Bitcoin & Blockchain概況

2016.12 by SATO

「Bitcoin2.0概況」「Blockchain2.0概況」から改題

過去7回（＋臨時1回）にわたり、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

TABLE OF CONTENTS

➔ 今回は、2016年8月～2016年11月の動きを中心に整理

■凡例：ブロックチェーン区分
（推察に基づく分類であることに注意）

- B Bitcoin関連
- E Ethereum関連
- （B・E）Public Blockchain
- D Private, Permissioned Blockchain Distributed Ledger関連

1. テクニカル分野

- Scaling Bitcoin関連
  - ✓ Fungiblility
  - ✓ TumbleBit
  - ✓ MimbleWimble
  - ✓ LightningNetwork
  - ✓ Segwit
  - ✓ Schnorr署名, Covenants, OpenTimeStamps
- Zcash

B E D

SCALING BITCOIN
1. FUNGIBILITY OVERVIEW

- トレーシングサービスの弊害
  - 自身に直接関係ない他人の活動に影響されるようになる。
  - コインを受け取ってそれが使えないようなことがあると取引拒否が起こる。
  - 取引に許可が必要な中央集権的なものになると機密性も失われてしまう。
- Fungibility確保にむけた工夫
  - CoinJoinはインプットおよびアウトプットというトランザクショングラフのプライバシーを保つもの。
  - スケーラビリティの面では、CoinJoinよりもTumblebit、さらにはLightningNetworkが強力。
  - LNはペイメント向けにOnionルーティングが可能なため、どこから来てどこに行くのかのプライバシーも向上。
  - プライベートビットコインであるMoneroにより開発されたリング署名も、アウトプットに対するインプットを特定せずにアウトプットを用いて、トランザクションの有効性を検証できるため、匿名性向上に重要。
  - インプットとアウトプットのプライバシーについては、OWAS(OneWayAgfregateSignatures)もある。
  - Zcashは更に進んでトランザクション発生したこと以外のトランザクションに関する全てを隠蔽するものであり、またzkSNARKsは新しくまだ研究が必要だがブロックが大きくトランザクション検証に時間を要するため、スケーラブルではない。
  - 残高に関するプライバシーとして、Confidential Transactionやその拡張であるMimbleWinmble。
  - こうした取り組みに対して、どのウォレットからのトランザクションかを特定するチェーン分析サービスがあり、一例がCoinSelection。注意を払うべきはLNのようなレイヤー2ソリューション。

→ 出典: https://scalingbitcoin.org/event/milan2016#workshop
→ 出典: https://scalingbitcoin.org/presentations
→ 出典: http://diyhpl.us/wiki/transcripts/scalingbitcoin/milan/
→ 出典: http://samwouters.com/the-future-of-bitcoin-and-9-ways-to-improve-it/

B E D

SCALING BITCOIN
2. TUMBLEBIT①

- 匿名のコインミキサー/ペイメントハブ。
  - トラストの無いプライベートビットコインペイメントシステム。
  - タンブラーとして用いて匿名性を提供することで、プライベートな支払いを提供する。
  - 以前のtumblerは、ユーザがtumblerサービス運営者を「ユーザの匿名性を暴くようなログ記録をしないはず」と信用する必要があった。
- ビットコインユーザのfungibility やプライバシーを改善するために提案されてきたtumblingメカニズムの流れをくむもの。
  - ミキシング技術を用いて払い手から受け手へのトランザクショングラフを不明瞭にし、それゆえ両者間のリンクを消し去る。
  - これら過去の取り組みを踏まえ、ペイメントハブを用いることで、リンク不可能とし、tumbler自身からもユーザを保護する。
  - つまりペイメントパスに関する情報も漏らさない。
- TumbleBitはリンク不可能に加え、ペイメントがオフチェーンで行なわれる。
  - ペイメントチャネルを作ることで、トランザクションをオフチェーンとし、大幅なスループット改善も。

→ 出典: https://scalingbitcoin.org/event/milan2016#workshop
→ 出典: https://scalingbitcoin.org/presentations
→ 出典: http://diyhpl.us/wiki/transcripts/scalingbitcoin/milan/
→ 出典: https://medium.com/@bergealex4/moving-forward-reflections-on-scaling-bitcoin-retarget-milan-5e70ba88b2ab#.sk5zp469f
→ 出典: https://blog.openbazaar.org/openbazaar-at-scaling-bitcoin-conference-in-milan/
→ 出典: http://samwouters.com/the-future-of-bitcoin-and-9-ways-to-improve-it/

B E D

SCALING BITCOIN
2. TUMBLEBIT②

- CoinSwapの欠点
  - ペイメントに仲介人を用いるため、送り手・受け手のアドレスのリンクがブロックチェーンに残ることは無いが、仲介人がビットコインを盗んだり支払いを拒むことができてしまう。

- HTLC（Hash Time-Locked Contracts）による対策と欠点
  - 太郎と仲介人が特別な種類のペイメントチャネルを立て、花子と仲介人も同様にペイメントチャネルを立てる。
  - トランザクション中にキーを埋め込み、これらペイメントチャネルを接続。花子は仲介人とのペイメントチャネルからビットコインを請求できる。
  - 仲介人も太郎とのペイメントチャネルからビットコインを請求できるので、誰も盗むことが出来ない。
  - このときの問題は、仲介人は「太郎が花子に送金した」ことを知りえているため、仲介人が（ブロックチェーン上には紐付け情報が残らないにも拘らず）紐付けを行えてしまうこと。

- TumbleBitによる対策
  - 大勢で匿名性を提供する。多くのユーザがペイメントチャネルを同じ仲介人に対して立てることができる。
  - 全ユーザが同じ仲介人を用いて互いに送金し合うことができる。

→ 出典：https://www.cryptocoinsnews.com/how-tumblebit-builds-on-coinswap-to-improve-bitcoin-privacy-and-fungibility/
→ 出典：https://bitcoinmagazine.com/articles/with-tumblebit-bitcoin-mixing-may-have-found-its-winning-answer-1477423607

B E D

Scaling Bitcoin
3. MimbleWimble

- MimbleWimbleは、新たなブロックチェーンのデザイン
  - 全トランザクションの履歴について同意する代わりに、現在の状態について同意する。
  - Confidential transaction で送金量を隠蔽し、OWAS（一方向集約署名）でトランザクションをブロックに組み合わせトランザクショングラフを不明瞭化する。
  - 送金量を隠蔽すると共にトランザクションを結合するためスケーラビリティ向上に寄与するが、現行のビットコインプロトコルとの互換性がないため、サイドチェーンとしての追加が考えられている。

- いったんマイナーがトランザクションを処理すると、ブロックチェーン履歴全体が、現時点の状態のみの形へ圧縮される
  - ブロックを一連の大きなcoinjoinトランザクションにしてしまう。
  - トランザクション履歴を用いて誰が誰に支払ったを暴くことが出来なくなる。
  - 新たなブロックが生成されるとトランザクションを除去してしまう。

- 100GBあるブロックチェーン全体が1MB以下に圧縮
  - ブロック中のデータの多くが抜け落ちてしまうため、ブロックチェーンが小さなサイズに圧縮できる。

→ 出典: https://blog.openbazaar.org/openbazaar-at-scaling-bitcoin-conference-in-milan/
→ 出典: https://m.reddit.com/r/Bitcoin/comments/578lal/mimblewimble_is_insane/
→ 出典: http://bitcoinbrasil10.blogspot.jp/2016/10/rootstock-developer-praises-privacy.html?m=1
→ 出典: https://hacked.com/mimblewimble-make-bitcoin-work-better/
→ 出典: https://medium.com/colu/reaching-affordable-consensus-what-made-scaling-bitcoin-awesome-1d029babbcf8#.pw7bxs6yo

B E D

SCALING BITCOIN
4. LIGHTING NETWORK①

- 利点：ブロックチェーン書込なしにトランザクション可能なレイヤー２ネットワーク
  - 参加者間で秒あたり多くのトランザクションをさばくことが可能となる
  - 署名されたコミットを交換することで二重使用問題を解決可能
  - チャネル内のロックアップのためにトークンとしてビットコインが必要でありビットコインユーザベース拡大に寄与する
- マイナス面のトレードオフも
  - ペイメントむけトランザクションはスケールするが、ユーザむけトランザクションはスケールしない。
    - LNチャネルの開閉はビットコインブロックチェーン上のトランザクションなので、ボトルネックの所在が、オンチェーンで処理されるトランザクションのリミットから、所定時間に開閉できるペイメントチャネル数のリミットに移るだけ。また、OP_RETURNを用いるセカンドレイヤーのカラードコインのオーバレイネットワークには有効ではない。
  - セキュリティモデルの問題。
    - ペイメントチャネルのセキュリティとして、コンスタントなモニタリングを必要とする。無効なチャネル状態を検知するためのソフトを実行するノードを立てたり、チャネル保証サービスを利用したり等が必要となる。
  - ペイメントハブの集中化。
    - ペイメントチャネルの経済性や、エンドポイント間の効率的ルーティングを考えると、ホップ数の最小化という意味で最も効率的な構成を持つところが大規模なペイメントハブになって皆にチャネルを開く。ハブは少ない方が効率的なので、ビットコインの自由資本が大きなハブがペイメントチャネルを維持するためには必要。マネーを多く持つほうが多くのペイメントチャネルを開いて維持しやすく、ペイメントチャネルになりやすい。となると、既存の銀行がペイメントチャネルに近いポジション。現行システムとの違いはペイメントハブ開始にライセンスが不用なことくらいなので、ペイメントハブを規制しないと不法なハブが登場する可能性も。

→ 出典：http://coincenter.org/entry/what-is-the-lightning-network
→ 出典：http://www.wallstreettechnologist.com/2016/10/03/lightning-network-will-it-save-bitcoin-or-break-it/

B E D

SCALING BITCOIN
4. LIGHTING NETWORK②

- Blockstream、Lightningによるマイクロペイメントトランザクションのテスト成功
  - Lightning Networkのテストをビットコインのテストネットで実施。
  - 完全にエンドツーエンドでのマイクロペイメントを成功させた。（同社初のライトニング・トランザクション成功）
  - Blockstreamの最新バージョンのライトニング・プロトコル・ソフトウェアである「C Lightning Prototype v0.5」を使って、Web店舗でデジタルな購入処理を行った。
  - Lightning Networkを通して、ビットコインの請求とマルチホップペイメント（複数ノードを経由した支払いルーティング）、実際の送金を含むトランザクションを実施。
  - 初めて構築した現実のブロックチェーンを用いたチャネルであり、デジタル商品の支払いを第三ノードを通じてノードからノードへ受け渡した初のマルチホップ・トランザクション。
  - ネコのアスキーアートを購入するというシチュエーション
    - ライトニングチャネルを開くためにテストネットでトランザクションを実行
    - トランザクションが確認された後、開設済みのチャネルを用い開設済みノードをルーティングして、100satoshiの支払い
    - 画像を閲覧

→ 出典：https://lists.linuxfoundation.org/pipermail/lightning-dev/2016-October/000627.html
→ 出典：https://blockstream.com/2016/10/05/blockstream-lightning-first-strike.html
→ 出典：https://asciinema.org/a/ergldrzd43j08klix08hf9yl3
→ 出典：http://btcnews.jp/blockstream-succeed-lightning-end-to-end-micropayment-channel/
→ 出典：https://www.coin-portal.net/2016/10/14/13745

B E D

SCALING BITCOIN
4. LIGHTING NETWORK③

- Onion routing in Lighting
  - 分散型TorをSphinx（匿名メッセージをリレーする暗号メッセージフォーマット）およびHORNET（高スピードなOnion Routing:インターネットスケールをターゲットとした、Sphinxの進化形）で構築。
  - ソースが全ルートを完全に特定する「ソースルーティング」を利用。
  - 効率的なインターネットスケールのデータ転送を実現するためのOnion Routingの進化形。
  - データ転送の間を通して、そのクリティカルパスになっている非対称暗号オペレーションが不要。
  - Hornetを使うことでノードは一定の状態を維持するだけで済む。
  - Hornetの統合に向けて、現在その前提となるSphinxの実装中。

- Flare routing in Lighting
  - ハイブリッドなルーティングアルゴリズムを通じて集めた情報をルーティングテーブルに格納する。
  - そのルーティングアルゴリズムは、スケジュールに基づく能動的パートと、ペイメントリクエストに基づく受動的パートから構成される。
  - 能動的ルーティングは変化の遅い静的情報（ノード間のペイメントチャネル）を近隣ノードやビーコンを見つけることを通じて収集する。
  - 受動的ルーティングは変化の早い動的情報（ノードの状態、ペイメントチャネル中の資金配分、チャネル使用料など）を候補ルートのランキングと選択を通じて収集する。

→ 出典: https://scalingbitcoin.org/event/milan2016#workshop
→ 出典: https://scalingbitcoin.org/presentations
→ 出典: http://diyhpl.us/wiki/transcripts/scalingbitcoin/milan/
→ 出典: http://samwouters.com/the-future-of-bitcoin-and-9-ways-to-improve-it/

SCALING BITCOIN
4. LIGHTING NETWORK④

- Scaling Bitcoin後に行われたLN標準化ミーティング
  - 現在LightningNetworkは8つのプロジェクトによって独自設計が進行中。
  - 今回ミラノでは、Scalingbitcoinにあわせて、これら全てのプロジェクトが従うべき標準ルールを定めるべく話し合いが持たれた。
  - 参加者は、Acinq, Amilo Pay, Bcoin/Purse.io, BitFufy Blockstream, LightningLabs。
  - 年末までに各自が持つ情報を共有する場を設けることが決まった。
  - チャネルの状態を管理するコアプロトコルや、ルーティング、オニオンルーティング、支払アドレスフォーマット、命名フォーマットなどが標準化される。
  - 今回相互運用性のためのルールが列挙されたことにより、今年末までにLightning Network の初期バージョンが利用可能となる見込み。

→ 出典: http://www.coindesk.com/bitcoin-lightning-network-interoperability-milan-scaling/
→ 出典: https://www.coin-portal.net/2016/10/25/14103/
→ 出典: https://medium.com/@lightningnetwork/lightning-network-meeting-on-interoperability-and-specifications-ea49e47696a4#.upkrabmus
→ 出典: http://btcnews.jp/lightning-devs-interoperablility/
→ 出典: https://blockstream.com/2016/10/18/outcomes-from-lightning-protocol-summit-milan.html
→ 出典: https://bitcoinmagazine.com/articles/after-scaling-bitcoin-a-lightning-winter-release-is-now-within-reach-1476814566

B E D

SCALING BITCOIN
5. SEGWIT

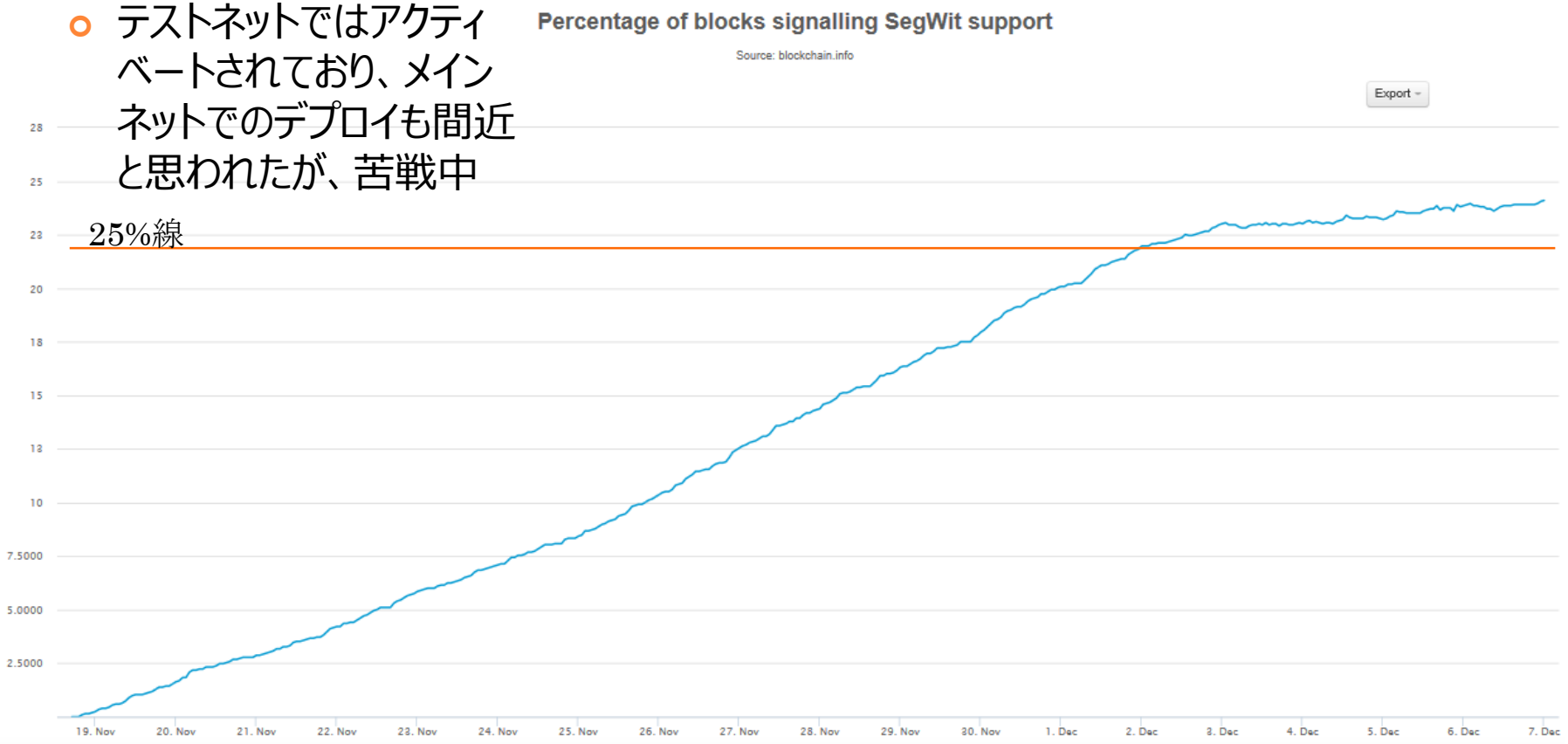
- 署名をトランザクションから分離し、署名のための分離されたデータレポジトリに格納した上で、伝播をオプション選択とする。
  - 通常のビットコイントランザクションでは、トランザクションメッセージに署名があり、署名がトランザクションが認証されたかどうかを証明する。
  - Segwitでは署名をトランザクションから分離し、署名はブロック内の別のデータベースに格納される。
  - 署名は分離されたデータレポジトリに移され、新しいスタイルのブロックとしては上限4MBに拡大される。ブロック内のスペースが空く。
  - ビットコインブロックチェーンサイズの６割を占める署名を外すことにより、ブロック内にスペースができ、マイナーがより多くのトランザクションをブロックに格納できる。
- Elements Alphaの一要素として開発された。
  - 意図しないトランザクション展性を解決。
  - 先に署名されたトランザクションを安全にチェーンに繋ぐもので、ペイメントチャネルやライトニングネットワークにとって重要。
  - txidの定義方法を変えるのみであり、ハードフォークは必要としない。
- ビットコインにとり最大の変更の一つになる。
  - P2Pやウォレット、コンセンサスなどあらゆる領域に影響。

→ 出典: https://scalingbitcoin.org/event/milan2016#workshop
→ 出典: https://scalingbitcoin.org/presentations
→ 出典: http://diyhpl.us/wiki/transcripts/scalingbitcoin/milan/
→ 出典: https://bitcoincore.org/en/2016/10/28/segwit-costs/
→ 出典: https://blockchainhub.net/blog/infographics/segregated-witness-overview/
→ 出典: http://samwouters.com/the-future-of-bitcoin-and-9-ways-to-improve-it/

B E D

Scaling Bitcoin
5. SegWit

- テストネットではアクティベートされており、メインネットでのデプロイも間近と思われたが、苦戦中



→ 出典: https://blockchain.info/ja/charts/bip-9-segwit

B E D

SCALING BITCOIN
6. SCHNORR SIGNATURES

- Shnorr署名は、ECDSAに変わる署名方式として提案されているもの。
  - 1988年に発明され2008年に特許切れを迎えた。
  - 1993年に署名の標準化を行った際は特許の問題もありDSAが採用された。
  - ビットコインも楕円曲線暗号で唯一の標準としてECDSAを利用。
  - セキュリティ強度に優れ、デジタル署名としてシンプルであり、実装も容易。

- 全ての署名を一つのトランザクションに集約できる。
  - コンパクトな署名であり、署名検証のスピードもECDSAより速いと言われている。
  - バッチ検証のスピード向上にも有用。
  - 複数のインプットから署名を統合して一つとし、個々のトランザクション検証にあてることができる。
  - 統合により移送が軽くすみ、ネットワーク上のピアによる検証や格納が節約できる。
  - ブロックチェーン上のスペース節約に効くということ。
  - 個々のユーザが大きな合同トランザクションに関わるコストをシェアするため、CoinJoinのような複数インプットと併用することでプライバシー改善にも働く。

→ 出典: https://scalingbitcoin.org/event/milan2016#workshop
→ 出典: https://scalingbitcoin.org/presentations
→ 出典: http://diyhpl.us/wiki/transcripts/scalingbitcoin/milan/
→ 出典: https://medium.com/@bergealex4/moving-forward-reflections-on-scaling-bitcoin-retarget-milan-5e70ba88b2ab#.sk5zp469f
→ 出典: http://samwouters.com/the-future-of-bitcoin-and-9-ways-to-improve-it/

B E D

Scaling Bitcoin
7. Covenants

- ビットコインは、将来のトランザクションがどのように使われるかを限定するスクリプトを持つ。
  - そうしたスクリプトを用いて、正しい署名が使われているかをアンロックや送金の前にチェックすることによって、正しい人がビットコインを使うことを確実にできる。
  - BlockstreamがElements Alpha sidechain上の新しいスクリプトのテストを行っていることを発表。
- Covenantsと呼ばれ、ビットコインユーザがどのようにマネーをコントロールしたり消費したりするか、マネーの保護の観点で可能性を拓くもの。
  - コベナンツはトランザクション使用時の制約。
  - ビットコイン保管向けに安全な金庫（vault）を設け、盗難時もリカバリ可能に。
  - 金庫には解錠キーとリカバリキーを与え、コインを金庫に預けるときに解錠期間を設定。
  - 解錠キーを用いてコイン移動や、解錠期間後の使用を可能に。
  - ハッカーが解錠キーを入手した際はリカバリキーを用いてトランザクションを取り消し。
  - ハッカーがリカバリキーを入手した際はコインをburn。
- 新opcode（CheckOutputVerify）のみを必要とするコベナンツを用いて金庫を実装。
  - 新しいopcodeは、bitcoin vaults等の形で実装することによって、ビットコイン取引所やユーザがマネーを盗まれてしまうことを防ぐのに役立つ可能性。
  - 課題は実装時の200ラインに及ぶ複雑さなど。

→ 出典: https://scalingbitcoin.org/event/milan2016#workshop
→ 出典: https://scalingbitcoin.org/presentations
→ 出典: http://diyhpl.us/wiki/transcripts/scalingbitcoin/milan/
→ 出典: http://www.coindesk.com/bitcoin-anti-theft-feature-sees-sidechains-testing/
→ 出典: http://samwouters.com/the-future-of-bitcoin-and-9-ways-to-improve-it/

B E D

Scaling Bitcoin
8. OpenTimestamps

- 典型的な公証役サービスはOP_RETURNを用いるため、スケールしない。
  - タイムスタンプにもよく使われるOP_RETURNトランザクションは１日あたり4000トランザクションでありネットワークキャパシティの2%。
  - タイムスタンプ毎に1トランザクションとなるため、この方法による公証役サービスの余地は限定的。
  - 大学の学位証明などに使うことを考えると、集約が必要。

- タイムスタンプのプルーフフォーマットとして、PeterToddにより提案・実装されたのがOpenTimestamps。
  - OpenTimestampsはマークルツリーを用いて存在証明を集約し、定期的にブロックチェーンへコミットする。
  - マークルツリーにトランザクションを集約するように、タイムスタンプのマークルツリーを構築。
  - このマークルツリーは、ブロックヘッダのマークルツリー中の単一トランザクション内に書き込む。

- 一方Chainpointはプルーフの所在を示すマークルツリーをJSON中に記述するもの。

→ 出典: https://scalingbitcoin.org/event/milan2016#workshop
→ 出典: https://scalingbitcoin.org/presentations
→ 出典: http://diyhpl.us/wiki/transcripts/scalingbitcoin/milan/
→ 出典: https://medium.com/@bergealex4/moving-forward-reflections-on-scaling-bitcoin-retarget-milan-5e70ba88b2ab#.sk5zp469f
→ 出典: http://samwouters.com/the-future-of-bitcoin-and-9-ways-to-improve-it/

B E D

SCALING BITCOIN
9. その他トピック

- Jute braiding
  - ブロックに複数の親を認める編み紐構造（braiding）を提示。
  - セルフィッシュマイニングやオーファンブロックを排除することが狙い。
  - あるマイナーがブロックを得てから全員がブロック情報を得るまでのレイテンシーがセルフィッシュマイニングの背景にあり、大きなマイナーはこのレイテンシーをベースに利益を得るためマイニングの集中化を招く。

- BIP151
  - ビットコインノード間のデータを暗号化。
  - ビットコイントラフィック中のデータは暗号化されてきていない。
  - OpenSSHなどに使われる暗号化標準であるChaCha20/Poly1305@openssshを利用する。
  - 計算の重いSHA256ハッシュと比べ、ネットワークトラフィックの高速化も可能。
  - ネットワークをモニタリングしてパッケージをビットコインとして認識できるが、その中身は参照できない。

→ 出典: https://scalingbitcoin.org/event/milan2016#workshop
→ 出典: https://scalingbitcoin.org/presentations
→ 出典: http://diyhpl.us/wiki/transcripts/scalingbitcoin/milan/
→ 出典: https://bitcoinmagazine.com/articles/bip-the-end-to-end-encryption-bitcoin-never-had-but-soon-will-1465401187
→ 出典: http://samwouters.com/the-future-of-bitcoin-and-9-ways-to-improve-it/

B E D

ZCASH ①

- ZCash は送り手・受け手・送金額を隠蔽する代わりに、トランザクションメタデータが暗号化され、対応する鍵を持つ人だけがトランザクションの中身を参照できる。
- Zerocashプロトコルをベースとし、zk-SNARK証明を利用。
  - zk-SNARKは、機密性を保持しつつ、トランザクションの整合性を確保するもの。
  - ゼロ知識証明は、秘密自身に関することを何も明かさずに、秘密を知っていることを示すものであり、
  - 誰がコインを持つかというステートメントが正しいということを、コインがどれだけあって誰から入手したかという他の情報を明らかにすることなく証明する。
  - 既にインターネットでは他の場面で適用されている。
  - 例えば、ゼロ知識証明を用いて、ウェブサイトのユーザパスワードを、パスワードの値をウェブサーバに送ることなく検証している。
  - これを用いて、他の参加者の協力に依存することなく、ZCashは参加者にトランザクションの有効性を保証することができる。
- ZCash は先進的な暗号通貨だが、新しく暗号技術がテスト不充分であり、いくつかのバグを検証する必要がある。
  - 匿名性の証明が大きく、計算パワーを大量に必要とする。
  - プライバシー保護トランザクションは、時間にして2分、RAMにして4GBを要する。
  - また、ZCash はマルチシグのトランザクションにはプライバシー追加を提供出来ない。

→ 出典: http://spectrum.ieee.org/tech-talk/computing/networks/zcash-truly-anonymous-blockchainbased-cryptocurrency
→ 出典: http://www.tomshardware.com/news/zcash-https-private-money-transactions,32948.html
→ 出典: https://medium.com/@DJohnstonEC/zcash-informational-report-the-zero-knowledge-privacy-protocol-launches-october-28th-2016-51717cb849d3#.6c3nrdl2n
→ 出典: http://consumersresearch.org/zcash-launches-offering-confidential-transactions-through-the-blockchain/

ZCASH ②

- 選択的透明性（selective transparency ）
  - ユーザは、誰が重要データを参照できるかをコントロールできる。
  - ZCashプロトコルはデフォルトでトランザクション関連の全情報を暗号化するが、データを選択的にディスクローズでき、どの部分を開示し、だれが参照可能とするかを設定できる。
  - ZCash では、transparentとshieldedという2種類のアドレスがある。
  - 前者の場合、ビットコイン同様に、どこからどこへいくら送金したか分かるが、後者ではパブリックな台帳において不明瞭となる。送り手と受け手の双方がshieldedアドレスを使うと金額も暗号化される。
  - ユーザは「参照キー」を使って第三者に自身のトランザクションに関する情報を明かすことができる。

→ 出典: http://spectrum.ieee.org/tech-talk/computing/networks/zcash-truly-anonymous-blockchainbased-cryptocurrency
→ 出典: http://www.americanbanker.com/news/law-regulation/how-zcash-tries-to-balance-privacy-transparency-in-blockchain-1092198-1.html

2．プラットフォーム分野

- 香港の取引所Bitfinexがハッキング被害
- Ethereumを用いたマイクロペイメント向けRaiden Network
- テックビューロ、仮想通貨やトークンの発行支援サービス「Zaica」
- アップデート可能な公証・タイムスタンプサービス、NEMアポスティーユ
- 中国マーケット向けデジタルアセットプラットフォーム、Antshares
- ブロックチェーンにログを記録するサービス、ProofLog
- Chronicled、EthereumベースのIoTレジストリをローンチ

香港の取引所BITFINEXがハッキング被害

- 8月3日（水）の午前3時頃に発覚。
- 約12万BTC（＝約72億円相当）の被害額。
- ビットコイン価格も600ドル前後から一時500ドル割れへ急落。
- Bitstamp、Gatecoin、Shapeshift等に次ぐ、取引所のハッキング被害。
- この損失を補填するために、「BFXコイン」なる社債のようなものの発行を検討中。
- 「BFXコイン」は、1ドル＝1BFXとして発行され、損失をドル建てで換算しユーザ資産に充当する仕組み。
- 「BFXコイン」は2ヶ月毎にBitfinexの収益から配当が出される債権的な機能を持つトークンであり、市場で自由に取引でき、引き出すこともできるとのこと。

- 出典：https://bitfinex.statuspage.io/
- 出典：http://btcnews.jp/bitfinex-hacked/
- 出典：https://coincheck.com/blog/1796
- 出典：http://btcnews.jp/what-is-bfx-coin/
- 出典：http://www.so-law.jp/archives/138
- 出典：http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfbfxnaorder060216.pdf

B E D

ETHEREUMを用いたマイクロペイメント向け RAIDEN NETWORK

- ビットコインブロックチェーンではLightning Networkがスケーラビリティを高めるべく取り組んでいる中、Ethereumブロックチェーンで登場したのがRaiden ネットワーク。
  - Raiden Networkは、Ethereumブロックチェーンにとって初めてのState Channelのインプリメントの一つ。
  - State Channelは、ブロックチェーンの様々なカテゴリーのアプリケーションにとって必要となる、スケーラビリティやプライバシーを改善する可能性ある技術。
  - また、ビットコインはトランザクション展性の解決のためSegWitのインプリメントが済むまではLightningNetworkを実装できない点も課題。
- Raiden Networkは、Ethereumの拡張として実装される。
- PoC-0における最初のトランザクションは、コペンハーゲンのクライアントから、ムンバイのクライアントに対して、ブラジルのフロリアーノポリスのノードを介して、トークンを送信するもの。
- Raidenのα版は2016年度の第３四半期にリリース予定。
  - アジア太平洋地域のパートナーがOmiseで、初期ステージにおけるRaidenの開発をサポート。
  - また Wanxiang Blockchain Labsも補助金面でサポート。

→ 出典: http://raiden.network/
→ 出典: https://github.com/raiden-network/raiden/wiki/Raiden-PoC%E2%80%900
→ 出典: http://www.coindesk.com/ethereum-bitcoin-mainstream-microtransactions/
→ 出典: https://bitcoinmagazine.com/articles/lightning-fast-raiden-network-coming-to-ethereum-blockchains-1471030245

B E D

テックビューロ、仮想通貨やトークンの発行支援サービス「ZAICA」を提供開始

- 発行したアセットトークンは、簡単に配布・送信・流通させることができる。
  - 仮想通貨のほか、電子トレカ、ポイント、投票券、チケットなどをトークンとしてブロックチェーン上で発行し、それと同時にビットコイン取引所Zaifにおける取り扱いが可能になる。
  - トークン投票システムZaif Voteにて、リアルタイム集計可能な投票権としても使用可能。
  - Counterpartyトークンと、MOSAICアセットに対応する他、mijinでプライベート型のブロックチェーンを使った仮想通貨やトークンを発行することも可能。
- 位置情報を活用した店舗向けキャンペーン機能「ZaicaでGo」を提供開始。
  - 地図上に配置したアイテムを収集、交換、取引、合成し賞金を獲得できるキャンペーン可能。
  - 「Zaica」で発行を支援したトークンをスマートフォンアプリの地図上に配置し、実際の位置へ行ったユーザーに取得させ、ウォレットアプリで交換や売買をさせることが可能。
  - ビットコイン取引所Zaifで複数を合成したトークンを賞金の仮想通貨と交換させたり、店舗などの位置情報を活用したゲーム性の高いキャンペーンを実施することが可能。
- 「合成(交換)機能」と「勾魂取引所」をリリース
  - 勾魂トークンの合成(交換)を可能とするもの。
  - takaraを通じて集めた同色の「一」から「七」までの勾魂を、取引所「Zaif」で大きなカラー勾魂に交換できる。
  - さらに、そのカラー勾魂を7色全て集めると、黒い「mijinの勾魂」に交換できる。

→ 出典: https://corp.zaif.jp/info/2807/
→ 出典: https://corp.zaif.jp/info/2869/
→ 出典: https://corp.zaif.jp/info/2645/
→ 出典: https://zaif.jp/event/mijinmagatama
→ 出典: https://medium.com/@IndieSquare_jp/

B E D

アップデート可能な公証・タイムスタンプサービス、NEMアポスティーユ

- Aposille（アポスティーユ）
  - ブロックチェーンの公証・タイムスタンプサービス。
  - 従来のタイムスタンプと異なり、アップデート可能。
  - ネーミングサービス、マルチシグアカウント、メッセージングを、NEMのAPIで実装。

- オープンソースの新型ウォレットとブロックチェーン証明書発行ツール
  - NanowalletはNEM/mijin双方に対応したマルチプラットフォームのウォレット。
  - 複数のMosaicアセットを作成・送金可能。
  - Nanowalletの一機能としてAposilleを提供。
  - mijinのプライベート環境で利用できるほか、mijinで生成したハッシュをNEMのパブリック環境に格納するアンカリングすることにより、高い信頼性・性能・プライバシーを両立可能。

→ 出典：http://japan.zdnet.com/article/35091786/
→ 出典：http://www.trend-stream.net/bitcoin/nem-apostille-whitepaper-japanese-3171/

B E D

中国マーケットにフォーカスしたデジタルアセットプラットフォーム、ANTSHARES

- コンセンサスアルゴリズム、分散台帳、P2Pプロトコル、スマートコントラクトVMなど、そのコアとして基本的なブロックチェーンレイヤーを含む。
  - パブリックチェーンを使う上でKYC/AMLのAPIをビルトイン。
  - マイクロソフトとのパートナーシップも発表。
  - AntsharesのサブエンティティであるOnchainと、LegalChainというコンソーシアムブロックチェーンも立ち上げ。
  - 他のブロックチェーンベースの金融アセットプラットフォームが暗号通貨をトランザクションに使うのに対し、法定通貨をブロックチェーン上で利用。
  - ゆえにデジタル通貨のボラティリティーに影響されず安定したプラットフォームになると主張。
  - Hyperleger同様にPBFTのコンセンサスメカニズム（DistributedBFTと呼んでいる）。

- 中国政府も、ChinaLedgerおよびShenzhen Consortiumによる戦略的アライアンスを発表。
  - ブロックチェーンをログストレージとして利用するサービス「Proof Log」のベータ版を公開。
  - システム管理者やシステム利用者の行動履歴などのログ情報をブロックチェーンに書き込むことにより、ログの変更・削除ができないようにする。
  - ブロックチェーンをログストレージとして利用するために、独自ブロックチェーンを開発。

→ 出典: https://www.cryptocoinsnews.com/antshares-blockchain-successful-ipo/
→ 出典: http://bravenewcoin.com/news/antshares-sets-out-to-be-the-peoples-digital-asset-blockchain/
→ 出典: https://cointelegraph.com/news/antshares-partners-with-microsoft-to-digitalize-real-world-assets-with-blockchain
→ 出典: https://www.antshares.org/zh-CN/Blog/Details/31
→ 出典: https://bitcoinmagazine.com/articles/strategic-alliance-formed-to-speed-up-adoption-of-blockchain-technology-in-china-1471884538
→ 出典: https://github.com/AntShares/AntShares/wiki/Whitepaper-1.1

B E D

ブロックチェーンにログを記録するサービス、PROOFLOG

- ブロックチェーンをログストレージとして利用するサービス「Proof Log」のベータ版を公開。
- 社内の記録を改ざんできないようにする仕組み。
- サテライトオフィス社と実証実験を行い、問題の早期発見や抑止力として機能することを確認。
- システム管理者やシステム利用者の行動履歴などのログ情報をブロックチェーンに書き込むことにより、ログの変更・削除ができないようにする。
- ブロックチェーンをログストレージとして利用するために、独自ブロックチェーンを開発。

→ 出典：http://www.fina-sol.com/news/102485.html
→ 出典：http://mainichi.jp/articles/20160901/k00/00e/020/302000c

CHRONICLED、ETHEREUMベースのIOTレジストリをローンチ

- Ethereumブロックチェーン上で接続されたデバイスの登録を行うツールをオープンソースとして開発。
- NFC、BLEチップ、IoTコンポーネント等のアイデンティティ情報を登録。
- Ethereumブロックチェーンを用いて、相互運用加納なIoTレジストリとする。
- これまでに限定品のスニーカーに埋め込まれたNFCやBLEチップの10000点をデプロイしてきている。
- 各デバイスがEtherteumブロックチェーン上のアイデンティティ記録とマッチングされることで、ラグジュアリーアイテムの詐欺を防ぐ。
- 半導体企業のSilicon Labsや、BLE企業のBlue BiteなどのIoT企業とコラボレーション。

→ 出典: http://chronicled.org/
→ 出典: http://www.coindesk.com/blockchain-startup-chronicled-launches-ethereum-iot-registry/

その他トピック①

- スイス国鉄、券売機でビットコイン販売へ
  - https://www.cryptocoinsnews.com/switzerlands-national-railways-operator-will-sell-bitcoin/
  - http://cryptocurrencymagazine.com/swiss-rail-operator-sbb-bitcoins
- ISOで国際標準化に関する議論が開始
  - http://www.meti.go.jp/press/2016/10/20161007002/20161007002.html
- エリクソン、ブロックチェーンフィンガープリント
  - http://www.coindesk.com/tech-giant-ericsson-blockchain-fingerprints-cloud/
- アララ、ブロックチェーン技術mijinの電子マネー分野への適用実証実験レポート公開
  - http://jp.techcrunch.com/2016/10/11/arara_adopts_blockchain/
  - http://knowledge.sakura.ad.jp/knowledge/6450/
- IndieSquareとテックビューロが業務提携しZaifモバイルアプリに技術提供
  - https://medium.com/@IndieSquare_jp/

その他トピック②

- 富士通研究所、取引先の制限や文書秘匿化などセキュリティ強化技術を開発
  - http://cloud.watch.impress.co.jp/docs/news/1025608.html

- テックビューロ、ブロックチェーンコア『Catapult』のホワイトペーパーを公開
  - http://mijin.io/ja/727.html
  - http://finance.yahoo.com/news/nem-blockchain-project-version-2-160100876.html
  - https://medium.com/nem-distributed-ledger-technology-blockchain/the-nem-blockchain-project-version-2-0-catapult-483e1eca5af8#.gcwxy3ocv

- 中国Onchain、Alibaba向けeメールエビデンスレポジトリを発表
  - https://coinreport.net/onchain-framework-alibaba-blockchain/

その他トピック③

- Colu、オフチェーンでのカラードコイントランザクションでLightningNetwork とのインテグレーションを発表
  - https://medium.com/colu/announcing-colored-coins-and-lightning-integration-8e54d5dbfd0e#.8bizdnlbg
  - http://www.coindesk.com/bitcoins-lightning-network-now-digital-asset-compatible/
  - https://bitcoinmagazine.com/articles/colu-announces-colored-coins-and-lightning-network-integration-1479312634

- 21 Inc、ビットコインマイニング特許申請
  - http://www.coindesk.com/21-inc-bitcoin-mining-patent/
  - http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=10&f=G&l=50&d=PG01&s1=%22bitcoin%22&p=1&OS=%22blockchain%22&RS=%22bitcoin%22

- ConsenSysのProject Alchemy、ZCashとEthereumのリレー"ZRelay"開発
  - https://github.com/ConsenSys/Project-Alchemy/blob/master/README.md

個別サービス①

名称	サービス概略	URL
HYPR	分散型生体認証	→ https://www.hypr.com/
IDENTITY CHAINS	トラストレスかつ分散的な方法で匿名のアイデンティティ認証サービスを提供（Ring Confidential Transactionsを採用）	→ http://eprint.iacr.org/2016/469.pdf
Iroha	Hyperledgerへコード提供	→ http://www.soramitsu.co.jp
Digital Bazaar, Inc.	アイデンティティ証明発行むけのLinked Data ledgerフォーマットを開発中。	→ https://www.dhs.gov/science-and-technology/news/2016/08/12/news-release-dhs-st-awards-13-million-small-businesses-cyber
Respect Network Corporation	分散レジストリ。パブリックブロックチェーンとのインテグレーション。	
Narf Industries LLC	パーミッションレスブロックチェーンにおけるアイデンティティ管理ソリューション	
Celerity Government Solutions, LLC	信用できるアイデンティティトランザクションを保持できるブロックチェーンソリューション	

個別サービス②

名称	サービス概略	URL
BitSquare	分散型ビットコイン取引所	→ https://bitsquare.io/bitsquare.pdf
WISeKey	デジタルID管理プラットフォーム	→ https://www.wisekey.com/press/wisekey-releases-new-wiseid-6-0-app-connecting-vertical-platform-sits-top-blockchain/
BSafe.network	MITによるブロックチェーン研究機関のネットワーク	→ http://bsafe.network/
Wings	DAOプラットフォーム	→ https://news.bitcoin.com/wings-dao-fail-slockit/
Uport	ConsenSysによる個人認証プラットフォーム	→ https://uport.me/library/pdf/whitepaper.pdf
Dragonchain	Disneyが開発した多通貨対応ハイブリッド型ブロックチェーン	→ https://github.com/dragonchain/dragonchain/blob/master/README.md → https://news.bitcoin.com/disney-dragonchain-interoperable-ledger/
Parity	パブリック・プライベートブロックチェーンの接続	→ http://dcebrief.com/connecting-public-and-private-blockchains-may-be-possible/

個別サービス③

名称	サービス概略	URL
Civic	アイデンティティ認証によるWebログインサービス	→ http://www.coindesk.com/civic-demos-vision-blockchain-web-login-service/
Blockstream	Sidechainの特許出願	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html
IPDB	ブロックチェーンデータベース	→ https://ipdb.foundation/
Golem	分散スーパーコンピュータ	→ https://www.smithandcrown.com/what-is-golem/
Expanse	スマートコントラクトプラットフォーム	→ http://www.expanse.tech/
ICONOMI	分散ファンドマネジメントプラットフォーム	→ https://www.smithandcrown.com/anatomy-ico-investments-iconomi/
Polcadot	パブリックチェーンとプライベートチェーンを繋ぐネットワーク	→ https://www.cryptocoinsnews.com/network-connects-public-private-blockchains/
CharityDAO	チャリティ特化型DAO	→ http://www.charity-dao.org/

3. ライフスタイル分野

① 経済エンタメ系テレビ番組『ビットガールズ』
② ブロックチェーンゲームプラットフォーム「Project ORB」
③ Yours Network、ビットコインベースでマネタイズを行う分散ソーシャルメディア
④ 広告ブロックブラウザのBrave、好きなサイトへ報酬をマイクロペイメントできるブラウザをローンチ

B E D

テックビューロ、経済エンタメ系テレビ番組『ビットガールズ』にブロックチェーン技術を提供

- 芸能プロダクション企業という設定で、インターネット上での所属メンバーのランキングや視聴者からの投票結果と、番組の内容とが連動する。
  - 各メンバーの「トレカブTM」（トレカ＋株）という、会社で言う「株式」に見立てた電子トレカ（仮想通貨トークン）をビットコイン取引所Zaifを通して仮想通貨であるビットコイン、XEM、ZAIFトークンとの交換によって売り出す。
  - その「トレカブ主」には議決権（仮想通貨トークン）が持ち「トレカブ比率」に応じて定期的に配当され、それを投票することによって視聴者自身が様々な意思決定を行う。
  - トレカブは仮想通貨として流通するため、出演メンバーは毎回の売上だけではなく、そのトレカブの時価をもって時価総額によるランキングにも参加する。
  - ビットガールズでは各メンバーがトレカブというトークンを発行し、そのICOを模したコンテンツを製作。
  - ブロックチェーン技術の活用により、透明性の高い、改ざんのできない投票システムと時価総額のランキング、そして偽造ができない限定数のトレカブ販売を実現する。
- 仮想通貨や独自トークンによる投票をリアルタイム集計できるサービスを利用。
  - テックビューロ、ビットコインなどの仮想通貨やCounterpartyトークン、NEM MOSAICなどによる投票をリアルタイム集計できるサービス。
  - 各投票が送信後約2秒から10秒でリアルタイムに集計される。
  - 投票の選択肢ごとにアドレスを指定し、投票期間を設定すると、それら個別のアドレスに指定した暗号通貨やトークンの送付を受付可能に。

→ 出典：https://corp.zaif.jp/info/2844/
→ 出典：https://corp.zaif.jp/info/2486/
→ 出典：http://n832.net/282.html

ビットガールズ、ICOプランとしてトークン売り出し

- ビットガールズのICOプラン
  - Zaifビットコイン取引所にて販売。
  - 期間は10/3から10/31まで。
  - メンバーあたり、500万トレカブを発行してロックした上で、そのうち350万をICOに充て、100万を留保、50万を半年の委員会運営ならびにマーケティング予算という配分。
  - トークンは11/1に配布され、11/4以降に取引可能に。

- トレード初日の時価総額5000万円
  - タレント毎に「トレカブ」（トレーディングカードと株の組み合わせ）という仮想通貨を発行。
  - 有価証券法に基づく証券化ではなく、ブロックチェーンによるトークン化による。
  - トレカブは11/4からZaifにて仮想通貨としてトレード可能。
  - 比較的無名な出演者によって数千万円単位の資金を集めた実績を残した。
  - 11/16からは第２期のトークンを売り出し。

→ 出典: http://bitgirls.io/ja/
→ 出典: http://marketcap.zaif.jp/ja/db30762552229b4c
→ 出典: http://cryptocurrencymagazine.com/bitgilrs-market-capitalization
→ 出典: https://corp.zaif.jp/info/3255/
→ 出典: http://thebridge.jp/prtimes/193260
→ 出典: https://www.smithandcrown.com/bitgirls-pushes-boundaries-crowdsale-sc-research-report/
→ 出典: http://bitgirls-nemkd12.hatenablog.com/entry/2016/11/21/003036

B E D

ブロックチェーンゲームプラットフォーム「PROJECT ORB」

- Spells of Genesisのモバイルソフトローンチのタイミングと合わせローンチ。
  - ORBは「Ownership Revolution on the Blockchain」の略。
  - プレイヤー間で自由に送受信やセキュアなP2P分散トレードが可能。
  - オープンなブロックチェーンの互換性を生かし、複数のゲームもしくはゲーム以外の分野でも使用可能。
  - ブロックチェーンの改ざん不能性と透明性を活かし、発行量が限定されている希少性が高いゲームアイテムを発行可能。
  - Project ORBのプロダクトとして「Book of Orbs」がAppstoreとGoogle Playで公開。
  - 「Book of Orbs」は、Counterpartyプロトコルを通してビットコインのブロックチェーン上で発行されたORBの収集、移動、トレードなどが一つのアプリ上で完結する、ゲーム特化型モバイルコレクションアプリ。
  - ローンチ時には、Spells of Genesis(SoG)とForce of Will(FoW)の2つのゲームに対応予定。
  - それぞれのゲームとBook of Orbsを連携させることで、自分のアドレス上のORBの保有をセキュアに証明し、実際のゲーム上でORBが使用可能になる。

→ 出典: https://medium.com/@IndieSquare_jp/
→ 出典: http://themerkle.com/project-orb-will-focus-on-tradeable-blockchain-based-in-game-items/
→ 出典: http://www.spellsofgenesis.com/play/

B E D

YOURS NETWORK、ビットコインベースでマネタイズを行う分散ソーシャルメディア

- コンテンツクリエイター自身によるコントロール可能なソーシャルメディア。
- ビットコインを用いて金銭的インセンティブを提供することによって、コンテンツ作成やインタラクションを促す。
- Synereo、Steemitといったブロックチェーンベースのソーシャルメディアがオルトコインを用いてマネタイズするのに対し、ビットコインによるマネタイズを行うもの。
- LNのローンチに先駆けて、自身で独立した仕組みとして、LNに触発された仕組みを構築することで、少額トランザクションに利用する予定。

→ 出典：https://news.bitcoin.com/yours-network-bitcoin-steemit/
→ 出典：http://www.livebitcoinnews.com/bitcoin-micropayments-based-use-lightning-like-system/
→ 出典：https://engineering.yours.network/
→ 出典：https://stories.yours.network/a-micropayment-to-corey-petty-ce861027e9f#.mw5vb4r3c
→ 出典：http://doublehash.me/yours-worlds-first-micropayments-web-wallet/
→ 出典：http://bravenewcoin.com/news/bitcoin-based-social-media-community-yours-completes-micropayment-system/

B E D

広告ブロックブラウザのBRAVE、好きなサイトへ報酬をマイクロペイメントできるブラウザをローンチ

- Brave Paymentsのベータ版をリリースし、気に入ったコンテンツのウェブサイトへ報酬としてマイクロペイメントを可能に。
- 既存のビットコインウォレットを使うか、インテグレーションしているCoinbaseを用いてウォレットを作成する。
- 予めサポートしたいサイトを選んで、ビットコインをデポジットしておくと、訪問回数などを算出してサイトへ支払いを行う仕組み。
- エスクローにビットコインが溜まり、100ドルに達したらシステムからサイトのウェブマスターとドメインオーナーに対してメール送信。

→ 出典: https://blog.brave.com/introducing-brave-payments/
→ 出典: http://cryptocurrencymagazine.com/brave-micro-payments-browser
→ 出典: http://www.coindesk.com/brave-browser-launch-bitcoin-micropayments/

個別サービス

名称	サービス概略	URL
takara	ビットコイン収集ゲーム	→ http://www.financemagnates.com/cryptocurrency/interview/bitcoin-go-geocaching-game-takara-lets-you-collect-counterparty-tokens/
Veredictum	映像・テレビ業界の台本・現行保護（不正ダウンロード対策）	→ http://www.zdnet.com/article/australian-blockchain-startup-takes-on-film-and-tv-industry-piracy/
Fermat	P2Pタクシープラットフォーム	→ http://www.fermat.org/p2p-taxi-platform/
SinglarDTV	デジタルコンテンツ配信プラットフォーム	→ https://singulardtv.com/resources/default/pdf/JAPANESE_SingularDTV%20CODE.pdf → http://is.shihp.in/2016/08/the-singuladtv.html
FirstBlood	Eスポーツプラットフォーム	→ http://bitcoinist.net/firstblood-esports-platform-crowdsale/
CoinTip	セレスとジャノムが共同開発したビットコイン送金サービス	→ http://host211006211247.stockdatabank.jp/tdnet/data/20161116/140120161116441397.pdf
BlockCDN	コンテンツ配信ネットワーク	→ http://bitcoin.xyz/chinese-video-hosting-service-youku-first-trial-blockcdns-blockchain-content-distribution-network-cdn/amp/

4.サプライチェーン系

- Marin Tranport International、運輸業界むけサプライチェーン
- Chronicled、アイデンティティチップ搭載のドローンでデリバリー実験
- Chronicled、CryptoSealを発表
- IBM、宅配荷物のトラッキングを行うストレージロッカーを開発
- ウォルマート、中国で食料品のサプライチェーン追跡のプロトタイプ開発
- ISID、ガードタイム、シビラ、地方創生を支援する研究プロジェクト
- オートバックス、中古カー用品の個人間売買の実証実験

トピックリスト①

- Marin Tranport International、パブリックチェーンによる運輸業界むけSCM
  - https://www.finextra.com/pressarticle/66223/marine-transport-international-applies-blockchain-to-shipping-supply-chain
  - http://www.the-blockchain.com/2016/09/24/mti-rolls-first-blockchain-project-global-shipping-industry/
  - https://blockchain.info/tx/cf6cd06580d11c1a40292573b898019d42aed0d14d5324100a889fc045791e03
- Chronicled、パブリックチェーンに格納したアイデンティティチップ搭載のドローンでデリバリー実験
  - https://news.bitcoin.com/chronicled-demo-blockchain-drone/
- Chronicled、CryptoSealを発表
  - https://www.cryptocoinsnews.com/chronicled-launches-physical-blockchain-based-tamper-proof-cryptoseal-strips/
  - http://www.chronicled.com/download/CryptoSeal-Datasheet.pdf

トピックリスト②

- IBM、FreshTurfと協業し宅配荷物のトラッキングを行うストレージロッカーを開発
  - http://www.coindesk.com/ibm-blockchain-pilot-delivery/
  - https://www-03.ibm.com/press/us/en/pressrelease/50862.wss
- ウォルマート、中国で食料品のサプライチェーン追跡のプロトタイプ開発
  - https://www.finextra.com/pressarticle/66661/walmart-to-apply-blockchain-to-supply-chain
- ISID、ガードタイム、シビラ、 ブロックチェーン技術を活用して地方創生を支援する研究プロジェクトを立上げ
  - http://www.isid.co.jp/news/2016/1019.html
- オートバックス、中古カー用品の個人間売買の実現可能性を検証する実証実験
  - http://s.response.jp/article/2016/08/09/279888.html
  - http://www.autobacs.co.jp/images/data/news/2016/11/16/2ohL28.pdf

個別サービス

名称	サービス概略	URL
Blockfreight	グローバルフリート管理	→ https://github.com/Blockfreight
Power Ledger	メーターネットワーク上のP2Pエネルギー取引	→ http://www.the-blockchain.com/2016/10/28/australias-power-ledger-expands-blockchain-energy-trials/
ChronoBank	豪州の労働力交換プラットフォーム	→ http://www.ibtimes.co.uk/chronobank-creating-global-blockchain-based-labour-exchange-1592019

5. シビックテック系

① 中国Wanxiang、スマートシティ構想におけるブロックチェーン応用を発表
② シーメンス、ブロックチェーンによるマイクログリッドに取り組み

中国WANXIANG、スマートシティ構想におけるブロックチェーン応用を発表

- 今後7年間で300億ドルの投資を見込みIBMやMicrosoft、ConsenSys、Ethereum Foundationの協力を得て杭州市でスマートシティ構想。
- Wanxiang（万向集団）は自動車部品メーカーだが、2015年には子会社を通じetherを購入した他、Wanxiang Blockchain Labを立ち上げ。
- 同様なスマートシティ構想へのブロックチェーン応用にはドバイでも。
- WanxiangはIoT分野での応用を考える他、スマートカー分野でのバッテリーのトラッキング等を検討。さらには、ソーラーIDや車両登録、インテリジェントコミュニティ、シェアリングエコノミー等も。

→ 出典：http://www.coindesk.com/blockchain-smart-cities-china-wanxiang/
→ 出典：http://www.coinfox.info/news/6460-wanxiang-smart-cities-to-partner-with-microsoft-and-ibm

シーメンス、ブロックチェーンによるマイクログリッドに取り組み

- LO3と協業し、TransActiveGridの活動推進。
- シーメンスのマイクログリッドコントロール技術と、LO3のP2P取引プラットフォームを組み合わせ。
- ブロックチェーンを用いて、エネルギー生産者と消費者の直接取引に関するデータを検証・格納。中央のモニタリング無しに分散システム上で追跡可能で不正改ざん困難に。
- 今後、マイクログリッドやスマートシティプロジェクトに取り組む。
- 他社の取組
  - ドイツの電力会社RWEがslockと充電ステーションの実験を行ったほか、ノルウェーの電力会社Vattenfallはオランダに立ち上げたスタートアップ PowerpeerとP2Pエネルギーマーケットを実験。
  - オランダではブロックチェーンベースのP2Pエネルギー取引プラットフォームEcoCoinが活動中。ウィーンのGridSingularityは新興国むけにpay-as-you-go型のエネルギー取引の認証を実験中。南アフリカのInviroHubはスマートメーターやブロックチェーンベースのソフトウェアを組み合わせ統合アプリを開発。豪州ではPowerLedgerがソーラーエネルギー取引プラットフォーム。SolarCoinはソーラー発電のインセンティブとしてデジタル通貨。

- 出典: http://www.coindesk.com/siemens-blockchain-microgrid-lo3-ethereum/
- 出典: https://www.finextra.com/blogposting/13394/blockchain-may-fuel-the-energy-industry
- 出典: http://news.usa.siemens.biz/press-release/energy-management/siemens-and-us-startup-lo3-energy-collaborate-blockchain-microgrids
- 出典: https://www.siliconrepublic.com/enterprise/solar-power-blockchain-siemens

その他トピックリスト

- MITメディアラボ、ビットコインブロックチェーン上で学位証明のオープンプラットフォーム開発
  - https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f#.xw4hts746
- ドバイ政府、2020年までに全公文書をブロックチェーン管理の方向
  - http://btcnews.jp/dubai-announced-migrating-all-government-documents-on-blockchain-by-2020/
- Factom、医療レコード記録システム構築へメリンダ財団から資金提供
  - http://coinjournal.net/blockchain-startup-receives-grant-gates-foundation-medical-records-project/
- マン島の当局がCreditsと協働でIoT向けブロックチェーンをテスト
  - http://www.efinancialnews.com/story/2016-08-08/isle-of-man-government-on-blockchain-iot-quest
- 米国保健福祉省、オープンイノベーションにより医療分野のブロックチェーンを推進
  - https://www.hhs.gov/about/news/2016/08/29/onc-announces-blockchain-challenge-winners.html

個別サービス

名称	サービス概略	URL
EmergencyChain	緊急時の医療データ配送インフラ	→ https://devpost.com/software/emergencychain
Blockcerts	デジタル学位証明のオープンスタンダード	→ https://news.bitcoin.com/mit-blockcerts-certification-bitcoin/
eGaaS	電子政府プラットフォーム	→ http://cryptocurrencymagazine.com/what-is-egaas
Smart Love	Bitnationの婚姻届	→ https://cointelegraph.com/news/bitnation-releases-marriage-app-smart-love-on-ethereum-blockchain
Power Ledger	豪州のエネルギー流通プラットフォーム	→ http://powerledger.io/

6.金融機関系の動き

① UBSの「Utility Settlement Coin」
② Santanderとethercamp、銀行口座とethereumのブリッジを構築するCashEthプロジェクトを発表
③ Accenture、金融機関向けにブロックチェーン編集ツールのプロトタイプ
④ VISA、Chainと協業で国際B2Bペイメントソリューション開発し来年ローンチ
⑤ PwC、デジタルアセットサービスVulcanを発表
⑥ GoldmanSachs、Santander、Morgan Stanley がR3のメンバシップを更新せず脱退

B E D

UBSの「Utility Settlement Coin」、BNY Mellon・Deutsche Bank・SantanderおよびIcapが参加

- 「Utility Settlement Coin」は、中央銀行にデポジットされた現物通貨の代理を果たし、米ドル・ユーロ・ポンド・スイスフランを含む主要通貨と等価交換可能。
- 中央銀行むけデジタルキャッシュの業界標準を目指す。
- UBSがClearmaticsと開発を進めてきた「Utility Settlement Coin」について、BNY Mellon・Deutsche Bank・SantanderおよびIcap が参加し、グローバルなクリアリング・セツルメントシステムの構築を目指す。
- UBSのR&D blockchain labによるCrypto 2.0 Pathfinder Programの一環として進められてきたもの。
- 2018年までにブロックチェーンシステムの商用化を予定。

→ 出典: http://www.coindesk.com/report-banks-band-together-launch-settlement-coin/
→ 出典: https://www.finextra.com/newsarticle/29345/ubs-wins-big-bank-backing-for-utility-settlement-coin-concept
→ 出典: http://www.cnbc.com/2016/08/24/four-top-banks-join-forces-on-new-digital-currency.html
→ 出典: https://bitcoinmagazine.com/articles/major-banks-developing-utility-settlement-coin-an-industry-standard-for-digital-central-bank-cash-1472140867

SANTANDERとETHERCAMP、銀行口座とETHEREUMのブリッジを構築するCASHETHプロジェクトを発表

- Ethereumのパブリックブロックチェーン上でデジタルキャッシュを発行。
- 銀行口座を介して、法定通貨とEthereum上のトークンを結びつけ、マイクロペイメントを可能にする。
- 銀行口座上のマネーをCashETHと呼ばれるトークン化されたオンライン通貨に変換し、紙幣への変換も可能もの。
- このトークンはSantanderのリアルマネーに裏づけされたものなので、いつでも換金できる。
- パブリックブロックチェーンと金融機関のつながりとして革新的な試み。

→ 出典: http://www.ibtimes.co.uk/devcon2-santander-ethercamp-building-bridges-between-bank-accounts-ethereum-1582242
→ 出典: http://www.coindesk.com/santander-vies-become-first-bank-issue-digital-cash-blockchain/

B E D

ACCENTURE、金融機関向けにブロックチェーン編集ツールのプロトタイプ

- ヒューマンエラーや法・規制当局要請などへの対応を想定したもの。
- 忘れられる権利やプライバシーなどへの要請に応える。
- 指定された管理者がおり、合意されたルールのあるPermissionedなブロックチェーン向け。
- オープンで単一の管理主体を持たず、改ざん困難性を有する、いわゆる暗号通貨のようなPermissionlessなブロックチェーンは対象外。
- チェーンを壊すことなしに、情報の編集・上書き・削除ができる。
- アルゴリズムを再生成できるカメレオンハッシュ機能を用いるもので、２つの分かれたブロックを繋ぐことができる。
- 米国およびEUへ特許出願中。

→ 出典：http://www.the-blockchain.com/2016/09/20/accenture-releases-patented-blockchain-editing-tool-banks/
→ 出典：https://newsroom.accenture.com/content/1101/files/Cross-FSBC.pdf

B E D

VISA、CHAINと協業で国際B2Bペイメントソリューション開発し来年ローンチ

- 金融機関むけに提供される、高速で安全なグローバルB2Bペイメント。
- プライベートブロックチェーンChain Coreを用いてChainと構築。
- Visa B2B Connectは2017年にパイロット予定。

→ 出典: http://www.businesswire.com/news/home/20161021005212/en/Visa-Introduces-International-B2B-Payment-Solution-Built
→ 出典: http://www.coindesk.com/visa-blockchain-payments-service/

B E D

PwC、デジタルアセットサービスVULCANを発表

- 銀行が既存顧客むけにビットコインを用いた新しいサービスを提供できるようにする。
- ビットコインやその他オルタナティブとの相互運用可能なデジタルアセット提供を可能に。例えばリワードポイント発行など。
- ウォレット発行やペイメントプロセスなどのインフラサポートも。
- Bloq, Netki, Libraとの協業。
- 分断されたブロックチェーンやデジタル通貨のエコシステム統合を目指す。

→ 出典: https://www.vulcandas.com/
→ 出典: http://www.coindesk.com/digital-asset-service-pwc-vulcan-bitcoin/

B E D

GoldmanSachs、Santander、Morgan Stanleyがr3のメンバシップを更新せず脱退

- メンバーシップを更新せず。
- R3は当初$200mをターゲットとした資金調達中だったが、ターゲットを$150mに引き下げ。結果、$59mの調達に留まった模様。
- 11/30にはCordaのオープンソース化。

→ 出典: http://www.coindesk.com/goldman-sachs-leaves-r3cev/
→ 出典: http://fortune.com/2016/11/21/goldman-sachs-r3-blockchain-consortium/
→ 出典: https://goldsilverbitcoin.com/r3-sends-cease-and-desist-to-peter-todd/

B E D

アーンストヤング、インボイスへのビットコイン支払受入へ

- スイス拠点のクライアントに対し、ビットコインによるインボイス決済を可能にする。
- チューリヒオフィスにビットコインATM設置し、従業員がビットコインの支払・受取ができるウォレット（EY wallet app）を使用可能に。
- EY Garage Labではスマートコントラクトを使ってクライアントと協業も。

→ 出典: http://www.newsbtc.com/2016/11/25/ey-unveils-strategy-create-mainstream-bitcoin-traction-switzerland/
→ 出典: https://webforms.ey.com/ch/en/newsroom/news-releases/news-release-ey-switzerland-accepts-bitcoins-for-payment-of-its-services

その他トピック①

- デロイト、トロントオフィスにビットコインATM（BitAccess製）を設置
  - http://themerkle.com/deloitte-unveils-bitcoin-atm-in-their-toronto-office/
- Symbiont、AllianzとNephila Capital recentlyの間でカタストロフィ・スワップ取引
  - http://www.artemis.bm/blog/2016/09/08/blockchain-catastrophe-swap-platform-ready-shows-insurtech-potential/
- TO、初のブロックチェーンエクイティ発行にむけてKeystone Capitalと提携
  - https://news.bitcoin.com/overstock-to-public-blockchain-equities/
- Goldman Sachs、外国為替取引への適用を目指した特許
  - http://qz.com/779660/goldman-sachs-wants-to-put-foreign-exchange-trades-on-the-blockchain/
- セネガル、自国通貨をブロックチェーンによるデジタル通貨へ
  - http://www.iafrikan.com/2016/11/24/senegal-to-introduce-a-new-blockchain-based-national-digital-currency-making-it-only-the-second-country-to-have-a-national-digital-currency/

その他トピック②

- JP Morgan、プライベートEthereum
  - http://www.coindesk.com/jpmorgan-ethereum-blockchain-quorum/
  - https://drive.google.com/file/d/0B42vMkapQi1MSEVaa2tuVEtXZXM/view
- スイスの金融マーケットブロックチェーン
  - http://www.coindesk.com/how-six-securities-is-trying-to-build-sixchain-into-its-swiss-value-chain/
- ロシア中央銀行、Masterchainプロジェクト立ち上げ
  - http://www.coindesk.com/russian-central-bank-blockchain-distributed-ledger-transactions/
- 中国の全国社会保障基金理事会、社会保障の支払い向けにブロックチェーン利用
  - https://news.bitcoin.com/china-social-security-blockchain/
- アブダビ証券取引所、上場会社の年次株主総会におけるブロックチェーン投票サービス
  - https://www.adx.ae/English/News/Pages/20161015140637422.aspx
- 三井住友信託、債権流動化業務およびグローバルカストディ開設業務で実証実験
  - http://www.coindesk.com/sumitomo-mitsui-trust-bank-testing-blockchain-ibm/

その他トピック③

- HSBC等が不動産モーゲージシステムを計画
  - http://dcebrief.com/hong-kong-finance-industry-planning-blockchain-mortgage-system/
- CapitalOne、Gemと協業し健康保険請求支払管理システム
  - https://bitcoinmagazine.com/articles/gem-partners-with-capital-one-for-blockchain-based-health-care-claims-management-1477502028
- MasterCard、実験的にブロックチェーンAPIをリリース
  - http://www.coindesk.com/credit-card-giant-mastercard-releases-experimental-blockchain-apis/
- 大和総研、ミャンマー資本市場における実証実験結果をレポート
  - http://www.dir.co.jp/release/2016/20161031_011348.pdf
- スウェーデン中央銀行、独自デジタル通貨の発行を検討
  - http://www.newsbtc.com/2016/11/16/sweden-digital-currency-2019/
- Visa Europe、マイクロペイメントの試行へむけてSatoshiPayと提携
  - http://www.coindesk.com/visa-europe-bitcoin-micropayments/
- 欧州の保険会社がコンソーシアム立ち上げ
  - http://www.coindesk.com/europe-insurance-blockchain-consortium/

その他トピック④

- 大手会計監査法人がコンソーシアム立ち上げへ
  - http://blockchain-finance.com/2016/08/12/new-blockchain-consortium-on-the-horizon/
- デロイト、ethereum ベースのアイデンティティプラットフォームSmart IDを開発中と発表
  - http://www.deloitte.co.uk/smartid/
- BofAML・HSBCおよびIDAシンガポール、トレードファイナンスのプロトタイプを開発
  - http://arxiv.org/pdf/1608.00771v2.pdf
- Infosys子会社、Emirates NBDおよびICICI銀行との間でトレードファイナンス
  - http://blockchain-finance.com/2016/10/19/blockchain-pilot-network-from-infosys-finacle-emirates-nbd-and-icici-bank/
- バークレイズ、Waveと協働でL/Cのトランザクションを分散台帳上で発行
  - https://www.finextra.com/newsarticle/29400/barclays-executes-live-letter-of-credit-transaction-using-distributed-ledger-technology
- IBM、中国UnionPayとロイヤリティポイント交換システムの実験
  - http://www.coindesk.com/ibm-china-unionpay-blockchain-loyalty-exchange/
- 中国Minsheng Life Insurance、ロイヤリティリワードシステム開発を計画
  - https://consensys.net/static/BlockApps-Minsheng-Consensys.pdf

その他トピック⑤

- R3コンソーシアムの15行、トレードファイナンス分野でプロトタイプを開発
  - http://www.bankingtech.com/551002/r3-blockchain-consortium-gets-smart-on-trade-finance
- R3、AXONIとデータマネジメントへの分散台帳応用を探索
  - https://r3cev.com/press/2016/9/20/press-release-r3-and-axoni-explore-the-use-of-distributed-ledger-technology-to-reduce-risk-in-reference-data-management-with-buy-and-sell-side-financial-services-firms
- R3、RippleのデジタルアセットXRPを用いた銀行間クロスボーダーペイメントを試行
  - https://ripple.com/ripple_press/r3-trials-interbank-cross-border-payments-ripples-digital-asset-xrp/
- R3、KYC向けアイデンティティ用レジストリを10行と試行
  - http://www.coindesk.com/r3-banks-trial-blockchain-identity-registry/
- R3、シンガポールMASとデジタル通貨の実証実験を開始
  - http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/MAS-experimenting-with-Blockchain-Technology.asp

その他トピック⑥

- 東京三菱UFJ銀行、日立製作所と小切手取引システムを開発
  - http://asia.nikkei.com/Business/Companies/BTMU-Hitachi-test-new-check-processing-system-in-Singapore
- 東京三菱UFJ銀行、IT契約管理への適用を目指す
  - http://www.coindesk.com/bank-tokyo-use-blockchain-contract-management-2018/
- 「ブロックチェーン技術等を活用した国内外為替一元化検討に関するコンソーシアム」が発足
  - http://www.sbigroup.co.jp/news/2016/0819_10389.html
- 静岡銀行、マネックスと地域活性化実証実験
  - http://www.shizuokabank.co.jp/pdf.php?id=2673
- 楽天証券、本人確認システムの開発へ
  - http://itpro.nikkeibp.co.jp/atcl/news/16/082302434/
- カブドットコム証券株式会社、企業内コイン「OOIRI」の検証を開始
  - http://cryptocurrencymagazine.com/kabu-com-ooiri-coin

8.金融系スタートアップの動き

① Digital Asset Holdings、
「Global Synchronization Log」発表

Digital Asset Holdings、「Global Synchronization Log」発表

- フルスタックではなくモジュラー型のアプローチによるソリューション。
- Digiatal Asset Platform の一つのコンポーネントとしての実装。
- 異なるプラットフォームとの相互運用性に注力しており、FabricやCordaなどと共に、Hyperledger コミュニティにおける共同実装を目指す。

→ 出典: http://www.coindesk.com/digital-asset-targets-biggest-big-banks-new-blockchain-tech/
→ 出典: http://digitalasset.com/static/documents/The_Global_Synchronization_Log.pdf

その他トピック

- Digital Asset Holdings、SIX Securities Servicesと協働でスイスの金融市場むけに証券ライフサイクルプロセスのプロトタイプ構築
  - http://www.six-group.com/dam/about/downloads/media/media-releases/2016/0922-e-SIX-DigitalAsset.pdf
- SETL、Cobalt DLと協業しFXポストトレードシステム
  - https://www.ftfnews.com/setl-cobalt-dl-to-create-fx-post-trade-dlt-solution/14828
- SETL、デロイトと非接触決済カード開発
  - http://btcnews.jp/deloitte-and-setl-tested-their-own-blockchain-based-contactless-card-system/
- Overstock、12月より同社の株式取引をブロックチェーンで開始へ
  - https://www.coin-portal.net/2016/10/31/14279/
- インドのUnocoin、クロスボーダーペイメントAPIリリース
  - http://www.ibtimes.co.uk/unocoin-releases-api-power-bitcoin-economy-india-1590196

その他の個別サービス

名称	サービス概略	URL
R3	銀行間接続プラットフォーム「Concord」のバックエンドシステム「Corda」の特許申請	→ http://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf
PAR	Productive Asset Record System Ripple Interledgerを利用した、ヘッジファンド向け監査アプリケーション。 パブリック／プライベートの台帳技術を併用。	→ http://par.io/whitepaper.pdf
Teambrella	ビットコインベースのP2P保険	→ https://teambrella.com/
Symbiont Assembly	金融機関むけスマートコントラクトに特化した分散台帳	→ https://symbiont.io/technology/introducing-symbiont-assembly/
inchain	ethereumスマートコントラクトベースの分散保険プラットフォーム	→ https://ico.inchain.io/app/docs/whitepaper2.pdf → https://ico.inchain.io/#about → https://www.smithandcrown.com/event/inchain-selling-tokens-insurance-dao/

9.参考資料リンク集

- 技術トピック
- 非金融分野トピック
- 金融分野トピック

技術トピック①

- 暗号通貨・ブロックチェーン論文　必読リスト
  - https://blog.visvirial.com/articles/702
  - ビットコイン系（４本）、コンセンサス系（２本）、支払いチャネル（２本）
  - マイニング関連（１本）、基礎知識系（３本）

- Satoshi Nakamoto Institute（サトシナカモト論文以前の各種論文）
  - http://nakamotoinstitute.org/literature/

- Courseraで暗号通貨コース開始
  - https://www.coursera.org/learn/cryptocurrency/

- ブロックチェーン・分散台帳技術・コンセンサスメカニズム、暗号通貨・デジタル通貨に関するホワイトペーパー集
  - http://bravenewcoin.com/industry-resources/whitepapers/a-e/

技術トピック②

- W3C Blockchain Workshop
  - http://diyhpl.us/wiki/transcripts/w3-blockchain-workshop-2016/
  - http://www.cio.com/article/3090143/security/highlights-from-the-w3c-blockchain-workshop-at-mit.html
  - https://prezi.com/m/wt2ioyhm-spn/?utm_campaign=share&utm_medium=copy
  - https://www.dropbox.com/s/c0dbtmfs1mp7d79/W3C%20Blockchain%20Workshop%20June%2029%2C%202016.pdf
  - W3Cブロックチェーンワークショップのトランスクリプト集、グラフィックレコーディング集。

- W3Cブロックチェーンワークショップに関するレポート
  - https://www.w3.org/2016/04/blockchain-workshop/report.html#exec
  - https://www.w3.org/blog/2016/08/building-blocks-to-blockchains/

- W3Cブロックチェーンワークショップのトランスクリプト集
  - http://diyhpl.us/wiki/transcripts/w3-blockchain-workshop-2016/

技術トピック③

- Programming The Blockchain in C#
  - https://www.gitbook.com/download/pdf/bok/programmingblockchain/programmingblockchain
- The Internet of Money
  - https://www.amazon.com/Internet-Money-collection-Andreas-Antonopoulos-ebook/dp/B01L9WM0H8
  - 「マスタリング・ビットコイン」著者Andreas M. Antonopoulosによる。
  - 2014年から2016年にかけて行われたBitcoin Meetupでの内容をもとに。
- The Trend Towards Blockchain Privacy: Zero Knowledge Proofs
  - http://sammantics.com/blog/2016/8/23/the-trend-towards-privacy-how-blockchains-plan-to-accomplish-this
- カリフォルニア集会2016 の日本語訳
  - http://dc.silsila.net/

技術トピック④

- Bitcoin Terminology
  - https://scalingbitcoin.org/terminology#terms
- Ethereum 2.0 Mauve Paper
  - http://vitalik.ca/files/mauve_paper3.html
- イリノイ大学のCryptocurrency Securityコース
  - http://soc1024.ece.illinois.edu/teaching/ece598am/fall2016/
  - ビットコイン、Ethereumからスマートコントラクト、プライバシー、セキュリティ等。
- Bitcoin, Blockchain, and the DLT Chimera
  - https://www.slideshare.net/mobile/Ferdinando1970/bitcoin-blockchain-and-the-dlt-chimera

技術トピック⑤

- Bitcoin's Security Model: A Deep Dive
  - http://www.coindesk.com/bitcoins-security-model-deep-dive/
- Proof of Stake FAQ
  - https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
- The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure
  - https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure

非金融分野関連トピック

- Blockchain-Enabled Convergence
  - https://medium.com/outlier-ventures-io/blockchain-enabled-convergence-9199c547f851#.wy6pxlls7
- Blockchain Graveyard
  - https://magoo.github.io/Blockchain-Graveyard/
  - 侵入を受けて資産の盗難にあった暗号通貨関連プロジェクトの一覧。
- Three blockchain benefits, above and beyond traditional databases
  - http://bravenewcoin.com/news/three-blockchain-benefits-above-and-beyond-traditional-databases/
- Six Blockchain Application Verticals
  - https://blog.bigchaindb.com/six-blockchain-application-verticals-1-bonus-aa7caa5764e2#.8ontf75dj
  - https://blog.bigchaindb.com/the-benefits-x-verticals-grid-bc07a13daba2#.h61hj2izo

金融関連トピック①

- Credit Suisse on the Challenges for blockchain going mainstream
  - http://www.businessinsider.com/credit-suisse-on-the-challenges-for-blockchain-going-mainstream-2016-8
- 世界経済フォーラム「The future of financial infrastructure」
  - http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf
- 日本取引所グループがブロックチェーン技術のワーキングペーパーを公開
  - http://www.jpx.co.jp/corporate/research-study/working-paper/tvdivq0000008q5y-att/JPX_working_paper_No15.pdf
- ESMA（欧州証券市場監督局）による分散台帳に関するレポート
  - https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf
  - http://coincenter.org/files/2016-09/coin-center-letter-to-esma.pdf

金融関連トピック②

- Moody'sが整理した、ブロックチェーン関連プロジェクト一覧表
  - http://www.businessinsider.com/moodys-releases-definitive-list-of-every-blockchain-project-out-there-2016-7?op=1
- Whitepaper On Distributed Ledger Technology
  - 香港金融管理局によるマネーロンダリングリスクに関するレポート
  - http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf
- Distributed Ledger Technology: Implications for Payments, Clearing, and Settlement
  - https://www.federalreserve.gov/newsevents/speech/brainard20161007a.htm
- Smart Contracts in Financial Services:Getting from Hype to Reality
  - https://www.capgemini-consulting.com/resource-file-access/resource/pdf/smart-contracts.pdf