Bitcoin & Blockchain概況

2017.10 by SATO

「Bitcoin2.0概況」「Blockchain2.0概況」から改題

過去10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）：**今回

第11回の臨時構成

- 第一部：通常編成で各分野の動向トピック
- 第二部：Scaling Bitcoin準備

TABLE OF CONTENTS

➔ 今回は、2017年8月～2017年10月の動きを中心に整理

1. ビットコインのスケーリング紛争

- Bitcoin Cash、UAHFによりビットコインからスピンオフ
- Segwitがアクティベート
- Segwit2x、オプトイン式のリプレイプロテクションをマージ
- Segwit2xハードフォーク後を見越した動き

Bitcoin Cashが UAHFによりビットコインからスピンオフ （1/2）

- 8/1（日本時間9:00）はBIP148によるUASFローンチ予定ではあったものの既にBIP91をアクティベートし有効化済のためUASFによる分岐は発生せず、一方同日の日本時間21:20にBitcoin Cashがローンチし分岐することとなった。
  - ビットコインのブロック高478558から、Bitcoin-ABCクライアントによるBitcoin Cashプロトコルに切り替わった。

- ハッシュパワーが低いことに加えて、最初のブロックは1MB以上とするという仕様のため時間を要し、切り替えから約6時間後、ViaBTCプールが1.9MBのBitcoin Cashブロック478559を生成。
  - ブロック高478558時点のビットコイン保有者がBitcoin Cashの保有者となった。
  - ビットコインブロックチェーンのハッシュパワーは6200PH/s。
  - ViaBTCによると、ビットコインプールが372PH/sに対して、Bitcoin Cashプールは8/1に128PH/s、8/2に215PH/sと増加後、8/3に70PH/s、その後23PH/sに減少。（8/6時点）

→ 出典: https://www.bitcoincash.org/activation
→ 出典: https://github.com/Bitcoin-UAHF/spec/blob/master/uahf-technical-spec.md
→ 出典: https://www.coindesk.com/bitcoin-cash-what-expect-fork-10000-foot-view/
→ 出典: http://btcnews.jp/5y9vqla912010/
→ 出典: https://coin.dance/nodes/share
→ 出典: https://cash.coin.dance/blocks
→ 出典: https://pool.viabtc.com/

Bitcoin Cashが UAHFによりビットコインからスピンオフ （2/2）

- ビットコインハッシュパワーのどれだけがBitcoin Cashに移るかによってインパクトが変わる。
  - 移るのが16%以下であればBitcoin Cashの最初のブロック生成に1時間要してビットコインのブロック生成時間に影響を与えないが、17-50%が移るとビットコインブロック生成時間が12-20分に延び、さらに50%超が移るとビットコインのブロック生成は20分以上となる。

- Bitcoin Cashのハッシュパワーが増えない場合、難易度調整が起こる。
  - ビットコイン同様の2週間毎の難易度調整に加えて、Bitcoin Cashは6ブロックの採掘に12時間以上かかった場合に難易度が20%下がる仕様。
  - 難易度調整の結果、ブロック生成間隔が短縮しているが、10ブロック採掘に18時間程度かかっている。（8/6時点）

- Bitcoin Cashのブロック生成を行なったマイニングプール分布
  - ViaBTCが24.36%、Bitcoin.comが3.85%、Supernovaが1.28%、その他が70.51%を占め（8/6時点）、その他となっているマイナーは、香港のMC Poolとされる。
  - ビットコインネットワークのノード数8968のうち、Bitcoin Coreが5563、Bitcoin UASFが1193、Bitcoin-ABCが791、Bitcoin Unlimitedが772、btc1が156という分布（8/6時点）。

→ 出典: https://blockchair.com/bitcoin-cash/blocks
→ 出典: https://www.btcforkmonitor.info/
→ 出典: http://www.jpbitcoinblog.info/entry/20170802/1501670971
→ 出典: https://medium.com/@jimmysong/bitcoin-cash-difficulty-adjustments-2ec589099a8e
→ 出典: https://news.bitcoin.com/the-trading-center-in-hk-where-they-mined-most-of-the-bitcoin-cash-blocks/

SEGWITがアクティベート

- 8/24の日本時間am11頃にブロック481822にてSegwitが公式にアクティベートされた。
- トランザクションinputからScriptSig部分がWitnessData領域へ移動することによるトランザクションの圧縮効果、トランザクション展性の解決などがもたらされるほか、手数料低減が期待される。
- Segwitトランザクション送付には、意図的にSegwit方式でトランザクションを送るために、利用ウォレットの対応が必要なことに留意要。
- Segwit導入によって、このアップデートに依存する他の技術、たとえばLightningNetwork、MAST、アトミックスワップ、Schnorr署名アルゴリズム、TumbleBitも開発ステージへ進むことが期待されている。

→ 出典: http://doublehash.me/bitcoin-20170824/
→ 出典: http://doublehash.me/segwit-address-transaction/
→ 出典: https://news.bitcoin.com/segregated-witness-has-officially-activated-on-the-bitcoin-network/
→ 出典: https://bitcoinmagazine.com/articles/long-road-segwit-how-bitcoins-biggest-protocol-upgrade-became-reality/

SEGWIT2X、オプトイン式のリプレイプロテクションをマージ（1/2）

- 一般にハードフォーク時には、フォーク前のコインが双方のチェーンに存在することになる。
  - そのため、リプレイプロテクションが無い場合、チェーンXにコインを送ると同じトランザクションがチェーンYでも有効になってしまうという脆弱性が問題となる。
  - こうしたリプレイ攻撃への対策として、Bitcoin Cashでは全てのトランザクションに署名をマーキングすることで、ハードフォーク後に元のチェーンでトランザクションが有効となることを防いだ。
  - この場合、意図せずリプレイ攻撃に遭うことはないため、チェーンXからトランザクションが漏れ出すことを防ぐ自動ロックのような役割を果たす。

- 一方、オプトインによるリプレイ保護では、チェーンXからのトランザクションは、チェーンYで無効化するために特別な行為を必要とするもの。
  - デフォルトではトランザクションはリプレイ攻撃にさらされるため、利用者が忘れずにロックしないとトランザクションが別チェーンに漏れ出してしまうことになる。
  - Segwit2xの開発者Jeff Garzikによるオプトインリプレイプロテクションでは、コインを送る際に、3Bit1xA4(以下略)のアドレスへ少額のコインを送ることによって、2xチェーンでのトランザクションを無効化する。
  - このリプレイプロテクションはチェーンのスプリット（11/18またはブロック494784）後にアクティベート。

→ 出典: https://bitcointechtalk.com/how-segwit2x-replay-protection-works-1a5e41767103
→ 出典: https://0bin.net/paste/nQwqU76pQ3CW00ZV#TUB68SXcEn-fSIQAWkULnUEL0NaUK/5TzPrQWEFwWyg

SEGWIT2X、オプトイン式のリプレイプロテクションをマージ （2/2）

- こうしたリプレイプロテクションをとることの背景には、ウォレットなどのサービス事業者のアップグレート作業を不要とすることにより、Segwit2x開発者がハードフォーク後にマジョリティをとりたい意向があると考えられる。

- それればかりでなく、Peter Toddにより、これには他の意図が含まれることが明らかにされた。

- 上述の3Bit1xA4(以下略)のアドレスはブラックリストアドレスとしてペイメントチャネルを用いることによって、コインを抜き取ることが可能となっているとのこと。
  - 例えば悪意を持った者マロリーが、「CLTV/CSVタイムアウト後に送金者アリスに署名を求めるペイメントチャネル」を開設。
  - このブラックリストアドレスはマイニングされることがないオフチェーントランザクションとして決済されるが、アリスはそれを知ることがないため、アリスがチャネルを閉じようとしてもブラックリストにより不可能であり、マロリーだけがCLTV/CSVタイムアウト後に全額払い戻すことができてしまう。

→ 出典: https://bitcointechtalk.com/how-segwit2x-replay-protection-works-1a5e41767103
→ 出典: https://0bin.net/paste/nQwqU76pQ3CW00ZV#TUB68SXcEn-fSIQAWkULnUEL0NaUK/5TzPrQWEFwWyg

SEGWIT2Xハードフォーク後を見越した動き（1/2）

- マイニングブロックから見るに、94%のマイナーがNY合意（NYA）を踏まえたSegwit2xサポートを表明しており、95%に迫る。
  - こうした中、BitfinexはNYA署名者によるSegwit2xハードフォークによるコインをB2Xというティッカーで呼ぶと表明し、B2X側が多くのハッシュパワーを持つ場合にも現行のビットコイン・コンセンサス・プロトコルに基づく実装をBTCとして取引継続することを表明し、Segwit2xコインをアルトコインとして扱うことを示した。
  - この中では、Segwit2xでは強制双方向リプレイプロテクションが無いために、顧客資産の保護を目的としてフォーク時にはBTCおよびB2Xの預入れ・引出しを一時停止することが含まれている。
  - Coinbaseも声明を発表し、「フォーク時点でCoinbaseにビットコイン残高を持つ顧客は（フォーク後も）双方のチェーンにアクセスできるものとし、顧客は特段のアクションを必要とすることなしに、ビットコインは従来どおり安全にCoinbaseに格納される」「フォーク後にそれぞれのブロックチェーンが安全で安定していることを判断した時点で顧客へのアクセスを解放する予定」といった旨に言及している。

→ 出典：https://coin.dance/blocks
→ 出典：https://www.bitfinex.com/posts/223
→ 出典：https://blog.coinbase.com/update-on-the-bitcoin-segwit2x-hard-fork-69426f14bc85
→ 出典：https://bitcoin.org/en/posts/denounce-segwit2x
→ 出典：https://news.bitcoin.com/another-bitcoin-fork-bitcoin-gold-project-plans-to-fork-bitcoin-next-month/

SEGWIT2Xハードフォーク後を見越した動き(2/2)

- 同様にBitcoin.orgサイトも、NYA署名事業者に下記について表明することを要求。
  - Segwit2xコインをビットコイン/BTCとして掲載しないこと
  - リプレイ攻撃プロテクション無しのSegwit2xソフトを使う・ユーザーのビットコインを自動的に売却する・ビットコイン預入れをSegwit2xコイン預入れとみなす等によってユーザーのビットコインを奪う行為をしないこと
  - Segwit2xコインでないビットコインユーザー向けサービスを継続提供すること
- 反対にSegwit2xコインをサポートする動きとして、ビットコインATMを提供するCoinfucius社が、「11月のハードフォーク後はビットコインをサポートせずにSegwit2x コインのみを扱う」旨を表明。
- 現時点で想定されるハードフォークは、既にフォーク済みのBitcoin Cash（BCH）、上記のSegwit2xコイン（B2X）、および10/25に予定されるとされるPoWとしてGPUベースのEquihashを利用するBitcoin Gold（BCG）の三種（ビットコイン含めた四つの比較表はnews.bitcoin.comのリンク参照）。
  - なお、この三種のほかにeBTCがあるが、これはEthereum上ERC20トークンとして作られたビットコイントークン。

→ 出典: https://coin.dance/blocks
→ 出典: https://www.bitfinex.com/posts/223
→ 出典: https://blog.coinbase.com/update-on-the-bitcoin-segwit2x-hard-fork-69426f14bc85
→ 出典: https://bitcoin.org/en/posts/denounce-segwit2x
→ 出典: https://news.bitcoin.com/another-bitcoin-fork-bitcoin-gold-project-plans-to-fork-bitcoin-next-month/

番外トピック
WizSec、MtGoxハッキング調査結果を発表

- ビットコインを巡る大規模なマネーロンダリングの嫌疑でロシア人容疑者がギリシャで逮捕された。
- この報を受けて、ビットコインセキュリティスペシャリスト集団であるWizSecが、MtGox事件と上記容疑者の繋がりについてレポートを発表した。
- 2011年9月、MtGoxのホットウォレットの秘密鍵（単純にコピーされたウォレットのdatファイル）が盗まれ、ハッカーが相当量のビットコインにアクセス可能となった。
- ハッカーは鍵を用いて定期的にコインを消費して、上記容疑者のコントロールするウォレットへ送付。
- 2013年半ばまでの間に、MtGoxからの盗難は63万BTCにおよんだ。
- 上記容疑者のウォレットに入ったビットコインの多くがBTC-eに移され、売却・ロンダリングされた。
- 上記容疑者は、ハッカーではなくロンダリングを行なったとされている。

→ 出典: https://medium.com/@jimmysong/mt-gox-hack-technical-explanation-37ea5549f715
→ 出典: http://blog.wizsec.jp/2017/07/breaking-open-mtgox-1.html
→ 出典: https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged
→ 出典: https://media.consensys.net/mtgox-btc-e-and-the-missing-coins-a-living-timeline-of-the-greatest-cyber-crime-ever-f94fbb1eb42

参考リンク集

- パリでBreaking Bitcoin開催。Wizsecが示したMtGoxハッキング、Christopher Jeffreyによる脆弱性のディスクロージャー等が話題に
  - https://breaking-bitcoin.com
  - https://youtu.be/eCE2OzKIab8
  - https://youtu.be/0WCaoGiAOHE
  - https://www.youtube.com/embed/l70iRcSxqzo
  - https://bitcoinmagazine.com/articles/breaking-bitcoin-paris-set-host-new-technical-bitcoin-conference/
  - https://bitcoinmagazine.com/articles/no2x-breaking-bitcoin-shows-no-love-segwit2x-hard-fork-paris/
  - https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-September/014983.html
  - http://cryptocrimson.com/2017/09/12/bitcoin-core-vulnerability-disclosed/
  - http://www.trustnodes.com/2017/09/10/bitcoin-core-vulnerability-disclosed-exploited-bitcoin-cash-developer-centralization-called-threat

参考リンク集

- コア開発者ミートアップでのトピック（BIP150,151、署名集約、MAST）
  - http://diyhpl.us/wiki/transcripts/sf-bitcoin-meetup/2017-09-04-jonas-schenlli-bip150-bip151/
  - http://diyhpl.us/wiki/transcripts/bitcoin-core-dev-tech/2017-09-05/
  - http://diyhpl.us/wiki/transcripts/bitcoin-core-dev-tech/2017-09-06-signature-aggregation/
  - http://diyhpl.us/wiki/transcripts/bitcoin-core-dev-tech/2017-09-07-merkleized-abstract-syntax-
  - trees/

2. プロトコル改善にむけた動向

- Bitcoin
  - Blockstream Satellite／アトミックスワップ／Proof of mainstake／lndデスクトップアプリ／Lightning Networkのスケーリング／Bitcoin Coreの脆弱性
- Ethereum
  - Plasma／PeaceRelay／Metropolisハードフォーク／µRaiden
- ブロックチェーン全般
  - OpenLaw／分散カギ管理／分散取引所／ブロックチェーンの分散性に関する定量分析／ブロックチェーン技術の１０か年ロードマップ

ビットコインブロックチェーンを宇宙からブロードキャストするBLOCKSTREAM SATELLITEを発表

- 地球上のあらゆる人々が無料でWiFi無しにビットコインによる経済的革命に参加する機会を得ることができるようにするもの。
  - インターネットアクセスの無い40億人の人々がビットコインを利用する機会を得ることが出来る。
  - SDR技術を用いて、衛星コミュニケーションのコスト効率においてブレークスルーを提供。

- ユーザがSatelliteネットワークにコンピュータを接続するのに必要なコストは100ドルのみ。
  - コスト面の障壁でビットコインのネットワークに参加できなかった人々がブロックを受け取ることが出来るようになる。

- 衛星からのブロードキャストを受けて、衛星アンテナおよびUSBレシーバーを備えていれば、ブロックを受信してノードを同期できる。
  - 3台の商用衛星が既にBlockstreamのビットコインサービスを動かしており、北米・南米・アフリカ・欧州をカバー。
  - そのほか地域は2017年第④四半期のフェーズ２にて。

→ 出典: https://blockstream.com/satellite/
→ 出典: http://www.ibtimes.com/blockstream-offers-satellite-bitcoin-network-broadcasting-space-2578464
→ 出典: http://doublehash.me/bitcoin-satellite-mining-decentralization/
→ 出典: https://www.google.co.jp/amp/s/m.japan.cnet.com/amp/story/35105967/
→ 出典: https://youtu.be/6iG-KLbViVc

DECRED、メインネット上でオンチェーンによるLTCとのアトミックスワップに成功

- 取引所に依存しないオンチェーンによるアトミックスワップのサポートを発表し、メインネット上でLTCとのスワップに成功
  - Litecoin-Decred間のアトミックスワップ。
  - クロスチェーンアトミックスワップは、あるコインから他コインへの価値交換にあたり、市場流動性を維持しながら取引プラットホームのプロセスを不要とするもの。
  - ユーザーAがユーザーBのビットコインアドレスにビットコインを送る一方で、ユーザーBがユーザーAのオルトコインアドレスにオルトコインを送る場合、取引終了まで担保するには従来互いに信頼する第三者を立てエスクローを行う必要があった。

- クロスチェーンアトミックスワップは、それぞれのブロックチェーンにコントラクトを設け、各当事者が使用可能なアウトプットをコントラクトに含めつつ、ある秘密を知らないと使えないというルールを組み込んでいる。
  - 暗号通貨間の相互運用性向上の他、トランザクション手数料以外のコストを軽減できる点がメリット。
  - Lightning NetworkのLitecoin版であるLitening Networkは用いず、オンチェーンによるものであり、クロスチェーンアトミックスワップが様々な方法で実装できることが示された。
  - クロスチェーンアトミックスワップは、現時点では暗号通貨間のものであり、法定通貨を交えたものではないという点が、残された課題。

→ 出典: https://bitcoinmagazine.com/articles/decred-adds-atomic-swap-support-exchange-free-cryptocurrency-trading/
→ 出典: https://github.com/decred/atomicswap/#first-mainnet-dcr-ltc-atomic-swap
→ 出典: https://themerkle.com/developers-complete-first-ever-atomic-swap-between-litecoin-and-decred/
→ 出典: https://youtu.be/Jw5icKcmdbA
→ 出典: http://btcnews.jp/4af0yu1d12773/

新たなサイドチェーンプロポーザル "PROOF OF MAINSTAKE"

- SPV proof-based sidechainやDrivechainに続くサイドチェーンプロポーザル。
- メインチェーン上のコイン持ち分（mainstake）により決定されるメンバシップを用いる。
- mainstake内のメインチェーンコインは、サイドチェーン内にありサイドチェーン上にロックされるコインとは区別され、サイドチェーンを保護するための持ち分としてメインチェーンに残る。

→ 出典：https://zmnscpxj.github.io/sidechain/mainstake/index.html

LIGHTNING NETWORKのLNDデスクトップアプリ、テスト向け利用可能に

- ビットコインの軽量オペレーティングモードのオープンソースであるneutrino対応。
- neutrinoの軽量クライアントはブルームフィルター（BIP37）に依存せず、代わりにクライアントサイドフィルタリング。
- segwit完全対応しており、ネイティブsegwitアドレスでの送受信が可能。

→ 出典：http://blog.lightning.engineering/announcement/2017/10/12/test-blitz.html

LIGHTNING NETWORKのスケーリングに関する問題提起

- Mathematical Proof That the Lightning Network Cannot Be a Decentralized Bitcoin Scaling Solution
  - Lightning Networkのスケーリングに関する問題提起。
  - 大量のチャネルを保有したり、大量のホップ数が必要となるため、資金を細切れにしてチャネルに分けるため少額の購入にしか使えない他、各人のお金が他の誰かのお金との結びつきが強くなる状態となる。
  - トランザクションに必要となる以上の資金をデポジットしておくか、或いは大きな集権型ハブへの依存度が高まり、分散型スケーリングではなくハブアンドスポークアーキテクチャになってしまう可能性がある。
  - https://medium.com/@jonaldfyookball/mathematical-proof-that-the-lightning-network-cannot-be-a-decentralized-bitcoin-scaling-solution-1b8147650800

BREAKING BITCOINでCHRISTOPHER JEFFREYがBITCOIN COREの脆弱性に言及

- Bitcoin CoreのUTXOを管理するchainstateデータベースでは、ノードが新しいトランザクションを受信する度に、トランザクションの全アウトプットをシリアライズしてデータベースの1レコードに保存する。
- ブロック内のトランザクションが多くの別々のトランザクションを参照するほど、ブロック検証時のメモリ使用量が増える。
- この問題を突いたブロックを作ることで、受信したノードは、検証時に大きなデータがロードされることになり、メモリ不足に陥る、というもの。
- 現在Bitcoin Coreはノードのシェアの70%を構成するが、分散ネットワークにおける実装の集中化・分散化について課題提起がなされたと見るべき。

→ 出典: http://btcnews.jp/1o8eq9uo12651/

スマートコントラクトのスケーリングソリューション、PLASMA （1/2）

- 「スケーラブルな自律スマートコントラクト」と題してホワイトペーパーが公開。
- ShardingやLNといったスケーリングソリューションの一つであり、トランザクションではなく計算パワーのスケーリングを実現するもの。
- メインネットからトランザクションおよび計算負荷をオフロードするための子ブロックチェーンのネットワーク。
- アセット移転だけでなく、スマートコントラクトの計算を新しいチャネルに移しオフチェーンで行う。
- 潜在的には秒間数十億回といった頻度でステートの更新を行うスケーラブルなスマートコントラクト。
- 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、大量の計算実行が可能な子ブロックチェーンからの少量のコミットメントを処理するのみ。

→ 出典: https://www.plasma.io/plasma.pdf
→ 出典: https://medium.com/chain-cloud-company-blog/plasma-in-10-minutes-c856da94e339

スマートコントラクトのスケーリングソリューション、PLASMA （2/2）

- コミットメントは定期的に子ブロックチェーンからルートブロックチェーンに対してブロードキャストされるため、この様は地方裁判所と最高裁判所の関係に例えられる。
- 全データが全参加者へブロードキャストされる訳ではなく、特定ステートを検証してほしい参加者のみであり、参加者は特定チェーンをモニタリングする責任を有し、不正は定期的にペナルティーが与えられる。
  - アタック時には参加者は子ブロックチェーンからルートブロックチェーンへの退避が速やか且つ安価に可能。
  - ブロックチェーンは階層的にツリーとして配置され（同様にブロックチェーンを階層的に配置するものとしてはCosmosやPolkadotがある）、データの可用性・セキュリティとコストのバランスをとり、マイニングはルート上でのみ行われ、証明はルートから流される。
  - それぞれの子ブロックチェーンは自身のトークンを持ちバリデータがFraud Proof Ruleに基づき不正保護を行う動機付けに使われる。
  - 子ブロックチェーンの全ステートはFraud Proofと呼ばれるスマートコントラクトロジックを介して、ステートの変移が有効化される。

→ 出典: https://www.plasma.io/plasma.pdf
→ 出典: https://medium.com/chain-cloud-company-blog/plasma-in-10-minutes-c856da94e339

PeaceRelay

- Ethereumスマートコントラクト内で動くビットコイン軽量クライアントであるBTCRelayに触発されて開発された。
- BTCRelayはEthereumスマートコントラクトがビットコイントランザクションを検証し、Ethereumアカウントがビットコインのペイメントを受け取ることができるもの。
- PeaceRelayは、EthereumとEthereum Classicのような異なるEthereumブロックチェーン間のやりとりを可能とするもの。
- 例えば、Ethereumスマートコントラクトが、Ethereum Classicのトランザクションやアカウントステータスを検証できる。
- サイドチェーン内の双方向ペグによるリレーにより実装。

→ 出典: https://medium.com/@loiluu/peacerelay-connecting-the-many-ethereum-blockchains-22605c300ad3

METROPOLISハードフォーク上で ZK-SNARKSを用いてZCASHトランザクションを検証

- Ethereum Metropolisハードフォークの第一弾となるByzantiumがテストネット上で稼働中。
- Byzantuimでは、zk-SNARKが新たなツールとして組み込まれ、スマートコントラクトを用いてzk-SNARKの検証が可能となる。
- この他、今回のアップグレードでは、ブロックタイム短縮（25secが15secに）やブロックリワード低減（5ETHが3ETHに）などが組み込まれている。

→ 出典: https://www.reddit.com/r/ethereum/comments/712idt/ethereum_testnet_just_verified_a_zcash_transaction/
→ 出典: http://www.trustnodes.com/2017/09/19/ethereums-metropolis-hardfork-activated-testnet-zcash-transaction-verified
→ 出典: https://z.cash/blog/ethereum-snarks.html

ETHEREUMテストネット上でのオフチェーンマイクロペイメント、MRAIDENをRAIDENがリリース

- Pay-per-useの即時ペイメントチャネルネットワークを、ERC20ベースのマイクロペイメントとして実現するもの。
- ペイメントに際してネットワークをルーティングするのでなく、ユーザー間で直接マイクロペイメントを行う。
- Raiden Networkが双方向のトークンペイメントチャネルでユーザーを接続するのに対して、このマイクロRaidenでは単一方向のペイメントチャネル。
- ニュース記事のペイウォールや、リクエスト払いのAPIなど分散アプリによるマイクロペイメントリクエストへの応用に期待。

→ 出典: https://www.ethnews.com/amp/the-raiden-network-announces-raiden-off-chain-micropayment-solution-using-ethereum
→ 出典: https://www.coindesk.com/raiden-release-simpler-micropayments-go-live-ethereums-testnet/

法的合意事項の生成・実行むけプロトコル、OpenLaw

- ブロックチェーンベースのスマートコントラクトを活用して、デジタル署名の上で法的合意事項を安全に格納。
- プログラム可能な法的言語を生成するために必要なツールを提供するLegal Markup言語を用いて、リーガルテンプレートを提供。
- OpenLawを用いることにより、Ethereumスマートコントラクトを法的合意事項の中に数行のコードとして埋め込むことができる。

→ 出典: http://openlaw.io/
→ 出典: https://media.consensys.net/introducing-openlaw-7a2ea410138b

パブリックブロックチェーンむけ分散カギ管理システム、NuCypher KMS

- パブリックブロックチェーン上でプライベートデータを安全に格納・共有・操作することが必要なユースケースにおいて、プライベートデータの保護・コントロールを可能にする。
- 中央のサービス提供者に依存することなく、暗号学的にアクセスコントロールを提供する。
- 分散ネットワークノードを用いて、秘密鍵やテキストデータにアクセスせずにカギ管理操作が可能。
- コアとなる技術は、PRE（プロキシ再暗号化）であり、サードパーティーが再暗号カギを用いて公開鍵から変形することが、メッセージを知ること無しにできる。
- 再暗号化ノードはPoS形式のトークンによりインセンティブを得て、再暗号化サービスを提供する。

→ 出典: https://hackernoon.com/nucypher-kms-decentralized-key-management-system-7783cdaad39e
→ 出典: https://cdn2.hubspot.net/hubfs/2807639/NuCypher%20KMS%20Technical%20White%20Paper.pdf

分散取引所の意義

- Why decentralized exchange protocols matter
  - 現行のDEXは、EtherDeltaやCoinfeinne、Bisq（元Bitsquare）等。
  - DEXの利点は、ユーザーが資金コントロールを保持できる点、流動性が高まる点、都度サインアップ不要でシームレスなユーザビリティを提供できる点などがある。
  - 逆にDEXの欠点となるのが、ユーザーが自身の資金を安全管理するためのツールが未成熟である点、ブロックチェーン同様スケーラビリティの課題を抱える点、まだ法定通貨をサポートできない点、ブロック報酬のようなネットワーク効果を効かせるインセンティブが欠如している点など。
  - これらに対して、0xやswapなどはDEXプロトコルと呼ばれる。
  - DEXプロトコルは、共通オーダーフォーマットや、オーダーをスプレッドする参加者へのリワード方法、マッチング時のトレード完結手段を提供するもの。
  - オープンスタンダードなAPIとして、DEXプロトコルは、Dapps作成時のカスタマイズを容易にする。
  - スマートコントラクトがより自律的で複雑なものになるにつれ、DEXに接続するAPIが必要になる。
  - 例えば、Ether、Filecoinなど複数トークンを必要とするDappがジャストインタイムでトークンを入手するため、Dapp中にDEXプロトコルを組み込む。
  - 或いは、日々のトピックに対してトークンを生成するマイクロ予測市場のように、膨大なトークンを処理するDappにおいても、DEXプロトコルのAPIを用いて新たなトークンを自律かつ即時がサポートすることが有効。
  - https://medium.com/@FEhrsam/why-decentralized-exchange-protocols-matter-58fb5e08b320

ブロックチェーンの分散性に関する定量分析

- Quantifying Decentralization
  - ブロックチェーンの分散性について、ジニ係数（0で完全平等、1で完全不平等）やローレンツ曲線で分析したもの。
  - 例えば上位100の暗号通貨のMarket Capについてジニ係数をとると0.91であり、BitcoinおよびEthereumへの集中が示される。
  - さらに、マイニング報酬、クライアントのコードベース、コミットする開発者、取引所の取扱高、国別ノード数、アドレス保有者数といった括りでジニ係数を算出。
  - マイニング報酬の分布でみると、Bitcoinが0.4、Ethereumは0.82であり、Bitcoinの方が分散。
  - クライアント数の分布では、それぞれBitcoin Coreやgethに集中しているため、0.9超とコードベースが集中傾向。
  - https://news.21.co/quantifying-decentralization-e39db233c28e

ブロックチェーン技術の10か年ロードマップ

- A 10 year blockchain tech roadmap
  - 暗号学的エンジニアリング面。複雑なプロトコルの実装用の安全で成熟したライブラリが必要。ゼロ知識証明のライブラリも成熟化が必要。全プログラム言語むけのデータ構造ライブラリや標準の整備。
  - ブロックチェーンプロトコル面。現実世界でテストされた安全で高速なコンセンサスシステム。Cosmosのようなブロックチェーン同士の接続プロトコル。安全で高速なスマートコントラクト開発言語。Lightningのようなレイヤー2プロトコル。
  - ガバナンス面。ブロックチェーンネットワークを統治する頑健な技術・社会的システム。Validatorは組織的に成熟する必要。スケーリング実現のためにも可用性・セキュリティを高度に運営できるガバナンスが必要。Validatorの管理・特定の仕組みが必要。企業間の共有ネットワークや、企業とパブリックネットワーク間のやりとりを統括するために社会的組織が必要。複数の開発チームが効果的に協調・貢献できるかの見極め。
  - マーケットインフラ面。アセット発行が成熟してライフサイクル全般を管理できるようになる必要。取引所は暗号通貨だけでなくデジタルアセットやブロックチェーンベースの証券まで含めて流動性提供できることが必要。分散メカニズムが流動性提供者になれるかどうかの見極め。
  - トラストコンピューティング面。SGX向けツールや複数のTEE提供ベンダーが必要。エッジデバイスにおいても、物理世界とブロックチェーンの境界面を安全に保てるTEEが利用可能になることが必要。
  - https://zaki.manian.org/blog/10-year-blockchain/

2017 2Qの動向 (1/6)

- 慶大と東大、ブロックチェーン技術のオープンな国際産学連携グループ「BASEアライアンス」を設立
  - http://mw.nikkei.com/sp/#!/article/DGXLRSP451847_Q7A720C1000000/

- Bitcoin Fungibilityフレームワーク、Zerolink
  - https://medium.com/@nopara73/introducing-zerolink-the-bitcoin-fungibility-framework-dc5338086198
  - http://blog.samouraiwallet.com/post/164175489287/introducing-zerolink-zerolink-is-a-collaborative
  - https://bitcoinmagazine.com/articles/hiddenwallet-and-samourai-wallet-join-forces-make-bitcoin-private-zerolink/

- Stratis、TumblebitをBreeze Walletに統合
  - https://news.bitcoin.com/breeze-wallet-integrates-trustless-payment-hub-tumblebit/
  - https://btcmanager.com/stratis-tumblebit-wallet-is-one-step-closer

2017 2Qの動向 (2/6)

- BitFuryとRippleがBTC-LTC間でLightningトランザクションのデモ実施
  - https://www.coindesk.com/lightning-bank-ledgers-bitfury-ripple-demo-new-twist-bitcoin-tech/
  - https://github.com/interledgerjs/ilp-lightning-demo/blob/master/README.md
- Intel SGXを用いたスマートコントラクト向け認証済みoracleデータフィード、Town Crier
  - http://www.town-crier.org
- Lightning Networkのlnd、v0.3alphaを発表
  - https://github.com/lightningnetwork/lnd/releases/tag/v0.3-alpha
- Lightning Networkの実装間の互換にむけて、Eclair、c-lightning、lndが検討
  - https://medium.com/@lightning_network/towards-a-unified-lightning-network-8c12cb35b83a
  - https://cdecker.github.io/lightning-integration/

2017 2Qの動向 (3/6)

- Bitmain、AI分野にも参入
  - https://qz.com/1053799/chinas-bitmain-dominates-bitcoin-mining-now-it-wants-to-cash-in-on-artificial-intelligence/
- LitecoinベースのLightning Networkトランザクション成功
  - https://pbs.twimg.com/media/DIqAsOHUIAAXv1Y
- Bitcoin/Zcash間でHTLC用いてクロスチェーンアトミックスワップ取引（XCAT）のデモ
  - https://news.bitcoin.com/engineers-demonstrate-zcashbitcoin-atomic-swaps/
- Raiden Network、テストネットローンチ
  - https://www.ethnews.com/raiden-active-on-ethereum-testnet
  - https://medium.com/@raiden_network/raiden-network-developer-preview-dad83ec3fc23
  - https://raiden.network/101.html

2017 2Qの動向 (4/6)

- Cosmosを通じたEthereumスケーリング
  - https://blog.cosmos.network/the-shanghai-accord-ethereum-scaling-agreement-via-cosmos-at-wanxiang-global-blockchain-summit-354efa27b158
- Ethereum上のSwapプロトコル
  - https://themerkle.com/what-is-the-swap-protocol/
  - https://blog.airswap.io/introducing-swap-a-protocol-for-decentralized-peer-to-peer-trading-on-the-ethereum-blockchain-d4058f3179cf
- Vitalik、Ethereumは2年でVisa並のトランザクション性能を実現すると表明
  - https://techcrunch.com/2017/09/18/vitalik-buterin-explains-ethereum-in-his-own-words-at-disrupt-sf/
  - https://youtu.be/WSN5BaCzsbo
- Vitalik、Cosmosネットワークを用いたEthereumスケーリングについて合意
  - https://blog.cosmos.network/the-shanghai-accord-ethereum-scaling-agreement-via-cosmos-at-wanxiang-global-blockchain-summit-354efa27b158

2017 2Qの動向 (5/6)

- Vitalik、買い手のアクションに応じたインタラクティブなICOプロトコルを発表
  - https://www.coindesk.com/ethereum-founder-vitalik-buterin-co-authors-plan-iterative-ico-protocol/
  - https://people.cs.uchicago.edu/~teutsch/papers/ico.pdf
- Bitcoin-Ethereum間でのアトミックスワップに分散トレードプラットフォームAltcoin Exchangeが成功
  - https://news.bitcoin.com/altcoin-exchange-performs-first-atomic-swap-between-bitcoin-and-ethereum/
- Ethereum向けのアイデンティティ検証における相互運用性を高める標準化提案、ERC725
  - https://www.ethnews.com/erc725-a-self-sovereign-identity-standard-for-ethereum

2017 2Qの動向 (6/6)

- Ethereum、Byzantiumハードフォーク
  - https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/
  - http://btcnews.jp/rwiprhw512972/
- Quorum、ゼロ知識セキュリティレイヤーを統合
  - https://www.coindesk.com/jpmorgan-integrates-zcash-privacy-tech-enterprise-blockchain/
  - https://github.com/jpmorganchase/quorum/blob/master/README.md
- Parity、Ethereumアドレスをアイデンティティに紐付けるPICOPS発表
  - https://paritytech.io/blog/parity-technologies-launches-picops.html
- Enterprise Ethereum Alliance、新たに47社加盟
  - https://entethalliance.org/hewlett-packard-enterprise-47-organizations-join-200-member-strong-enterprise-ethereum-alliance/

3. プラットフォーム分野

① BitFury、Lightning Networkのテスト成功と
エンタープライズブロックチェーンExonumを発表
② 中国AntShares、NEOと改称し中国版Ethereumを狙う
③ Microsoft、エンタープライズ向けCoco Framework発表

BitFury、Lightning Networkのテスト成功とエンタープライズブロックチェーンExonumを発表

- Exonumベースのスマートコントラクトは、2.5秒のクリアリング時間にて、秒あたり3000トランザクションを処理。
- BitFuryはLightningむけルーティングFlareをテストするなどしていたなど、Lightning Network実装にも積極的。
- 同じ週には、BitFuryとしてビットコインのmainnet上でLightning Networkのテストを実施している。
- またBitFuryは、Richard Branson氏のネッカーアイランドで今月7/25-29で行われるブロックチェーンサミットのホストを務めることも発表された。
- 加えて、Bitfury Groupとして、東京オフィスを開設することも発表。

→ 出典: https://cointelegraph.com/news/bitcoin-mining-giant-bitfury-releases-enterprise-grade-blockchain
→ 出典: http://bitcoinist.com/bitfury-host-upcoming-blockchain-summit-sir-richard-bransons-private-necker-island/

中国ANTSHARES、NEOと改称し中国版ETHEREUMを狙う

- Onchain傘下のオープンソースプロジェクト。
- NEOにリブランディング。
- Ethereumの中国版として位置付け。
- ネイティヴ通貨ANS（NEOに変更予定）が中国内の取引所で取扱済。
- Ethereum同様にANSトークンをトランザクションガスとして支払う。
- スマートコントラクトを取扱う他、クロスチェーンの相互運用についても特許。
- EthereumのSolidityと違い、Antsharesはコンパイラを介して多くの言語と互換（.net、Java、Go、Pythonなど）。
- スマートコントラクトを用いたアセットのデジタル化にむけて、中国の認証機関と提携中。
- EthereumのThe DAOに似たものとして、Nest Fundがあり、ホワイトペーパー公開予定。

→ 出典: https://cointelegraph.com/news/is-antshares-poised-to-be-chinas-ethereum
→ 出典: https://www.financemagnates.com/cryptocurrency/bloggers/whats-big-deal-chinas-first-open-source-blockchain-platform-neo/
→ 出典: https://github.com/neo-project/docs/blob/master/en-us/index.md

MICROSOFT、エンタープライズ向けCOCO FRAMEWORK発表

- 各ブロックチェーンと互換であり、既にEthereumのインテグレーションを開始しているほか、R3 CordaやHyperledger SawtoothおよびQuorumともインテグレーション予定。
  - プライベート版Ethereum上で秒間1600トランザクションの処理性能がデモで紹介された。
  - フレームワークのオープンソースコードは2018年までにアクセス可能となる予定。

- Intelがハードウェア及び開発パートナーとして選定。
  - Intel SGXはTEE（Trusted実行環境）を用いてスループットおよびプライバシーに係る企業向け要件を充足。
  - Intel SGXにより、ブロックチェーンデータはトランザクションから必要とされるまで暗号化した状態で保持され、許可された参加者のみが参照できる領域ゆ復号化される。
  - またSGXでは再検証が回避され、代わりにリーダーが新しいブロックを作成および検証して、適切トランザクションだと検証済みと認証しブロックチェーンへポストすることでスケーラビリティを高めている。

→ 出典: https://azure.microsoft.com/ja-jp/blog/announcing-microsoft-s-coco-framework-for-enterprise-blockchain-networks/
→ 出典: https://software.intel.com/en-us/blogs/2017/08/10/collaborating-with-microsoft-to-strengthen-enterprise-blockchains
→ 出典: http://www.ibtimes.com/microsoft-announces-groundbreaking-blockchain-innovation-coco-framework-2576625
→ 出典: https://github.com/Azure/coco-framework/blob/master/docs/Coco%20Framework%20whitepaper.pdf
→ 出典: https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/08/blockchain-infographic.pdf

2017 2Qの動向 (1/4)

- Parityのマルチシグウォレットに脆弱性あり、31百万ドル相当のEtherが被害
  - https://blog.parity.io/security-alert-high-2/
  - https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce
  - http://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/

- Serpent言語に脆弱性。Augurむけ監査でZepperin Solutionsが指摘
  - https://www.coindesk.com/one-of-ethereums-earliest-smart-contract-languages-is-headed-for-retirement/

2017 2Qの動向 (2/4)

- IOTAホワイトペーパーv1.1日本語版
  - http://lhj.hatenablog.jp/entry/iota#IOTA-Whitepaper-v11-in-Japanese-UTC-20170815-公開版
- IOTA、ナノペイメントを可能とするFlash Networkを発表
  - https://www.cryptocoinsnews.com/iota-unveils-flash-network-allowing-for-true-nanopayments/
- IOTAに脆弱性
  - https://medium.com/@neha/cryptographic-vulnerabilities-in-iota-9a6a9ddc4367
  - https://www.forbes.com/sites/amycastor/2017/09/07/mit-and-bu-researchers-uncover-critical-security-flaw-in-2b-cryptocurrency-iota/
  - https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md

2017 2Qの動向 (3/4)

- Microsoft社、Project Bletchleyにエンタープライズ・スマートコントラクトを導入
  - https://www.ethnews.com/microsofts-azure-stack-releases-enterprise-smart-contracts
- Oracle社、ブロックチェーン基盤Oracle Blockchain Cloud Serviceを発表
  - https://www.oracle.com/corporate/pressrelease/oow17-oracle-launches-blockchain-cloud-service-100217.html
  - https://cloud.oracle.com/ja_JP/blockchain
  - https://japan.techrepublic.com/article/35108306.htm
- SAP社も、”SAP Leonardo Blockchain Early Access”発表
  - http://cloud.watch.impress.co.jp/docs/column/infostand/1085120.html
- 日立、生体情報から電子署名を生成してブロックチェーンの秘密鍵として付与できる技術を開発
  - http://www.itmedia.co.jp/news/spv/1710/05/news113.html

2017 2Qの動向 (4/4)

- GMOインターネットおよびDMMがビットコインマイニングに参入
  - https://www.gmo.jp/news/article/?id=5775
  - https://dmm-corp.com/press/press-release/17477

- GMOインターネット、OSS第五弾としてKYCのオープンソースを公開
  - https://guide.blockchain.z.com/ja/docs/oss/kyc/

個別サービス

名称	サービス概略	URL
Filecoin	ストレージ向け分散マーケット	→ https://filecoin.io/
Presearch	コミュニティベースの分散サーチエンジン	→ https://www.presearch.io/
Multichain	ビットコイン互換プライベートブロックチェーン	→ https://www.multichain.com/
BlockCAT	誰もが使えるスマートコントラクト	→ https://blockcat.io/
Cypherium	Bitcoin NGおよびByzcoinをベースとしたハイブリッドチェーン基盤	→ https://www.cypherium.io/
Ocean	分散型データ交換プロトコル	→ https://oceanprotocol.com
AirSwap	Swapプロトコルを実装するDEXプラットフォーム	→ https://www.airswap.io
Keep network	パブリックスマートコントラクト上でプライベートデータの計算可能	→ https://keep.network
Reality Check	スマートコントラクトoracleのクラウドソーシング	→ https://medium.com/@edmundedgar/snopes-meets-mechanical-turk-announcing-reality-check-a-crowd-sourced-smart-contract-oracle-551d03468177

4. ライフスタイル分野

① 2017 第二四半期の動向
② 個別サービスリスト

2017 2Qの動向 (1/2)

- ロシアのエアラインS7、Alfabankと共同でチケットをEthereumで発行
  - https://futurism.com/an-airline-just-started-using-ethereum-blockchain-to-issue-tickets/
- EMotorWerks、カリフォルニアでEV充電マーケットプレイス
  - https://www.greentechmedia.com/articles/read/blockchain-enabled-electric-car-charging-california
- エネルギー分野でブロックチェーンを活用する実証実験にmijinを提供
  - http://mijin.io/ja/923.html
- ソフトバンク、Sprint他とCarrier Blockchain Study Group設立
  - https://www.softbank.jp/corp/group/sbm/news/press/2017/20170908_01/
- KDDI、Quorumを用いた実証実験開始を発表
  - http://news.kddi.com/kddi/corporate/newsrelease/2017/09/27/2694.html

2017 2Qの動向 (2/2)

- GMOインターネット、転売抑止チケットのオープンソースを公開
  - https://iotnews.jp/archives/68535

- 中国Wanxian、スマートシティの電気自動車における大規模試行を発表
  - http://readwrite.jp/cities/34137/

個別サービス①

名称	サービス概略	URL
Indorse	分散プロフェッショナルクラウドソースプラットフォーム	→ https://indorse.io/
Rex	不動産MLSプラットフォーム	→ http://www.rexmls.com/index.html
Propy	分散不動産トランザクション	→ https://tokensale.propy.com/
Aventus	イベントチケット交換	→ https://aventus.io/doc/whitepaper.pdf
District0x	P2Pマーケットプレイス・コミュニティ	→ https://district0x.io/
Po.et	デジタルクリエイティブアセット向け所有権トラッキング	→ https://po.et/
Viberate	ミュージシャン向けペイメント	→ https://www.viberate.io/ https://www.viberate.com/
WePower	グリーンエネルギー取引プラットフォーム	→ https://wepower.network/
Soma	C2Cマーケットプレイス	→ http://soma.co/
ATLANT	不動産売買プラットフォーム	→ https://atlant.io/

個別サービス②

名称	サービス概略	URL
WePower	グリーンエネルギー取引所	→ https://wepower.network/
AdEx	デジタルアド取引所	→ https://www.adex.network/
NetObjex	IoTソリューション	→ http://www.netobjex.com/
MyBit	特定IoTアセット所有権を投資家どうしで流通	→ https://mybit.io/
Working Traveller	旅行者が小さな仕事を得ながら世界を旅できるプラットホーム	→ https://www.workingtraveller.com
Decentraland	VRコンテンツ向けプロパティ所有権購入できるサービス	→ https://decentraland.org
Doc.ai	人工知能と組み合わせ蓄積した医療情報もとにパーソナライズした情報提供	→ https://doc.ai/
Cointal	マルチカレンシーP2Pマーケットプレイス	→ https://www.cointal.com/
DOVU	モビリティデータのオープンマーケット	→ https://dovu.io

個別サービス③

名称	サービス概略	URL
CarbonX	ConsenSysが立ち上げたERC20トークンによるカーボンクレジット取引	→ https://www.carbonx.ca/
PROPS	ビデオアプリケーション向け分散エコシステム	→ https://www.propsproject.com
Blokur	音楽の権利管理	→ http://www.blokur.com
Yalls	Lightning Networkを使い記事をマネタイズするプラットフォーム	→ https://yalls.org/
WePower	グリーンエネルギーの取引プラットフォーム	→ https://wepower.network/

5.サプライチェーン系

① 2017 第二四半期の動向
② 個別サービスリスト

2017 2Qの動向 (1/5)

- ルノー、自動車修理データの安全確保への取り組み試行
  - 自動車メンテナンスログのプロトタイプ開発をMicrosoftなどと実施。
  - 自動車修理履歴はディーラーやリペアショップなど広範囲で管理されており、新たな変更のトラッキングが困難。
  - 今後のユースケースとして、自動車ベースのマイクロトランザクションなども視野。
  - https://www.coindesk.com/automaker-renault-trials-blockchain-bid-secure-car-repair-data/

2017 2Qの動向 (2/5)

- WalmartやNestle、Doleなど食品メーカーが食品安全にむけてIBMとコンソーシアム設立
  - https://www.coindesk.com/walmart-kroger-nestle-team-with-ibm-blockchain-to-fight-food-poisoning/
- NTTデータ、貿易情報連携基盤に向けたコンソーシアム設立
  - http://www.nttdata.com/jp/ja/news/services_info/2017/2017081501.html
- Xerox、ブロックチェーンタイムスタンプの特許申請
  - https://www.coindesk.com/proof-xerox-copier-giant-pursues-blockchain-time-stamping-strategy/
- 運送業界コンソーシアム、Blockchain in Trucking Alliance (BiTA)
  - https://bita.studio
  - https://bitcoinmagazine.com/articles/blockchain-trucking-alliance-seeks-revolutionize-transport-industry/

2017 2Qの動向 (3/5)

- 海上保険むけにMaersk、EYおよびMicrosoftが共同でプラットホーム開発
  - https://www.cnbc.com/2017/09/05/ey-microsoft-maersk-blockchain-for-marine-insurance.html
- サプライチェーン国際規格策定組織GS1、IBMおよびMicrosoftと標準化検討
  - https://www.gs1.org/articles/2256/blockchain-gs1-ibm-and-microsoft-collaborate-leverage-standards
- コンテナ大手Maersk、EY・Microsoft・Guardtimeと共同で海上保険プラットホーム構築
  - https://www.ft.com/content/d7e08624-918b-11e7-a9e6-11d2f0ebb7f0
- TencentとIntel、IoT向けブロックチェーン分野で提携
  - https://www.coindesk.com/tencent-taps-intels-hardware-for-iot-blockchain-solution/

2017 2Qの動向 (4/5)

- Bosch、BNY Mellon、Cisco等によるTrusted IoT AllianceがIoTむけオープンソースプロトコル確立に向けて公式ローンチを発表
  - https://s3.amazonaws.com/dive_static/paychek/Trusted_IoT_Alliance_press_release_Sept._19_2017_FINAL_as_of_Sept12_11am.pdf
- Pfizer、Quorumを用いた偽薬防止プラットフォームMediLedgerプロジェクトを発表
  - https://btcmanager.com/pharma-giants-use-ethereum-network-prevent-counterfeit-medicine/amp/
- BP、オイル・ガスのトレードシステムへの適用を試行
  - https://www.ft.com/content/100622d0-a680-11e7-93c5-648314d2c72c
- ジビエ食肉トレーサビリティへのmijin適用
  - http://jp.techcrunch.com/2017/10/03/blockchain-traces-gibier/

2017 2Qの動向 (5/5)

- 日立、みずほFGと共同で自社グループのサプライチェーンへの活用への実証実験
  - http://www.hitachi.co.jp/New/cnews/month/2017/09/0921c.html
- Air France、メンテナンス部品管理への適用を検討
  - http://www.aviationtoday.com/2017/10/03/air-france-klm-evaluating-mro-potential-blockchain/
- Cisco、IoTデバイスのモニタリング利用へ特許
  - 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=20170302663.PGNR.&OS=dn/20170302663&RS=DN/20170302663

個別サービス

名称	サービス概略	URL
SAMPLプロジェクト	3Dデータのライセンスマネジメント	→ https://www.tuhh.de/fks/010_research/projects/sampl/en/index_en.html
ExportPortal	国際貿易むけプライベートブロックチェーンソリューション	→ https://www.exportportal.com/
Ambrosus	食料品のトラッキング・フードサプライチェーン	→ https://ambrosus.com/
BlockFreight	コンテナフリート管理	→ https://blockfreight.com/
Lelantos	匿名配送システム	→ https://github.com/mhgharieb/Lelantos-Smart-Contract/blob/master/README.md
AgriDigital	食品のサプライチェーントラッキング	→ http://www.agridigital.io/
Sweetbridge	グローバルサプライチェーンネットワーク	→ https://www.sweetbridge.com/
modum	医薬業界むけサプライチェーンのモニタリング	→ https://modum.io/
iSolve	製薬会社むけサプライチェーン・マーケットプレイス	→ http://isolve.io/

6. シビックテック系

① 2017 第二四半期の動向
② 個別サービスリスト

2017 2Qの動向 (1/5)

- ネッカーアイランドで開催されたBlockchain Summitにおいて、World Identity Networkがローンチ
  - ユニバーサルIDや安全なデジタルアイデンティティシステムにむけた推進を目的とする活動。
  - 技術的に中立な活動であり、BitcoinやEthereumなどのみに依存しないものとしている。
  - BitFury、ConsenSys uPort、IOTAなどが参加。
  - http://www.prnewswire.com/news-releases/world-identity-network-launched-on-sir-richard-bransons-necker-island-this-week-300496195.html
  - https://www.win.systems/

2017 2Qの動向 (2/5)

- エストニア、e-residents向けに暗号トークンestcoin発行の提案を発表
  - 公式な暗号通貨ICOとしてコインを発行するもの。
  - Estcoinの便益を享受できるのは130万人のエストニア国民だけでなく、e-Residencyプログラムを通じて世界中の誰もが参加できる（現在e-Residentsには約23000人が138ヶ国から登録）。
  - 実現すると、エストニアは初めてICOを行なった国となる。
  - 従来、政府はICOのコンセプトに関心を示してこなかったが、エストニアの事例が変化をもたらす可能性も。
  - https://e-resident.gov.ee/estcoin
  - https://medium.com/e-residency-blog/estonia-could-offer-estcoins-to-e-residents-a3a5a5d3c894
  - https://themerkle.com/what-are-estcoins/
  - https://app.cyfe.com/dashboards/195223/5587fe4e52036102283711615553

2017 2Qの動向 (3/5)

- Sony Global Education、教育データの認証・共有システムへの応用
  - https://www.sony.co.jp/SonyInfo/News/Press/201708/17-071/
- UNICEF、スマートコントラクトを用いたアセット移転を試行
  - http://unicefstories.org/2017/08/04/unicef-ventures-exploring-smart-contracts/
- UNICEF、独自ICO検討
  - https://www.coindesk.com/no-token-response-unicef-is-open-to-doing-its-own-ico/
- イリノイ州、Hashedhealthと提携し医療ライセンス証明
  - https://medium.com/the-illinois-blockchain-initiative/illinois-opens-blockchain-development-partnership-with-hashed-health-fe3891e500bb

2017 2Qの動向 (4/5)

- EU、難民向けアイデンティティ管理に分散台帳技術を検討
  - https://www.ethnews.com/eu-2018-budget-amendment-calls-for-development-of-dlt-based-identities-for-refugees
- 米国疾病管理予防センター、災害時のリアルタイムデータ収集への活用を試行
  - https://www.coindesk.com/us-centers-disease-control-launch-first-blockchain-test-disaster-relief/
- BitNation、P2Pガバナンスシステム Pangeaのトークンセールを発表
  - http://cryptocurrencymagazine.com/wp-content/uploads/2017/10/bitnation_1006.pdf
  - https://github.com/Bit-Nation/Pangea-Docs/blob/master/BITNATION%20Pangea%20Whitepaper%202017.pdf
- EU、企業むけ情報共有ゲートウェイ開発を計画
  - https://www.coindesk.com/eu-developing-prototype-blockchain-platform-public-company-data/

2017 2Qの動向 (5/5)

- アルゼンチン、公示事項のタイムスタンプに七月からOpenTimestampのDapp利用
  - https://otslist.boletinoficial.gob.ar/ots/

- MIT、ビットコインブロックチェーンによる学位授与
  - http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017

個別サービス

名称	サービス概略	URL
SilentNotary	チャットボット上で行う公証サービス	→ https://silentnotary.com/
Arabianchain	UAEのパブリックチェーン	→ https://www.arabianchain.org/index.php/en/
DocStamps	Ethereum上のドキュメント公証	→ https://docstamp.io/
Eth4harvey	ハリケーン被害向けETH寄付	→ https://eth4harvey.com
Kleros	分散組織による法廷紛争解決	→ https://kleros.io
ClearPoll	意見収集への投票プラットホーム	→ https://www.clearpoll.io/
burstIQ	医療記録ストレージ	→ https://www.burstiq.com
Horizon State	投票・意思決定プラットフォーム	→ https://horizonstate.com
Pokitdok	ヘルスケアAPIプラットフォーム	→ https://pokitdok.com/
Patientry	患者情報のストレージサービス	→ https://patientory.com/

7.金融機関系の動き

① 2017 第二四半期の動向

米SEC、THE DAOに関して有価証券にあたる旨の声明を発表

- The DAOにより販売されたトークンが未登録の有価証券提供にあたるとのレポートを発表した。
- 併せて投資家向けに"Investor Bulletin"を発表し、ICOに参加する投資家が留意すべきポイントを開示した。
- DAOトークンは米国1933年法の定める有価証券の定義における投資契約。
- The DAOはコンピュータコードに組み込まれブロックチェーン上で実行されるとしても、有価証券の発行者にあたる。
- The DAOはDAOトークン提供にあたりSECに登録するか、有価証券法の適用除外に従い提供すべきであった。
- DAOトークンのプラットフォームは取引所にあたり、SECに登録するか、代替取引システム（ATS）の適用除外に従うべきであった。
- プロジェクトに資金調達するThe DAOの計画を実装することは、1940年法に基づく投資会社あるいは投資アドバイザーのステータスに疑問を投げかけるものであった。

→ 出典: https://www.sec.gov/litigation/investreport/34-81207.pdf
→ 出典: https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings
→ 出典: http://btcnews.jp/2nb2krci11936/
→ 出典: https://www.virtualcurrencyreport.com/2017/07/blockchain-and-digital-token-update-sec-releases-investigative-report-and-investor-bulletin/

2017 2Qの動向 ICO①

- 中国国内でのICO推進にむけたサンドボックス
  - 7/25に貴陽市（Guiyang）でICO規制カンファレンスを開催し、Guiyang ICO Consensusを発表。
  - 併せて、Guiyang Sandbox Planを発表。
  - ICOにより配布されたトークンの権利として、インフラ利用権或いはサービス利用料の事前支払いにあたるとしている。
  - http://news.8btc.com/guiyang-release-ico-regulatory-sandbox-consensus

- シンガポールMAS、国内でのデジタルトークン提供（ICO）への規制を発表
  - http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx

- 豪州証取、ICOへのガイドライン
  - http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/#what

2017 2Qの動向 ICO②

- 英FCS、米SEC・シンガポールMAS・中国PBOC・香港SFC・カナダCSAに続きICOに関する声明発表
  - https://www.fca.org.uk/news/statements/initial-coin-offerings
  - http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm
  - http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx
  - https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings
  - http://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=17PR117
  - http://www.nifa.org.cn/nifa/2955675/2955761/2967610/index.html

- Filecoinのトークンプレセールで適用された投資契約スキーム、SAFTのホワイトペーパーが公開
  - https://protocol.ai/blog/announcing-saft-project/
  - https://saftproject.com/

2017 2Qの動向 ICO③

- モーニングスター、仮想通貨およびICOの格付けサービス開始
  - http://www.sbigroup.co.jp/news/2017/1011_10830.html

- ベンチャー・中小企業の資金調達をサポートする「SBI CapitalBase」設立
  - http://www.sbigroup.co.jp/news/2017/1012_10832.html

2017 2Qの動向 証券①

- ロシア、ICOの合法化を準備へ
  - https://news.bitcoin.com/russia-legalize-icos/
- ベラルーシの中央銀行、証券市場へのブロックチェーン活用を発表
  - https://www.ethnews.com/republic-of-belarus-to-utilize-blockchain-for-securities-market
- ロシアNSD、Wavesと提携しデジタルアセットプラットフォーム開発へ
  - https://www.cryptoninjas.net/2017/07/29/waves-develop-digital-asset-platform-moscow-exchange/amp/
- ロシアNSD、暗号通貨向けウォレット開発
  - https://www.coindesk.com/russias-central-depository-plans-build-cryptocurrency-wallet/

2017 2Qの動向 証券②

- ロンドン証取、中小企業むけ株主情報管理をIBMとFabricで開発へ
  - http://www-03.ibm.com/press/us/en/pressrelease/52836.wss
- ジブラルタル証券取引所、取引・決済システムのブロックチェーン適用を計画
  - https://www.coindesk.com/gibraltar-stock-exchange-plans-blockchain-powered-trading-system/
- Nasdaq、時刻センシティブデータの配布に関する特許
  - https://www.coindesk.com/patent-reveals-nasdaq-planning-blockchain-powered-data-system/
- Nasdaq、スイスSIXとOTCプロダクトで協業
  - https://www.coindesk.com/nasdaq-inks-blockchain-trading-deal-swiss-stock-exchange/

2017 2Qの動向 証券③

- 香港証券取引所、ブロックチェーンベースのマーケットを開設へ
  - https://www.coindesk.com/hong-kong-stock-exchange-launch-blockchain-powered-private-market-2018/
- デラウエア州、株主名簿のブロックチェーン記載を合法化
  - http://fortune.com/2017/08/01/blockchain-shareholders-law/
- Gemini、シカゴオプション取引所むけにビットコインマーケットデータ提供
  - http://bitcoinist.com/winklevoss-gemini-exchange-to-allow-cboe-to-use-bitcoin-market-data/
- Bank of England、証券決済向け分散台帳技術に関してレポート発表
  - http://www.bankofengland.co.uk/research/Pages/workingpapers/2017/swp670.aspx

2017 2Qの動向 証券④

- Euroclear、CATボンドのセツルメント実施に続き、ブロックチェーン証券の上場検討
  - http://www.artemis.bm/blog/2017/08/04/first-blockchain-settlement-for-cat-bond-completed-by-solidum/
  - https://www.coindesk.com/euroclear-alternative-seeks-public-listing-blockchain-securities/

- シカゴマーカンタイル取引所、分散データベース関連で特許
  - http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20170295023.PGNR.&OS=dn/20170295023&RS=DN/20170295023

2017 2Qの動向 銀行①

- MUFGコイン、スマホ決済や自販機決済での利用をCEATECで一般公開
  - http://www.itmedia.co.jp/news/spv/1710/02/news105.html
- みずほ銀行、円との等価交換を想定したデジタルマネー"Jコイン"を構想
  - http://mw.nikkei.com/sp/#!/article/DGKKZO21231550X10C17A9MM8000/
- SBIホールディングス、独自決済プラットフォーム「Sコインプラットフォーム」構築開始を発表
  - http://www.sbigroup.co.jp/news/2017/0928_10815.html
- 全銀協、ブロックチェーン連携プラットホームのパートナーベンダー発表
  - https://www.zenginkyo.or.jp/news/detail/nid/8407/
- 三メガバンク、富士通と個人間送金サービスの実証実験
  - http://pr.fujitsu.com/jp/news/2017/10/10-2.html

2017 2Qの動向 銀行②

- タイKbank、貿易保証状サービスをIBMと開発
  - http://allcoinsnews.com/2017/08/08/kbank-and-ibm-develop-letter-of-guarantee-service-on-blockchain/
  - https://www.ethnews.com/kbank-releases-a-letter-of-guarantee-service-backed-by-blockchain-technology
- 中国中信銀行、クレジット決済システムBCLC開発
  - https://cointelegraph.com/news/chinese-banks-launch-first-blockchain-enabled-credit-applications
- イスラエルHapoalim銀行、Microsoftと銀行保証むけプラットホーム開発
  - https://www.coindesk.com/israels-largest-bank-begins-blockchain-trial-microsoft/
- W3C、暗号通貨によるブラウザペイメントAPIを検討中
  - https://www.coindesk.com/bitcoin-browser-google-apple-move-adopt-crypto-compatible-api/

2017 2Qの動向 銀行③

- UBS、ZFおよびIBMと開発した自動車用支払プラットフォームCar e Walletを発表
  - https://www.finextra.com/newsarticle/31057/ibm-and-ubs-team-on-blockchain-payments-for-cars
- UBS、Commerzbank等４行およびIBMとトレードファイナンスプラットフォーム開発を発表
  - http://www-03.ibm.com/press/us/en/pressrelease/53208.wss
- Credit Suisse、スマートコントラクトによるシンジケートローンを2018年商用化へ
  - https://www.coindesk.com/credit-suisse-could-be-using-smart-contracts-in-production-next-year/
- スイスFalcon Private Bank、アセット管理サービスの一環としてETHやLTC取扱へ
  - https://www.ethnews.com/bitcoin-suisse-ag-works-with-falcon-private-bank-to-offer-ether

2017 2Qの動向 銀行④

- 中央銀行デジタル通貨向けUSC（Utility settlement coin）へMUFGやBarclays、HSBCなど6行が参画表明
  - http://www.ibtimes.co.uk/utility-settlement-coin-blockchain-stepping-stone-fiat-digital-currency-1637807
  - https://www.coindesk.com/blockchain-ready-fiat-banks-see-big-promise-crypto-cash/
  - https://www.coindesk.com/hsbc-barclays-join-utility-settlement-coin-as-bank-blockchain-test-enters-final-phase/

- BoA、アイデンティティ認証むけ特許
  - http://bitcoinist.com/bank-of-america-files-three-new-blockchain-patents/

- 英FCA、RBSと共同でCordaによるモーゲージトランザクションレポートのプロトタイプを開発
  - https://www.coindesk.com/uk-financial-regulator-builds-blockchain-app-r3s-corda/

2017 2Qの動向 銀行⑤

- SWIFT、ノストロ照合の実証実験の中間報告を発表
  - https://www.swift.com/news-events/press-releases/swift-tests-show-blockchain-has-potential-for-global-liquidity-optimisation
- JP Morgan、Quorum上で銀行間ペイメントプラットフォーム
  - https://www.coindesk.com/jpmorgan-launches-interbank-payments-platform-quorum-blockchain/
- IBM、Stellarとクロスボーダーペイメントネットワーク構築
  - https://www.stellar.org/blog/IBM-KlickEx-Partnership/
- BoA、リアルタイムデータトラッキング関連で特許
  - http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20170293503.PGNR.&OS=dn/20170293503&RS=DN/20170293503
  - 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=20170295232.PGNR.&OS=dn/20170295232&RS=DN/20170295232

2017 2Qの動向 中央銀行①

- シンガポールMAS、DLTを用いたデジタルマネープロジェクトUbinを発表
  - 三段階で世界の中央銀行をDLTを介して接続するもの。
  - クロスボーダートランザクションをリアルタイムでDLTを介して行う。
  - ゼロ知識証明やIntel SGXを用いてトランザクションのプライバシーを保護。
  - 参加するのは、R3, BAML, Credit Suisse, JPMorganおよびMUFG。
  - 第1フェーズ（国内の銀行間ペイメント）は2016年末に完了し、SGDのトークン化についてホワイトペーパーとして公開済。同ペーパー内では、カナダ中央銀行でのEthereumベースプロトタイプであるプロジェクトJasperからの教訓も触れられている。
  - 現在推進中の第2フェーズではCSDとのインテグレーションを確認中。
  - 第3フェーズでは、銀行発行暗号通貨に取り組む予定。
  - http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx
  - http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf
  - https://www.coindesk.com/details-emerge-on-monetary-authority-of-singapore-plan-for-blockchain/

2017 2Qの動向 中央銀行②

- 日銀、ECBとの共同実験レポートを発表
  - http://www.boj.or.jp/announcements/release_2017/rel170906a.htm/
- ドバイ、デジタル通貨emCashを計画
  - http://www.trustnodes.com/2017/09/28/dubai-launch-state-issued-blockchain-based-digital-currency
- インド中央銀行、デジタル通貨Lakshmi発行を検討
  - http://www.india.com/news/india/reserve-bank-of-india-considering-to-introduce-its-own-cryptocurrency-similar-to-bitcoin-report-2478723/amp/
- ナイジェリア中央銀行も、デジタル通貨発行を計画
  - https://m.guardian.ng/business-services/cbn-mulls-digital-currency/

2017 2Qの動向 中央銀行③

- IMF、電子マネーとは異なるカテゴリーとしての仮想通貨の可能性に言及
  - http://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world

- カナダ中銀のProject Jasper、証券決済を対象とした第三フェーズへ
  - https://www.ethnews.com/project-jasper-enters-phase-three-of-testing

2017 2Qの動向 規制

- ジブラルタル政府、ブロックチェーン利用企業への規制を検討
  - http://gibraltarlaws.gov.gi/articles/2017s204.pdf

2017 2Qの動向 保険・カード

- AXA、スマートコントラクトによるフライト遅延保険をサービスイン
  - https://www.coindesk.com/axa-using-ethereums-blockchain-new-flight-insurance-product/
- 保険コンソーシアムB3i、IBMとプロトタイプ開発へ
  - http://blockchain-finance.com/2017/09/16/blockchain-in-the-insurance-industry-ibm-and-b3i-leverage-distributed-edger-technology/
- Mastercard、暗号通貨による払い戻しの特許
  - http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2F
- MasterCard、提携銀行むけにブロックチェーンAPIを解放
  - https://newsroom.mastercard.com/press-releases/mastercard-opens-access-blockchain-api-partner-banks-merchants/?__prclt=l29f9htk

8.金融系スタートアップの動き

① 2017 第二四半期の動向
② 個別サービスリスト

2017 2Qの動向

- Ripple、新たなプロダクトラインナップを発表
  - xCurrent、xRapid、xViaの３つのソリューションに体系化された。
  - xCurrent
    - Rippleのエンタプライズソフトウェアソリューション
    - 即時クロスボーダーペイメントをエンドトゥエンドでトラッキング可能な形で提供する
    - 銀行は互いにリアルタイムでメッセージしてペイメント詳細を確認することが可能となる
    - 各トランザクションのオペレーション面・リーガル面について明確にすべく、RippleNet Advisory Boardとの協力で開発したRulebookが含まれる。
  - xRapid
    - 顧客経験を改善しながらも流動性コストを最小化することを望むペイメントプロバイダーや金融機関むけに、低コスト流動性を提供するソリューション。
    - 新興市場むけペイメントは流動性コストが高く、xRapidは流動性に必要な資本を劇的に低減する。
  - xVia
    - 多様なネットワークを横断する形で送金を行いたい一般企業やペイメントプロバイダーや銀行むけに、標準のペイメントインターフェースを提供する。
    - シンプルなAPIであり、ソフトウェアのインストールを必要としない他、ユーザがシームレスで透明性高いペイメントを行い、インボイスのような豊富な情報を付与することが可能
  - https://ripple.com/solutions/

2017 2Qの動向

- テックビューロ、資金調達プラットフォームCOMSAを発表
  - COMSA自身のトークンセールに参加したCMSトークン保有者は、COMSAプラットフォームでICOを行うプロジェクトにて、CMSトークンで払い込む場合に追加ボーナスを得ることができる。
  - COMSAのICOソリューションとして、トークンを用いたビジネスプラン・サービスデザイン、既存ビジネスのアセットのサイバースペース上でのトークン化、ICO・トークン化におけるリーガルサポート、他言語のホワイトペーパー作成、クラウドセールプラットフォームを用いたトークンの作成・販売、などを提供。
  - NEMとEthereumでペッグされたハイブリッドトークンの発行とICOソリューション、NEMとEthereum上の暗号通貨・法定通貨とペッグしたトークン、内部高速トークン勘定としてのプライベートブロックチェーンmijin、ペッグされたトークンの裏付けとなるZaif取引所とそこでのトークンの取引取扱、を提供。
  - COMSA COREが、NEM、Bitcoin、Ethereumのブロックチェーン間でトークンのペッグと制御を司り、複数暗号通貨間で価値をトークンに変換し、総量をコントロールする。暗号通貨とペッグされたトークンの変換に特化して履歴記録する第一層、ペッグされたトークン間の変換履歴を記録する第二層という二層構造。中央集権化されたサーキットブレーカーとしてシステム障害に備える。
  - 複数のトランザクションを一つのセットとしてとりまとめ、該当当事者のマルチシグが完結した場合にその全てを同時にアトミックスワップとして実行するAggregate transactionを実装。

  - http://jp.techcrunch.com/2017/08/03/ico-platform-comsa/
  - https://comsa.io/ja/
  - https://comsa.io/ja/download/52740/

2017 2Qの動向

- Tether、Ethereumベースにトークン化した米ドルをBitfinexからスピンオフしたEthfinexと協業でローンチ
  - https://www.financemagnates.com/cryptocurrency/innovation/tether-launch-tokenized-us-dollars-ethereum-blockchain/
- R3、Corda v1.0をリリース
  - https://www.corda.net/2017/10/corda-v1-0-released/
  - https://docs.corda.net
  - https://www.r3.com/blog/2017/10/03/r3-launches-version-1-0-of-corda-distributed-ledger-platform/
- Bill & Melinda Gates財団、Rippleと貧困層むけ送金プラットフォームmojaloop開発へ協業
  - https://www.finextra.com/pressarticle/71169/gates-foundation-backs-ripple-collaboration-on-payments-platform-for-the-poor
  - https://ripple.com/insights/news/ripple-the-gates-foundation-team-up-to-level-the-economic-playing-field-for-the-poor/
  - http://mojaloop.io/

2017 2Qの動向

- ICOソリューションRICO
  - https://prtimes.jp/main/html/rd/p/000000001.000028957.html
- ConsensusBase、トークン発行・売出機能を集約したICOパッケージを開発
  - http://www.consensus-base.com/info/ico-package-release20171011/
- DG Lab、独自仮想通貨を発行できる「DG Lab DVEP」を開発
  - https://bitpress.jp/news/etc/entry-6575.html
- Tezos、ICO後に創業者と基金のと間でトラブル
  - https://archive.is/rUYeJ
  - https://www.reuters.com/article/us-bitcoin-funding-tezos-specialreport/special-report-backroom-battle-imperils-230-million-cryptocurrency-venture-idUSKBN1CN35K
  - https://medium.com/@arthurb/the-path-forward-eb2e6f63be67
  - https://hackernoon.com/tezos-tested-bbeeaa7a5449
  - https://restislaw.com/current-cases-investigations/tezos-initial-coin-offering/
  - http://blockesq.com/contact-us/

個別サービス①

名称	サービス概略	URL
Billon	リアルタイム送金	→ http://billongroup.com/en/
Enigma Catalyst	暗号通貨アセットのアルゴリズム取引・投資プラットフォーム	→ https://www.enigma.co/
ACT	ソーシャルファンディング	→ https://daoact.org/
Dether	P2Pによるether売買	→ https://dether.io/
Aigang	デジタル保険プラットフォーム	→ https://aigang.network/
ETHLend	ICO前プロジェクト向け貸し付け	→ https://about.ethlend.io/
HelloGold	少額でゴールド購入積立貯蓄	→ https://www.hellogold.com/
Bloom	分散クレジットスコアリング	→ https://hellobloom.io
dYdX	DEXプロトコル0x上に構築する分散型デリバティブ	→ https://dydx.exchange
Ripio	P2Pクレジットネットワーク	→ https://ripiocredit.network
Paradex	0xプロトコルを用いてウォレット上でERC20トークンをトレード	→ https://paradex.io
Templum	t0に続く規制対応トークンセールプラットフォーム	→ http://www.tradetemplum.com

9. 中国･ロシア の動き

① 中国の動向トピック
② ロシアを巡る動向トピック

中国の動向トピック (1/2)

- 中国当局によるビットコイン取引所への操業停止要求を受け、中国大手取引所が九月末で取引停止宣言
  - http://www.pbc.gov.cn/english/130721/3377816/index.html
  - http://btcnews.jp/5dek951l12593/
  - http://m.finance.caixin.com/m/2017-09-08/101142797.html
- 中国のビットコイン取引所に対する規制と各取引所の対応
  - https://ethereum-japan.net/bitcoin/chinese-bitcoin-regulation/
- 中国、海外ビットコイン取引所へのアクセス封鎖、取引所代表者の出国禁止措置
  - http://btcnews.jp/318ze96312625/
  - http://btcnews.jp/5upfb8z812720/
- 中国のビットコイン規制によりマイナーがASICとGPUを売却開始
  - https://ethereum-japan.net/bitcoin/chinese-miners-start-selling-their-asics-and-gpus/

中国の動向トピック (2/2)

- 中国で初めてのビットコインドキュメンタリー"Bitcoin-Shape the future"公開
  - http://news.8btc.com/the-first-chinese-bitcoin-documentary-provides-glimpse-into-the-future
  - https://youtu.be/MeRmVRFaTIY
- 人民銀行の研究者は、中国は速やかに自国のデジタル通貨を発行すべきと言及
  - http://www.zerohedge.com/news/2017-09-18/pboc-researcher-china-should-start-its-own-sovereign-digital-currency-soon-possible
- 中国、徴税と電子インボイスにむけGAchain開発へ
  - https://dcebrief.com/china-to-use-blockchain-for-taxes/
- 中国、Trusted Blockchain Open Lab開設
  - http://k.caixinglobal.com/web/detail_20491
  - http://www.trustnodes.com/2017/09/20/china-launches-trusted-blockchain-lab

ロシアを巡る動向トピック（1/3）

- ロシアがブロックチェーンスタンダードの開発に着手
  - https://www.cryptocoinsnews.com/russia-begins-work-developing-blockchain-standards/
  - https://www.ethnews.com/russias-rosstandart-working-to-establish-blockchain-standards
- ロシアで大規模マイニングセンター設立計画
  - http://btcnews.jp/4ibecgin12144/
- ロシア、国内マイニング産業への助成を計画
  - https://dcebrief.com/russia-reportedly-making-plans-to-subsidize-domestic-crypto-mining/
- モスクワ証券取引所、暗号通貨取引へ準備
  - https://news.bitcoin.com/moscow-stock-exchange-trade-cryptocurrency/

ロシアを巡る動向トピック (2/3)

- Ethereum Foundation、ロシア開発銀行と提携
  - https://www.coindesk.com/ethereum-foundation-strikes-deal-russian-development-bank/
- ロシア発電大手EvroSibEnergo、マイニングに余剰電力供給
  - https://www.rt.com/document/59a40520fc7e9376728b4567/amp/401183-russia-power-plant-crypto-mining
- ロシア保健省、患者の履歴交換にむけた実験
  - https://www.coindesk.com/russias-ministry-health-launching-blockchain-pilot/
- ロシア、環境配慮型暗号通貨コンセプトONF
  - https://www.coindesk.com/putin-backed-political-group-advances-green-cryptocurrency-concept/

ロシアを巡る動向トピック （3/3）

- ロシア中央銀行、暗号通貨取引所のサイトへのアクセスをブロックへ
  - https://www.reuters.com/article/us-russia-cenbank-bitcoin/russian-central-bank-to-ban-websites-offering-crypto-currencies-idUSKBN1CF0RF
- ロシア中央銀行、クリプトルーブル発行を検討
  - https://btcmanager.com/russian-central-bank-pivots-cryptocurrency-stance-endorses-crypto-ruble/
- ロシア、クリプトルーブル発行後は国内でのマイニングを禁止
  - https://www.rt.com/business/406960-russia-issue-blockchain-cryptoruble-putin/

10.参考資料リンク集

① 教材リスト
② 統計情報
③ 公開レポート
④ カンファレンス
⑤ 業界動向
⑥ ICO関連
⑦ 各国事情
⑧ スケーリング
⑨ ブロックチェーンの課題
⑩ 各種プロトコル

教材リスト (1/2)

- Stanford大学のビットコイン・暗号通貨講座のシラバス・教材が公開
  - https://crypto.stanford.edu/cs251/syllabus.html
- プリンストン大学のビットコイン講義のスライド&動画
  - https://piazza.com/princeton/spring2015/btctech/resources
- Courseraによる暗号通貨コース教材
  - https://www.coursera.org/learn/cryptocurrency
- Learn to build a blockchain: Beginner to Advanced
  - https://docs.google.com/spreadsheets/d/1jECwhJmDb6qEhVSVvIb2EJ00oraZBs_QDWuvdig2SnE/htmlview
- 68 Blockchain Articles & Whitepapers that Shaped Crypto into What it is Today
  - https://medium.com/founder-playbook/67-blockchain-articles-whitepapers-that-shaped-crypto-into-what-it-is-today-c538facfceb9

教材リスト (2/2)

- Selected resources on Bitcoin, Blockchain & Decentralization
  - https://medium.com/birds-view/selected-resources-on-bitcoin-blockchain-decentralization-e1b3e8457d3
- Learning Bitcoin from the Command Line
  - https://github.com/ChristopherA/Learning-Bitcoin-from-the-Command-Line/blob/master/README.md
- Khan AcademyによるJourney into cryptography
  - https://www.khanacademy.org/computing/computer-science/cryptography
- Jameson Lopp :: Bitcoin Resources
  - http://lopp.net/bitcoin.html
- Ethereumリーディングリスト
  - https://github.com/Scanate/EthList/blob/master/README.md

統計情報

- Investor Bitcoin and Altcoin Charts
  - http://charts.woobull.com
- Bitinfocharts
  - https://bitinfocharts.com/
- OP_RETURN Stats
  - http://opreturn.org/
- The best educational tool to understand how data are stored in Bitcoin blockchain
  - http://srv1.yogh.io
- A Glimpse at Unique Cryptocurrency Visualization Websites
  - https://bitbonkers.com
  - https://blocks.wizb.it
  - http://www.bitlisten.com
  - http://mapofcoins.com/bitcoin

公開レポート (1/4)

- A Bitcoin Standard: Lessons from the Gold Standard
  - http://www.bankofcanada.ca/wp-content/uploads/2016/03/swp2016-14.pdf
  - https://bitcoinmagazine.com/articles/bank-canada-report-imagining-bitcoin-standard-financial-system/

- IMF Proposes Central Bank Digital Currencies To Crush Cryptocurrencies
  - http://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985
  - https://www.technocracy.news/index.php/2017/08/11/imf-proposes-central-bank-digital-currencies-crush-cryptocurrencies/

公開レポート (2/4)

- Distributed ledger technical research in Central Bank of Brazil
  - http://www.bcb.gov.br/htms/public/microcredito/Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf
- Federal Reserve Next Steps in the Payments Improvement Journey
  - https://www.federalreserve.gov/newsevents/pressreleases/files/other20170906a1.pdf
- JPXによるDLTワーキングペーパー第二弾
  - http://www.jpx.co.jp/corporate/research-study/dlt/01.html
- フィンランド中央銀行によるビットコインペイメントシステムのレポート
  - https://helda.helsinki.fi/bof/bitstream/handle/123456789/14912/BoF_DP_1727.pdf;jsessionid=2F1E2EDBF1180739B5C13906CA99260E?sequence=1
  - https://dcebrief.com/bank-of-finland-economists-revolutionary-bitcoin-cannot-be-regulated/

公開レポート (3/4)

- BISによる中央銀行暗号通貨のレポート
  - https://www.bis.org/publ/qtrpdf/r_qt1709f.htm
  - https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf

- 欧州中央銀行（ECB）による証券ポストトレードへのDLT適用レポート
  - https://www.ecb.europa.eu/paym/intro/governance/shared/pdf/201709_dlt_impact_on_harmonisation_and_integration.pdf

- カナダ中央銀行による銀行間ペイメント決済への適用実験Project Jasperレポート
  - https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf

- Smart Contracts and Distributed Ledger - A Legal Perspective
  - https://www2.isda.org/attachment/OTU3MQ==/Smart%20Contracts%20and%20Distributed%20Ledger%20%20A%20Legal%20Perspective.pdf

公開レポート (4/4)

- Regulatory treatment of initial coin offerings(FINMA)
  - https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20170929-finma-aufsichtsmitteilung-04-2017.pdf
- Cryptocurrencies - Beneath the bubble (UBS)
  - https://www.scribd.com/mobile/document/361862351/Cryptocurrencies-Beneath-the-bubble
- Regulatory sandbox lessons learned report(FCA)
  - https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf
- Primer on Virtual Currencies (CFTC)
  - http://www.cftc.gov/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf

カンファレンス

- Blockstack Summit 2017
  - https://m.youtube.com/watch?v=3PcR4HWJnkY&feature=youtu.be
  - https://m.youtube.com/watch?v=4UXT5YVJwB4&feature=youtu.be
  - https://m.youtube.com/watch?feature=youtu.be&v=EtYJ748LA1M
- 10/2-10/3でCryptoeconomic Security Conference開催
  - https://cesc.io/#schedule
  - https://www.ethnews.com/amp/cryptoeconomic-security-conference-day-1-recap
  - https://www.ethnews.com/amp/cryptoeconomic-security-conference-day-2-recap
- 10/6-10/8でHacker Congress開催
  - https://liberate.hcpp.cz
  - https://youtu.be/mmSuxqaKR2U
  - https://youtu.be/WYMMeqXVEYo

業界動向

- CoindeskによるState of blockchainレポート2017 2Q編
  - https://media.coindesk.com/uploads/2017/09/state_of_blockchain_q2_2017.pdf
- Quarter Two 2017 in Review: massive growth in the blockchain industry
  - https://www.smithandcrown.com/quarter-two-review/
- Global Blockchain Benchmarking Study
  - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224
- Global Blockchain Startup Map
  - https://ww2.frost.com/news/press-releases/frost-sullivan-identifies-2017-global-blockchain-startup-map/
- Top 100 Blockchain Organisations
  - https://richtopia.com/top-lists/top-100-blockchain

ICO関連 (1/2)

- SECからICO投資家への注意喚起
  - http://btcnews.jp/3g3uwba011995/
  - https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings
- Token Salesについて
  - https://www.slideshare.net/mobile/masamasujima/token-sales
- ICOの正体
  - http://startupinnovators.jp/blog/647/
  - http://startupinnovators.jp/blog/655/
  - http://startupinnovators.jp/blog/657/
- 10億集めたICOが何もプロダクトをローンチできない理由
  - http://btcnews.jp/2ojkkse512376/

ICO関連 (2/2)

- ICOの概要徹底解説その１
  - http://btcnews.jp/3yul2byr11782/
- サンフランシスコで語られたICO（Initial Coin Offering）の論点
  - http://media.dglab.com/2017/07/17-matsuo-03/
- Coindesk ICO Tracker
  - https://www.coindesk.com/ico-tracker/
- Regulation Authorities Pick Up Pace Issuing Guidelines On ICOs
  - https://diarweekly.com/regulatory-authorities-initial-coin-offerings-examination-picks-up-pace-as-markets-continue-to-grow/

各国事情

- 世界各国の仮想通貨動向と規制最新動向リポート（欧州+α編）
  - http://btcnews.jp/3p6ksx6t11814/

スケーリング (1/4)

- 「ビットコイン分裂」の真相と深層
  - http://btcnews.jp/49vdi2of11755/
- Segwit/フォーク問題の簡単なまとめと私見
  - http://www.jpbitcoinblog.info/entry/20170718/1500364413
- Bitcoin Core :: Segwit2xとbtc1の誤った情報に関する訂正
  - https://bitcoincore.org/ja/2017/08/18/btc1-misleading-statements/
- ビットコインのブロックサイズ問題とSegWitの歴史(前編)
  - https://ethereum-japan.net/bitcoin/blocksize-problem-with-history-to-adapt-segwit/
- SegWitアクティベーションまでの長い道のり（後編）
  - http://btcnews.jp/4jib09mt12508/

スケーリング (2/4)

- ビットコインで有効化された「SegWit」を技術的に理解する
  - http://btcnews.jp/a9p28hth12470/
- Bitcoin Fork Wars: from xt to 2 x
  - https://www.slideshare.net/mobile/FedericoTenga/bitcoin-fork-wars-from-xt-to-2-x/1
  - https://youtu.be/Rnvo4muAXB4
- Correcting misinformation on Segwit2x and btc1
  - https://bitcoincore.org/en/2017/08/18/btc1-misleading-statements/
- 福岡ブロックチェーンエコノミー勉強会Vol.3「Segregated Witness」
  - https://www.slideshare.net/mobile/hawinternational/vol3segregated-witness
- Bitcoin: Segwit後の世界
  - https://www.slideshare.net/mobile/takayaimai/bitcoin-segwit

スケーリング (3/4)

- Lightning Networkの説明用スライド
  - http://joemphilips.com/post/lightningnetwork/
- Lightning技術のBOLT日本語訳
  - https://github.com/takaya-imai/lightning-rfc-japanese/blob/master_japanese/00-introduction.md
- Markdown Notebook - Ride the Lightning: How to use the Lightning Network on the Bitcoin Mainnet
  - https://interfect.github.io/#!/posts/009-Ride-the-Lightning.md
- Discreet Log Contracts(DLC)を読む
  - https://www.slideshare.net/mobile/takayaimai/discreet-log-contractsdlc
- Drivechain
  - https://github.com/drivechain-project/docs/blob/master/README.md

スケーリング (4/4)

- NYA(Segwit2x)への反対派リスト
  - http://nob2x.org/
- Segwitウォレット開発ガイド
  - https://bitcoincore.org/ja/segwit_wallet_dev/
- A Bitcoin Beginner’s Guide to Surviving the Bgold and SegWit2x Forks
  - https://bitcoinmagazine.com/articles/bitcoin-beginners-guide-surviving-bgold-and-segwit2x-forks/
- Preparing for the Bitcoin Hard Forks: A Step-by-Step Walkthrough
  - https://news.bitcoin.com/preparing-for-the-bitcoin-hard-forks-a-step-by-step-walkthrough/
- Bitcoin Cash is Bitcoin
  - https://www.bitcoin.com/info/bitcoin-cash-is-bitcoin

ブロックチェーンの課題 (1/2)

- 法律的な視点から見たブロックチェーンの課題
  - http://media.dglab.com/2017/07/19-matsuo-04/
- Open Source Operational Risk and Public Blockchains
  - https://speakerdeck.com/angelawalch/open-source-operational-risk-and-public-blockchains
- Bitcoin and Blockchain Technology: Hayek Money
  - https://speakerdeck.com/nando1970/bitcoin-and-blockchain-technology-hayek-money
- Blockchains Are Hard to Scale
  - https://hackernoon.com/blockchains-are-hard-to-scale-ca7dc80e9d8
- The very volatile value of cryptocurrencies
  - https://bankunderground.co.uk/2017/08/24/bitesize-the-very-volatile-value-of-cryptocurrencies/amp/

ブロックチェーンの課題 (2/2)

- Quantum Computing's Threat To Bitcoin And Cryptocurrency Appears To Be A Long Way Off
  - https://www.forbes.com/sites/amycastor/2017/08/25/why-quantum-computings-threat-to-bitcoin-and-blockchain-is-a-long-way-off/#260d7f002882
- The Distributed Future: How the Eventual Migration from Permissioned to Permissionless Ledgers
  - https://etherreview.info/the-distributed-future-how-the-eventual-migration-from-permissioned-to-permissionless-ledgers-will-50a7ecdb55e9
- Crypto 2.0 Musings - A Question Of Trust
  - https://www.linkedin.com/pulse/crypto-20-musings-question-trust-alex-batlin
- Don’t Write your Own Smart Contracts
  - https://blog.sia.tech/dont-write-your-own-smart-contracts-24e8fc9f71ec

各種プロトコル (1/2)

- IOTA:【技術解説】トランザクション大解剖！ウォレットは裏で何をやっているか
  - http://qiita.com/ABmushi/items/e271ff05884a7d47658d
- Blockchain and IoT: A Conversation with Dominik Schiener of the IOTA Foundation
  - https://www.cleantech.com/blockchain-and-iot-a-conversation-with-dominik-schiener-of-the-iota-foundation/
- DAG型暗号通貨のすすめ
  - http://btcnews.jp/2x5fpwlo12702/
- Hyperledger architecture working paper volume1 Concensus
  - https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf
- 分散システムについて語らせてくれ
  - https://www.slideshare.net/mobile/kumagi/ss-78765920

各種プロトコル (2/2)

- 分散型取引所についての考察（AirSwap(旧称:Swap), KyberNetwork, 0x）
  - http://btcnews.jp/2nt8f52212956/
- トークンの流動性リスクとBancor Protocol
  - https://speakerdeck.com/amachino/tokunfalseliu-dong-xing-risukuto-bancor-protocol
- How To Choose Your Favorite Cryptocurrency
  - http://bitemycoin.com/wp-content/uploads/2017/10/Choose-your-favourite-cryptocurrency.jpg

11.論文リスト

2017 2Qの関連論文リスト(1/4)

サービス概略	URL
Lelantos: A Blockchain-based Anonymous Physical Delivery System	→ https://eprint.iacr.org/2017/465.pdf
ClaimChain: Decentralized Public Key Infrastructure	→ https://arxiv.org/abs/1707.06279
NuCypher KMS: Decentralized key management system	→ https://arxiv.org/abs/1707.06140
Teechain: Scalable Blockchain Payments using Trusted Execution Environments	→ https://arxiv.org/abs/1707.05454
Image-based Proof of Work Algorithm for the Incentivization of Blockchain Archival of Interesting Images	→ https://arxiv.org/abs/1707.04558
Z-Channel: Scalable and Efficient Scheme in Zerocash	→ http://eprint.iacr.org/2017/684
On the Necessity of a Prescribed Block Validity Consensus: Analyzing Bitcoin Unlimited Mining Protocol	→ https://eprint.iacr.org/2017/686
Proofs of Work for Blockchain Protocols	→ https://eprint.iacr.org/2017/775
When the cookie meets the blockchain: Privacy risks of web payments via crypto currencies	→ https://arxiv.org/ans/1708.04748

2017 2Qの関連論文リスト(2/4)

サービス概略	URL
qBitcoin	→ https://arxiv.org/abs/1708.04955
Ontology of Blockchain Technologies. Principles of Identification and Classification	→ https://arxiv.org/abs/1708.04872
Merged Mining: Curse of Cure?	→ https://eprint.iacr.org/2017/791
Blockchain: A Graph Primer	→ https://arxiv.org/abs/1708.08749
Blockchain Based Intelligent Vehicle Data sharing Framework	→ https://arxiv.org/abs/1708.09721
Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin	→ https://arxiv.org/abs/1708.09790
A Note on Cryptocurrency Stabilisation: Seigniorage Shares	→ https://bravenewcoin.com/assets/Whitepapers/A-Note-on-Cryptocurrency-Stabilisation-Seigniorage-Shares.pdf

2017 2Qの関連論文リスト(3/4)

サービス概略	URL
Central Bank Digital Currency And The Future Of Monetary Policy	→ http://www.hoover.org/research/central-bank-digital-currency-and-future-monetary-policy
Blockchains and Distributed Ledgers in Retrospective and Perspective	→ https://arxiv.org/abs/1703.01505
BlockSci: Design and applications of a blockchain analysis platform	→ https://arxiv.org/pdf/1709.02489.pdf
A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform	→ https://arxiv.org/abs/1709.06921
Redesigning Bitcoin's fee market	→ https://arxiv.org/abs/1709.08881
Using Blockchain and smart contracts for secure data provenance management	→ https://arxiv.org/abs/1709.10000
A Petri Nets Model for Blockchain Analysis	→ https://arxiv.org/abs/1709.07790

2017 2Qの関連論文リスト(4/4)

サービス概略	URL
Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104
Non-interactive proofs of proof-of-work	→ https://eprint.iacr.org/2017/963.pdf
The Nuts and Bolts of Micropayments: a Survey	→ https://arxiv.org/pdf/1710.02964.pdf
Non-interactive proofs of proof-of-work	→ https://eprint.iacr.org/2017/963
Blockchain-based Smart Contracts: A Systematic Mapping Study	→ https://arxiv.org/abs/1710.06372
Link Before You Share: Managing Privacy Policies through Blockchain	→ https://arxiv.org/abs/1710.05363
Casper the Friendly Finality Gadge	→ https://ethresear.ch/uploads/default/original/1X/1493a5e9434627fcf6d8ae62783b1f687c88c45c.pdf

お役に立てば嬉しいです

- **BTCアドレス**

  1PAXBwKnZwNphWK7Wr9cdE8t1ESZ8xi5U1

→おしまい

Bitcoin & Blockchain概況

2017.10 by SATO

「Bitcoin2.0概況」「Blockchain2.0概況」から改題

第二部：Scaling Bitcoin準備

SCALING BITCOIN[11/4-5]のプログラム (1/4)

分野	タイトル	関連論文リンク
Privacy and Fungibility	BOLT Anonymous Payment Channels for Decentralized Currencies	https://eprint.iacr.org/2016/701.pdf https://z.cash/blog/bolt-private-payment-channels.html https://www.coindesk.com/anonymous-blockchain-micropayments-bolt/
	ValueShuffle: Mixing Confidential Transactions	https://eprint.iacr.org/2017/238.pdf https://bitcoinmagazine.com/articles/valueshuffle-brings-together-the-best-of-both-worlds-for-privacy-1483557170/ https://www.deepdotweb.com/2017/01/26/valueshuffle-comprehensive-transaction-privacy-bitcoin-users/
Scalability	FlyClient: Super Light Clients for Cryptocurrencies	特に無し
	BlockSci: a Platform for Blockchain Science and Exploration	https://freedom-to-tinker.com/2017/09/11/blocksci-a-platform-for-blockchain-science-and-exploration/ https://arxiv.org/abs/1709.02489 https://github.com/citp/BlockSci

SCALING BITCOIN[11/4-5]のプログラム (2/4)

分野	タイトル	関連論文リンク
Scalability	Graphene: A New Protocol for Block Propagation Using Set Reconciliation	https://people.cs.umass.edu/~gbiss/graphene.pdf
	Measuring maximum sustained transaction throughput on a global network of Bitcoin nodes	https://ja.scribd.com/document/359889814/ScalingBitcoin-Stanford-GigablockNet-Proposal
Smart Contracts	Atomically Trading with Roger: Gambling on the success of a hardfork	http://homepages.cs.ncl.ac.uk/patrick.mc-corry/atomically-trading-roger.pdf https://breaking-bitcoin.com/slides/AtomicallyTrading%20withRoger.pdf http://hackingdistributed.com/2017/07/11/atomic-transfer/
	Discreet Log Contracts	https://adiabat.github.io/dlc.pdf http://techmedia-think.hatenablog.com/entry/2017/07/08/181338 https://www.slideshare.net/takayaimai/discreet-log-contractsdlc
	Bitcoin script 2.0 and strengthened payment channels	特に無し

SCALING BITCOIN[11/4-5]のプログラム (3/4)

分野	タイトル	関連論文リンク
Proof Of Work	The Future of Proof of Work	特に無し
	Bobtail: A Proof-of-Work Target that Reduces Blockchain Mining Variance	http://export.arxiv.org/pdf/1709.08750
	The State of Cryptography	特に無し
Layer 2	How to Charge Lightning	特に無し
	Using the Chain for what Chains are Good For	特に無し
	Concurrency and Privacy with Payment-Channel Networks	https://eprint.iacr.org/2017/820.pdf

SCALING BITCOIN[11/4-5]のプログラム (4/4)

分野	タイトル	関連論文リンク
Consensus	Microchains	特に無し
	Incentives and Trade-offs in Transaction Selection in DAG-based Protocols	特に無し
	Changes without unanimous consent	特に無し
Fees and Radio	Optimizing fee estimation via the mempool state	特に無し
	Redesigning Bitcoin's fee market	https://export.arxiv.org/pdf/1709.08881 https://medium.com/@avivzohar/rethinking-bitcoins-fee-market-ea9319e4ea57
	Weak-Signal Radio Communications for Bitcoin Network Resilience	特に無し
	Plasma for Bitcoin	特に無し

①Bolt: Anonymous Payment Channels for Decentralized Currencies
分散通貨むけ匿名ペイメントチャネル(1/5)

- BOLT (Blind Off-chain Lightweight Transactions)。
  - Lightning Networkに触発された、高速なプライベートペイメントチャネルプロトコル。

- パブリックな台帳への記録による課題
  - ビットコインの成功は、そのトランザクションが透明な形でブロックチェーンという、信頼される機関の必要性を排除するパブリックなグローバル台帳へ記録されるという事実に拠るところが大きい。
  - ビットコインは大きな成功を勝ち得た一方で、ブロックチェーンへ全レコードを記録することは、プライバシーやレイテンシーやスケーラビリティの問題をもたらす。
  - 暗号通貨は、スケーラビリティ・遅い・コンファメーションに時間がかかる、という三つの課題に直面。
  - Lightning NetworkやThunder Networkといったマイクロペイメントチャネルは、新たなレイヤーへトランザクションを移すことによって、前者２つの課題を解決した。
  - 全てのトランザクションをブロックチェーンに記録する代わりに、ユーザはチャネルを開設し、トランザクションを必要に応じてブロックチェーン上でセツルメント。
  - プライバシーの課題はZerocoinやZcashといった匿名型の暗号通貨によって解決するとされるが、チャネルの開設・閉鎖に際する情報開示からガードするまでであり、マイクロペイメントチャネル上の情報はほぼ隠蔽されないことが課題。

→ 出典: https://eprint.iacr.org/2016/701
→ 出典: https://z.cash/blog/bolt-private-payment-channels.html
→ 出典: https://www.coindesk.com/anonymous-blockchain-micropayments-bolt/

①Bolt: Anonymous Payment Channels for Decentralized Currencies
分散通貨むけ匿名ペイメントチャネル(2/5)

- 代表的なオフチェーンペイメントとしての「ペイメントチャネル」のプライバシー課題
  - たとえば、Lightning Networkであったり、Duplex Micropayment Channelsなど。
  - 個々のペイメントトランザクションをブロックチェーンへポストする代わりに、チャネルはブロックチェーンを使って、二者間の共有デポジットを作る。
  - 参加者は、デポジットのそれぞれの持分を調整しながら、直接ペイメントを作ってやりとりする一方、ブロックチェーンとのやりとりは、チャネルクローズのときもしくは参加者間の紛争解決のために限られる。
  - ペイメントチャネルの主な利点は、新たな信頼される中央管理者を追加することなしに、トランザクションボリュームの劇的な低減できることであり、ペイメントチャネルはスケーリング問題への解を提供するものの、プライバシー面の課題がある。
  - ペイメントはオフチェーンで処理されるが、どの参加者も仮名のアイデンティティや、初期のチャネルの残高を知ることが出来る。
  - さらには、ペイメントチャネルはトランザクション相手に対するプライバシー保護をほとんど提供しない。
  - あるウェブコンテンツむけの支払いのためにペイメントチャネルを構築することによって、ユーザは暗黙のうちに、所与のチャネル上の各ペイメントを、当該チャネル上の他ペイメントとリンクする。
  - これはペイメントが取引所のような共通の仲介ピアを介してルーティングされる場合に、特に問題になる。

→ 出典: https://eprint.iacr.org/2016/701
→ 出典: https://z.cash/blog/bolt-private-payment-channels.html
→ 出典: https://www.coindesk.com/anonymous-blockchain-micropayments-bolt/

①Bolt: Anonymous Payment Channels for Decentralized Currencies
分散通貨むけ匿名ペイメントチャネル(3/5)

- Lightning Networkのプライバシー課題
  - Lightning Networkはチャネル参加者間の匿名性を提供するものではない。
  - Lightning Networkはこの問題に対して、複数の仲介ノードを介してペイメントをルーティングすることによって対処するものだが、この場合は、ペイメントチャネル構築の複雑性をかなり高める他、仲介人の一部でも裏切ればペイメント情報が漏れてしまう。
  - オニオンルーティングネットワークに類似した原則に従って、不正を働かない複数の仲介人を用いることによって、経路上の出発地や目的地を不明瞭化するものの、裏切りの問題は残るため、A→B→C→D→Eへと繋ぐとき、BとDが裏切るだけでAとEの身元は暴露される。
  - これは、パス上の全トランザクションは同じHTLCのIDを共有するためである。

- Boltは、プライバシーを保持したままリンク不能なペイメントチャネルを構築する技術
  - 高速でプライベートなオフチェーントランザクションを提供しつつ、プライバシー保持分散ペイメントを拡張するもの。
  - 単純に参加者のアイデンティティを中間介在人から見えなくするのではなく、匿名のダイレクトチャネルを構築する。

→ 出典: https://eprint.iacr.org/2016/701
→ 出典: https://z.cash/blog/bolt-private-payment-channels.html
→ 出典: https://www.coindesk.com/anonymous-blockchain-micropayments-bolt/

①Bolt: Anonymous Payment Channels for Decentralized Currencies
分散通貨むけ匿名ペイメントチャネル(4/5)

- BOLTを用いると、同一チャネル上の複数ペイメントが互いにリンクすることがない。
  - チャネル内のペイメントをリンク不能とすることによって、プライバシーの課題に対処。
  - セキュアで即時のプライベートペイメントによって、ペイメントネットワーク状のストレージ負荷を軽減する。
  - 例えばZcashでその強力なプライバシー保護を維持したまま、よりスケーラブルに出来る可能性。
  - 支払いは数ミリ秒の内に行われ、ブロックコンファメーションを必要としない。
  - マーチャントが分かるのは、自分がオープンしたチャネル上で支払いが行われたということのみ。
  - 支払いはサードパーティを介してルーティングされ、顧客とマーチャントが直接チャネルを持つ必要がない。
  - 参加者匿名性維持／送金額隠蔽の双方を通じて、悪意あるサードパーティからプライバシーを保護。

- Boltの提案は、「一方向ペイメントチャネル」「双方向ペイメントチャネル」「間接チャネル」の３つから成る。

- 「一方向ペイメントチャネル」は、顧客が自身のアイデンティティを明かすことなしに支払いを行い、同じチャネル上で実行されたトランザクションをリンクすることを許すもの。
  - 従来型ペイメントチャネルの匿名性や機能性を保持しながら、顧客～店舗間の固定値トークンの簡潔な支払いを可能とする。

→ 出典: https://eprint.iacr.org/2016/701
→ 出典: https://z.cash/blog/bolt-private-payment-channels.html
→ 出典: https://www.coindesk.com/anonymous-blockchain-micropayments-bolt/

①Bolt: Anonymous Payment Channels for Decentralized Currencies
分散通貨むけ匿名ペイメントチャネル(5/5)

- 参加者が相互に直接接続してペイメントを更新する「双方向ペイメントチャネル」。
  - 一方向ペイメントチャネル技術を拡張して、チャネル横断で変動値ペイメントを可能とするもの。
  - ペイメントが顧客～店舗間でいずれかの方向で流れるもの。このチャネルによって参加者は正負任意の値を交換できる。
  - 二者が紛争解決のためだけに台帳を用いるという「マイクロペイメントチャネル」をもとに、匿名ペイメントチャネルを構築。
  - コミットメントおよびブラインド署名を用いることによって、マイクロペイメントチャネル中のIOUを匿名化。
  - コミットメントはペイメントの値を隠蔽し、ブラインド署名は何が署名されたかを明らかにすることなくトランザクションへ署名できるようにする。
  - 信用されない中間介在人を通じたペイメントを許可する技術。

- 「間接チャネル」はサードパーティペイメントを可能とするもので、これは信用されない中間介在人がブリッジとして機能して、値の交換を許すもの。
  - 中間介在人は参加者のアイデンティティもトランザクション量も知ることが無い。
  - この技術が利用可能となると、匿名ペイメントチャネルが利用不能となる。
  - M人の参加者において必要とされるオープンチャネル数をO(M^2)からO(M)へと低減するため。

→ 出典: https://eprint.iacr.org/2016/701
→ 出典: https://z.cash/blog/bolt-private-payment-channels.html
→ 出典: https://www.coindesk.com/anonymous-blockchain-micropayments-bolt/

②ValueShuffle: Mixing Confidential Transactions ミキシング秘匿トランザクション(1/6)

- ブロックチェーンのパブリックな性質はビットコインユーザのプライバシーにとって深刻な脅威。
  - ファンドは追跡できるため、二つのコインが同一であるということは無く、fungibility（可換性）という全ての通貨に必要とされる基本的性質がリスク。
  - こうした脅威を踏まえ、いくつかのプライバシー拡張技術が、ビットコインのトランザクションプライバシーを改善するために提案されてきた。
  - しかしながら、通貨の再設計や、現在実装されている機能を破壊することを必要であったり、特定のプライバシー課題を解決するだけのものであったりする。

- CoinJoin/CoinShuffleは、信頼された参加者を必要とすることなく、複数のトランザクションを１つにマージする方法。
  - 誰が誰に支払ったというコインの証跡を難読化することが出来る。
  - トランザクション中のコインの金額は明かされるため、難読化は可能性にすぎない。
  - もしあるトランザクションが5BTCを送金し、他のトランザクションが7BTCを送金し、これらを１トランザクションにマージするだけでは、金額を「マッチング」することで誰が誰に送金したか明らかになる点が問題。

→ 出典: https://eprint.iacr.org/2017/238
→ 出典: https://bitcoinmagazine.com/articles/valueshuffle-brings-together-the-best-of-both-worlds-for-privacy-1483557170/
→ 出典: https://www.deepdotweb.com/2017/01/26/valueshuffle-comprehensive-transaction-privacy-bitcoin-users/

②ValueShuffle: Mixing Confidential Transactions ミキシング秘匿トランザクション(2/6)

- プライバシーの問題を克服するための様々な提案がされているが、プライバシーの１側面（支払い者の匿名性、受け手の匿名性、支払い金額のプライバシー）にフォーカス。
  - Confidential Transactionは支払い金額のプライバシーであり、ステルスアドレスは支払い者がユニークなワンタイムアドレスを生成することによって受け手の匿名性を改善するもの。
  - 支払い者の匿名性としては、CoinJoin等のコインミキシングが、ユーザグループが互いのコインを交換することによって、ファンドとオーナーの関係性を隠蔽する。

- 包括的なプライバシーを実現するために、上記の３つ（Confidential Transaction、ステルスアドレス、コインミキシング）を組み合わせることが必要だが、課題がある。
  - ストレスアドレスはコインミキシングと容易に組み合わせることが可能だが、Confidential Transactionのトラストモデルと、P2Pコインミキシングが互換性あるものかどうかが明確でない。
  - Confidential Transactionの設計は、トランザクションが１ユーザによって生成されるものと仮定しているのに対し、P2Pコインミキシングでは、互いに信用しないユーザグループが合体してCoinJoinトランザクションを生成しているという問題がある。

- インプットとアウトプットの関係や、互いの送金額を明かすことの無いような、P2Pコインミキシングプロトコルを設計できないか、というのが問題。

→ 出典: https://eprint.iacr.org/2017/238
→ 出典: https://bitcoinmagazine.com/articles/valueshuffle-brings-together-the-best-of-both-worlds-for-privacy-1483557170/
→ 出典: https://www.deepdotweb.com/2017/01/26/valueshuffle-comprehensive-transaction-privacy-bitcoin-users/

②ValueShuffle: Mixing Confidential Transactions ミキシング秘匿トランザクション(3/6)

- ValueShuffleは、CoinJoinをもとに、Confidential Transactionと互換性のある、初のコインミキシングプロトコルを設計したもの。
  - ミキシング参加者の匿名性を保証するとともに、送金額を隠蔽する技術であるConfidential Transaction技術を用いて、送金額の秘匿性を保証するコインミキシングプロトコル。
  - Confidential Transactionの技術を用いてトランザクション中の金額を隠蔽することによって、金額マッチング問題を解決する。
  - CoinJoinとConfidential Transactionを組み合わせることで、CoinJoinが信頼される参加者を必要とすることなく、異なるトランザクションを１つにマージし送金アドレスを難読化する一方、Confidential Transactionが金額を隠蔽しリンク不可能とする。

- Confidential Transactionは、Blockstream社のElements Alphaサイドチェーンに実装されており、ビットコインのテストネット上でアクティブになっている。
  - Confidential Transactionは通常のトランザクションより費用がかさむため、SegWitによるWitnessの「ディスカウント」が一助となるほか、もしSchnorr署名アグリゲーションがSegWitを通じてデプロイされれば効率面でより恩恵となる。
  - Confidential Transactionがビットコインプロトコルに統合されると仮定すると、ValueShuffleは、異なる価値のファンドをミックスしたり、同一トランザクション内でファンドをミックスして消費することを可能とし、従来のコインミキシングプロトコルの制約を克服する。

→ 出典: https://eprint.iacr.org/2017/238
→ 出典: https://bitcoinmagazine.com/articles/valueshuffle-brings-together-the-best-of-both-worlds-for-privacy-1483557170/
→ 出典: https://www.deepdotweb.com/2017/01/26/valueshuffle-comprehensive-transaction-privacy-bitcoin-users/

②ValueShuffle: Mixing Confidential Transactions ミキシング秘匿トランザクション(4/6)

- ステルスアドレスを組み合わせることによって、基本的デザインや既存の機能を壊すことなしに、包括的なプライバシーを提供する。
  - ステルスアドレスやConfidential Transactionと組み合わせることによって、包括的なプライバシーを提供（追跡不能性、送受信者の匿名性、送金額プライバシー）。
  - ブロックチェーンの観察者もミキシングの参加者も、インプットやアウトプットをトレースできない。
  - そのためアウトプットトランザクションを送金者のアドレス特定のために用いることが出来ない。
  - またステルスアドレスがワンタイムアドレスを生成してペイメントを受け取り、トレースを回避。
  - 受け手とやりとりをする必要なしにダイレクトに送金可能であり、匿名でのペイメントがブロックチェーン上に１トランザクション文記録されるだけで送金できる。
  - CoinJoinトランザクションのインプット／アウトプットの紐付けを防ぐため、Torネットワークのような、外部の匿名チャネルを利用しない。

→ 出典: https://eprint.iacr.org/2017/238
→ 出典: https://bitcoinmagazine.com/articles/valueshuffle-brings-together-the-best-of-both-worlds-for-privacy-1483557170/
→ 出典: https://www.deepdotweb.com/2017/01/26/valueshuffle-comprehensive-transaction-privacy-bitcoin-users/

②ValueShuffle: Mixing Confidential Transactions ミキシング秘匿トランザクション(5/6)

- 関連技術との比較
  - TumbleBit
    - ユーザがタンブラーを信用する必要が無いプロトコル。
    - TumbleBitを用いた通常のペイメントでは少なくとも２つの連続したビットコイントランザクションが必要。
    - ValueShuffleは一つのトランザクションしか必要しない。
  - CryptoNote
    - リング署名を用いて、トランザクション送信者の匿名性を提供。
    - 拡張版CryptoNoteはConfidential Transactionと互換性があり、Moneroに実装されている。
    - ValueShuffleと違い、オンラインミキシングプロトコルを必要とせず、オフラインのファンドを用いて匿名セットを生成可能。
    - CryptoNoteはブロックチェーン上でミキシングを行い、匿名セットのサイズnとしたとき、各トランザクションにO(n)サイズのリング署名を含む。
    - リング署名を格納することはブロックチェーン上の多くのスペースを必要とし、その検証は全ノードに大きな負荷をかける。
    - 一方、ValueShuffleはミキシングをオフチェーンで行い、ブロックチェーンへ結果のみを格納するという利点がある。
    - CryptoNoteはプルーニングと互換性がない。
    - プルーニングは、古いブロックや検証された使用済みトランザクションを消去することによって、ノードの必要ストレージを劇的に削減するもの。
    - CryptoNoteではリング署名を使っているため、クライアントが、トランザクションアウトプットが使用済みでプルーニング可能かどうかを決定することができないため、こういったことが不可能。
    - ValueShuffleのようなCoinJoinベースのアプローチの場合、こうした問題がなく、プルーニングとの互換性がある。

→ 出典: https://eprint.iacr.org/2017/238
→ 出典: https://bitcoinmagazine.com/articles/valueshuffle-brings-together-the-best-of-both-worlds-for-privacy-1483557170/
→ 出典: https://www.deepdotweb.com/2017/01/26/valueshuffle-comprehensive-transaction-privacy-bitcoin-users/

②ValueShuffle: Mixing Confidential Transactions ミキシング秘匿トランザクション(6/6)

- 関連技術との比較
  - Mimblewimble
    - トランザクションのアグリゲーションを行うことによって、ブロックチェーンのスケーラビリティに大きな利点があるが、マイナー等、アグリゲーションを実行する参加者に対して、インプット・アウトプット間のリンク不能性を保証しない。
    - スクリプトのサポートが無く、ValueShuffleはビットコインに実装されているスクリプトをサポートする。
  - Zcash
    - 匿名性を提供する暗号通貨であり、強力なプライバシー保証を行う一方で、zkSNARKSを用いているため、広く普及するかどうか明確でないほか、どのアウトプットが使用済みかを観察できないため、プルーニングが不可能。

→ 出典: https://eprint.iacr.org/2017/238
→ 出典: https://bitcoinmagazine.com/articles/valueshuffle-brings-together-the-best-of-both-worlds-for-privacy-1483557170/
→ 出典: https://www.deepdotweb.com/2017/01/26/valueshuffle-comprehensive-transaction-privacy-bitcoin-users/

③BlockSci: a Platform for Blockchain Science and Exploration

ブロックチェーンサイエンスおよび調査むけプラットフォーム(1/2)

- ブロックチェーン分析むけのオープンソースソフトウエアプラットフォーム。
  - ブロックチェーンサイエンスを可能とするためのソフトウェアプラットフォーム。
  - Bitcoinブロックチェーンは140GBであり成長を続けており、ユーザ・事業者・マイナー等といった、Bitcoinエコシステムへの洞察をもたらす大量のデータを保持している。
  - ブロックチェーンデータの分析は、科学研究および商用の双方にとって有用。
  - BlockSciは、Bitcoinや他ブロックチェーンの分析を可能にし、異なるブロックチェーンや分析作業のためのサポートにおいて有用。

- カスタムなインメモリーデータベースを利用することで高速化。
  - 既存ツールの課題は、低パフォーマンス、ケイパビリティ不足、扱いにくいプログラミングインタフェース。
    - BlockSciは、既存ツールより15倍～600倍高速な他、アドレスクラスタリングといった分析モジュールを備え、共通インタフェースで異なるブロックチェーンに対応して為替レートやmempoolデータのインポートなどが可能。
  - 現在のブロックチェーン分析ツールは、ACIDを保証する汎用データベースに依存している。
    - BlockSciは、インメモリーの分析データベース（トランザクションデータベースではなく）を組み込んでいるため、既存のツールと比べて数百倍高速。
    - カスタムデータフォーマットを用いており、bitcoindのような暗号通貨ノードによって記録されるシリアライズされたブロックチェーンフォーマットからデータを生成する。
    - オープンソースでパブリックに利用可能であり、ビットコインブロックチェーンデータや追加ツールを含んだ、EC2イメージを用いてスタートできる。

→ 出典: https://arxiv.org/abs/1709.02489
→ 出典: https://github.com/citp/BlockSci
→ 出典: https://freedom-to-tinker.com/2017/09/11/blocksci-a-platform-for-blockchain-science-and-exploration/

③BlockSci: a Platform for Blockchain Science and Exploration
ブロックチェーンサイエンスおよび調査むけプラットフォーム(2/2)

- BlockSciのアーキテクチャ
  - 「P2PノードからのJSON-RPC」および「ブロックチェーンローデータ」という２つのルートがあるが、どちらを通ったデータも、同じ中間フォーマットに変換され、パーサーに渡される。
  - ブロックチェーンデータはトランザクション検証や改ざん困難性、メモリ消費最小化を目的とした構造のため、そのままでは分析に使いにくい。
  - パーサーは、分析向けデータセットである「コアブロックチェーンデータ」を生成し、これは新しいブロックが来るたびにインクリメンタルに更新される。
  - このデータを分析ライブラリーがインメモリデータベースへロードして、ユーザは直接あるいはPythonインタフェースを介してクエリを投げることが可能。

- BlockSciの有用性を示すべく４つの分析結果を提示している。
  - ブロックチェーンサイエンスを効率的にサポートするBlockSciの応用として、４つの分析を実施。
  - 前半２つはプライバシーや機密性に関するもの、後半２つは暗号通貨の経済に関するもの。
  - マルチシグがプライバシーや機密性をどの程度弱めるか
  - プライバシーフォーカスのアルトコインであるDashへのクラスター交点攻撃
  - ブロックスペースの利用における非効率性
  - コイン保有の変更頻度の見積方法

→ 出典: https://arxiv.org/abs/1709.02489
→ 出典: https://github.com/citp/BlockSci
→ 出典: https://freedom-to-tinker.com/2017/09/11/blocksci-a-platform-for-blockchain-science-and-exploration/

④Graphene: A New Protocol for Block Propagation Using Set Reconciliation
セットリコンサイルを用いたブロック伝播むけ新プロトコル

- 効率的なブロック伝播のためのインタラクティブなセットリコンサイル方法を提案。
  - ブロックチェーンではネットワーク遅延やオーバヘッドが顕著。
  - 伝播の遅延や新ブロックの流通にかかるネットワーク費用は、ブロックのサイズに依存し、遅延短縮・トラフィック混雑緩和が望まれている。
  - 本提案では、ブロックの効率的な伝達方法を提案するもの。
  - BitcoinやEthereumなどの様々なブロックチェーンネットワークへ適用が可能。

- Grapheneは、Bloomフィルタ（確率的データ構造）をIBLTと組み合わせるもの。
  - パフォーマンス評価を行い、Grapheneのブロックが常に通常より小さくなることを示す。
  - 例えば、Xtreme ThinblockはCompact Blockにより10KBにエンコードされるが、同じ情報がGrapheneでは2.6KBにエンコード。

- IBLT（Invertible Bloom Lookup Tables）の概観。
  - ２者間のセットリコンサイル向けに効率的なデータ構造。
  - Bloomフィルタ同様に、IBLTはセット中のどの値を共通のものとしてシェアするかを、2者が決定することを許可する。一方で、Bloomフィルタと異なり、IBLTは、固定長と想定できてバイナリ文字列として暗号化される値の欠落についてリカバリーを可能とする。

→ 出典：https://people.cs.umass.edu/~gbiss/graphene.pdf

⑤Measuring maximum sustained transaction throughput on a global network of Bitcoin nodes
グローバルネットワーク上での最大安定トランザクションスループット測定

- Bitcoinのブロックサイズ上限を挙げることはトランザクション手数料低減に繋がる一方、トランザクションスループットの増加を安全に取り扱うネットワーク能力に関する懸念は残る。

- この懸念を検証するため、Bitcoinマイニングノードのグローバルネットワークを構築し、現在の上限1MBよりも1000倍大きな1GBのブロックを受容できるよう設定した。
  - トランザクション件数を秒間１件から秒間1000件まで級数的曲線で増加するよう設定し、ボトルネックを特定しパフォーマンス統計を測定。
  - 大量のトランザクションスループットを扱う上で必要となるBitcoinクライアントのバグフィックスや設定パラメータの調整、およびノードのハードウェア要件を確認。
  - nChainやUBC（University of British Columbia）との共同実験（実験期間は5年）。

- 実験による相関関係を観察。
  - ①ブロック伝播やブロック検証時間とブロックサイズの相関。
    - Mempoolにおいて詰まりが発生し、ノード間不一致の増大とブロック伝播の遅延が発生。
    - ビッグブロックの伝播と検証それ自体は滞りなく行われ、Mempoolに問題が発生するまではボトルネックにはならず。
  - ②Xthinブロックやブルームフィルタサイズとブロックサイズの相関。
  - ③ネットワークオーファンレートとトランザクションスループットの相関。

→ 出典：https://www.scribd.com/mobile/document/359889814/ScalingBitcoin-Stanford-GigablockNet-Proposal
→ 出典：http://btcnews.jp/3ze2s42613065/

⑥Atomically Trading with Roger: Gambling on the success of a hardfork
Rogerとのアトミックトレード：ハードフォーク成功におけるギャンブル(1/7)

- フォークの歴史
  - 暗号通貨は、明確にコンセンサスルールを定義し、それに従って、全ネットワークの参加者（マイナー、リレーノードの双方）がスクリプトやトランザクションやブロックの検証結果について合意。
    - これらのルールはトランザクションのフォーマット、新コインの採掘レート、最大ブロックサイズなどのパラメータなどのを規定。
  - アップデートのためにこれらコンセンサスルールを変更することは、コミュニティレベルでのコーディネーションが必要であり、そのアプローチは大きく２つに分けられる。
    - ソフトフォークは、アップグレードしないノードによって有効と考えられるコンセンサスルールの導入。
    - ハードフォークは、アップグレードしないノードによって有効とみなされないコンセンサスルールの導入。
    - 双方のケースにおいて、フォークの提案は「フラグ日」というアクティベーションタイムと、ビルトインされたアクティベーション条件（サポート表明するマイナーの閾値を必要とするなど）がある。
  - ソフトフォークとハードフォークの差異は、アップグレードしないノードが影響を受けるかどうか。
    - ソフトフォークの場合、アップグレードしないノードはマイナーの多数派に従うのに対し、ハードフォークの場合には、アップグレードしないノードはネットワークとして分断される。
  - ビットコインはこれまで６回のソフトフォークを行ってきた（BerkeleyDBの設定ミスによるハードフォークという例外を除く）が、Ethereumはハードフォークを行ってきた。

→ 出典：http://homepages.cs.ncl.ac.uk/patrick.mc-corry/atomically-trading-roger.pdf
→ 出典：http://hackingdistributed.com/2017/07/11/atomic-transfer/

⑥Atomically Trading with Roger: Gambling on the success of a hardfork
Rogerとのアトミックトレード：ハードフォーク成功におけるギャンブル(2/7)

- リプレイプロテクション
  - リプレイ攻撃は、送り手がトランザクションに意図的に署名して、ブロックチェーンＡに受け入れられたときに、別のブロックチェーンＢにも受け入れられる場合に起きる。
  - そのため、リプレイプロテクションの目的は、どちらのブロックチェーンが新たに署名されたトランザクションを受け入れるかを、ユーザが決めることができるようにすること。
  - EthereumのThe DAOハードフォークではリプレイプロ会苦ションが無かったため、いくつかの会社が多くのコインを失った。

→ 出典：http://homepages.cs.ncl.ac.uk/patrick.mc-corry/atomically-trading-roger.pdf
→ 出典：http://hackingdistributed.com/2017/07/11/atomic-transfer/

⑥Atomically Trading with Roger: Gambling on the success of a hardfork
Rogerとのアトミックトレード：ハードフォーク成功におけるギャンブル(3/7)

- BitcoinおよびEthereumむけアトミックトレードプロトコル
  - BitcoinおよびEthereum向けに、ハードフォークの結果に関する賭けを行うことが出来る新しいプロトコルを設計した。
  - ２つのブロックチェーンが単一の「フォーク前」ブロックチェーンから出現するイベントにおいて、コインをスワップするために２つの参加者を結びつける。
  - ハードフォーク時のリプレイプロテクションを提供するための方法について検討されている。

- 本論考は、ビットコインコミュニティ内の二人のメンバー同士の賭けに動機付けられたもの。
  - Bitcoin Unlimitedの計画したハードフォークが発生し、ブロックチェーンが２つに分派するというイベントについて、60000ビットコインのトレードを行う。
    - ハードフォークに先立ち、2人の参加者がコインをデポジットして賭けにコミット。
    - ハードフォークが起きた後、コインは両フォークの上でスワップされる。
  - このプロトコルは、Bitcoin Unlimitedのハードフォークの際に60000コインをスワップすることを、Loaded氏がRoger氏に働きかけたことに触発されたもの。

→ 出典：http://homepages.cs.ncl.ac.uk/patrick.mc-corry/atomically-trading-roger.pdf
→ 出典：http://hackingdistributed.com/2017/07/11/atomic-transfer/

⑥Atomically Trading with Roger: Gambling on the success of a hardfork
Rogerとのアトミックトレード：ハードフォーク成功におけるギャンブル(4/7)

- この賭けを行う上で技術的にどのようなアプローチが最適かの検討。
  - Loadedは、トレードをアトミックスワップとして行ってはどうかと言及した。
  - ビットコインにおけるアトミックスワッププロトコルとして、Tier Noran's Protocolがすぐ思いつく。
  - しかしRogerとLoadedがTierNolanをトレードのコミットに使うことが、Bitcoin Unlimitedのハードフォークのアクティベーションに先立って行えないため、賭けに向かないという意見が出た。
  - その後、リプレイプロテクションを用いて、新たなアトミックトレードプロトコルを構築すればどうか、という案が出た。
  - そこで、LoadedとRogerがハードフォークのアクティベーションに先立ってコインをデポジットし、ブロックチェーンの分派後にアトミックスワップを実行することが出来る新たなアトミックトレードプロトコルを開発。

- アトミックトレードプロトコルを、BitcoinおよびEthereumの双方について提示している。
  - Bitcoin Unlimitedだけでなく、リプレイプロテクションを備えたどんなハードフォークにも適用できる。

- Bitcoinのアトミックトレードプロトコルは、「①コインのデポジット」「②オフチェーンのセットアップ」そして「③アトミックトレード」の３ステージから成る。
  - 次ページに詳述。

→ 出典：http://homepages.cs.ncl.ac.uk/patrick.mc-corry/atomically-trading-roger.pdf
→ 出典：http://hackingdistributed.com/2017/07/11/atomic-transfer/

⑥Atomically Trading with Roger: Gambling on the success of a hardfork
Rogerとのアトミックトレード：ハードフォーク成功におけるギャンブル(5/7)

- 最初のステージである「①コインのデポジット」では、双方がコインを単一トランザクション上へデポジットする。

- 次ステージの「②オフチェーンのセットアップ」
  - まずRogerが「オフチェーンセットアップが完了しない場合にはアトミックトレードをLoadedがキャンセルすることを認めるキャンセルトランザクション」に署名。
  - 次に、Rogerがトレードトランザクションに署名し、Loadedに送付する。
    - このトランザクションは、RogerがH(A)の秘密Aを明かした場合に、「Bitcoin Unlimitedでは無いブロックチェーン」上にある双方のデポジットをLoadedが請求することを認めるもの。
  - そして、Loadedはトレードトランザクションに署名し、Rogerに送付する。
    - このトレードトランザクションはリプレイプロテクションが備わっており、Bitcoin Unlimitedのブロックチェーンへのみ受容される。
    - このトランザクションは、H(A)の秘密Aを明かした場合に、Rogerが双方のデポジットを請求することが出来る。
  - 双方のトレードトランザクションが交わされると、Rogerは二つの没収トランザクションに署名し、Loadedに送付。
    - 没収トランザクションの目的は、Rogerが秘密Aを明かさない場合に、Loadedが双方のブロックチェーン上にある全てのコインを請求することが出来るようにするもの。
  - 上記ステップが完了し、Loadedがトレードをキャンセルしなければ、Rogerが双方をトレードにロックするコミットトランザクションをブロードキャストする。

→ 出典：http://homepages.cs.ncl.ac.uk/patrick.mc-corry/atomically-trading-roger.pdf
→ 出典：http://hackingdistributed.com/2017/07/11/atomic-transfer/

⑥Atomically Trading with Roger: Gambling on the success of a hardfork
Rogerとのアトミックトレード：ハードフォーク成功におけるギャンブル(6/7)

- 最後のステージである「③アトミックトレード」
  - Rogerはハードフォークが起きたら、トレードトランザクションをBitcoin Unlimitedのブロックチェーンへブロードキャストできる。
    - これは、双方のデポジットを請求すべく、Rogerに秘密Aを明かすことを求めるものでもある。
  - ブロックチェーンが２つに分派しているとすれば、Loadedは秘密Aを使って、トレードトランザクションを「Bitcoin Unlimitedでは無いブロックチェーン」へブロードキャストできる。
  - 当然、もしRogerが中断しコインを請求しないと決めれば、トレードは消滅し、Loadedは双方のブロックチェーン上にある全コインを請求できる。

- このプロトコル（およびビットコインコントラクト全般）のキーポイントは、トランザクション展性の解決しないと公平な交換が難しい点。
  - 論文の付録で、トランザクション展性が解決した場合のプロトコルについて言及している。

→ 出典：http://homepages.cs.ncl.ac.uk/patrick.mc-corry/atomically-trading-roger.pdf
→ 出典：http://hackingdistributed.com/2017/07/11/atomic-transfer/

⑥Atomically Trading with Roger: Gambling on the success of a hardfork
Rogerとのアトミックトレード：ハードフォーク成功におけるギャンブル(7/7)

- Ethereum向けのアトミックトレードプロトコル
  - ハードフォークというイベント発生時にアトミックトレードを行うスマートコントラクトとして設計。
    - ハードフォークのOracleを使って、他のコントラクトがフォーク１（古いコンセンサスルール）なのかフォーク２（新しいコンセンサスルール）なのかを検知する。
    - 参加者双方がトレードコントラクトおよびハードフォークOracleコントラクトを監査する。
    - 双方がコインをトレードコントラクトへデポジットし、ハードフォークがアクティベートするまでデポジットをロック。
    - ハードフォークがアクティベートした後、それぞれのフォーク中のコントラクトから両方のデポジットを引き出す。
  - トレードコントラクトは、引出の認証を行う前に、ハードフォークOracleコントラクトとやりとりして、どちらのブロックチェーンなのかを特定する。

→ 出典：http://homepages.cs.ncl.ac.uk/patrick.mc-corry/atomically-trading-roger.pdf
→ 出典：http://hackingdistributed.com/2017/07/11/atomic-transfer/

⑦Discreet Log Contracts
口外しないログコントラクト/離散対数コントラクト(1/2)

- スマートコントラクトは、ビットコインなどの暗号通貨システムの特徴として謳われるが、まだ金融むけ利用として広まっていない。
  - 実装にむけた大きな障壁は、スマートコントラクトのスケーラビリティと、外部データをスマートコントラクトへ取り込むことの難しさ。

- Discreet Log Contractsは、外部データを提供するオラクルに必要とされる信頼を最小化することを目指す。
  - コントラクトはトランザクションログにおいて口外することないため、外部の観察者はトランザクション中のコントラクトの存在を検知できない。
  - Lightning Networkに似た、ビットコインを用いたスマートコントラクトだが、誰もコントラクトを参照できないのが特徴。

→ 出典: https://adiabat.github.io/dlc.pdf
→ 出典: http://techmedia-think.hatenablog.com/entry/2017/07/08/181338
→ 出典: https://www.slideshare.net/takayaimai/discreet-log-contractsdlc

⑦Discreet Log Contracts
口外しないログコントラクト/離散対数コントラクト(2/2)

- 予測される未来の通貨価格に基づいた決済を実行できるコントラクト
  - 契約を結ぶにあたり、両者のマルチシグに資金を入れる（funding output）
  - このfunding outputを使う多数のトランザクションで構成されるコントラクトを作成
    - 各トランザクションは、入力にfunding output、出力が相手へのP2PKHと独自スクリプトハッシュを格納
    - 両者はどのコントラクトが最終的にブロードキャストされるか分からないので、全トランザクションの署名
  - オラクルが「正しい状態である」と承認したトランザクションのみがブロードキャストされる
    - オラクルは、観察結果を観測して、その数値に署名
    - 署名すると、両者が既に計算している点の離散対数があきらかになる

- オラクルがトラストポイントとなるが、不正検知可能で、不正を行ったオラクルは以降信頼されずオラクルとして使用されない
  - 例えば、価格を誤って報告→全ユーザがエラーを識別して、オラクルの使用を停止

→ 出典: https://adiabat.github.io/dlc.pdf
→ 出典: http://techmedia-think.hatenablog.com/entry/2017/07/08/181338
→ 出典: https://www.slideshare.net/takayaimai/discreet-log-contractsdlc

⑧Bobtail: A Proof-of-Work Target that Reduces Blockchain Mining Variance
ブロックチェーンマイニングの分散を低減するPoWターゲット(1/2)

- ブロックチェーンシステムは一定の平均レートでブロックを生成するように設計されている。
  - 最もポピュラーなシステムはPoWアルゴリズムをブロック生成の手段として利用。
  - ビットコインは平均して10分毎にブロックを生成。
  - PoWを実装するブロックチェーンシステムの制約は、ブロック間の時間に大きなバラつきがあること。
  - 例えば、ビットコインのinter-block時間は少なくとも40分。
  - こうしたバラつきはシステム内の検証済みトランザクションの一定の流れを阻害。

- そこでPoWベースのブロック探索に代替プロセスを提案するものであり、より小さなバラつきでinter-block時間を可能とする。
  - Bobtailアルゴリズムは、k lowest order statisticsの平均をターゲットと比較することによって、現在のアルゴリズムを一般化するもの。
  - kを増やすほど、inter-block時間のバラつきが低減することが示される。
  - このアプローチがビットコインに採用されると、80%のブロックが7-12分以内に見つけることができ、ほとんど全てのブロックを5-18分以内にみつけることができ、また平均inter-block時間は10分を保ったまま。

→ 出典: https://eprint.iacr.org/2017/820.pdf

⑧Bobtail: A Proof-of-Work Target that Reduces Blockchain Mining Variance
ブロックチェーンマイニングの分散を低減するPoWターゲット(2/2)

- さらに、こうしたバラつきの小さなマイニングは、二重使用やセルフィッシュマイニング攻撃を阻止することにもなる。
  - BitcoinやEthereumにおいて現在k=1で、マイニングパワーの40%をもつ攻撃者は、マーチャントが８ブロックの禁輸を設定している場合、30%の確率で成功する。
  - これをKを20以上にすると、成功確率は１%以下に下がる。
  - 同様に、BitcoinやEthereumにおいて現在マイニングパワーの40%をもつセルフィッシュマイナーはブロックの66%を請求。
  - しかしKを５以上にすると、セルフィッシュマイニングを見つける同じマイナーは正直なマイニングよりも成功確率が落ちる。

- このアプローチに要するコストはブロックヘッダーがより大きなものになる点。

→ 出典: https://eprint.iacr.org/2017/820.pdf

⑨Concurrency and Privacy with Payment-Channel Networks

ペイメントチャネルネットワークにおける同時並行性とプライバシー(1/4)

- ビットコインユーザーの増大の中で、スケーラビリティはコミュニティの重要懸念事項
  - ビットコインは、コンセンサスアルゴリズムのパーミッションレスな特性のため、トランザクションレートに秒間１０件の上限があり、Visaが秒間47000件のトランザクションをサポートするのと大きな開きがある。
  - ビットコインのペイメントチャネルは、オフチェーンペイメントを用いてビットコインのスケーラビリティ課題に取り組むもの。
  - ペイメントチャネルとは、ユーザのペアがブロックチェーンへ単一トランザクションを追加することによってペイメントチャネルを開設し、そこに自身のビットコインをデポジットとしてビットコインのスマートコントラクトによってロックするもの。
  - デポジット残高の配分について合意しながら、複数のオフチェーンペイメントがローカルに実行される。
  - 最終的には、ペイメントチャネルを共有するユーザが、最終残高を付加するためのビットコイントランザクションを実行し、ペイメントチャネルを閉じる。
  - この方法において、ブロックチェーンはペイメントチャネル開閉のために必要であり、個々のペイメントにおいて必要とならず、よってブロックチェーンの付加低減やトランザクションスループット改善に寄与する。
- ペイメントを決済できる十分なキャパシティを有したペイメントチャネルのパスをレバレッジして、ペイメントチャネルネットワーク（PCN）を生成することが可能。
  - PCNが伸び行くペイメントやユーザに広く対応するには多くの課題があるが、まだ未成熟でありさらなる研究が必要。
  - 本論考では、PCNの同時並立性やプライバシーについて整理する。

    → 出典：https://eprint.iacr.org/2017/820.pdf

⑨Concurrency and Privacy with Payment-Channel Networks

ペイメントチャネルネットワークにおける同時並行性とプライバシー(2/4)

- ビットコインのようなパーミッションレスブロックチェーンプロトコルは、本来的にトランザクションスループットに制限・レイテンシーがある。
  - この種の課題への現在の取り組みは、オフチェーンペイメントチャネル。
    - ペイメントチャネルネットワーク（PCN）と組み合わせて、ブロックチェーンへのアクセスを、初回と最後のチャネル登録以外に必要とすることなく、無数のペイメントを行うもの。
  - このアプローチは低レイテンシーで高スループットのペイメントへの道筋を示すものだが、その実装には、いくつかのプライバシー懸念や、技術上の課題。

- 本論文では、PCNのプライバシーや同時並行性むけの土台を構築。
  - ユニバーサル・コンポーザビリティ・フレームワークの定義および、実践的で安全性証明可能な解を提示。
    - FulgorはPCNむけに証明可能なプライバシー保障者を提供し、ビットコインのスクリプトシステムと互換性のある初のペイメントプロトコルだが、Fulgorはブロッキングプロトコルであり、同時ペイメントのデッドロックとなりがち。
    - 一方、Rayoはノンブロッキング（少なくとも同時ペイメントの１つが終結）。
    - FulgorおよびRayoのコアは、マルチホップのHTLCという新たなスマートコントラクトであり、Bitcoinのスクリプトシステムと互換性があり、秘匿ペイメントを提供する。その一方で実行時間やコミュニケーション負荷を低減する。
  - 評価を行ったところ、10人の中間介在ユーザとのペイメントで5秒というフィージブルな結果が示された。

→ 出典：https://eprint.iacr.org/2017/820.pdf

⑨Concurrency and Privacy with Payment-Channel Networks

ペイメントチャネルネットワークにおける同時並行性とプライバシー(3/4)

- プライバシーの課題
  - 現時点では、PCNが十分なプライバシーを提供できるか明確でない。
  - 最近の研究では、プライバシー保護プロトコルが、全ユーザがユニークな仲介人を通じてオフチェーンペイメントを実行するペイメントハブネットワーク向けに提案されている。
  - 残念ながら、これらがマルチホップPCNに適用できるか定かでない。
  - Lightning Networkは最も有名なPCNだが、PCNにおいてプライバシー保証を提供できるものではない。
  - 例えば、ペイメントパスを通じてルーティングされる最大許容値の計算は、ユーザに送り手へのペイメントチャネルの現在のキャパシティを明かすことを求めるため、機微情報が漏れる。
  - また、Lightning Networkにおいてペイメントチャネルの更新の原子性を保つために用いられるビットコインスマートコントラクトは、パス中のユーザに共通のハッシュ値を明かすことを求める。
  - 実際、多くの学術論文がビットコインペイメントのプライバシー保証について研究しているが、現時点において、PCNに求められる厳密なプライバシー保証の分析は無い。

→ 出典: https://eprint.iacr.org/2017/820.pdf

⑨Concurrency and Privacy with Payment-Channel Networks

ペイメントチャネルネットワークにおける同時並行性とプライバシー(4/4)

- 同時並立性の課題
  - 所与の時間においてあらゆる同時ペイメントへのアクセス権を有するマイナーは、容易にそれらをシリアライズ可能（ペイメント手数料によってソートする等のルールに従って）。
  - しかし、PCNではこれがあてはまらない。
  - オフチェーンペイメントの束はブロックチェーンへ付加されず、コンセンサスを通じてシリアライズされることが無い。
  - さらに、ペイメントが複数のユーザを巻き込むため、個々のユーザは同時並立制の課題を避けることが出来ない。
  - Lightning NetworkのようなPCNにおいて、パス中のペイメントチャネルが十分なキャパシティが無い場合、ペイメントは中断される。
  - 現在のPCNが大量のユーザやオフチェーンペイメント対応可能なものへスケールすると、同時ペイメントが発生しうる。

→ 出典：https://eprint.iacr.org/2017/820.pdf

⑩Redesigning Bitcoin's fee market
ビットコイン手数料市場の再設計(1/4)

- ビットコインシステムのセキュリティ
  - 正直なマイナーの手による大量の計算パワーに基づく。
  - ブロック生成者に対してプロトコルから支払われる報酬によって、マイナーはシステムへの参加およびトランザクション検証を動機付けられる。
  - ほぼ４年おきの半減期によって、新たなビットコイン生成レートが減少するにつれて、トランザクション手数料に由来する報酬が重要な位置づけとなる。

- ビットコインのトランザクション手数料メカニズムに望む特質
  - マイナーやユーザによる様々な操作（例えば追加トランザクションを含める等）に対する頑健性。
  - Bitcoinのブロック報酬が減少するにつれて、トランザクション手数料の重要性が高まり始める。
  - 結果的に十分なマイニングによって高いレベルでセキュリティが保たれることを望みたい。

- オークション理論やアルゴリズムゲーム理論を用いて、手数料市場メカニズム改善を検討
  - ①ユーザ向け手数料決定をシンプルにしたい。
  - ②手数料からのマイナーの取り分となる報酬を改善する（少なくとも現状維持）ことによって、マイニング参入の魅力を高め、セキュリティを向上させたい。
  - ③ブロックサイズの課題を手数料決定メカニズムから出来る限り分離したい。

→ 出典: https://arxiv.org/pdf/1709.08881.pdf
→ 出典: https://medium.com/@avivzohar/rethinking-bitcoins-fee-market-ea9319e4ea57

⑩Redesigning Bitcoin's fee market
ビットコイン手数料市場の再設計(2/4)

- Bitcoinの現行メカニズム（pay-your-bid（差別価格方式）オークション）の問題
  - ビットコインの現在の手数料マーケットは、ブロックが充填されない場合に報酬を取り出すことができない。
    - この効果はスケーラビリティ論争にかかわりがあり、トランザクション手数料からの報酬は、ブロックサイズが大きくなると減少。
  - 問題点の１つは、ユーザがセットする手数料が、他の未確定トランザクションに依存すること。
    - マネー節約のため、ユーザは支払える最大限の手数料をセットせず、次ブロックの一つに含まれるのに十分なだけ。
      - これはウォレットソフトウェアが正しい手数料を見積もろうとする。
      - 手数料見積は難しく、またもし次ブロックが遅くなるとmempoolのステータスは変わりやすい。
    - するとユーザは次のような被害を受ける。
      - ①高い手数料をセットしたトランザクションは払い過ぎで終わる
      - ②誤って低い手数料をセットしたトランザクションは遅延して調整が必要となりトランザクションをモニタリングし続けないといけなくなる。
  - もう一つの問題点は、マイナーの報酬が最善から遠いこと。
    - ブロックがなんらかの理由から満タンにならない場合、ユーザは極度に低い手数料をセットしがちで、低い報酬しかマイナーに入らない。
  - そこでオークション理論やアルゴリズムゲーム理論を援用する。

→ 出典: https://arxiv.org/pdf/1709.08881.pdf
→ 出典: https://medium.com/@avivzohar/rethinking-bitcoins-fee-market-ea9319e4ea57

⑩Redesigning Bitcoin's fee market
ビットコイン手数料市場の再設計(3/4)

- ２つの代替メカニズムを提案
  - ひとつは独占的プライスメカニズム。
  - もう一つはRSOP（ランダムサンプリング最適プライス）オークションだが、残念ながら操作されがちであり、実装がやや難しい。

- 独占的プライスメカニズム
  - マイナーは、ブロック中に受け入れられるトランザクション数を選択し、全トランザクションがブロック中に含まれる最小ビッドを支払う。
    - このようにしてメカニズムがブロックサイズを動的に設定。
    - ユーザは自身の入札を正直に自分がトランザクションに支払いたい額に設定することができ、手数料見積メカニズムを用いる必要なく、mempoolが成長すればトランザクション手数料を（replace by feeメカニズムを通じて）調整する必要もない。
  - ルール①：ユーザがトランザクションにおいて自身が支払う最大限の手数料を指定する
  - ルール②：マイナーはブロックに含める（ブロックサイズ上限まで）トランザクションを選択するが、ブロック全体を満タンにする必要はない。
  - ルール③：ブロック内の全トランザクションは、同額の手数料を支払うものとし、その金額は誰かが指定した最低額とする。（ここで留意すべきは、マイナーは高い手数料を支払うトランザクションを最初にブロックへ含める動機が働くこと）

→ 出典：https://arxiv.org/pdf/1709.08881.pdf
→ 出典：https://medium.com/@avivzohar/rethinking-bitcoins-fee-market-ea9319e4ea57

⑩Redesigning Bitcoin's fee market
ビットコイン手数料市場の再設計(4/4)

- 独占的プライスメカニズムの魅力
  - ①ユーザはブロックを含める限界コストを支払う
  - ②mempoolが混雑している場合に、トランザクションの再調整を行う必要がない
    （支払うことに同意すれば限界プライスを課されるだけ）
  - ③マイナーはメカニズムに従う動機がある
    （少なくとも短期的にはマイナーの報酬を最大化するようにセットされる）
  - ④もしブロックサイズが大きくなれば、マイナーは同じトランザクションセットを含め、同じ報酬を得る。

→ 出典：https://arxiv.org/pdf/1709.08881.pdf
→ 出典：https://medium.com/@avivzohar/rethinking-bitcoins-fee-market-ea9319e4ea57

お役に立てば嬉しいです

- **BTCアドレス**

  1PAXBwKnZwNphWK7Wr9cdE8t1ESZ8xi5U1

→おしまい