しているエンタープライズスマートコントラクトとしてAzure上で動くフレームワーク
  - Quorumは、パーミッション付きネットワーク向けにエンタープライズ機能としてプライバシーおよび100TPS相当のパフォーマンスを付加した、Gethの軽量フォーク
  - Sikorkaは、スマートコントラクトをセンサーに埋め込みProof of Presenceを提供するもの
  - CreDBは、安全なハードウェア上（コードやデータをEnclaveするセキュアなプロセッサ）に実装される新しいデータベース
  - TownCrierは、スマートコントラクトのコレクトレスを高めるためのOracle

- Ethereumの次世代ロードマップ

ETHEREUMの次世代ロードマップ （1/8）

- 11月25日のBeyond Block TaipeiでVitalikがEthereumプラットフォームの3-5年計画を発表した。
  - Ethereumの次世代バージョンとしてのEthereum 2.0プラン。
  - Devcon3でもこのトピックについて触れられたが、今回は新たな詳細についても明らかにされた。

- 急速な成長の中で、Ethereumは、プライバシー、コンセンサス安全性・スマートコントラクト安全性、スケーラビリティが大きな問題になっている。

- プライバシーについての問題
  - 最近のByzantiumハードフォークでzk-SNARKsやリング署名がサポートされ、トランザクションを隠蔽しながらも誰にトランザクションを見せるかを選択できるようになった。
  - とはいえ、プライバシー問題を完全解決するものではない。

→ 出典: https://www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding
→ 出典: http://www.tomshardware.com/news/ethereum-roadmap-next-generation-sharding,35999.html
→ 出典: https://www.financemagnates.com/cryptocurrency/news/buterin-unveils-ethereum-2-0-roadmap-coin-nears-500/
→ 出典: http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding
→ 出典: https://bitcoinmagazine.com/articles/ethereum-killer-ethereum-20-vitalik-buterins-roadmap/#1511975683
→ 出典: https://btcnews.jp/f629wm8i13887/

ETHEREUMの次世代ロードマップ （2/8）

- コンセンサス安全性についての問題
  - PoWシステムにおけるマイニングの電力消費が課題であり、Ethereumは電力消費を必要としないPoSシステムへと緩やかに切り替えるCasperプロジェクトを開始している。
  - Casperは2018年夏までの準備を予定しているが、このリリースにより、EthereumはPoWから”PoWとPoSのハイブリッド”へと移行する。
  - そのスキームではPoWの仕組みは全て継続しながら追加でPoSの仕組みがアドオンされる。
  - こうしたコンセンサスメカニズムの変更は、Ethereumの将来的開発計画の前提条件となっている。

- スマートコントラクト安全性についての問題
  - コントラクト中にバグがあると多くの参加者にコスト負担を強いることになることから、形式的検証を導入したり、Pythonに似たスマートコントラクト開発言語であるViperを導入することによって、さらに安全なアプリケーション開発を可能としていく。

- 出典：https://www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding
- 出典：http://www.tomshardware.com/news/ethereum-roadmap-next-generation-sharding,35999.html
- 出典：https://www.financemagnates.com/cryptocurrency/news/buterin-unveils-ethereum-2-0-roadmap-coin-nears-500/
- 出典：http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding
- 出典：https://bitcoinmagazine.com/articles/ethereum-killer-ethereum-20-vitalik-buterins-roadmap/#1511975683
- 出典：https://btcnews.jp/f629wm8i13887/

ETHEREUMの次世代ロードマップ （3/8）

- Ethereumが直面する問題のうち、最も根本的な問題はスケーラビリティ。
  - 分散化・スケーラビリティ・セキュリティという、ブロックチェーンが具備すべき３つの重要特性を同時に解決するトリレンマが課題。
  - 例えば10GBのようなビッグブロックは分散性が犠牲になるが、Ethereumではそれらを犠牲にすることなく両立することを目指す。
  - TrueBitやGolemのような対話型検証ソリューションは重い計算を必要とするアプリケーションには向いているものの、大半はそうではない。
  - 他にもPlasma、Raidenのようなセカンドレイヤーソリューションがあるが、Ethereumはトリレンマの同時解決を全てオンチェーンで実現することを目指している。

- そこで次世代Ethereumでは、シャーディングと呼ばれる新しいアーキテクチャを利用するとしている。

→ 出典：https://www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding
→ 出典：http://www.tomshardware.com/news/ethereum-roadmap-next-generation-sharding,35999.html
→ 出典：https://www.financemagnates.com/cryptocurrency/news/buterin-unveils-ethereum-2-0-roadmap-coin-nears-500/
→ 出典：http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding
→ 出典：https://bitcoinmagazine.com/articles/ethereum-killer-ethereum-20-vitalik-buterins-roadmap/#1511975683
→ 出典：https://btcnews.jp/f629wm8i13887/

ETHEREUMの次世代ロードマップ （4/8）

- シャーディングの基本的な構造
  - ブロックチェーンネットワークをいくつかの小さなコンポーネントネットワーク（シャード）に分割し、トランザクション処理を並行実行可能とするもの。
  - VISAレベルの秒間数千トランザクションを、マスターノードといった中央集中的なやり方無しにオンチェーンで達成することを目指している。

- シャーディングを構成するユニバース
  - 多くのユニバースを作り、その間でデータやリソースの移送が可能。
  - 100の異なるユニバースがあれば、それぞれが異なるアカウントスペースとなる。
  - 各ユニバースにアカウントを持ったり、コントラクトを持ったり、トランザクションを送ることが可能。
  - 複数のパラレルユニバースを同じネットワーク上に存在させることが可能だが、各ユニバース内のトランザクションは当該ユニバース内部にのみ影響を与え、他ユニバースのネットワークスピードには影響しない。
  - 異なるユニバースと接続するプロトコルも提供させるものの、ユニバース内と異なり非同期であり、他ユニバースへのデータ移送は2週間かかるなどの制限を伴う。

→ 出典：https://www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding
→ 出典：http://www.tomshardware.com/news/ethereum-roadmap-next-generation-sharding,35999.html
→ 出典：https://www.financemagnates.com/cryptocurrency/news/buterin-unveils-ethereum-2-0-roadmap-coin-nears-500/
→ 出典：http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding
→ 出典：https://bitcoinmagazine.com/articles/ethereum-killer-ethereum-20-vitalik-buterins-roadmap/#1511975683
→ 出典：https://btcnews.jp/f629wm8i13887/

ETHEREUMの次世代ロードマップ （5/8）

- ユニバースの耐攻撃性
  - 各ユニバースは単なる分割ブロックチェーンではなく、相互接続可能なシステムとなる。
  - ユニバースはコンセンサスを共有するため、攻撃者が或るユニバースを乗っ取ろうとすれば、Ethereumネットワーク全体を乗っ取る必要がある。

- メインブロックチェーンに対する耐攻撃性
  - メインブロックチェーンを破壊することのないように、新たに後方非互換のプロトコルを導入することによって、新しいタイプのアドレスを生成する。
  - つまり、片方の世界では、現在のようにスケーラビリティが制限され各トランザクションがノードに複製されるオペレーションとなる一方で、他方の世界では、ノードは或るシャードのみ検証しながら、他シャード向けには軽量クライアントとして機能するようなオペレーションがなされるため、スケーラビリティ向上が可能となる。

- 出典: https://www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding
- 出典: http://www.tomshardware.com/news/ethereum-roadmap-next-generation-sharding,35999.html
- 出典: https://www.financemagnates.com/cryptocurrency/news/buterin-unveils-ethereum-2-0-roadmap-coin-nears-500/
- 出典: http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding
- 出典: https://bitcoinmagazine.com/articles/ethereum-killer-ethereum-20-vitalik-buterins-roadmap/#1511975683
- 出典: https://btcnews.jp/f629wm8i13887/

ETHEREUMの次世代ロードマップ （6/8）

- シャーディングの実装方法（短期）
  - 短期的にはValidator Manager Contract（VMC）がメインチェーンに配置され、PoSコンセンサスシステムを統括する構成をとる。
  - VMCは、各シャードのユニバースをトラッキングし、各シャードの次ブロック生成権利を持つバリデータをランダムアサインする。
  - ブロックバリデータは、必要量のETHをVMCへ提出し、ランダムに選択されるとトークンを拠出しこれを持ち分として、ブロック上のトランザクション有効性を検証する役割を果たす。
  - シャード上のトランザクションはCollationsとしてまとめ、Collationヘッダーが紐付けられる。
  - CollationヘッダーにはPoS署名が含まれ、VMCへプッシュされるが、シャード内の実トランザクションやシャードステートやCollationはオフチェーンであり、オンチェーンとなるのはCollationヘッダーのみに限られる。
  - メインチェーンにはCollationヘッダーが現れて、VMCはそれらをトラッキングすると共に各シャードのステートルートをトラッキングしながらも、実際のトランザクションやCollation自身はベースレイヤーの外に残るため、スケーラビリティが確保される。
  - このように、メインチェーン上のVMCによって仲裁されるPoWと言えるようなメカニズム。

→ 出典：https://www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding
→ 出典：http://www.tomshardware.com/news/ethereum-roadmap-next-generation-sharding,35999.html
→ 出典：https://www.financemagnates.com/cryptocurrency/news/buterin-unveils-ethereum-2-0-roadmap-coin-nears-500/
→ 出典：http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding
→ 出典：https://bitcoinmagazine.com/articles/ethereum-killer-ethereum-20-vitalik-buterins-roadmap/#1511975683
→ 出典：https://btcnews.jp/f629wm8i13887/

ETHEREUMの次世代ロードマップ （7/8）

- シャーディングの実装方法（中期）
  - しかし、こうした姿をとるのは初期段階のシャーディングであり、成熟するにつれて、双方向兌換性を備えるべくシステムを再編成して、シャードの位置づけがメインチェーンにおける論理的ポジションの性格を強めていく。
  - シャードがトランザクションの代わりにUncleになるイメージ。

- シャーディングの実装方法（長期）
  - さらにステージが進むと、Tight Couplingを通じてプロトコルレベルにシャーディングが組み込まれる。
  - その場合、あるブロックチェーンが無効なシャードヘッダーを含むとブロックチェーン全体が無効となるといった具合に、セカンドレイヤーの有効性がベースレイヤーの有効性の必要条件。
  - この結果、シャーディングシステム全体が、同一レベルのセキュリティを保持するようになる。

- 出典：https://www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding
- 出典：http://www.tomshardware.com/news/ethereum-roadmap-next-generation-sharding,35999.html
- 出典：https://www.financemagnates.com/cryptocurrency/news/buterin-unveils-ethereum-2-0-roadmap-coin-nears-500/
- 出典：http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding
- 出典：https://bitcoinmagazine.com/articles/ethereum-killer-ethereum-20-vitalik-buterins-roadmap/#1511975683
- 出典：https://btcnews.jp/f629wm8i13887/

ETHEREUMの次世代ロードマップ （8/8）

- Ethereum2.0からEthereum3.0へ
  - Ethereum2.0では、このようにシャーディングを通じてスケーラビリティおよびプライバシーを向上させることになっている。
  - その上で、Ethereum3.0では、さらにSTARKs、マルチレイヤーシャーディング、クロスシャードコミュニケーションを取り込んでいくとしている。

- 出典：https://www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding
- 出典：http://www.tomshardware.com/news/ethereum-roadmap-next-generation-sharding,35999.html
- 出典：https://www.financemagnates.com/cryptocurrency/news/buterin-unveils-ethereum-2-0-roadmap-coin-nears-500/
- 出典：http://www.trustnodes.com/2017/11/25/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding
- 出典：https://bitcoinmagazine.com/articles/ethereum-killer-ethereum-20-vitalik-buterins-roadmap/#1511975683
- 出典：https://btcnews.jp/f629wm8i13887/

- Ethereumエコシステムにおける主なニュース
  - 攻撃
  - スケーラビリティ
  - Vitalik
  - プロトコル
  - Stablecoin

- Ethereumエコシステムにおける主なニュース
  - 資産流出・資産ロック
    - Parity、マルチシグのハッキングで170億円相当の資産がロック
    - 分散取引所EtherDelta、DNSサーバへの攻撃で資産流出
  - スケーラビリティ
  - Vitalik
  - プロトコル
  - Stablecoin

PARITY、マルチシグのハッキングで170億円相当の資産がロック

- Parityの脆弱性によりPolcadotなどのICO資産170億円相当がロックされる
  - https://ethereum-japan.net/ethereum/another-hardfork-might-be-caused-by-parity/
  - http://individua1.net/vulnerability-in-the-parity-wallet-library-contract-of-the-standard-multi-sig-contract/
  - http://coffeetimes.hatenadiary.jp/entry/2017/11/16/005652

- Parity、マルチシグハッキングされた資金の凍結解除・返却へEthereumハードフォークを提案
  - https://paritytech.io/blog/on-classes-of-stuck-ether-and-potential-solutions-2.html
  - http://hackingdistributed.com/2017/12/13/ether-resurrection/

分散取引所EtherDelta、DNSサーバへの攻撃で資産流出

- Cloudflareアカウントが攻撃されたもの。
- 308ETH以外に他トークンが別アドレスへ移された。
- 全ETHトランザクションの10%に相当。
- 事態解決までサイトへアクセスしないことが推奨されている。
- こうした状況には、分散されておりハイジャックに遭いにくいENSシステム（Ethereum Name Service）が寄与するとされる。

→ 出典: https://www.ethnews.com/etherdelta-com-exchange-warns-users-that-it-was-attacked
→ 出典: http://www.trustnodes.com/2017/12/21/etherdelta-hacked-dns-compromised-funds-stolen

- Ethereumエコシステムにおける主なニュース
  - 資産流出・資産ロック
  - スケーラビリティ
    - 子猫収集飼育アプリのCryptoKitties、Ethereumトランザクションを詰まらせる
    - Ethereum Foundation、スケーラビリティの研究プロジェクトに助成金
    - マイクロRaidenがローンチ
    - Ethereumのスケーラビリティソリューション、Trusted Relay Networks
  - Vitalik
  - プロトコル
  - Stablecoin

子猫収集飼育アプリのCryptoKitties、Ethereumトランザクションを詰まらせる

- ゲームの概略
  - Etherを使って購入したオリジナルの子猫を飼育することができ、2匹の子猫を交配させることもできる。
  - ゲームを管理している中心的な存在はなく、ユーザーがEthereumブロックチェーンの上で永遠に生き続ける自分の子猫を所有できる。スマートコントラクトと取引して子猫を売買したり、繁殖させる。
  - 収益モデルは、最初の100匹の仔猫を売ったことで回収したetherと、15分ごとに新しく生まれて売られる子猫。この他、オークションの手数料を徴収。
- トークンの位置づけ
  - 利益を生む投資として販売されていないほか、子猫の所有により配当や利益流入を得る権利は伴わないため、証券とはみなされないと考えられている。
- トランザクション渋滞の発生
  - Ethereumネットワークの全トラフィックの20%がこの子猫取引トランザクションによって消費された。
  - この渋滞により、新しい子猫を生む手数料が0.001ETHから0.002ETHへ上昇、Ethereumブロックチェーンのスケーラビリティ課題が改めて表面化した。
  - また、この渋滞のため、ICO参加のためのEthereumトランザクションにも待ち時間が発生。
  - こうした渋滞解消には子猫売買をオフチェーンで行うほか、PlasmaやShardingといったスケーリングソリューションなどが必要。

→ 出典: https://medium.com/@aidobreen/how-does-cryptokitties-co-work-e5071c0abf73?source=linkShare-ba099158cf56-1512751285
→ 出典: https://coincenter.org/link/good-news-ethereum-s-cryptokitties-are-probably-not-securities
→ 出典: https://www.cryptokitties.co/faq
→ 出典: https://etherscan.io/txsPending
→ 出典: https://ethgasstation.info/

ETHEREUM FOUNDATION、スケーラビリティの研究プロジェクトに助成金

- Ethereumのスケーリングに向けて、Shardingおよびレイヤー2技術（Plasma、State channels、Raiden）を相互に補完するキーテクノロジーとして提示。
- Shardingクライアントおよびレイヤー2技術を対象として助成。
- 前者は、マルチクライアントエコシステムとなるために必要となるShardingテストネットおよびShardingメインネットを実現するためのもの。

→ 出典：https://blog.ethereum.org/2018/01/02/ethereum-scalability-research-development-subsidy-programs/

マイクロRAIDENがローンチ （1/2）

- マイクロRaidenとは何か
  - RaidenはLightning NetworkのEthereumシンプル化バージョン。
  - マイクロRaidenは、所定の受け手に対する単方向ペイメントチャネル。
  - オフチェーンにより、安価で低レイテンシーでスケーラビリティを提供する。
  - マイクロRaidenはRaiden Networkのパーツという訳ではないが、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した実装。
  - Raiden Networkのような多対多双方向ではなく、多対一の単一方向State Channelプロトコル。

→ 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

マイクロRAIDENがローンチ （2/2）

- マイクロRaidenにおけるチャネル
  - 送り手は、受け手との間にマイクロペイメントチャネルを開設し、チャネルにトークン（ERC20またはERC223準拠）をファンディングして使う。
  - エスクローされたトークンは、チャネルの開閉を管理するサードパーティーにより保持される。
  - チャネルに参加する当事者同士であれば、ペイパービューのようなマイクロペイメントを手数料ゼロで可能。

- マイクロRaidenにおけるチャネル残高管理
  - チャネル残高は送り手が支払う都度計算され、移送されたトークン量について証明するバランスプルーフへ送り手が署名し、バランスプルーフを受け手のサーバーへ送り、受け手が残高を新しいものへ入れ替える。
  - 送り手がチャネルクローズ時は、最終バランスプルーフを受け手へ送り、クローズ署名を得る。
  - 受け手の署名とバランスプルーフがチャネルを管理するスマートコントラクトへ送られると、チャネルが閉鎖され、債務が決済されるが、このとき余りのトークンがあれば送り手へ返却。

→ 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

ETHEREUMのスケーラビリティソリューション、TRUSTED RELAY NETWORKS （1/3）

- アトミックスワップ
  - アトミックスワップは単一チェーン上あるいはチェーンをまたぐアカウント間でアセットのトレードを行う方法。
  - アリスとボブの双方が自分のアセットをそれぞれのブロックチェーン上で開けるために双方の署名が必要となる「ロックされた箱」へ置く。

- アトミックスワップの課題
  - アトミックスワップはユーザーのアセット移動の問題解決にはならない。
  - というのも、スワップされたアセットはそれぞれのチェーン上に残る。
  - また、ユーザーは秘密鍵・公開鍵のペアにより表現されるため、アリスとボブは双方のネットワーク上のアクターとして同時に存在することになる。
  - そこで、「Trusted Relay Networks」は、EVMベースブロックチェーン間でアセットを移動するスキームを提示するもの。

→ 出典：https://gridplus.io/assets/TrustedRelayerNetwork.pdf
→ 出典：https://blog.gridplus.io/introducing-trusted-relay-networks-6c168f72a6f6

ETHEREUMのスケーラビリティソリューション、TRUSTED RELAY NETWORKS （2/3）

- Trusted Relay Networksの概要
  - 望むネットワークへメッセージをリレーすべく動機付けされたRelayerを最低限信用の前提。
  - アセットを初期のチェーンにロックした上で、新しいチェーンへコピーし、その後に移動が起こる。このスキームはEthereumスマートコントラクトに基づく。

- Relayerの振る舞い
  - EVMベースのブロックチェーン間でトークンやアセットを移動するメカニズムをリレーと呼び、メッセージを他のブロックチェーンへ運ぶために、トラストされたRelayerを必要とする。トラストされたリレーと称しているが、Relayerはアセットを盗難することができないほか、手数料によりメッセージを伝えるインセンティブがある。
  - Relayerは対応するゲートウェイコントラクト（送り手ブロックチェーンおよび宛先ブロックチェーンの双方に存在する）と共に動くが、それぞれのゲートウェイは、コントラクトのオーナーとして、トラストされたRelayerをエンコードし、そのオーナーだけがメッセージを送り手チェーン上のゲートウェイから宛先チェーン上のゲートウェイへとリレー出来る。
  - リレーネットワークはそれぞれのネットワーク上のスマートコントラクトのセットとして機能する。コントラクトはRelayerにより所有され、Relayerは秘密鍵・公開鍵のペアにより表現され、それぞれのチェーンへデプロイされる。
  - シンプルなリレーネットワークは、二つのチェーン間に一つのRelayerが介在する構成。

→ 出典：https://gridplus.io/assets/TrustedRelayerNetwork.pdf
→ 出典：https://blog.gridplus.io/introducing-trusted-relay-networks-6c168f72a6f6

ETHEREUMのスケーラビリティソリューション、TRUSTED RELAY NETWORKS （3/3）

- 二段階で行われるRelayの手続き
  - まず送り手チェーン上でゲートウェイコントラクトの関数をコール。
    - 以下の情報を含む：（宛先チェーン上のゲートウェイコントラクトのアドレス、送り手チェーン上にデポジットされたトークンのアドレスと数量、Relayerに渡す手数料、メッセージが署名されたタイムスタンプ、これら情報のハッシュ値）。
    - この時トークンは送り手チェーン上のゲートウェイコントラクト内にロックされている。
  - その上で次に、Relayerが宛先チェーンへのメッセージを送る、という流れとなる。

- リレーとアトミックスワップの相違点
  - 「カウンターパーティ無しにチェーン間のアセット移動を行う点」において大きく異なる。
  - アトミックスワップは二つのアクター間のトレード。
  - これに対してリレーは、ユーザーのメッセージを他のチェーンへ運ぶものであり、リレーされるアセットはまず宛先チェーン内に複製される。

→ 出典：https://gridplus.io/assets/TrustedRelayerNetwork.pdf
→ 出典：https://blog.gridplus.io/introducing-trusted-relay-networks-6c168f72a6f6

- Ethereumエコシステムにおける主なニュース
  - 資産流出・資産ロック
  - スケーラビリティ
  - Vitalik
    - Vitalik、5000億ドルの時価総額に対して自戒のコメントを発表
    - Vitalik、DAOの要素をICOに組み込んだ”DAICO”を提案
  - プロトコル
  - Stablecoin

VITALIK、5000億ドルの時価総額に対して自戒のコメントを発表

- どれだけのUnbankedな人びとを救えているか？
- どれだけ検閲耐性ある商取引を可能とできているか？
- どれだけのDappsが利用されているか？
- スマートコントラクトに格納された価値がどれだけ面白いことに使われているか？
- どれだけのベネズエラの人びとをハイパーインフレから保護できているか？
- どれだけのマイクロペイメントチャネルが実際使われているか？
- これらの問いへの答えは必ずしもゼロではないものの、5000億ドルレベルかというと十分たりえない。

→ 出典：https://cryptovest.com/news/vitalik-buterin-thinks-crypto-space-hasnt-earned-the-05-trillion-market-cap-yet/
→ 出典：https://mobile.twitter.com/VitalikButerin/status/940744724431982594

VITALIK、DAOの要素をICOに組み込んだ”DAICO”を提案

- ICOに関わる複雑性やリスクを軽減することを図るもの。

- 「群衆知を活用すること」「単一の中央集権チームのみを信用するのでない」「時間をかけて資金を拡げていくこと」を可能とするモデル。
  - DAICOコントラクトは、Contributionモードからスタート。誰もがETHを提供して交換でトークンを得ることができる。トークン発行量にキャップを設定することの有無や、ダッチオークションなどが設定可能。
  - Contribution期間が終わると、ETH提供は出来なくなり、初期のトークン残高が決定され、トークンが取引可能となる。その後は、開発チームが資金を引き出すことが可能に（秒あたりのweiで引き出し可能資金量を規定するTAP）。

- トークン保有者による投票による意思決定メカニズムを導入し、「TAPを高める」或いは「コントラクト閉鎖してETH引き出し」を投票。
  - 投票によりTAPを落とすことはできず、開発チームのみが落とすことができるが、開発チームはTAPを高めることは出来ない。
  - トークン保有者は開発チームの開発進捗に不満があれば、投票を行いシャットダウンさせて資金を戻すことが可能。

  → 出典：http://ethresear.ch/t/explanation-of-daicos/465

- Ethereumエコシステムにおける主なニュース
  - 資産流出・資産ロック
  - スケーラビリティ
  - Vitalik
  - プロトコル
    - Casper FFGアルファ版がTestnetリリース
    - COSMOS、ETGateをアルファ版リリース
    - 分散取引所Radar Relay、ウォレット間トレード実現へ向けてハードウェアウォレットLedgerサポートを表明
    - INGにより開発されたZKRP（ゼロ知識範囲証明）
  - Stablecoin

CASPER FFGアルファ版がTESTNETリリース

- Casper The Friendly Finality Gadget（FFG）のテストネットがリリースされ、PoS移行に向けて一歩を踏み出した。

- CasperにはFFGとCBC（Correct-by-Construction）の二つがあるが、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に使われる。

- 今回のFFGテストネットは、Pyethereumクライアントを通じてのみ利用可能であり、テストネットへのstakeとして最低1500ETHを必要としている。

→ 出典：https://www.bitsonline.com/casper-testnet-released/
→ 出典：https://hackmd.io/s/Hk6UiFU7z

COSMOS、ETGATEをアルファ版リリース （1/3）

- EthereumブロックチェーンとTendermintゾーンのブリッジ
  - 「双方向ペグ」を用いることによって、EthereumトークンをTendermintゾーンへ送受信できるようにしている。
- Relayerとサイドチェーンの働き（送るとき）
  - ユーザーがデポジットメッセージをコントラクトへ送信する都度、イベントが生成される。
  - 一方でRelayerはEthereumヘッダをTendermintゾーンへアップロード。
  - Ethereumヘッダにはレシートのマークルルートが含まれるため、イベントはマークル経路を使って証明され、このスキームをサイドチェーンと呼ぶ。
  - Relayerがイベントをアップロードすると直ぐにゾーンが新しいコインを鋳造する。
- Relayerとサイドチェーンの働き（戻すとき）
  - 引き出しにはValidatorの2/3以上のマルチシグを用いる。RelayerはTendermintヘッダもコントラクトへ送る。コントラクトはValidatorの2/3以上の署名でヘッダを承認する。
  - 対応したヘッダが承認された後、宛先や値といった必要情報およびそのマークル証明を提示することを通じて、ユーザーはトークンを引き出すことが出来る。
  - コントラクトが証明を検証すると、トークンがリリースされる。

→ 出典：https://gist.github.com/mossid/98b7388ba7c24fce68ff27d82af3eee3
→ 出典：https://github.com/mossid/etgate
→ 出典：https://drive.google.com/file/d/1jtyYtx7t1xy9gxEi2T5lXFNd8xUY7bhJ/view

COSMOS、ETGATEをアルファ版リリース （2/3）

- IBCプロトコル
  - Cosmos NetworkにおけるIBC（Inter Blockchain Communication）プロトコルを用いて個々のブロックチェーン間でコミュニケーションしてゾーンを跨いでトークンを送ることが出来る（例えば、ペグされたビットコインをEthereumゾーン上のスマートコントラクトへ送信）。
  - IBCプロトコルはTCP/IPの様な汎用コミュニケーションプロトコルであり、理論上はPolkadotにおける並列処理可能チェーン間のメッセージをリレーすることにも使用可能。
  - しかし、IBCプロトコルは、トランザクションファイナリティや効率的やコミット証明のあるコンセンサスアルゴリズム向けであり、ビットコインやEthereumと言ったそうではないブロックチェーンでは、アセットをチェーン間で送るためにペグゾーンを設ける必要がある。

→ 出典: https://gist.github.com/mossid/98b7388ba7c24fce68ff27d82af3eee3
→ 出典: https://github.com/mossid/etgate
→ 出典: https://drive.google.com/file/d/1jtyYtx7t1xy9gxEi2T5lXFNd8xUY7bhJ/view

COSMOS、ETGATEをアルファ版リリース （3/3）

- 双方向ペグ
  - 双方向ペグは分散的な方法でクリプトアセットをチェーン間で送るものであり、IBCプロトコルでは、Relayerが継続的にチェーンのヘッダを相互に提示することによって、双方のチェーンが相手の直近の状態を認識することが出来る。
  - ビットコインをEthereumへ送りたい場合、ユーザーは特別な送金トランザクションに署名して自身のビットコインをロックする。数ブロック後にトランザクションが承認されると、送金トランザクションがビットコイントランザクションに含まれることを示すマークル証明を使ってEthereum上でeビットコインアセットを鋳造し、これがファンドがロックされていることを意味する。
  - 同様のことが、eビットコインアセットの所有者が（実際のビットコインを受け取るためにeビットコインを）引き出すときにも発生する。
  - Ethereum上の送金トランザクションに署名してeビットコインをburnして承認を待ち、オリジナルブロックチェーン上のビットコインをリリースし、eビットコインアセットが本当にburnされたことを証明する。

→ 出典: https://gist.github.com/mossid/98b7388ba7c24fce68ff27d82af3eee3
→ 出典: https://github.com/mossid/etgate
→ 出典: https://drive.google.com/file/d/1jtyYtx7t1xy9gxEi2T5lXFNd8xUY7bhJ/view

分散取引所Radar Relay、ウォレット間トレード実現へ向けてハードウェアウォレットLedgerサポートを表明

- Ledgerウォレットユーザーがウォレットからウォレットへ直接etherやERC20トークンを移動可能とするもの。
- Radar Relayは既にブラウザベースウォレットMetaMaskとは統合済み。
- LedgerをPCへ接続して、Ledger上でEthereumアプリケーションを起動した後、Radar Relayアプリでウォレットをセットアップすることにより利用可能に。

→ 出典：https://www.coindesk.com/ledger-to-ledger-hardware-wallet-integrates-with-decentralized-exchange/
→ 出典：https://medium.com/radarrelay/ledger-integration-update-994ce2c5ac93?source=linkShare-ba099158cf56-1516422572

INGにより開発されたZKRP（ゼロ知識範囲証明）1/2

- ゼロ知識証明の応用として考えられる事項
  - 秘密鍵を持つことの証明による所有権証明、取引に必要な残高があることを証明
  - アイデンティティをあかすことなくグループメンバーであることを証明
  - 宝探しで実際の位置そのものを明かすことなく隠されたお宝の位置を知っていることを証明
  - シールドビッドオークションでビッドを明かすことなく誰が競り落としたかを証明

- ゼロ知識証明は次の三つを満たす。
  - 完全性（Completeness）:ステートメントが正しければ、正直な検証者は正直な証明者によって納得させられる。
  - 健全性（Soundness）:ステートメントが誤りならば、不正を働く証明者は正直な検証者を「それが正しい」と納得させることは出来ない。
  - ゼロ知識性: ステートメントが正しい場合、不正を働く検証者は、「そのステートメントが正しい」という事実以外に知ることがない。

- JP Morgan Quorumへのゼロ知識セキュリティ導入
  - 初めてゼロ知識セキュリティ層（ZSL）をエンタープライズブロックチェーンへ導入。

→ 出典: https://cms.ingwb.com/media/2122048/zero-knowledge-range-proof-whitepaper.pdf

INGにより開発されたZKRP（ゼロ知識範囲証明）2/2

- ゼロ知識範囲証明（ZKRP）とは
  - 或る値が所定の範囲内にあることを証明するものであり、INGにより開発された。
- ゼロ知識範囲証明（ZKRP）の応用として考えられる事項
  - 所得が不動産購入に充分なだけあることや、支払額が限度額内であることを実際の金額そのものを明かすことなく証明できる。
  - 位置に基づく証明として、或る国の中にいることを実際の位置そのものを明かすことなく証明できる。
- ゼロ知識範囲証明（ZKRP）の計算効率
  - 対話型のゼロ知識証明は分散ネットワークでは実用的でないため、結果を示せば他の検証者か証明自身を検証できる非対話型である必要があり、ZK-SNARKsのような非対話型のゼロ知識証明が有効とされる。
  - ただし、ZK-SNARKsは190万gasを必要とするのに対し、範囲証明であるZKRPは18万Gasで済むため、10倍の計算効率。

→ 出典：https://cms.ingwb.com/media/2122048/zero-knowledge-range-proof-whitepaper.pdf

- Ethereumエコシステムにおける主なニュース
  - 資産流出・資産ロック
  - スケーラビリティ
  - Vitalik
  - プロトコル
  - Stablecoin
    - Tether、Ethereumブロックチェーン上でERC20互換USDTトークン・EURTトークンの導入を発表
    - MakerDAOによるStablecoinであるDaiがEthereum Mainnet上で稼働
    - 通貨バスケットに連動したStablecoinである ARC Reserve Currencyが発表

TETHER、ETHEREUMブロックチェーン上でERC20互換USDTトークン・EURTトークンの導入を発表

- より安価なトランザクション手数料を狙いとしてEthereum上でUSDバックおよびEURバックのトークン発行。
- 取引所に統合されることにより、取引所のアービトラージを効率的に行なえる。
- Omniレイヤープロトコルを介してビットコインベースのUSDを補完する位置付けだが、クロスチェーンでの互換性は無い。
- コントラクトの監査はZeppelinにより行われた。

→ 出典: https://tether.to/usd?-and-eur?-now-supported-on-ethereum/
→ 出典: https://themerkle.com/tether-issues-usdt-and-eurt-tokens-on-top-of-the-ethereum-blockchain/
→ 出典: https://blog.zeppelin.solutions/tether-token-audit-438d561a380

MakerDAOによるStablecoinであるDaiがEthereum Mainnet上で稼働 （1/3）

- Stablecoinとは
  - BTCやETHは普段使いの通貨とするにはボラティリティが高く、価格安定性を志向したStablecoinが登場している（例えば米ドルと連動したTether）。
  - 価格安定性あるStablecoinは、頑健な分散トレーディングプラットフォームに必要。

- 担保を裏づけとしたDai
  - StablecoinであるDaiは、担保に裏づけされた暗号通貨（ERC20トークン）であり、その価値が米ドルと連動。
  - 負債担保ポジション（Collatetalized Debt Pisition:CDP）と呼ばれる動的システムのスマートコントラクトを通じて、Daiの価値は安定化される。
  - CDPはユーザーがDaiアセットを受け取り、利子付き負債として運用するスマートコントラクト。ユーザーは負債ポジションを保証するため、ローンの価値を上回る担保を差し入れる。

→ 出典: https://medium.com/@MakerDAO/dai-is-now-live-ad87e34fc826
→ 出典: https://makerdao.com/whitepaper/DaiDec17WP.pdf

MakerDAOによるStablecoinであるDaiがEthereum Mainnet上で稼働 （2/3）

- CDPスマートコントラクト
  - ユーザーによりデポジットされた担保資産を保持して、ユーザーがDaiを生成する許可を与えるとともに負債を生成する。
  - この負債は、相当するDaiの払い戻して担保を引き出すことでカバーされるまでの間、デポジット済み担保資産をCDP内にロックするもの。
  - アクティブなCDPは常に担保超過であるため、担保価値は負債価値を上回る。
  - CDPのプロセスは、「1．CDP生成と担保デポジット」「2．担保付きCDPからDai生成」「3．負債および安定化手数料支払い」「4．担保引き出しとCDPクローズ」から成る。

- 価格安定化メカニズムとしてのターゲットプライス
  - 一つはCDPの担保/負債比率を計算するのに使われる。
  - このほか、Dai保有者がグローバルセツルメント時（ターゲットレートを保証するための最終手段としてプラットフォームをシャットダウンしてアセットのネット価値をユーザーが受け取る）に受け取る担保資産の価値を決めるのに使われる。
  - ターゲットプライスは初期はドル建てで米ドルと1:1ペグされる。

→ 出典: https://medium.com/@MakerDAO/dai-is-now-live-ad87e34fc826
→ 出典: https://makerdao.com/whitepaper/DaiDec17WP.pdf

MakerDAOによるStablecoinであるDaiがEthereum Mainnet上で稼働 （3/3）

- ターゲットレートフィードバックメカニズム
  - シビアな市場安定化を図る場合に備え、ターゲットレートフィードバックメカニズムを持つ。
  - これは、Daiの市場価格をターゲットプライス近傍への安定性を保持すべくターゲットレートを調整する自動メカニズム。
  - ターゲットレートはターゲットプライスの変更を決定づけるものであり、Daiの保有インセンティブ（ターゲットレートが正の場合）或いはDaiの借り入れインセンティブ（ターゲットレートが負の場合）となる。

→ 出典：https://medium.com/@MakerDAO/dai-is-now-live-ad87e34fc826
→ 出典：https://makerdao.com/whitepaper/DaiDec17WP.pdf

通貨バスケットに連動したSTABLECOINであるARC RESERVE CURRENCYが発表

- 発行条件
  - コイン購入者が充分な資金を送り、購入者がKYC/AML等の規制をクリアしており、購入者がコインあたりに正しい価格を支払っていること。
  - 新規発行は制限が無く、既存保有者にとり希薄化しない点がStablecoinの特徴。

- 価格安定化の仕組み
  - 次の機能により、価格を狭いレンジ内に収める。
  - 一つは通貨の多様性との相関。
    - 主要法定通貨の貿易量加重に基づくものであり、国際決済銀行（BIS）の三カ年レポートで5%以上の貿易量を持つ法定通貨が含まれる。
    - 米ドル以外の多様な通貨とすることにより米ドルとの相関を小さくしている。
  - 二つ目はアセットクラスによるもの。
    - コインの年間上昇率をG10諸国の平均インフレ率や、米国・欧州・日本の中央銀行平均レートを上回るようにする。
  - 三つ目は交換レートコントロール。
    - Net Asset Value（全アセットの価値をトータルコイン数で割ったもの）との相関で予測可能な範囲に収める。

→ 出典：https://bitcointalk.org/index.php?topic=2589946.0

- Ethereum技術トピックの解説
  - スケーリング
  - CasperによるPoS
  - 分散型取引所（DEX）およびDEXプロトコル
  - 応用サービス

- Ethereum技術トピックの解説
  - スケーリング
    - Plasmaによるスケーリング
    - Shardingによるスケーリング
    - TrueBitによるスケーリング
    - Cosmosによるインターブロックチェーンプロトコル
    - Cosmosネットワークを支えるTendermint
  - CasperによるPoS
  - 分散型取引所（DEX）およびDEXプロトコル
  - 応用サービス

PLASMAによるスケーリング

- 複数のブロックチェーンツリー状の階層構造
  - それぞれの枝が自身の履歴を持つ一つのブロックチェーンとして扱われ、子チェーンはプラズマブロックチェーンと呼ばれる。
  - 子チェーン（プラズマブロックチェーン）はルートチェーン上の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。
- 有効性を保証する仕組み
  - 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。
  - ルートチェーン上に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。
  - ステートを更新するために全参加者がオンラインである必要は無く、トランザクション確認のために参加者はルートチェーンへデータを提示する必要も無い。
- 提供される価値
  - ルートチェーンは子チェーンからのわずかなコミットメントのみを処理するのみなので、ルートチェーンへ渡されるデータ量が減少し、多くの計算が可能となる。
  - データは特定のステートを検証することを希望するノードにだけ伝播されるので、全ノードが全チェーンを確認せずに済み、コントラクトの実行をスケールできる点がポイント。

→ 出典: https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

SHARDINGによるスケーリング

- データベースシャーディングとの対比
  - データベースのデータパーティション毎に異なるデータベースサーバーインスタンスに格納するのがデータベースシャーディング。
  - これと同様に、ブロックチェーン全体のステートを異なるシャードに分割し、ステートの各パーツを異なるノードに格納するもの。
- シャーディングにおけるトランザクション処理プロセス
  - ・トランザクションは影響を受けるシャードに応じて異なるノードに振り向けられ、各シャードはステートの一部パーツを並行で処理する。
  - ・シャード同士のコミュニケーションにはメッセージ交換が必要だが、Ethereumではレシートの仕組みが考えられており、自身のローカルシャードのステートを変更する際に、後日別のシャードが参照可能な分散共有メモリに格納されるレシートを生成する。
- 課題
  - 全ノードがトランザクションの一部のみを処理するに留まりながらも、セキュリティを担保する上では、各ノードが互いにトラストせず、トランザクションは異なるマシン上で処理される共通ステートに同意されなくてはいけないという前提が課題となる。
  - 各ノードは互いにトラストしないので、あるシャード上でトランザクションを処理するノードにとって、別のシャード上でトランザクションを処理するノードと対話するだけでは不十分で、なんらか証明が必要となる点が課題。

→ 出典: https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

TRUEBITによるスケーリング

- 計算処理をオフチェーン実行
  - Ethereumのスマートコントラクトにおける計算をブロックチェーン外のレイヤーを用いて検証可能な形でオフチェーン実行することによって、トランザクションをスケールさせるもの。
  - 計算プロセスと検証プロセスをEthereumブロックチェーンから切り出すことによって、ガスリミットに制約されることなく多くの計算をこなすスケールが可能となる点がポイント。

- 計算処理の正しさを保証する仕組み
  - 全ノードが計算に参加する代わりにSolverと呼ばれ特定の参加者がスマートコントラクトによる計算を実行して回答をデポジットを添えて提出し、回答が正しければ報酬を受け取りデポジットが返金される。
  - 回答が不正であればデポジットは没収され、ブロックチェーン上でVerificationGameを用いた紛争解決プロセスが動く。
  - VerificationGameでは、Solverの働きをオフチェーンでチェックするVerifierと呼ばれる参加者を置き、VerifierがエラーシグナルをSolverの回答を受け入れる。
  - もしVerifierがSolverの回答の正しさにエラーシグナルを出すと、限られた計算パワーを持つJudgeが解決する。
  - 誰もが計算タスクをポストでき、また誰もがそのタスクをこなすことで報酬を受け取ることができ、回答の正しさを保証するインセンティブの仕掛けを組み込んだプロトコルとなっている。

→ 出典: https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

COSMOSによるインターブロックチェーンプロトコル

- 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。
- ハブ・ゾーン間でトークン流通を行うInter Blockchain Communication。
  - インターネットに例えると、複数のブロックチェーンが、CosmosにおけるTCP/IPのような位置付けでIBCプロトコルを用いてコミュニケーションを行う。ISPのようにハブがIBCパケットをルーティング。
  - IBCでは各ゾーンの独立性を保ち、プライベートチェーンのセキュリティを維持しながら、トークンをパブリックチェーンへ送受信できる。
  - IBCを使う前提として、ブロックチェーンのファイナリティが必要なため、PoSのバリデータが投票都度資金を賭けることで、確率的ファイナリティではない形で分岐を防ぐべく、Tendermintを利用。
- BitcoinやEthereumのような確率的ファイナリティの場合はIBCを利用出来ないため、別途ペグシステムが必要。
  - ETGateは、Ethereum/Tendermint間の双方向トークンのやりとりを行うが、双方向ペグ実現の仕組みとしてDrivechainを応用（マイナー投票ではなくバリデータ投票）。
  - Cosmosハブでは、StakeとしてAtomトークンを用いてバリデータ投票。
  - このほか、トランザクション手数料を払うためPhontonトークンを用意して使い分けることにより、PoSコンセンサスアルゴリズムへの攻撃を抑止。

→ 出典：https://zoom-blc.com/what-is-cosmos

COSMOSネットワークを支えるTENDERMINT

- 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。
  - Tendermint PoSでは、提案されたブロックに対して、他バリデータがデポジット量に応じて投票を行うことを通じて承認する。
  - ブロック生成時間が1-3秒と短い他、ブロック生成時にファイナリティを得られる点が特徴。
  - 二段階の投票プロセスを通じてそれぞれで2/3以上の票数を必要とすることによって、同じブロック高に複数のブロックが作成されるフォークを防いでいる。

- Dapps開発者むけインタフェースとしてABCI（Application Blockchain Interface）と呼ばれる仕組みを提供。
  - 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。

→ 出典：https://zoom-blc.com/what-is-tendermint

- Ethereum技術トピックの解説
  - スケーリング
  - CasperによるPoS
    - Casperのコンセンサスアルゴリズム
    - Casperの移行ステップ
    - Casper移行のインセンティブ
  - 分散型取引所（DEX）およびDEXプロトコル
  - 応用サービス

CASPERのコンセンサスアルゴリズム （1/5）

- TendermintにおけるPoSの仕組み
  - PBFTに由来する、PoSの初めての実装。
  - BFTベースのPoSでは、新ブロックを提案する権利をマルチラウンド投票を通じて擬似的にランダムな方法でバリデータに割り当てる。

- Tendermintにおけるバリデータ
  - ブロックのコミットやファイナライズはバリデータの2/3以上を必要で、ファイナライズ迄に数度のラウンドを要する。
  - 投票ラウンドは、バリデータがブロックを提案し、コミット意思をシグナリングし、ブロックに署名しコミットするという三ステップ。
  - ブロックチェーンのフルコピーを保持して公開鍵で特定されるバリデータは、各ブロック高において順番にブロックを提案する。

→ 出典：https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae

CASPERのコンセンサスアルゴリズム （2/5）

- Tendermintにおけるプロポーザ
  - 投票ラウンドあたり一人のプロポーザが割り当てられ、各提案に対してバリデータは自分の秘密鍵で署名して投票するが、問題があるとバリデータを特定される。
  - プロポーザがオフラインであったり、ネットワーク遅延があるとコミットがうまくいかないので、バリデータをスキップするタイムアウトの仕組み。

- Tendermintの特徴
  - 100%のアップタイムをバリデータに求め、1/3以上がオフラインだとネットワークが止まる。
  - 1/3未満のビザンチン問題であれば安全を保障でき、同じブロック高で競合ブロックをコミットしないためフォークも発生しない。
  - そのため、応答性よりも安全性やファイナリティを優先したものと言える。

→ 出典: https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae

CASPERのコンセンサスアルゴリズム （3/5）

- Casper the Friendly Finality Gadget(FFG)
  - 既存のEthereum PoW上にPoSをオーバーレイするので、PoWとPoSのハイブリッド。
  - PoWが確率的ファイナリティであるのに対して、ファイナリティや51%攻撃を付与するのがCFFG。

- Casper FFGにおけるファイナライズ
  - 50ブロックのセグメント（エポック）としてバリデータによる投票を行うことにより、2エポックの時間をかけてブロックをファイナライズする。
  - エポック1のブロックはバリデータの2/3以上の投票により正当とみなされた後、その子ブロックであるエポック2のブロックがバリデータの2/3以上の投票を得るとファイナライズされる。
  - バリデータ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つの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が減らされる。
  - バリデータは２つの分岐に投票するとペナルティが課されるので、正統なチェーンに収斂していくインセンティブとなる仕組み。

→ 出典: https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae

CASPERのコンセンサスアルゴリズム （4/5）

- Casperには、the FriendlyFinality Gadget(FFG)とthe Friendly Ghost(TFG。CBCとも呼ばれる)の二つがあり、分岐時にどのチェーンをメインチェーンとするかのファイナリティアルゴリズムが異なる。
- FFGはPoWとPoSのハイブリッドであり、ブロックチェーンのファイナリティとBFT両者に基づいて合意形成。
- TFGは、PoWで用いられているGHOSTをPoSに応用する、ブロックチェーンのファイナリティに基づく合意形成。
- FFGにおける投票
  - ブロック高100毎にチェックポイントを設けて、このチェックポイントのあるチェーンは正当なメインチェーンかについて、Validatorがデポジットして投票を行う（デポジット額に応じた議決権）。
  - 投票後、他ノードにより事実認定がされると、正しい投票をしたValidatorには報酬が、不正な投票をしたValidatorには罰金が科される（懲罰の仕組みをSlasherと呼ぶ）。

→ 出典：https://zoom-blc.com/casper-the-friendly-finality-gadget

CASPERのコンセンサスアルゴリズム （5/5）

- Casper the Friendly Ghost(TFG)
  - PoWにおける分岐したフォークで最も重いブロックを選択するGHOST(Greedy Heaviest Observed SubTree)をPoSに適用するもの。
  - Casper TFGは、バリデータに友好的なカルテルを形成するようにインセンティブを与える。

- TendermintとCasperの違い
  - Tendermint PoSではファイナリティ上ブロック生成時間が短く、そのため収容可能なバリデータ数に上限がある。
  - これに対し、Casper PoSでは多くのバリデータを収容することでブロック生成時の安全性を確保する。

→ 出典: https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae

CASPERの移行ステップ

- Casperのもたらすインパクトは、Nothing at Stake問題を解決した「セキュリティの高いPoS」を実現すること。
- ルール違反時に保有ETHを没収するペナルティを課すことにより、「大量のETHを所有する攻撃者が計算リソースを割かずに攻撃する） PoSの問題を解決。
- 現行のEthashによるPoWから、「PoWでマイニング後にPoSでファイナライズする方式」次いで「PoWとPoSのハイブリッド（PoW上にPoS） 」を経てCasperへ移行する計画。
- PoS移行により、Validatorがブロック生成報酬を得るためにETH現物を保持するインセンティブが高まることが見込まれる。

→ 出典：https://ethereum-japan.net/ethereum/casper-ffg-testnet-release/

CASPER移行のインセンティブ

- PoS移行にはハードフォークが前提として開発が進められており、エコシステム全体が分裂無しに新しいチェーンへ移行するインセンティブが必要。
- 移行インセンティブを与える仕組みが「ディフィカルティ・ボム」。
  - マイニング難易度が指数関数的に上昇してブロックタイムが遅延していくことによって、プロトコルが凍結するもの。
- PoWからPoS on PoWへ移行する際には、PoWを使い続けると動かなくなるアイスエイジが組み込まれる。
- PoS on PoWからPoSへの移行時には、徐々にPoSでマイニングされるブロックを増やしていく仕組み（始めは50ブロックに一度PoSとし、その割合を徐々に増やす）が組み込まれる。

→ 出典：https://coinchoice.net/casper_eth/
→ 出典：https://medium.com/@udon_crypto/イーサリアムによくある疑問に答えます-565cacf9ddf0

- Ethereum技術トピックの解説
  - スケーリング
  - CasperによるPoS
  - 分散型取引所（DEX）およびDEXプロトコル
    - DEXの概要説明
    - EtherDelta
    - 0xプロトコル
    - AirSwap
    - KyberNetworks
  - 応用サービス

分散型取引所（DEX）およびDEXプロトコル

- DEXの概要説明
  - DEXでは自身の保有する暗号通貨やアセットを第三者に預けることなく、自身の管理する秘密鍵の管理下で（個人のウォレット間で）交換可能。
  - 中央集権型取引所のセキュリティ脆弱性を狙って攻撃されるのに対して、DEXではブロックチェーンネットワークで分散的に管理することでハッキングリスク・カウンターパーティリスクを回避。このほか、ダウンタイム発生リスクが無いことや個人情報開示が必要ないことがメリットとされる。
  - トレーダーやマーケットメーカーの絶対数が少なく流動性が低いことや、取引処理の遅さ、取引手数料の安さやユーザビリティ・カスタマーサポート面、スマートコントラクトの欠陥リスクから、現時点では取引のほとんどが中央集権型取引所となっている。
  - スマートコントラクトを用いて第三者へのトラストを最小限でトークン交換を行える（透明性も高い）ため、DEXの多くがEthereum上に構築されている。
  - DEX以外に、アトミックスワップはトラストレスを保ちながらクロスチェーンでアセット交換を行うものだが、メイカーとテイカーを引き合わせるための仕組みが別途必要。

- DEXが提供する機能
  - 1)オンチェーン取引、2)ユーザーによるアセット管理権維持、3)分散化されたオーダーブック。
  - 以下に、EtherDelta、0xプロトコル、AirSwapおよびKyberNetworksについてまとめる。

→ 出典：http://individua1.net/dex-2017/
→ 出典：https://zoom-blc.com/what-is-0x-project-for-dex
→ 出典：https://consensysmediajapan.com/3357.html

分散型取引所（DEX）およびDEXプロトコル

- EtherDelta
  - 概要：
    - Ethereumのコントラクト利用率でも常に上位を占めている、活発なDEX。
  - 収益モデル：
    - ETHやトークンをデポジットする事で売買が出来るが、デポジット・オーダー・約定のそれぞれにおいて手数料（対Ethereumネットワークおよび対プラットフォーム）がかかる。
    - オーダーはオンチェーンで処理され、取引の活発さに応じて開発者が収益を得る仕組み。
  - 取引スピード：
    - 買い手と売り手の自動マッチングは無く、オーダーブックにある売り手の価格を買い手が選択する事で取引が成立する仕組みであり、取引スピードが遅い。

→ 出典：http://individua1.net/dex-2017/
→ 出典：https://zoom-blc.com/what-is-0x-project-for-dex
→ 出典：https://consensysmediajapan.com/3357.html

分散型取引所（DEX）およびDEXプロトコル

- 0xプロトコルの概要
  - DEXを可能とするためのプロトコル（0x上に様々なDEXアプリケーションが作られる）。
  - オーダー管理をオフチェーンで行うため、安価で高速なオーダー管理ができる点が特徴。

- 0xプロトコルの収益モデル
  - 注文を提示するメイカーと注文を受けるテイカーの売買情報を中継するRelayer（例：Rader）に対して手数料が必要。
  - DEX運営はRelayerが行い、Relayerが手数料を設定して報酬を得る仕組み。

- 0xプロトコルの目指すスケーリングとオフチェーン活用
  - DEX取引をスケールさせ、高速な取引や低い手数料を実現させることを目指している。
  - そのため、0xではトークン取引決済のみをオンチェーン、それ以外の注文などはオフチェーンで行っている（オーダーブックマッチングをブロックチェーンに記録せずに署名検証のみ行うため高速。
  - 従来のDEXではトークン交換取引以外の取引注文（メイカーとテイカーの注文を管理するオーダーブック作成）・注文修正・注文取消もオンチェーンのブロックチェートランザクションで行う。
  - オフチェーンでメイカーとテイカーのメッセージに署名し、オンチェーンでテイカーの署名入りトランザクションを決済）。

→ 出典：http://individua1.net/dex-2017/
→ 出典：https://zoom-blc.com/what-is-0x-project-for-dex
→ 出典：https://consensysmediajapan.com/3357.html

分散型取引所（DEX）およびDEXプロトコル

- 0xプロトコルにおけるメイカー／テイカーの役割
  - メイカーでメッセージとハッシュの署名を含めてテイカーへ送る。
  - テイカーが受け取ると自身の署名でトランザクションを生成してブロードキャストすることでマッチング成立となる。
  - これがブロックに含められることによりトランザクション決済完了となる。

- 0xプロトコルにおけるRelayerの役割・課題
  - ブロックチェーン上で安全性が保たれるオンチェーン処理と違い、オフチェーンのオーダーブック管理を別途安全に行う必要がある。
  - そのため、Relayerが主体となって、取引手数料をインセンティブとしてオーダーブック管理（メイカーの注文の正当性を管理し適切な手数料を定め、テイカーへ最善の価格を提示する）を行いつつも、取引トークンは奪えない仕組みを導入。
  - 将来的には多数のRelayerが市場原理の下にバランスのとれた手数料で取引仲介を行う。
  - EtherDelta同様、買い手と売り手の自動マッチングが無くRelayerを介する方式のため取引スピードがネック。
  - 通常の取引所並みにオンライン決済が高速で実施できるには、PlasmaやRaidenの早期実装が必要。

→ 出典：http://individua1.net/dex-2017/
→ 出典：https://zoom-blc.com/what-is-0x-project-for-dex
→ 出典：https://consensysmediajapan.com/3357.html

分散型取引所（DEX）およびDEXプロトコル

- AirSwap
  - 概要：
    - P2Pトークン交換を行うもの。
    - オーダー管理をオフチェーン、トークン交換をオンチェーンで行う。
  - トークン交換の仕組み：
    - トークン交換情報を仲介する存在をIndexerと呼ぶ。
    - AirSwapチームがIndexerを運営するとされる。
    - 注文処理のみをオンチェーンで行う。
  - 取引スピード：
    - トークン交換したい参加者同士をマッチングし、オフチェーンで取引レートを決めさせて両者が合意する条件で取引を成立させる（オラクルにより適切なレートを提示）仕組みのため、取引スピードが速い。

→ 出典：http://individua1.net/dex-2017/
→ 出典：https://zoom-blc.com/what-is-0x-project-for-dex
→ 出典：https://consensysmediajapan.com/3357.html

分散型取引所（DEX）およびDEXプロトコル

- KyberNetworks
  - 概要：
    - オーダー管理および約定を共にオンチェーンで行う。
  - 流動性提供の仕組み：
    - KyberNetworks自身あるいはサードパーティーにより運営されるReserve Entity（マーケットメイカーのような機能を果たして流動性を提供することでスプレッドを設定して収益を得る）が他のReserve Entityと競争しながら流動性を提供する。
  - 取引スピード
    - 売り手がトークンをリザーブし、買い手がリザーブにある通貨を取引する。
    - KyberNetworksが複数のリザーブの中からレートの良いものを自動選択して買い手に提供する自動マッチングのため、取引スピードは速い。

→ 出典：http://individua1.net/dex-2017/
→ 出典：https://zoom-blc.com/what-is-0x-project-for-dex
→ 出典：https://consensysmediajapan.com/3357.html

- Ethereum技術トピックの解説
  - スケーリング
  - CasperによるPoS
  - 分散型取引所（DEX）およびDEXプロトコル
  - 応用サービス
    - 予測市場Gnosisの概要
    - トークン流動性を提供するBancorプロトコル概要
    - その他のトピックニュース

予測市場Gnosisの概要 （1/3）

- 予測市場とは
  - ギャンブルとアンケートを合わせたようなアプリケーション。
  - 賭けるユーザーにとってはギャンブルであり、市場作成者にとってはアンケート・市場調査。
  - 回答者にインセンティブを与えながら、分散化したバイアスの無いデータを低コストで収集可能。

- Gnosisの概要
  - スマートコントラクトやオラクル等を用いて予測市場システムを構築。
  - トークンのウォレット、DEX、そして予測市場が互いに連携するエコシステムを想定している。
  - Ethereum上に外部情報をもたらすオラクルやマーケットメイクなどのGnosis Core層、その上にWIZトークンにより手数料を払うなどのGnosis Service層、そしてトップが保険等のアプリケーション層、という四層構造。

- Gnosis Service層
  - トークンの発行や決済、価格の決定、オラクルとのやり取りなどを定義するスマートコントラクトを実行。

→ 出典：https://zoom-blc.com/what-is-gnosis
→ 出典：https://zoom-blc.com/how-gno-and-wiz-token-are-working-in-gnosis
→ 出典：https://zoom-blc.com/how-uport-is-working

予測市場GNOSISの概要 （2/3）

- Gnosis Service層の主要コントラクト
  - イベントコントラクト
    - オラクルからの外部情報を参照して予測結果を判断する他、賭け金となるETHなどの賭けトークンをその予測市場で使われる選択肢トークン（明日の天気予測であれば晴トークンや雨トークンなどのOutcomeトークン）に変換する。
  - マーケットコントラクト
    - Outcomeトークンを市場原理に基いてトークン価格をマーケットメーカーが自動的にリアルタイムで決定してさらに流動性付与することによって市場売買可能にする。

- Gnosisの収益モデル
  - Gnosis Core層は無料で利用でき、サービス層やアプリケーション層で課金するモデル。
  - サービス層では拡張機能として、トランザクションをオフチェーンで高速処理処理するためのState Channelのほか、価格の安定したStablecoinが提供される。
  - こうした拡張機能を利用するためにプロトコル利用手数料を徴収するモデル。
  - さらにアプリケーション層では賭けトークンの0.5%を手数料とする。

→ 出典: https://zoom-blc.com/what-is-gnosis
→ 出典: https://zoom-blc.com/how-gno-and-wiz-token-are-working-in-gnosis
→ 出典: https://zoom-blc.com/how-uport-is-working

予測市場GNOSISの概要 （3/3）

- GnosisにおけるトークンモデルとDEX必要性
  - 手数料を払うためのWIZトークン
    - ユーザーが予測市場に参加するための手数料、開発者がプロトコルを利用するための手数料
  - プロトコルで使われるGNOトークン
    - 予測市場の報酬を受け取ったり賭けを行うため、およびWIZトークンを生成するための価値の担保としても機能
  - さらに、および資金投入するためのETHトークンなど多くのトークンがあるため、これらを効率的に運用するDEXの仕組みが必要となる。
  - 外部でも使えるGNOトークンと別に内部でのみ使えるWIZトークンを用意し、Gnosisのリピーターを増やすためにこのWIZトークンを用いることによって、ネットワーク効果を高めるトークンモデルを描いている点が特徴。
  - 現在、誰でも参加できる予測トーナメントOlympiaを開催し、トークンで遊んでみることができるようにしている。

- 認証システムとしてのuPort活用
  - uPortは、ブロックチェーンを活用して個人情報を一元管理することに加えて、スマートコントラクトを活用することによって適切な相手に適切な情報のみ柔軟に情報公開許可を自分だけが与えることができるようにすることによって、簡単・安全にデジタル身分証明を提供することを目指している。

→ 出典：https://zoom-blc.com/what-is-gnosis
→ 出典：https://zoom-blc.com/how-gno-and-wiz-token-are-working-in-gnosis
→ 出典：https://zoom-blc.com/how-uport-is-working

トークン流動性を提供するBANCORプロトコル概要

- トークン種類が増えることに伴って顕在化することが想定される流動性リスクの解決策を提示するのがBancor Protocol。
- Bancor Protocolに準拠したトークン（Smart Token）は一定比率（Weightと呼ばれる準備率）の準備金を保持し、トークン価格はスマートコントラクトにより変動。
- この準備金をConnector Tokenと呼び、これによりトークンの流動性を担保。
- 一定比率で他アセットをConnector Tokenとして保持するBancor Networkで繋がったトークンどうしは、人手を介さずに（マーケットを必要とせずに）スマートコントラクト上で交換可能。
- 2種類のConnectorトークンを持つToken Relayにより、既存のERC20トークンをBancor Networkに載せることか可能。
- さらに、3種類以上のConnectorトークンを持たせることにより、分散投資を行うToken Basketを生成可能。

→ 出典：https://medium.com/@mach/bancor-protocol-はトークンエコノミーを支える大発明となるか-後編-cc09dec779f4

分散ファイルシステム

- ストレージ提供インセンティブとしての仮想通貨導入が特徴。
- Filecoin（開発中）
  - IPFSの分散ファイルシステムを利用し、その上に仮想通貨Filecoinによるインセンティブ発行。
  - IPFSはファイル配置の他、IPNSによる名前解決が可能。
  - ノードがデータを正しく保持していることを検証するProof of Storageの計算方法として、Proof of ReplicationおよびProof of Spacetimeの二つが提案されている。
- Storj（稼働済）
  - アップロードしたファイルを分割し、40のshardに分散して配置し、半数の20shardが失われない限り復元可能。
  - アカウントや課金システムは集中管理。
  - ファイルの存在確認処理としては、Proof of Replicationに似たProof of Retrievabilityを利用。
- Swarm（PoC稼働中）
  - Ethereum公式の分散ファイルシステム。
  - EVMやSolidityとの結合によりDAppから利用しやすくなるのが特徴。
  - ノードインセンティブはStorage incentiveとBandwidth incentiveの二つ（後者を重視）。

→ 出典：http://tech.mercari.com/entry/2017/12/01/093000

その他のトピックニュース

- EthereumのYellowPaper、Byzantium Revisionとしてアップデート
  - https://ethereum.github.io/yellowpaper/paper.pdf
- PlasmaプロトコルによるETH取引所実装案
  - https://github.com/BankEx/PlasmaETHexchange/blob/master/README.md
- ERC721: 非代替性トークンNFT（Non-fungible Token）のスタンダード
  - https://github.com/ethereum/EIPs/issues/721#issuecomment-343246872
- PlasmaのMVP(Minimum Viable Product）レポジトリオープン
  - http://ethresear.ch/t/minimal-viable-plasma/426
- MonacoinとDecredがアトミックスワップに成功
  - http://blog.utyuu.space/2018/01/20/monacoin-decred-atomicswap/

3. プラットフォーム分野

① ブロックチェーン普及に向けた六つの主要課題
② パブリックブロックチェーンの課題
③ ビットコインとブロックチェーン、分散台帳技術
④ Intel、PoWのDNA配列決定への応用で特許
⑤ IOTAの安全性についてMIT Media Labが反論
⑥ ２０１７ 3Qの動向トピック
⑦ 個別トピックリスト① Startup
⑧ 個別トピックリスト② Enterprise

ブロックチェーン普及に向けた六つの主要課題

- 米IC3の取り組む、ブロックチェーン普及に向けた六つの主要課題。
- スケーリングとパフォーマンス。
  - Permissionless/Permissioned双方でグローバル規模のワークロードをハンドリングするためのブロックチェーンのスケールアップ。
- 設計・開発の正確性。
  - 開発者が安全なプロトコルやコードを生成することをより容易・自動的なものとする。コード生成のプログラミング言語、セキュリティ証明付き暗号プロトコル。
- 機密性。
  - 暗号技術とTrustedハードウェアを活用することによりブロックチェーンに透明性と機密性を組込。
- 真正なデータフィード。
  - ブロックチェーン向けに信用に足るデータフィードの頑健なエコシステムをサポートすると共に、高度に信頼できるデータフィードソリューションに貢献。
- 安全性とコンプライアンス。
  - ブロックチェーンへのモニタリングや介入にむけた技術およびプロトコル。
- マイグレーション。
  - ブロックチェーンデプロイへのマイグレーション、レガシーシステムとブロックチェーンシステムの統合。

→ 出典：http://www.initc3.org/projects.html

パブリックブロックチェーンの課題(1/2)

- パブリックチェーンの課題について、スケーラビリティ、プライバシー、コントラクト検証、ストレージ制約、コンセンサスメカニズムの持続可能性、ガバナンスや標準の欠如、ツールの不十分さ、量子コンピュータ耐性を取り上げ、課題の概要と現時点でのソリューションを整理。
- スケーラビリティについて
  - スループットおよびトランザクション時間が課題。
  - ソリューションとして、オフチェーンペイメントチャネル（LightningやRaiden）、シャーディング、オフチェーン計算（EthereumのTrueBit）、DAG構造（IOTA、SPECTRE）がある。
- プライバシーについて
  - 金融・医療・アイデンティティ・証明書管理の分野で課題。
  - ソリューションとして、Diffie Hellman鍵交換を用いた楕円曲線Diffie-Hellmanマークルアドレス（Peter Toddによるステルスアドレスや、BIP47/BIP75）、ミキシング（CoinJoin、CoinShuffle）、リング署名（Monero）、ゼロ知識証明（zkSNARKs、zkSTARKs）、コードの難読化、オラクル、TEEがある。
- ストレージ制約へのソリューション
  - SwarmやIPFS、Decentがあげられている。

→ 出典：https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428

パブリックブロックチェーンの課題(2/2)

- コンセンサスメカニズムについて
  - PoWの課題として「特別仕様のハードウェアが有利な点のほか「マイニングプールの集中化」「エネルギー浪費」が課題。
  - ソリューションとして、PoWをAIアルゴリズム計算に利用しようとするものの他、PoSがあるがPoSにも「Nothing at Stake攻撃」「Long Range攻撃」「カルテル形成」といった課題がある。
- ツールについて
  - 未整備なものが多く、IDEの他、ビルドツール・コンパイラ、デプロイツール、技術ドキュメント、テストフレームワーク、デバッグツール、ロギングツール、セキュリティ監査、ブロックエキスプローラなどが整備要。
- 量子コンピュータ耐性のある暗号
  - 格子暗号の他、多変数暗号・ハッシュベース暗号・コードベース暗号・超特異楕円曲線同種暗号などが考えられる。

→ 出典: https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428

ビットコインとブロックチェーン、分散台帳技術（1/6）

- PoWの計算パワーはビットコインブロックチェーンのセキュリティ上で重要な役割。
  - それは、ビットコインネットワークでは正直な振る舞いが通貨発行益によって動機付けされているためである。重要なポイントは、ナカモトコンセンサスはコンピュータサイエンスではなくゲーム理論により達成されるところにある。

- ビットコインを拠り所として、ビットコインブロックチェーンは分散P2P暗号を用いて仲介人をリプレイスすることが可能としている。
  - ソフトウエアがオープンソースであり参加者はノードを動かしてトランザクションを監査することにより、システムを正直なものに保つことができる。
  - ビットコインの無いブロックチェーンを考えると、ハッシュポインタによりリンクされたブロックリストであり、追記のみ可能なシーケンシャルデータ構造と言える。

- ブロックチェーンは分散化された仮想通貨と組み合わせたときにのみ、ネイティブアセットの通貨発行益を使って分散ネットワークのコンセンサスに必要な経済的インセンティブを提供できて意味をなすものとなる。
  - ネイティブアセットの無いブロックチェーンはマイナーへの報酬を使えないため、指名された機関がトランザクションのバリデータとなるが、中央権威によって任命されるとすれば、通常の共有データベースの代わりにブロックチェーンを使う理由は何処にあるだろうか。

    → 出典：https://t.co/HpDhxuGUo1

ビットコインとブロックチェーン、分散台帳技術（2/6）

- ビットコイン以外にブロックチェーンのリアルなアプリケーションはなかなか見当たらないものの、有望なアプリケーションとしてタイムスタンプを挙げることが出来る。
  - タイムスタンプは、ドキュメントのタイムスタンプや、大きなデータセットのアンカリングを行うもの。
  - データファイルをハッシュして短い識別子を作って、ビットコイントランザクションと組み合わせる。
  - ビットコインの金額と関係無くブロックチェーンに登録できるため、ブロックチェーン上でのハッシュコミットの改ざん困難性によりデータ保有者が後日ハッシュを比較することにより、疑い無しにそのデータが改ざんされてないことが確認できる。
  - ビットコインのブロックチェーンを、プライベートブロックチェーンのためのコンセンサスサービスとして提供するアンカーとして使うことも可能なため、セキュリティをビットコインネットワークにアウトソースする手段としてアンカリング技術を考えることができる。

- DLTについては、プロダクトグレードの実装レファレンスや、厳密な標準技術仕様が現時点で存在しないため、ここでは暗号ツールを使った共有台帳とする。
  - 金融分野の他、サプライチェーン・パワーグリッド管理・土地登記・デジタルアイデンティティなどへのポテンシャルが注目されているものの、DLT向けのリアルなユースケースがあまり無く、解決されるべき実際の問題を探索している段階。

→ 出典：https://t.co/HpDhxuGUo1

ビットコインとブロックチェーン、分散台帳技術（3/6）

- しばしば「DLTによるイノベーションはデータベースを使って中央機関を巻き込んで出来ないのか」と尋ねられるが、そうした場合なぜ彼らが分散技術からメリットを得られるのか分からない。
  - ビットコインはUTXOデータベースをLevelDBを使って実装しているが、ブロックチェーンからナカモトコンセンサスを無くすと残るのは暗号技術を備えたデータベースが残るのみ。
  - ブロックチェーン自体は分散データベースではないので、低レベルなブロックチェーンのデータ構造をデータベースと比較しても意味がない。
  - ブロックチェーンはデータベースのコンセンサスステータスを達成するために用いられるため、ブロックチェーンのアーキテクチャスタックの主要要素としてデータベースは残っている。
  - またノード間で複製を持つためブロックチェーン上に置かれるデータ量はごく僅かに過ぎない。
  - このようにブロックチェーンはデータベースをリプレイスするものではなくCordaもRDBにより支えられている。

→ 出典：https://t.co/HpDhxuGUo1

ビットコインとブロックチェーン、分散台帳技術（4/6）

- ビットコインの台帳はネイティブデジタルアセットをベースとしているが、DLTはネイティブアセットを無くそうとしている。
  - 本来、分散トランザクション経済はネイティブデジタルアセットをペイメントや担保の手段としていて、ブロックチェーンにより誰かの負債をトラッキングしているが、ネイティブキャッシュが無ければ負債だけを抱えることになる。
  - また、台帳上のキャッシュとして価値を持つネイティブアセットが無ければトランザクションのベースとなるDvP（Delivery versus Payment）も実現できない。
  - 加えて、トランザクションの検証をボランティアでやるわけにはいかないので、ネイティブアセットが無ければマイニング報酬を払えずナカモトコンセンサスが実現できない。

- DLTにおけるコンセンサスとして、トランザクションに関わる二者間の同意だけで済ます二者間コンセンサスは論じるまでもないが、これをもってDLTのイノベーションとする意見もある。
  - また、Intel SGXのようにコードやデータを開示や改ざんから守るためEnclavesと呼ばれる保護領域を用いるものもあるが、ハードウェアベースのコンセンサスではハードウェアプロバイダーが中央権威となるためバックドアや不正を調べることが困難となる。
  - このように、プロダクトレベルの分散コンセンサスとしてはナカモトコンセンサスが長らく唯一のものであり、現時点ではその頑健性に迫るものはまだ現れていない。

→ 出典：https://t.co/HpDhxuGUo1

ビットコインとブロックチェーン、分散台帳技術（5/6）

- DLTのベネフィットとして、即時クリアリング・セツルメントは最有望なものとされるものの、その制約となっているのは技術面ではなくリコンサイルプロセスの存在である。
  - またその実現には台帳上のキャッシュがDvP実装のために不可欠だが、台帳上の中央銀行マネーへ直接アクセス可能とすることは、誰もが商業銀行マネーより中央銀行マネーを持ちたがると考えられ、リテール銀行システムに与えるシステミックリスクの面で容易ではない。
  - 加えて、既存インフラへの統合リスクも無視できず、イノベーションのために既存のビジネスプロセスや規制を変更するのと考えるのはあまり現実味が無い。

- DLTにとって現実的なアプローチとして、PoWの代替となるのは中央集権コンセンサス。中央のカウンターパーティとやりとりする上で分散コンセンサスは必要ない。
  - 中央のカウンターパーティがコンセンサスオーソリティとなって、トランザクションの暗号的証明を提供すれば済む。

→ 出典：https://t.co/HpDhxuGUo1

ビットコインとブロックチェーン、分散台帳技術（6/6）

- スマートコントラクトは本来的には、法的システムや人間の介在が必要とされないものであり、ビットコインにはトランザクションを条件付けるスクリプトとして実装されている。
  - これに対してR3のようなDLTでは、企業間の個別同意事項として法的条項を考慮する必要がある他、紛争時にどのように解決するかをコンセンサスシステム以外に必要としているため、本来的な意味とはかけ離れてきている。

- まとめると、ブロックチェーンにはビットコインのようなネイティブデジタルアセットが不可欠であり、それらの無いブロックチェーンを考えるのは難しい。
  - ビットコイン以外のブロックチェーンの用途としてはタイムスタンプやアンカリングが有望。
  - 一方でDLTはディスラプティブとは呼べず、即時セツルメントや中央銀行マネーやスマートコントラクトによる自動化を実現するのは容易ではない。

→ 出典：https://t.co/HpDhxuGUo1

INTEL、PoWのDNA配列決定への応用で特許

- プロセシングパワーをDNAやRNA配列の研究に振り向けるマイナーに対してデジタルアセットを発行するシステム。
- ブロックチェーン上のトランザクション履歴の真正性検証目的だけの計算にあてるだけでなく、DNA配列に関するデータプロセシングにマイナーを使うことによって、PoWマイニングの非効率性を補うことを狙う。
- PoWを生成しつつも、追加で有用なワークも行うという「多目的PoW」としてのコンセンサスメカニズム。

→ 出典：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=20170359374.PGNR.&OS=dn/20170359374&RS=DN/20170359374

IOTAの安全性についてMIT MEDIA LABが反論

- MITテクノロジーレビュー記事に挙げられた「IOTAがビットコインより優れている」とする内容について反論するもの。
- 提携関係
  - IOTAの分散マーケットプレイスへ参加するとされたMicrosoftやCiscoとの関係は不透明なままである。
- 分散性
  - IOTAネットワークは11月に三日をわたり利用不能となっているが、このネットワークはコーディネータに依存しており、単一障害点となっていて分散化されていない。
  - IOTAツリー経路は、IOTAファウンデーションにより運営されるコーディネータノードを通して指示される。IOTAの開発者はユーザーのアカウントから資金を移動可能。
- デバイス上でのPoW
  - ビットコインはマイナーがユーザーのためにPoWを計算するのに対し、IOTAではユーザーが自身のデバイス上でトランザクション毎にPoWするとしているが、デバイス上のPowは21 Incが試みてピボット。
  - ビットコインではトランザクションにワークが必要だが、IOTAトランザクションの方が容易という訳ではない。
- ハッシュ関数の安全性
  - 八月にもMITおよびボストン大学がIOTAで使われるCurlハッシュ関数に脆弱性があると報告した際にも、矛盾した説明がされている。最初はそうした欠陥をコピー保護の意図的なものとして、オープンソースコミュニティに反するものと批判を受けたが、次の説明では自分でCurlを書いてないとしている。

→ 出典：https://www.media.mit.edu/posts/iota-response/

2017 3Qの動向トピック (1/3)

- Bsafe.network、中立な国際学術ネットワークによる実験と評価を行うブロックチェーンLayer 2 Technology Competition開催を発表
  - http://bsafe.network/technology-competiton/leyer2competition/index.html
  - http://bsafe.network/DEV++Announce_Nov32017.pdf
  - https://media.dglab.com/2017/12/28-layer2competition-01/

- ISO/TC307、東京で11/14-17に国際会議開催
  - https://www.iso.org/committee/6266604.html

2017 3Qの動向トピック (2/3)

- 2.0Catapult、クローズドβテストプログラム開始
  - http://mijin.io/ja/1230.html

- ビヨンドブロックチェーン、BBc-1を公開
  - https://prtimes.jp/main/html/rd/p/000000001.000029278.html

2017 3Qの動向トピック (3/3)

- Hewlett Packard Enterprise、BasSプラットフォーム「HPE Mission Critical Blockchain」を発表
  - http://www.ibtimes.co.uk/hewlett-packard-enterprise-introduces-blockchain-service-1646775
- Amazon Web Services（AWS）、ブロックチェーンソリューションの導入を支援するAWS Blockchain Partners Portalを発表
  - http://www.atmarkit.co.jp/ait/spv/1712/22/news083.html
  - https://aws.amazon.com/blogs/apn/introducing-aws-blockchain-partners/
- GMOインターネット、「Z.com Cloud ブロックチェーン」正式版を提供開始
  - https://www.gmo.jp/news/article/?id=5897
- 富士通研究所、ブロックチェーン同士を安全につなげるセキュリティ技術を開発
  - http://pr.fujitsu.com/jp/news/2017/11/15.html

個別トピックリスト① STARTUP

名称	サービス概略	URL
Datum	パーソナルデータのマーケットプレイス	→ https://datum.org/
Databroker DAO	IoTセンサーデータの分散マーケットプレイス	→ https://databrokerdao.com/
Politeia	Decredにより提案されたタイムスタンプ付きファイルシステム	→ https://github.com/decred/politeia/blob/master/README.md
1protocol	余剰のトークンやマシンパワーを拠出して持分とするプロトコル	→ http://1protocol.com/
Ocean	分散データ交換プロトコル	→ https://oceanprotocol.com/
Cosmos	Internet of Blockchainsによりhorizontalなスケーリングを目指す	→ https://cosmos.network/
DFINITY	インテリジェントな分散クラウド構築を目指す	→ https://dfinity.org/

個別トピックリスト① STARTUP

名称	サービス概略	URL
Lambda Protocol	Dapps向け分散アクセス	→ http://lambdaprotocol.io/
Blockchain Interoperability Alliance	AionやICONによる相互運用ワーキング	→ https://blog.aion.network/blockchaininteroperabilityalliance-cf595dd6010
Qlink	WiFiスポットのP2Pシェアリングなど分散モバイルネットワーク	→ https://www.qlink.mobi/f/qlink/
ioNEM	NEMベースのIoTデバイス所有権情報管理	→ https://gitlab.com/nikhiljha/ionem
AlphaPoint Public Network	Intel SGXベースのパブリックブロックチェーンネットワーク	→ https://alphapoint.com/
Auditchain	分散型監査・レポーティングプロトコル	→ https://auditchain.com/

個別トピックリスト① STARTUP

名称	サービス概略	URL
OpenMined Project	準同型暗号やマルチパーティ計算およびブロックチェーンを用いて機械学習モデル訓練むけデータ集中を解決するもの	→ https://openmined.org/
NEM Mosaic Page	NEM Loginと連携して、特定モザイク所有者のみ閲覧できるページを作成できるサービス	→ https://nem-mosaic-page.c-rtx.com/

個別トピックリスト② ENTERPRISE

名称	サービス概略	URL
Verisign	DNSへの応用へ特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html
ソニー	ユーザー認証への応用で特許申請	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2F
Comcast	オペレーションデータ格納の特許	→ 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=20170322992.PGNR.&OS=dn/20170322992&RS=DN/20170322992

個別トピックリスト② ENTERPRISE

名称	サービス概略	URL
VMWare	ブロックチェーンによるデータ移送高速化の特許	→ 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=20170329980.PGNR.&OS=dn/20170329980&RS=DN/20170329980
Wanxian Blockchain	ホワイトペーパー発表	→ https://doc-08-9g-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/kdt80pvtleol4vcruht01vvri9gjhv4q/1512403200000/16849719228147759099/*/1bI7JIOe-CfJ5fPHKxYlFub2Kg-KCGU6r?e=download

4. ライフスタイル分野

① Startup / Dapps
② Enterprise

① STARTUP / DAPPS

名称	サービス概略	URL
IOTA【マッチング・マーケット】	データマーケットプレイスを発表	→ https://blog.iota.org/iota-data-marketplace-cb6be463ac7f
Gnosis【予測市場】	予測市場トーナメントのオフィシャル版Olympia	→ https://olympia.gnosis.pm/markets/list
GiveTrack【寄付】	ビットコイン寄付	→ https://givetrack.org/
CryproKitties【ゲーム】	Etherを使って購入したオリジナルの子猫を飼育することができ、2匹の子猫を交配させることもできるゲーム	→ https://www.cryptokitties.co/
Xarcade【ゲーム】	NEMベースのゲーム配信・交換プラットフォーム	→ https://www.xarcade.io/
SNEMS【コミュ】	メッセージ付きでNEMを送金すると投稿できる無記名掲示板	→ http://tinytintoy.com/snems/
Moneo【マッチング・マーケット】	フリーランスブロックチェーンエンジニアと企業のマッチング	→ https://moneo.io/

① STARTUP / DAPPS

名称	サービス概略	URL
BlockchainTaxi【乗り物】	ドローンタクシーと提携してフライト履歴に基づきタクシーサービス提供	→ https://blockchaintaxi.io/
Pindify【音楽】	音楽・アート・メディアの提供者むけマーケット	→ https://pindex.uci.global/
ODEM【マッチング・マーケット】	生徒と教師を直接結ぶ教育マーケット	→ https://odem.io/
TraDove【マッチング・マーケット】	B2B売買マッチング	→ https://bbcoin.tradove.com/
DNX Community【マッチング・マーケット】	ノマドコミュニティ向けネットワーク	→ https://digitalnomad.community/
ConnectJob【マッチング・マーケット】	労働力のP2Pマーケットプレイス	→ https://ico.connectjob.io/
e-Chat【コミュ】	ペイメント可能なマルチタスクメッセンジャー	→ https://ico.echat.io/?utm_source=echat-io

① STARTUP / DAPPS

名称	サービス概略	URL
Telcoin【コミュ】	モバイルネットワークによる会話と金融包摂	→ https://www.telco.in/
TransCrypt【コミュ】	Telegramメッセンジャーインタフェースのビットコイン送金	→ https://tsrpay.com/ru/
Earn.com【コミュ】	トークンベースのソーシャルネットワーク	→ https://earn.docsend.com/view/f2qmsnm

② ENTERPRISE

名称	サービス概略	URL
ニュージーランド航空【エアライン】	スイストラベルとWinding Tree設立	→ https://www.reuters.com/article/us-blockchain-travel-airnewzealand/air-new-zealand-swiss-travel-platform-winding-tree-in-blockchain-tie-up-idUSKBN1DM2KQ
British Airways【エアライン】	Heathrow空港・Geneva空港・Miami International空港、スマートコントラクトを用いて唯一の真実データの共有コントロールを行うFlightChain構想	→ https://www.sita.aero/resources/type/white-papers/flightchain-shared-control-of-data → https://apex.aero/2017/11/08/flight-data-blockchain-experiment-results-sita

5.サプライチェーン系

① Startup / Dapps
② Enterprise

① STARTUP / DAPPS

名称	サービス概略	URL
Chronicled 【IoT】	zk-snarksによるサプライチェーン向け匿名トランザクション	→ https://www.prnewswire.com/news-releases/chronicled-completes-technical-pilot-demonstrating-cryptographic-anonymous-transfer-of-sgtins-for-supply-chain-applications-300496402.html
Solar Bankers 【エネルギー】	P2Pエネルギートレード	→ https://solarbankers.com/

② ENTERPRISE

名称	サービス概略	URL
BPとRoyal Dutch Shell【エネルギー】	エネルギーコモディティトレーディングのプラットフォーム開発へ	→ http://www.ibtimes.com/bp-shell-plan-blockchain-platform-energy-trading-2611126
UPS【貨物】	Blockchain in Trucking Alliance (BiTA)に加盟	→ https://www.ethnews.com/what-can-brown-do-for-blockchain-ups-joins-blockchain-in-trucking-alliance → https://www.coindesk.com/ups-joins-blockchain-trucking-consortium/
GE【航空機補修部品】	航空機のモニタリング・メンテナンスへむけた特許	→ https://www.coindesk.com/ge-patent-filings-hint-at-blockchain-role-in-aircraft-management/
みずほ、日本郵政、NTT東日本【貿易金融】	登録情報の共有による自動反映	→ http://www.yomiuri.co.jp/economy/20171115-OYT1T50139.html
Bosch【自動車】	オドメーターの改竄防止	→ https://www.bosch-si.com/media/bosch_si/iot_summit/program/bosch_iot_strategy_summit_bosch.pdf

② ENTERPRISE

名称	サービス概略	URL
Emirates Innovation Lab【貨物】	ドバイで航空貨物むけに実証実験	→ https://www.dnata.com/media-centre/dnata-cargo-successfully-tests-the-use-of-blockchain-technology-with-its-programme-partners
イスラエル海運大手ZIM【海運】	船荷証券のペーパーレス化へWaveと協業	→ http://www.zim.com/newsandpress/recentnews/pages/zim-block-chain-technology.aspx
De Beers【貴金属】	ダイヤモンドのトラッキングプラットフォーム開発へ	→ http://www.debeersgroup.com/en/news/views/expectations-changing-changing-expectations--diamond-traceabilit.html
ユニリーバ、セインズベリー【食品】	BNP Paribas・Barclays・Standard Charteredとマラウイ共和国からの紅茶サプライチェーンのトラッキングを実証	→ https://www.cisl.cam.ac.uk/business-action/sustainable-finance/banking-environment-initiative/news/blue-chips-and-startups-launch-new-fintech-pilot
商船三井【海運】	SMBC等とクロスボーダートレードをHyperledger Fabricで実施	→ http://www.mol.co.jp/en/pr/2017/17090.html
楽天【エネルギー】	エネルギークレジット取引システム	→ https://corp.rakuten.co.jp/news/press/2017/1211_02.html

6. シビックテック系

① Startup / Dapps
② Government / Enterprise

① STARTUP / DAPPS

名称	サービス概略	URL
IPFS【公的証明】	カタルーニャ独立運動の国民投票アナウンス	→ http://www.ibtimes.co.uk/catalonia-looks-estonias-e-residency-considers-cryptocurrency-option-1644838
Karpersky LabとParity Technologies【投票】	投票システムを開発	→ https://bitcoinmagazine.com/articles/kaspersky-lab-and-parity-technologies-launch-blockchain-based-voting-system/
uPort【アイデンティティ】	スイスZug向けデジタルアイデンティティ	→ https://medium.com/uport/first-official-registration-of-a-zug-citizen-on-ethereum-3554b5c2c238
SecureKey Technologies【アイデンティティ】	デジタルアイデンティティを開発中	→ https://www.bloomberg.com/news/articles/2017-11-14/forget-iris-scans-canadians-to-use-blockchain-for-digital-ids
Smart One	クリプトコミュニティ向けリーガルソリューション	→ https://smartone.legal/

① STARTUP / DAPPS

名称	サービス概略	URL
MintHealth【医療情報】	患者主体の医療データコントロールを目指すパーソナルヘルスデータ管理	→ https://www.vidamints.com/
Health Wizz【医療情報】	電子医療レコードのアグリゲート	→ https://www.healthwizz.com/
Mudasium【不動産】	不動産プロパティ管理	→ http://midasium.herokuapp.com/
REALISTO【不動産】	投資プロジェクトをトークン化する不動産投資プラットフォーム	→ https://realisto.io/
Guardian	仮想通貨の税務サポート	→ https://www.aerial-p.com/guardian/

② GOVERNMENT / ENTERPRISE

名称	サービス概略	URL
米国疾病予防管理センター【医療情報】	IBMと医療分野の応用で提携	→ https://www.ethnews.com/cdc-ibm-watson-health-to-explore-medical-blockchain-applications
英国法務省【公的証明】	犯罪の証拠をブロックチェーンに記録する提案	→ https://btcnews.jp/2b5pcixh13471/
米国州政府医療機関連盟【医療情報】	医療教育証明書発行のパイロット実施	→ http://www.learningmachine.com/case-studies-fsmb
MIT【公的証明】	ビットコインブロックチェーンを用いた卒業証書を授与	→ http://web.mit.edu/registrar/records/certs/digital_faqs.html
Samsung【電子行政】	ソウル市向けにNexledger構想	→ https://image.samsungsds.com/global/en/support/resources/__icsFiles/afieldfile/2017/08/09/Samsung_SDS_Nexledger_Blockchain_Platform_and_Solutions_v1.3_170808.pdf
バミューダ【不動産】	土地登記システムを計画	→ https://www.coindesk.com/bermuda-launch-blockchain-land-registry/

② GOVERNMENT / ENTERPRISE

名称	サービス概略	URL
Nokia【医療情報】	ヘルスケアデータの格納にむけたパイロット実施	→ https://blog.networks.nokia.com/mobile-networks/2017/11/30/time-give-people-control-health-data-blockchain/
モスクワ【投票】	EthereumによるPoAベースの投票システムのパイロットを発表	→ https://www.ethnews.com/moscows-ethereum-voting-system-launches
エストニアe-Residency【電子行政】	Estcoin立ち上げ準備を進めていることを表明	→ https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790
エストニア	豪州LaborX社とTokenEST発行を計画	→ https://www.ethnews.com/estonia-plans-to-engage-in-state-sponsored-token-offering
カナダ政府	研究機関NRCの助成金や資金調達の透明化へ応用	→ https://globalnews.ca/news/3977745/ethereum-blockchain-canada-nrc/
国連	温暖化対策へ向けてClimate Chain Coalition (CCC)立上	→ https://cop23.unfccc.int/news/un-supports-blockchain-technology-for-climate-action

7.金融機関系の動き

① 金融機関
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

①金融機関 – 日本(1/2)

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/0000000162579.html

①金融機関 – 日本(2/2)

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

①金融機関 – 海外銀行業界(1/4)

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

①金融機関 – 海外銀行業界(2/4)

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
クレディセゾンなど	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

①金融機関 – 海外銀行業界(3/4)

名称	サービス概略	URL
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/
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
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/
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/

①金融機関 – 海外銀行業界(4/4)

名称	サービス概略	URL
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/
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
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
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/
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/

①金融機関 – 海外証券業界(1/3)

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
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/
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

①金融機関 – 海外証券業界(2/3)

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
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
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/
UCバークレー	分散取引所のリサーチてKyberNetworksと協業	→ https://blockchain.berkeley.edu/

①金融機関 – 海外証券業界(3/3)

名称	サービス概略	URL
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

①金融機関 – 海外カード業界

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

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 – 北南米

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
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

②規制・制度 – 欧州

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
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

②規制・制度 – 欧州

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
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
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/

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 – 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 – 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 – アジア

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
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
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
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/

②規制・制度 – アジア

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
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
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

②規制・制度 – アフリカ他

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
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

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 – 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/

④ICO – 日本

名称	サービス概略	URL
日本	多摩大学、三メガバンクと共同でICOビジネス研究会を発足	→ https://prw.kyodonews.jp/opn/release/201711017492/ → http://www.tama.ac.jp/topics/news/2017/11/ico-initial-coin-offering-20ico.html
日本	JCBA（日本仮想通貨事業者協会）、ICOに関する考え方・指針を発表	→ https://cryptocurrency-association.org/cms2017/wp-content/uploads/2017/12/20171208_01.pdf

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 → https://lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/virtual-currency-orders-issued-against-plexcorps-plexcoin-dl-innov-inc-gestio-inc-and-dominic/
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-

④ICO – 米国以外

名称	サービス概略	URL
シンガポール	MAS、A Guide to Digital Token Offeringsを発表	→ http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20%2014%20Nov%202017.pdf
ドイツ	BaFin、ICO注意喚起を発表	→ https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Meldung/2017/meldung_171109_ICOs_en.html
オランダ	AFM、ICO注意喚起を発表	→ https://www.ethnews.com/dutch-markets-authority-chair-warns-against-token-offering-investment
欧州	ESMA、ICO注意喚起を発表	→ https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf
イスラエル	イスラエル税務当局、ICOへのVAT課税へむけたドラフト案を発表	→ https://taxes.gov.il/incometax/documents/hozrim/hoz_xx_2018_acc.docx.pdf → https://www.ccn.com/the-holy-land-to-impose-ico-tax/
国際機関	IOSCO（証券監督者国際機構）、ICO関連リスクについて投資家へ警告	→ https://www.iosco.org/news/pdf/IOSCONEWS485.pdf

⑤中央銀行・デジタル法定通貨 – 欧州

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/
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/

⑤中央銀行・デジタル法定通貨 – アジア・中東

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
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

⑤中央銀行・デジタル法定通貨 – 南米

名称	サービス概略	URL
ベネズエラ	原油を裏付けとした暗号通貨Petroを発表	→ https://www.reuters.com/article/us-venezuela-economy/enter-the-petro-venezuela-to-launch-oil-backed-cryptocurrency-idUSKBN1DX0SQ → https://af.reuters.com/article/africaTech/idAFL1N1OS1GY
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/

8.金融系スタートアップの動き

① 個別サービスリスト

個別サービスリスト（1/3）

名称	サービス概略	URL
R3	Corda上での国際ペイメントソリューション開発	→ https://www.r3.com/blog/2017/10/31/r3-and-22-banks-build-real-time-international-payments-solution-on-corda-dlt-platform/
Stratumn	欧州系保険会社14社と保険会社切り替え規制対応プロセスの実証実験	→ http://stratumn.com/press/ffa-blockchain-network-insurance/
Square	ビットコイン売買をテスト中	→ https://www.reuters.com/article/us-square-bitcoin/payments-company-square-tests-bitcoin-buying-and-selling-idUSKBN1DF2N6?il=0
Coinbase	機関投資家むけストレージCoinbase Custodyを発表	→ https://custody.coinbase.com/
R3	Corda、AWS上で利用可能に	→ https://www.r3.com/blog/2017/12/05/r3s-corda-becomes-one-of-the-first-dlt-platforms-available-on-aws-marketplace/
PUBLIC FUND	NPO向けICO支援プラットフォーム	→ http://public.fund/

個別サービスリスト（2/3）

名称	サービス概略	URL
Basecoin	為替安定を追求した Stablecoin	→ http://www.getbasecoin.com/
MakerDAO	分散Stablecoin“Dai”を発表	→ https://makerdao.com/
dYdX	分散デリバティブプロトコル	→ https://dydx.exchange/
Radar Relay	アカウント開設や他人のトラスト無しに暗号通貨取引を可能に	→ https://radarrelay.com/
Paradex	0xプロトコルを使ってERC20トークンをウォレット上で取引可能に	→ https://paradex.io/
Kyber Networks	オンチェーンによる為替・ペイメント向け流動性提供プラットフォーム	→ https://kyber.network/
AirSwap Token Trader	Ethereum版ShapeShift	→ https://blog.airswap.io/introducing-the-airswap-token-trader-c97a840bd82d
NaPoleonX	分散自律ファンド管理	→ https://www.napoleonx.ai/#about-anchor
CoinLoan	P2Pローンのレンディングプラットフォーム	→ https://coinloan.io/
Etherisc	分散型保険	→ https://etherisc.com/

個別サービスリスト （3/3）

名称	サービス概略	URL
ARC Reserve Currency	法定通貨や現物資産価格をトラッキングするStablecoin	→ http://www.arccy.org/
Aurus	ゴールドに裏付けされたトークン	→ http://aurus.io/
Nivaura	ETHによる社債発行	→ https://www.coindesk.com/who-needs-a-csd-nivaura-to-issue-first-regulated-bond-in-ethereum/
G-Tax	仮想通貨の売買損益を計算できるサービス	→ https://crypto-city.net/
SALT	トークンを担保とした法定通貨の貸与	→ https://www.saltlending.com/
Jibrel Network	法定通貨および金融商品のトークン化	→ https://jibrel.network/
ETHLend	借り手と貸し手をつなぐプラットフォーム	→ https://ethlend.io/en/
ZigZag	Lightning Networkを用いてビットコインと他暗号通貨を交換可能とするデジタルアセット取引プラットフォーム	→ http://zigzag.bitlum.io/
TrueCoin	米ドルをバックとしたStablecoin	→ https://truecoin.com/

10.参考資料リンク集

① 教材リスト
② 統計情報
③ 技術解説（Bitcoin）
④ 技術解説（Ethereum）
⑤ Scaling Bitcoin
⑥ DevCon
⑦ ICO関連
⑧ 技術解説（ILP）
⑨ 技術解説（NEM）
⑩ 仮想通貨関連
⑪ 中央銀行関連
⑫ ブロックチェーン技術横断
⑬ 応用むけレポート

①教材リスト

- BITCOIN RESOURCES
  - https://lopp.net/bitcoin.html
- Bitcoin Edge Workshops
  - https://bitcoinedge.org/tutorials
  - 2017年11月のScalingBitcoin前にStanfordで開催されていたワークショップの模様が動画公開
- The Internet of Money Volume 2
  - https://www.youtube.com/playlist?list=PLPQwGV1aLnTu0KFDbHk4AUiiyce0xLX7p
  - https://www.goodreads.com/book/show/36804136-the-internet-of-money-volume-two
- Sixty free lectures from Princeton on bitcoin and cryptocurrencies
  - https://www.reddit.com/r/Bitcoin/comments/7m0gu3/sixty_free_lectures_from_princeton_on_bitcoin_and/

①教材リスト

- Deep Dives - Blockchain at Berkeley Research and Development
  - https://docs.google.com/document/d/12w7rAEQUSFd6NbLr6dUxJcLbF70YHcnzhG6mHZQjYCA/edit
- おすすめの暗号通貨系YouTubeチャンネル、ポッドキャスト（英語）
  - http://individua1.net/recommendable-cryptocurrency-youtube-channel-podcast/
- Banking On Bitcoin - Full Documentary Film
  - https://youtu.be/7Jts0OMAhTw
- Learning Bitcoin From Command Line
  - https://github.com/ChristopherA/Learning-Bitcoin-from-the-Command-Line
- Mastering Ethereum、GitHubにコンテンツ
  - https://github.com/ethereumbook/ethereumbook/blob/develop/README.md

②統計情報

- Johoe's Mempool Statistics
  - https://jochen-hoenicke.de/queue/#3m
- Cryptocompare
  - https://www.cryptocompare.com/coins/btc/analysis/USD
- Segwit導入状況
  - http://segwit.party/charts/
- Bitcoin Energy Consumption Index
  - https://digiconomist.net/bitcoin-energy-consumption
- Coindesk State of Blockchain Q3 2017
  - https://www.coindesk.com/coindesk-state-of-blockchain-q3-2017/

②統計情報

- Charts from the Ethereum Network
  - https://www.etherchain.org/charts
- Top 10 ETH Contracts By Transaction Count Over Last 1,500 Blocks
  - https://ethgasstation.info/gasguzzlers.php
- Four Years of Token Sales, Visualized in One Graphic
  - https://elementus.io/blog/token-sales-visualization/
- Ethereum Transaction Growth Chart
  - https://etherscan.io/chart/tx
- Ethereum ChainData Size Growth
  - https://etherscan.io/chart/chaindatasizefull

②統計情報

- Cryptocurrency charts
  - https://bitinfocharts.com/cryptocurrency-charts.html
- Percentage of Total Market Capitalization (Dominance)
  - https://coinmarketcap.com/charts/
- Ethereum blockchain visualization
  - http://ethviewer.live/
- State of the DApps - A curated list of 912 decentralized apps built on ethereum
  - https://www.stateofthedapps.com/
- Cryptoacademia / Comprehensive collection of papers and other resources compiled and managed by Blockchain at Berkeley
  - https://drive.google.com/drive/mobile/folders/0B7TsBdkClBm1c3lzaHBneEt1dU0

②統計情報

- OP_RETURN Statistics
  - https://p2sh.info/dashboard/db/op_return-statistics
- Bitnodes - Blocks Propagation
  - https://bitnodes.earn.com/dashboard/?days=730
- Bitcoin Hashrate
  - http://bitcoin.sipa.be/
- Mt Gox Chart
  - https://bitcoincharts.com/charts/mtgoxUSD
- Ethereum Pending Transactions
  - https://etherscan.io/chart/pendingtx

②統計情報

- Cryptoasset rankings &metrics for investors
  - https://onchainfx.com/v/1Edfgw
- Bitcoin Cash Accepting Stores in Tokyo
  - https://docs.google.com/spreadsheets/d/1XRdgqMHzZXtvhz-y6PEAh0uU8vzbG2xne6jtPSeptfA/htmlview
- LNMainnet
  - https://lnmainnet.gaben.win/#
- Lightning Network Statistics
  - http://lnstat.ideoflux.com:3000/dashboard/db/lightning-network?refresh=5m&orgId=1
- ビットコイン相場.com
  - http://xn--eck3a9bu7cul981xhp9b.com/

③技術解説（BITCOIN）

- Lightning Network入門
  - https://www.slideshare.net/mobile/takashimitsuta/lightning-network-82041404
- Mimblewimbleホワイトペーパー解説
  - https://www.slideshare.net/mobile/takayaimai/mimblewimble
- Merkle Treeの重複エントリー問題の解消とパフォーマンスを向上するFast Merkle Treeについて定義したBIP-98
  - http://techmedia-think.hatenablog.com/entry/2017/11/16/224259
- ビットコインをスケールさせる新しいデータ構造「MAST」とは
  - https://zoom-blc.com/what-is-bitcoin-mast
- MASTを実現するMERKLEBRANCHVERIFYを定義したBIP-116
  - http://techmedia-think.hatenablog.com/entry/2017/11/17/211150

③技術解説（BITCOIN）

- Lightning Networkを実際に体験してみよう
  - https://youtu.be/YIgcuprvuos

- Lightning Networkの仕様BOLT解説
  - http://blog.nayuta.co/blockchain/2017/11/24/ln000-basis-of-lightning-technologyboltについて/
  - http://blog.nayuta.co/blockchain/2017/11/24/ln002-noise-protocol/
  - http://blog.nayuta.co/blockchain/2017/11/24/ln003init/
  - http://blog.nayuta.co/blockchain/2017/11/27/ln004鍵/
  - http://blog.nayuta.co/blockchain/2017/11/29/ln005establish-channel-前半/
  - http://blog.nayuta.co/blockchain/2017/12/01/ln006establish-channel-後半/
  - http://blog.nayuta.co/blockchain/2017/12/04/ln007%e9%80%81%e9%87%91-1/
  - http://blog.nayuta.co/blockchain/2017/12/06/ln008送金-2/
  - http://blog.nayuta.co/blockchain/2017/12/08/ln009送金-3/

- シュノア署名がビットコインのスケーラビリティ問題に与える衝撃
  - https://zoom-blc.com/schnorr-signature

③技術解説（BITCOIN）

- Bitcoinマイニングにおけるハッシュレートと収益の歴史
  - https://medium.com/@minecc/bitcoinマイニングにおけるハッシュレートと収益の歴史-as-of-11-27-2019-c023844d83d
- Bitcoin Cash上でネイティブにカラードコインをサポートするOP_GROUP
  - http://techmedia-think.hatenablog.com/entry/2017/11/30/230017
  - https://github.com/BitcoinUnlimited/BUIP/blob/master/077.mediawiki
- 任意のデータに対する署名検証を行うOP_DATASIGVERIFY（BUIP-78）
  - http://techmedia-think.hatenablog.com/entry/2017/12/01/192732
- AsicBoostとSegwitの関係
  - https://techblog.picappinc.jp/asicboostとsegwitの関係-56a7c8429341
- The case for increasing Bitcoin's block weight limit
  - http://blog.zorinaq.com/block-increase-needed/

③技術解説（BITCOIN）

- サイドチェーンにBitcoinをペグしてみる。
  - http://techmedia-think.hatenablog.com/entry/2017/12/11/232023
- ElementsでConfidential Transactionを作ってみる
  - http://techmedia-think.hatenablog.com/entry/2017/12/13/184006
- BOLTのこと 1
  - https://qiita.com/nayuta-ueno/items/3992bcc27b6b74b2646d
- Bitcoin Lightning Network FAQ
  - https://cryptoinsider.21mil.com/bitcoin-lightning-network-faq/
- ブロックチェーンの新たな言語　Simplicityの論文を読む　?Core Simplicity編?
  - https://recruit.gmo.jp/engineer/jisedai/blog/simplicity-a-new-language-for-blockchains-core-simplicity/

③技術解説（BITCOIN）

- ビットコイン開発の今後とCBOE, CMEビットコイン先物の詳細
  - https://ethereum-japan.net/bitcoin/lightning-network-and-bitcoin-future/
- SegWitの普及が進まない理由と考えられる対策
  - http://coinandpeace.hatenablog.com/entry/segwit_low_penetration
- ウォレットの概要とHDウォレットの仕組み
  - http://blockchain.gunosy.io/entry/2017/12/21/165314
- 【暗号通貨輪読会#14】confidential transaction
  - https://www.slideshare.net/mobile/hawinternational/14confidential-transaction

③技術解説（BITCOIN）

- Mimblewimble with Andrew Poelstra
  - https://moneromonitor.com/episodes/2017-12-05-Episode-016.html
- Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa
  - ビットコインマイニング消費電力と各国消費電力の比較
  - https://powercompare.co.uk/bitcoin/
- Schnorrベースのマルチシグネチャスキーム「MuSig」
  - https://blockstream.com/2018/01/23/musig-key-aggregation-schnorr-signatures.html
  - http://techmedia-think.hatenablog.com/entry/2018/01/25/125426
- ビットコインの最適な取引手数料を決める方法
  - http://www.jpbitcoinblog.info/entry/20171230/1514617969

③技術解説（Bitcoin）

- LND Developer Site | Lightning Network Developers
  - http://dev.lightning.community/
  - http://dev.lightning.community/overview/

- A curated list of awesome Lightning Network resources, apps, and libraries
  - https://github.com/bcongdon/awesome-lightning-network/blob/master/readme.md#lightning-network-protocol

- What is the Bitcoin Lightning Network? A Beginner’s Explanation
  - https://99bitcoins.com/what-is-the-bitcoin-lightning-network-a-beginners-explanation/

- The Lightning Network
  - https://blog.bitmex.com/the-lightning-network/

③技術解説（Bitcoin）

- Bisq - A decentralized bitcoin exchange
  - https://docs.google.com/presentation/d/14yTWXvevSTAedFaKYbPjtgyR0J_ejjJQVdJlWj9_9bo/mobilepresent?slide=id.p
- Lightning App Directory
  - http://dev.lightning.community/lapps/
- A Tale of Two Bitcoins
  - https://vinnylingham.com/a-tale-of-two-bitcoins-20375d49d3d3
- Why Scaling Bitcoin With Sharding Is Very Hard
  - https://petertodd.org/2015/why-scaling-bitcoin-with-sharding-is-very-hard
- Transcript: Mimblewimble and scriptless scripts from RealWorldCrypto 2018
  - http://diyhpl.us/wiki/transcripts/realworldcrypto/2018/mimblewimble-and-scriptless-scripts/

④技術解説（ETHEREUM）

- Ethereumはどのように動いているのか
  - http://coffeetimes.hatenadiary.jp/entry/2017/11/07/082426
- 「Ethereum in 25 minutes」でワールドコンピュータを理解する
  - http://individua1.net/vitaliks-ethereum-25-minutes-2017/
- 【比較アルゴリズム論】PoWとPoSの違い -ブロック生成者編-
  - http://individua1.net/comparative-algorithm-pow-pos-miner-and-validator/
- Ethereum PoSアルゴリズム「Casper」6つの設計原理
  - http://individua1.net/ethereum-pos-casper-6-design-principles/
- EthereumのPoS「Casper」の概要をまとめてみる
  - http://individua1.net/overview-of-ethereum-pos-casper/

④技術解説（ETHEREUM）

- オフチェーン処理の要「ステートチャネル」の概要を掴む
  - http://individua1.net/state-channel-general-form-of-payment-channel/
- アトミックスワップを実例を用いて紹介する
  - http://individua1.net/explanation-of-atomic-swaps-with-actual-case/
- プラズマがイーサリアムのスケーラビリティ問題を解決する理由と仕組み
  - https://zoom-blc.com/plasma-ethereum
- Casper FFGはプロトコル内で機能するバリデーターをどのように扱うか？ ~Dynamic Validator Setsの仕組み~
  - http://individua1.net/casper-ffg-dynamic-validator-sets/
- 【比較アルゴリズム論】PoWとPoSの違い -ブロック生成者編-
  - http://individua1.net/comparative-algorithm-pow-pos-miner-and-validator/

④技術解説（ETHEREUM）

- オフチェーンとは？
  - https://ethereum-japan.net/wiki/off-chain/
- プラズマとは？
  - https://ethereum-japan.net/wiki/plasma/
- マイクロライデンとは？
  - https://ethereum-japan.net/wiki/microraiden/
- 「zk-SNARK」とは
  - https://zoom-blc.com/what-is-ethereum-zk-snark
- ブロックチェーンのスケーラビリティ問題に対する１１の解決策
  - https://zoom-blc.com/blockchain-scalability

④技術解説（ETHEREUM）

- 分散型アプリケーションプラットフォーム「EOS」
  - https://zoom-blc.com/what-is-eos
- 0xがJavascriptライブラリー「0x Connect」をリリース
  - http://individua1.net/javascript-library-0x-connect/
- 創設者による「Ethereum in 25 minutes」でワールドコンピュータを理解する
  - http://individua1.net/vitaliks-ethereum-25-minutes-2017/
- Ethereumはどのように動いているのか
  - http://coffeetimes.hatenadiary.jp/entry/2017/11/07/082426
- イーサリアムの不変条件から考察するハードフォーク
  - https://ethereum-japan.net/ethereum/consider-variants-to-parity-hardfork/

④技術解説（ETHEREUM）

- Ethereum上で猫を育てる「CryptoKitties」最高落札額は1300万円、運営報酬は2100万円 仕組みとビジネスモデル
  - http://individua1.net/ethereum-cryptokitties-business-model/

- 仮想仔猫ゲーム CryptoKitties のコントラクトを読んでみる
  - https://qiita.com/blueplanet/items/fa005a1c9457169a7391

- スマートコントラクトによるDapp（分散型アプリケーション）の５つの課題点
  - https://zoom-blc.com/dapps-and-smart-contracts

④技術解説（ETHEREUM）

- 【イーサリアムとは？総まとめ】仮想通貨/ブロックチェーン技術仕組み/変遷
  - https://consensysmediajapan.com/3429.html
- シャーディングがイーサリアムのスケーラビリティ問題を解決する理由
  - https://zoom-blc.com/sharding-ethereum
- 仮想子猫経済を支える ERC721
  - https://m0t0k1ch1st0ry.com/blog/2017/12/19/erc721/
- 【DEXとは】イーサリアムベースの仮想通貨取引システム(分散型取引所)
  - https://consensysmediajapan.com/3357.html
- 0xProtocolの事例から見る現状のDappsスケール手法
  - https://qiita.com/syrohei/items/04d2a7d695b2cf76f622

④技術解説（ETHEREUM）

- 分散型取引所(DEX)で高速かつ安価な取引を目指す「0xプロジェクト」とは
  - https://zoom-blc.com/what-is-0x-project-for-dex

- Bancor プロトコル:Smart Tokenの革新性とは。「Coincidence of Wantsの解決」とそれがもたらす「取引の再発明」
  - https://qiita.com/ABmushi/items/e0886421617d4632c42b

④技術解説（ETHEREUM）

- How does Ethereum work, anyway?
  - https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369
- Ethereum Casper 101
  - https://medium.com/@jonchoi/ethereum-casper-101-7a851a4f1eb0
- Ethereum Sharding: Overview and Finality
  - https://medium.com/@icebearhww/ethereum-sharding-and-finality-65248951f649
- Life Cycle of an Ethereum Transaction
  - https://medium.com/blockchannel/life-cycle-of-an-ethereum-transaction-e5c66bae0f6e

④技術解説（ETHEREUM）

- Notes on Blockchain Governance | Vitalik Buterin's website
  - http://vitalik.ca/general/2017/12/17/voting.html
- Sharding FAQ
  - https://github.com/ethereum/wiki/wiki/Sharding-FAQ
- What is Ethereum Casper Protocol? Crash Course
  - https://blockgeeks.com/guides/ethereum-casper/
- Ethereum and Scalability Technology（Sharding）
  - http://unitimes.media/file/pdf/02-Ethereum-and-Scalability-Technology(Sharding).pdf
- Introduction to Quorum: Blockchain for the Financial Sector
  - https://blockchainatberkeley.blog/introduction-to-quorum-blockchain-for-the-financial-sector-58813f84e88c

⑤Scaling Bitcoin

- ScalingBitcoin
  - https://bitconseil.fr/scaling-bitcoin-synthese-partie-1/
  - https://bitconseil.fr/scaling-bitcoin-synthese-2-scalabilite/

⑥DevCon

- Ethereum Devcon3
  - https://blog.ethereum.org/2017/11/16/devcon3/
  - https://tokeneconomy.co/token-economy-21-the-post-devcon3-edition-f87b4b715e3b
  - https://medium.com/@brandon.obrien/ethereum-devcon3-summary-day-4-a5e87829164e
  - https://medium.com/@brandon.obrien/ethereum-devcon3-summary-day-3-c374c1dd9f48
  - https://medium.com/@brandon.obrien/ethereum-devcon3-summary-day-2-b45832d7d748
  - https://techburst.io/ethereum-devcon3-summary-day-1-1de50737d40
  - https://qz.com/1126398/inside-devcon3-the-euphoric-gathering-for-ethereum-diehards/
  - https://a16z.com/2017/11/24/devcon3-notes/
  - https://drive.google.com/file/d/1i-8dSXgg25tDNjQgIOSmdxS4jnZx8Ba1/view
- Devcon3、セッション別ビデオ動画を公開
  - https://blog.ethereum.org/2017/11/26/devcon3-vids-available-now/

⑦ICO関連

- ICOマーケットウォッチ「2017年ICO市場分析」
  - http://cryptocoinportal.jp/market-watch/icoanalysis/
- icoトークンセールの正体
  - https://www.slideshare.net/masamasujima/ico-82137906
- ICOと日本法
  - http://www.so-law.jp/pdf/171026.pdf
- ICOの法的整理
  - http://www.so-law.jp/wp-content/uploads/2018/01/180104_ICOの法的整理.pdf
- ICO時代の新しい企業のカタチ「自壊企業」
  - http://jp.techcrunch.com/2017/12/28/2017-12-26-this-company-will-self-destruct-after-its-ico/

⑦ICO関連

- Q3 2017 in Review: New Records and Competing Trends in an Evolving Market
  - https://www.smithandcrown.com/q3-2017-review-new-records-competing-trends-evolving-market/
- Observations on the Geography of Token Sales
  - https://www.smithandcrown.com/observations-geography-token-sales/
- Initial Coin Offerings - A strategic perspective: Global and Switzerland
  - https://cryptovalley.swiss/wp-content/uploads/20171221_PwC-S-CVA-ICO-Report_December_final.pdf
- Revisiting The DAO
  - https://blog.bitmex.com/revisiting-the-dao/

⑦ICO関連

- NOT SO FAST—RISKS RELATED TO THE USE OF A “SAFT” FOR TOKEN SALES
  - https://cardozo.yu.edu/sites/default/files/Cardozo%20Blockchain%20Project%20-%20Not%20So%20Fast%20-%20SAFT%20Response_final.pdf
- Overview of ICO regulation in different counties
  - https://en.bitnovosti.com/2018/01/17/overview-of-ico-regulation-in-different-countries/
  - https://en.bitnovosti.com/2018/01/18/overview-of-ico-regulation-in-different-counties-chapter-2-middle-east-usa-uk/
- ICO関連の各国声明リスト
  - http://www.iosco.org/publications/?subsection=ico-statements
- Bitcoin, Blockchain & Initial Coin Offerings
  - 英国ピンセントメイソンズ法律事務所による各国の規制動向まとめ
  - https://www.pinsentmasons.com/PDF/2017/FinTech/Bitcoin-Blockchain-guide.pdf

⑦ICO関連
GDAX Digital Asset Framework

- Coinbaseが運営する取引所であるGDAXが示しているデジタルアセット取扱の枠組み。
- 1. ミッションおよび価値観（当該デジタルアセットが我々のミッションや価値観と合致するか）
  - 1.1 オープンな金融システム（皆に利用可能であり且つ単一主体によりコントロールされていない）
    - 1.1.1 イノベーション又は効率性向上（問題解決や新たな市場創造、市場ニーズとの不整合解決、ネットワーク参加者への価値創造）
    - 1.1.2 経済的自由（社会のメンバーが当該経済に容易に参加可能。個人が自身の富や資産をコントロール可能。消費や生産や投資を選択する自由）
    - 1.1.3 機会の平等（スマホやインターネットを通じて誰もがアクセス可能）
    - 1.1.4 非中央集権（ネットワークがパブリックであり、非中央集権であり、且つトラストレスなコンセンサスを可能とする）

→ 出典：https://www.gdax.com/static/digital-asset-framework-2017-11.pdf

⑦ICO関連
GDAX Digital Asset Framework

- 2. テクノロジー（アセットおよびネットワークのアセスメント）
  - 2.1 セキュリティおよびコード（エンジニアリングおよびプロダクト品質のアセスメント）
    - 2.1.1 ソースコード（オープンソースのコード、ドキュメントのピアレビュー、開発チームと独立した貢献者によるテスト）
    - 2.1.2 プロトタイプ（テストネット或いはメインネット上にアルファ版またはベータ版が存在）
    - 2.1.3 セキュリティ（脆弱性開示後のコード改善、バグバウンティプログラム、第三者によるセキュリティ監査）
  - 2.2 チーム（短期的な運営および意思決定のアセスメント）
    - 2.2.1 ファウンダーとリーダーシップ（ビジョンや戦略・ユースケースを描いて開発をドライブでき、経験の記録をトラック可能）
    - 2.2.2 エンジニアリング（エンジニアチームのアセスメントおよびチームのデッドライン設定・達成の記録のトラッキング）
    - 2.2.3 ビジネスおよびオペレーション（コミュニティとのやりとりの履歴、リーズナブルな予算と資金の管理、プロジェクトマイルストーンの達成。キャッシュマネジメントはプロジェクトの長期的成功における主要ドライバー）
    - 2.2.4 特殊知識および主要人物（プロジェクトリーダーシップが集中しておらず少数の主要人物に依存しない。専門知識が少数グループに限定されない）
  - 2.3 ガバナンス（長期的な運営および意思決定のアセスメント）
    - 2.3.1 コンセンサスプロセス（コードのメジャーアップデートの提案・実装にむけた構造的プロセスの存在、或いは衝突解消にむけたシステムまたは投票プロセスの存在）
    - 2.3.2 将来の開発資金（将来的開発にむけて資金調達・報酬・資金割当の計画またはビルトインメカニズムが存在）
    - 2.3.3 ホワイトペーパー（分散ネットワークのユースケースを正当化し、事業および技術的観点からプロジェクトゴールを示すものであり、プロジェクト理解に重要ではあるが、要件ではない）

→ 出典：https://www.gdax.com/static/digital-asset-framework-2017-11.pdf

⑦ICO関連
GDAX Digital Asset Framework

- 2. テクノロジー（アセットおよびネットワークのアセスメント）
  - 2.4 スケーラビリティ（スケーリングへむけたネットワークの潜在的障壁およびユーザーアドプションの拡大・ハンドリング能力のアセスメント）
    - 2.4.1 ロードマップ（開発ステージのタイムライン、プロジェクトマイルストーン、或いはビルトインされた開発インセンティブ）
    - 2.4.2 ネットワーク運営コスト（ネットワークのスケーリングへむけた障壁が特定され、そのソリューションが提案されている。バリデータやマイナーにとってリソース消費が参加の主たる抑制とならない）
    - 2.4.3 実用的アプリケーション（現実世界における実装例或いは将来的な実用アプリケーションがある）
    - 2.4.4 ブロックチェーンの種類（アセットは新しいアーキテクチャのシステムやネットワークを伴う別のブロックチェーンである。またはシナジーやネットワーク効果において既存ブロックチェーンを利活用する）
- 3. リーガルおよびコンプライアンス（法規制およびコンプライアンス面のベストプラクティス）
  - 3.1 規制（当該アセットを合法的に提供可能か）
    - 3.1.1 米国証券法（当該アセットは証券として分類されない）
    - 3.1.2 コンプライアンス義務（アンチマネロンや送金ライセンスなどの遵守義務に抵触しない）
  - 3.2 整合性および評判リスク（当該アセットの上場がポリシーと不整合を来さないか）
    - 3.2.1 ユーザーの同意（アセットやネットワークが禁止事項に抵触しない）

→ 出典：https://www.gdax.com/static/digital-asset-framework-2017-11.pdf

⑦ICO関連
GDAX Digital Asset Framework

- 4. マーケットサプライ（価格操作リスクを制限する上でどのメトリクスを考慮することが重要か）
  - 4.1 流動性標準（当該アセットはどれだけ流動性があるか）
    - 4.1.1 グローバルマーケット資本（他アセットのマーケット資本と比較してどうか）
    - 4.1.2 アセット流通速度（取引速度は当該アセットがどれだけ容易に他アセットと交換できるがを示す指標となる）
    - 4.1.3 発行量（新規発行はコンセンサスプロトコルを通じて行われる。供給量に上限がある場合は合計トークン量がパブリックに参照可能）
  - 4.2 グローバル流通（当該アセットはどこでトレード可能か）
    - 4.2.1 取扱取引所数（当該アセットをサポートする取引所の数）
    - 4.2.2 地理的流通（当該アセットは単一ちいきに限定されず、分散された取引所にお会いするてトレード可能）
    - 4.2.3 法定通貨とのペア（法定通貨と暗号通貨のトレーディングペアが存在する）
    - 4.2.4 取引所の取扱量分散（セカンダリーマーケットが存在する場合、その取引ボリュームは取引所横断で分散）

→ 出典：https://www.gdax.com/static/digital-asset-framework-2017-11.pdf

⑦ICO関連
GDAX Digital Asset Framework

- 5. マーケットデマンド（アドプションやネットワーク効果をモニタリングする為にどのメトリクスが重要か）
  - 5.1 デマンド（当該アセットへの需要をドライビングするのは何でありそれはネットワーク効果向上に繋がるか）
    - 5.1.1 顧客の需要（顧客の需要は注意して考慮されるが、フォークやエアドロップや自動トークン配布については別途基準に従う）
    - 5.1.2 開発者および貢献者（レポジトリやコミットや貢献者の数によって、開発者のベースや進捗は計測できる）
    - 5.1.3 コミュニティの活動（開発者やサポーターやユーザーやファウンダーがやりとりしてコミュニティ構築しているフォーラムが利用可能。チームが定期的にアップデートを提供している）
    - 5.1.4 外部ステークホルダー（暗号通貨ビジネスと関わる経験あるベンチャーファームやヘッジファンドからの投資を得ている。企業との提携やジョイントベンチャーやコンソーシアムがある）
  - 5.2 ネットワーク標準（ネットワーク効果向上にむけた基礎的アセスメント）
    - 5.2.1 市場資本の変更（ネットワークのアクティベート後に市場資本が伸びたり、プロジェクトローンチ後にアセット需要が伸びたりしている）
    - 5.2.2 ノード（ブロックチェーン上のノードの数が伸びている。グローバルに分散したノードネットワークがある）
    - 5.2.3 トランザクション手数料およびアドレス（トランザクション数や手数料が伸びている）

→ 出典：https://www.gdax.com/static/digital-asset-framework-2017-11.pdf

⑦ICO関連
GDAX Digital Asset Framework

- 6. クリプトエコノミクス（エコシステムの参加者の行動がどのように動機付けられるかのアセスメント）
  - 6.1 経済的インセンティブ（全参加者かネットワークの最善の便益に則り行動するように経済的構造から設計されているか）
    - 6.1.1 トークンの種類（サービスやワークのトークン、或いはそのハイブリッドのトークンである。法定通貨や他の物理的アセットに裏づけられたトークンは証券として分類されるためここでは対象外）
    - 6.1.2 トークンの機能（トークンの獲得・保持・参加・消費により実用性がある。主要目的を資金調達とせず、ネイティブデジタルトークンの存在理由を特定できる）
    - 6.1.3 インフレ（セキュリティやネットワーク効果を動機付けるために、アルゴリズムによりプログラムされたインフレレートが存在する。或いは総供給量に上限ある場合はトークンの大部分がトレードに利用可能）
    - 6.1.4 報酬およびペナルティ（マイナーやバリデータを誠実な行動へと動機付けるためトランザクション手数料などのメカニズムがある）
  - 6.2 トークンセールの構造
    - 6.2.1 セキュリティ（スキャムやハッキングや資金盗難を防ぐためにセキュリティプロトコルにフォーカスしている）
    - 6.2.2 参加の平等（少数の投資家が供給量の大半を占めるリスクを限定するため購入量上限を設けるなど、トークンの公平な流通を図っている）
    - 6.2.3 チームのオーナーシップ（チームに保持される持ち分は少数。将来的なネットワーク改善へ経済的にインセンティブを持たせるためロックアップ期間を設定）
    - 6.2.4 透明性（プロダクト・トークンセール・資金使途について質問やフィードバックを複数のフォーラムで利用可）
    - 6.2.5 トータルサプライ（チームは総供給量の一定割合を売却し、参加者は総供給量に占める割合を知れる）
    - 6.2.6 倫理および行動規範（ホワイトペーパーやプロジェクトサイトに、倫理的でプロフェッショナルな行動規範）

→ 出典：https://www.gdax.com/static/digital-asset-framework-2017-11.pdf

⑧技術解説（ILP）

- ILPワークショップ東京　レポート（デモ編）
  - http://gtgox.com/ripple/20171124/ilp-workshop-tokyo-report-demo-part/
- 世界で一番分かりやすい Interledger Protocol
  - https://medium.com/@dora_gt/世界で一番分かりやすい-interledger-protocol-a6e6e3d11d80
- XRPの流動性を高める基盤「XRP Ledger」の仕組み
  - https://zoom-blc.com/what-is-ripple-xrp-ledger
- Interledger Presentation - Background, Streaming Payments, and Implications
  - https://www.slideshare.net/mobile/Interledger/34c3-interledger-presentation-background-streaming-payments-and-implications

⑨技術解説（NEM）

- NEM - Mycryptopedia
  - https://www.mycryptopedia.com/cryptocurrencies/nem/

- NEMのマルチシグをAPIレベルで紐解く
  - https://ryuta46.com/839

⑩仮想通貨関連

- 日本仮想通貨事業者協会（JCBA）、会員取扱い仮想通貨一覧並びに仮想通貨概要説明書を公開
  - https://cryptocurrency-association.org/cms2017/wp-content/uploads/2017/12/20171212_gaiyou.xlsx

- 「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）」のポイント
  - https://www.shinnihon.or.jp/corporate-accounting/accounting-topics/2017/2017-12-18-02.html

- 仮想通貨の会計処理案
  - http://www.dir.co.jp/research/report/law-research/accounting/20171218_012571.html

⑪中央銀行関連

- Here’s What the World's Central Banks Really Think About Bitcoin
  - https://www.bloomberg.com/news/articles/2017-11-26/what-the-world-s-central-banks-are-saying-about-cryptocurrencies
- Here’s What the World’s Central Banks Are Saying About Bitcoin
  - https://www.bloomberg.com/news/articles/2017-12-13/what-the-world-s-central-banks-are-saying-about-cryptocurrencies
- Central Bank Digital Currency: Motivations and Implications
  - https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf

⑫ブロックチェーン技術横断

- ブロックチェーンという言葉に騙されないために
  - https://imoz.jp/note/blockchain.html

- Ten years in, nobody has come up with a use for blockchain
  - https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100
  - https://chibicode.com/jp/blockchain/
  - 発明から10年もたったのに、誰もブロックチェーンを有効活用できていない。
  - 仮想通貨には大量の資金と労力が投下されたが、まともな使い道は通貨投機と違法取引のみ。

⑬応用むけレポート

- 日本取引所、約定照合業務におけるブロックチェーン(DLT)適用検討
  - http://www.jpx.co.jp/corporate/news-releases/0010/20180118-01.html
- 決済の経済学から見た電子決済と金融システム
  - http://www.mof.go.jp/pri/research/seminar/fy2017/lm20171114.pdf
- 仮想通貨「Zen」社会実験 第1フェーズ レポート
  - http://bccc.global/wp-content/uploads/2017/12/Zen-Report-p1c09-final.pdf
- R3による”Implementing Derivatives Clearing on Distributed Ledger Technology Platforms”
  - https://www.r3.com/wp-content/uploads/2017/11/implementing-derivatives-clearing_R3_.pdf

⑬応用むけレポート

- Cryptocurrencies and blockchains - their importance in the future (Deutsche Bank)
  - https://www.finextra.com/finextra-downloads/newsdocs/cio_insights_reflections_-_cryptocurrencies_and_blockchains_-_emea_-_client_ready.pdf
- Distributed Ledger Technologies for Public Good: leadership, collaboration and innovation
  - http://chrisholmes.co.uk/wp-content/uploads/2017/11/Distributed-Ledger-Technologies-for-Public-Good_leadership-collaboration-and-innovation.pdf
- Hack the Future of Development Aid
  - http://um.dk/~/media/UM/English-site/Documents/Danida/Goals/TechVelopment/Hack%20The%20Future%20December%202017v2.pdf?la=en
- Blockchain for education
  - http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf

11.論文リスト

2017 3Qの関連論文リスト(1/9)

タイトル	URL
A Fair Protocol for Data Trading Based on Bitcoin Transactions	→ https://eprint.iacr.org/2017/1018
An E-voting Protocol Based on Blockchain	→ https://eprint.iacr.org/2017/1043
Strain: A Secure Auction for Blockchains	→ https://eprint.iacr.org/2017/1044
Blackchain: Scalability for Resource-Constrained Accountable Vehicle-to-X Communication	→ https://arxiv.org/abs/1710.08891
Bulletproofs: Efficient Range Proofs for Confidential Transactions	→ http://web.stanford.edu/~buenz/pubs/bulletproofs.pdf
Scalable Funding of Bitcoin Micropayment Channel Networks	→ https://www.tik.ee.ethz.ch/file/a20a865ce40d40c8f942cf206a7cba96/Scalable_Funding_Of_Blockchain_Micropayment_Networks%20(1).pdf

2017 3Qの関連論文リスト(2/9)

タイトル	URL
Mempool optimized fees, and the correlation between user costs, miner incentives, and block capacity	→ https://bc-2.jp/mempool.pdf
Towards an Economic Analysis of Routing in Payment Channel Networks	→ https://arxiv.org/abs/1711.02597
A Searchable Symmetric Encryption Scheme using BlockChain	→ https://arxiv.org/abs/1711.01030
Quantum attacks on Bitcoin, and how to protect against them	→ https://arxiv.org/abs/1710.10377
Analysis of the Communication Traffic for Blockchain Synchronization of IoT Devices	→ https://arxiv.org/abs/1711.00540
Analysis of the Bitcoin UTXO set	→ https://eprint.iacr.org/2017/1095
Blackchain: Scalability for Resource-Constrained Accountable Vehicle-to-X Communication	→ https://arxiv.org/abs/1710.08891
Proposal for Protocol on a Quorum Blockchain with Zero Knowledge	→ https://eprint.iacr.org/2017/1093
Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts	→ https://eprint.iacr.org/2017/1090

2017 3Qの関連論文リスト(3/9)

タイトル	URL
Sharding PoW-based Blockchains via Proofs of Knowledge	→ https://eprint.iacr.org/2017/1067
Bulletproofs: Efficient Range Proofs for Confidential Transactions	→ https://eprint.iacr.org/2017/1066
CP-consensus: a Blockchain Protocol Based on Synchronous Timestamps of Compass Satellite	→ https://eprint.iacr.org/2017/1059
An E-voting Protocol Based on Blockchain	→ https://eprint.iacr.org/2017/1043
An Investigation into the Potential for Using the Bitcoin Blockchain as the World's Primary Infrastructure for Commerce Over the Internet	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3065857
Mechanising Blockchain Consensus	→ http://ilyasergey.net/papers/toychain-accepted.pdf
Efficient Zero-Knowledge Range Proofs in Ethereum	→ https://cms.ingwb.com/media/2122048/zero-knowledge-range-proof-whitepaper.pdf

2017 3Qの関連論文リスト(4/9)

タイトル	URL
Stampery Blockchain Timestamping Architecture (BTA) - Version 6	→ https://arxiv.org/abs/1711.04709
Beyond the Hype: On Using Blockchains in Trust Management for Authentication	→ https://arxiv.org/abs/1711.04591
Towards ECDSA key derivation from deep embeddings for novel Blockchain applications	→ https://arxiv.org/abs/1711.04069
Consensus in the Age of Blockchains	→ https://arxiv.org/abs/1711.03936
Proposal for Protocol on a Quorum Blockchain with Zero Knowledge	→ https://eprint.iacr.org/2017/1093
Analysis of the Bitcoin UTXO set	→ https://eprint.iacr.org/2017/1095
Dynamic Distributed Storage for Scaling Blockchains	→ https://arxiv.org/abs/1711.07617
Solida: A Blockchain Protocol Based on Reconfigurable Byzantine Consensus	→ https://eprint.iacr.org/2017/1118
A formal model of Bitcoin transactions	→ https://eprint.iacr.org/2017/1124

2017 3Qの関連論文リスト(5/9)

タイトル	URL
A scalable verification solution for blockchains（TrueBitホワイトペーパー）	→ http://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf
Tesseract: Real-Time Cryptocurrency Exchange using Trusted Hardware	→ https://eprint.iacr.org/2017/1153
Designing Secure Ethereum Smart Contracts: A Finite State Machine Based Approach	→ https://arxiv.org/abs/1711.09327
A blockchain-based Decentralized System for proper handling of temporary Employment contracts	→ https://arxiv.org/abs/1711.09758
On the linkability of Zcash transactions	→ https://arxiv.org/abs/1712.01210
Cryptocurrency Voting Games	→ https://eprint.iacr.org/2017/1167
Blockchains and Data Protection in the European Union	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322

2017 3Qの関連論文リスト(6/9)

タイトル	URL
Some Simple Economics of the Blockchain	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598
MODERN MONETARY CIRCUIT THEORY, STABILITY OF INTERCONNECTED BANKING NETWORK, AND BALANCE SHEET OPTIMIZATION FOR INDIVIDUAL BANKS	→ https://bus.wisc.edu/~/media/bus/knowledge-expertise/academic-departments/finance/2016-lipton-modern-monetary-circuit-theory-ijtaf.pdf?la=en
Performance Analysis and Application of Mobile Blockchain	→ https://arxiv.org/abs/1712.03659
The Blockchain Revolution: Insights from Top-Management	→ https://arxiv.org/abs/1712.04649
Information Propagation on Permissionless Blockchains	→ https://arxiv.org/abs/1712.07564

2017 3Qの関連論文リスト(7/9)

タイトル	URL
Designing Proof of Transaction Puzzles for Cryptocurrency	→ http://ia.cr/2017/1242
How to Charge Lightning	→ https://arxiv.org/abs/1712.10222
Designing Secure Ethereum Smart Contracts: A Finite State Machine Based Approach	→ http://amavridou.com/papers/mavridou2018SC.pdf
Mobius: Trustless Tumbling for Transaction Privacy	→ https://eprint.iacr.org/2017/881.pdf
An Analysis of Acceptance Policies For Blockchain Transactions	→ https://eprint.iacr.org/2018/040
Applications of Blockchain Technology beyond Cryptocurrency	→ https://arxiv.org/abs/1801.03528
A First Look at Identity Management Schemes on the Blockchain	→ https://arxiv.org/abs/1801.03294
Towards Application Portability on Blockchains	→ https://arxiv.org/abs/1801.01421
ZK-STARKS - Scalable, transparent, and post-quantum secure computational integrity	→ https://eprint.iacr.org/2018/046

2017 3Qの関連論文リスト(8/9)

タイトル	URL
Truebit Light's Incentive System	→ http://chriseth.github.io/notes/articles/truebit_incentive/truebit_light_incentives.pdf
Price Manipulation in the Bitcoin Ecosystem	→ https://www.sciencedirect.com/science/article/pii/S0304393217301666
Decentralization in Bitcoin and Ethereum Networks	→ https://arxiv.org/abs/1801.03998
Why Bitcoin is Not a Currency But a Speculative Real Asset	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3098765
Smart Contracts for Bribing Miners	→ http://homepages.cs.ncl.ac.uk/patrick.mccorry/minerbribery.pdf

2017 3Qの関連論文リスト(9/9)

タイトル	URL
When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis	→ https://arxiv.org/abs/1801.07501
Block arrivals in the Bitcoin blockchain	→ https://arxiv.org/abs/1801.07447
Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

お役に立てば嬉しいです

- **BTCアドレス**

  1QEvtDMDLrdNVMG3xBJj4684G9pGJSNtJJ

→おしまい