Bitcoin & Blockchain概況

2017.03 by SATO

「Bitcoin2.0概況」「Blockchain2.0概況」から改題

過去8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
- **第８回（2016年12月）：**2016年8月～2016年11月の動き

TABLE OF CONTENTS

➔ 今回は、2016年12月～2017年3月の動きを中心に整理

1. テクニカル分野
2. プラットフォーム分野
3. ライフスタイル分野
4. サプライチェーン分野
5. シビックテック分野
6. 金融機関の動き
7. 金融系スタートアップの動き
8. 参考資料リンク集

■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
- D Private, Permissioned Blockchain Distributed Ledger関連

Public Blockchain

1. テクニカル分野

- ビットコインのスケーリングにハードウェアを利用した、Teechan
- ビットコインマイニングのリソース消費節約へのIC3による代替案
- Bitcoin Lightning 仕様アップデート
- Blockstream、Sidechain(Strong Federations)ホワイトペーパ
- ビットコインスケーリング論争とハードフォーク危機
- Bitcoin Unlimitedのブロックサイズ提案とコンセンサス投票
- SegWitへむけたUser Activated Soft Fork提案

B E D

ビットコインのスケーリングにハードウェアを利用した新たなオプション、TEECHAN

- オフチェーンのトランザクションプロトコルで、トラストされた実行環境（TEE）を利用して高スループット・低レイテンシが実現可能な全二重ペイメントチャネルを構築する。
- Segwitなどのプロトコル変更を必要とせずに、インテルSGXを用いて既存のビットコインネットワーク上に構築し、実験では秒間2480トランザクション（レイテンシ0.4ミリ秒）到達。
- インテルSGXはCPUのソフトウェアガード拡張の意味で、enclaveという特殊構造のチップを持ち秘匿実行可能な命令セット。
- LNのようにソフトウェア実装ではなくハードウェア面からTEEを用いて軽量な二重ペイメントチャネルを構築するため単一メッセージによる高速送金可能。
- セキュアなハードウェア上にセキュアなペイメントチャネルを実装することにより、プロトコル変更を伴わずにLNに相当するメリットを得られる点が特長。
- チャネルの確立、チャネルの操作、チャネルのセツルメントの３つのフェーズから成る。

→ 出典: http://hackingdistributed.com/2016/12/22/scaling-bitcoin-with-secure-hardware/
→ 出典: https://www.cs.cornell.edu/People/egs/papers/teechan.pdf
→ 出典: https://eprint.iacr.org/2016/086.pdf

B E D

ビットコインマイニングのリソース消費節約へのIC3による代替案

- PieceWork
  - PoWの改良版であり、浪費したマイニングリソースの再利用を可能にする
- Resource Efficient Mining
  - ハッシュベースのPoWの代わりにPoUWと称する
  - 「UW」はUseful Workの意味
  - 任意のワークロードを検証するために、インテルSGXのtrustedハードウェアを利用
- Snow White
  - 厳密なセキュリティを保証するPoS

→ 出典: http://hackingdistributed.com/2017/02/23/green-blockchains/

BITCOIN LIGHTNING 仕様アップデート

- 基本的な用語としては以下のとおり。
  - Funding Transaction
    （チャネル上の両ピアに対してペイメントを行う、オンチェーンの不可逆的トランザクション。双方同意によってのみ使用可）
  - Channel
    （両ピア間で双方向送金をオフチェーンで高速に行う方法。資金移動には更新されたComittment transactionに対する署名を交換する）
  - Commitment Transaction
    （Funding transactionを消費するためのトランザクション）
  - HTLC:Hashed Time Locked Contract
    （２つのピア間の条件付きペイメント。受け手は自身の署名およびPayment preimageを示すことでペイメントを消費可能）
  - Payment hash, payment preimage
    （最後の受け手のみがPayment preimageを知っており、これを明かすことで、ペイメントを受けたことの証しとなる。HTLCはPayment preimageのハッシュを持っておりこれがpayment hash）

→ 出典：https://medium.com/@rusty_lightning/the-bitcoin-lightning-spec-part-1-8-a7720fb1b4da
→ 出典：https://github.com/lightningnetwork/lightning-rfc/blob/master/00-introduction.md

B E D

BLOCKSTREAM、SIDECHAIN(STRONG FEDERATIONS)ホワイトペーパー発表

- Strong Federationsの最初の実装としてLiquidについて記載。
- Strong Federationは、トランザクションにおけるアセットタイプや数量に関するプライバシーを保護しつつ、トランザクションのレイテンシーや相互運用性を改善。
- 併せて、Elements Projectのアップデートも発表された。

→ 出典: https://blockstream.com/2017/01/16/strong-federations-paper-released-liquid.html
→ 出典: https://arxiv.org/pdf/1612.05491v2.pdf

ビットコインスケーリング論争とハードフォーク危機

- ペイメント手段／デジタルゴールドとしてのビットコイン
  - ビットコインは、ビール一杯のような小額決済には、クレジットカードより不向きになっている。
  - 現在0.7ドル相当の手数料がかかるため、検閲耐性に照らしても高額なものに。
  - 多くのトランザクションが処理されるようになるにつれ、フルノードのオペレーションコストも上昇。
  - 分権的方法によるコンセンサスが必要な、変更のしにくさはビットコインの利点でもあり欠点でもある。
  - なお、ペイメント起点のユースケースは手数料上昇に伴い存在感が低下しており、レイヤー2実装を待つ必要があるが、デジタルゴールド（デジタル無記名資産）としてのユースケースは有益。
- ビットコインのスケーリングを阻む社会的要因
  - ハードフォークに伴い、マイナーはBTC/BTU双方のマイニングハードを購入が必要となる。
  - マイニングハードの売上が、ブロックサイズ拡大無しに維持しようという経済的インセンティブを阻害。
  - ビットコインは経済的利益がネットワークセキュリティの統制に寄与すると言う前提の上に成り立ってきた。
  - マイニングハードウェアが一握りの企業により製造され、かつマイニングプールをコントロール。
  - マイニングが集中化しプロ化しているが、マイニングはもっとアマチュアによるものになる必要がある。
- BUの品質への懸念
  - “NULL pointer dereference,” および “reachable assertion”といった脆弱性の指摘。
  - ピアレビュープロセスやテストなど、コードの品質確保上の問題点も指摘されている。

→ 出典: https://medium.com/@nicolasdorier/the-real-root-of-all-evil-in-bitcoin-f34f3d3a096e
→ 出典: https://vinnylingham.com/a-fork-in-the-road-70288fd3c046
→ 出典: https://bitcoinmagazine.com/articles/security-researcher-found-bug-knocked-out-bitcoin-unlimited/
→ 出典: https://cryptoinsider.com/bitcoins-killer-app-still-digital-gold-thats-needs-now/

B E D

BITCOIN UNLIMITEDのブロックサイズ提案とコンセンサス投票①

- ViaBTC、GBMiners、BTC.TOPなどのマイニングプールが支持を表明済み。
- BUIP001に記載されている考え方は、ブロックサイズリミットのコントロールをユーザやマイナーに取り戻そうというもの。
- 現在のビットコインブロックチェーンでは1MB以上のブロックは無効となりチェーンに取り込まれないが、BUではブロックサイズリミットを無くして、MG・EB・ADという３つのオプションでリプレイスすることを提案。

- MG(Maximum Generation Size)
  - マイナーが生成するブロックのサイズを設定可能。
- EB(Excessive Block Size)
  - ノードとマイナーが受け入れたブロックのサイズに決定。splitの可能性あり。
- AD(Excessive Acceptance Depth)
  - EBに加え、ブロック受け入れ前に必要となる追加confirmation数（デフォルトは4)を決めておく。

→ 出典: https://bitcoinmagazine.com/articles/why-bitcoin-unlimiteds-emergent-consensus-gamble/
→ 出典: https://bitcoinmagazine.com/articles/how-bitcoin-unlimited-users-may-end-different-blockchains/
→ 出典: https://bitcoinmagazine.com/articles/closer-look-bitcoin-unlimiteds-configurable-block-size-proposal/

B E D

BITCOIN UNLIMITEDのブロックサイズ提案とコンセンサス投票②

- BUには、全員がBUに切り替える・全員が切り替えない・全員がADとして4cobfirmを設定する等のシナリオが想定される。
- BUIP001ではメカニズムコンセンサスではなくユーザがノードをconfigureするため、チェーンがsplitする可能性あり。
- BUIP001にはビットコインコンセンサスルールのように信頼できるテクニカルコンセンサスは含まれていない。
- その代わりに、チェーンが１つに収斂するためにBUが指針として言っているのがEmergent Consensus。ソフトウェアが自動的にせずともエコシステムとして単一チェーンへのコンセンサスをとるように自らconfigureするインセンティブがあるはずというもの。
- このコンセンサスは、フォーラムやブログのようなオフチェーン環境で行なわれる。ここで、ビザンチン将軍問題のような事象が生じる可能性があることに留意が必要。

→ 出典: https://bitcoinmagazine.com/articles/why-bitcoin-unlimiteds-emergent-consensus-gamble/
→ 出典: https://bitcoinmagazine.com/articles/how-bitcoin-unlimited-users-may-end-different-blockchains/
→ 出典: https://bitcoinmagazine.com/articles/closer-look-bitcoin-unlimiteds-configurable-block-size-proposal/

SegWitへむけたUser Activated Soft Fork提案

- 本来なら95%のマイナーサポートが必要なところ、25%にとどまるSegWitのアクティベートについて、マイナーサポート（ハッシュパワー投票によるシグナリング）なしにアクティベートするソフトフォークを認める代案として浮上。
- マイナーではなくビットコインユーザーとしての取引所などが、所定の日付を定めてソフトをアクティベートし、そのポイント以降は新しいルールに沿わないトランザクションをブロックするもの。
- ただしUASFも、ハッシュレートを持つマイナー大半が反対すれば、ビットコインが複数種類存在するようなブロックチェーンの分裂を招くとの意見あり。
- 中国のマイナーではハードフォークとソフトフォークの中庸として、コンセンサスルールを一定度緩和させつつチェーン分裂を回避するものとしてSynthetic Forkについても会話されているとのこと。

→ 出典: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-February/013643.html
→ 出典: https://bitcoinmagazine.com/articles/latest-twist-block-size-debate-called-uasf/
→ 出典: https://news.bitcoin.com/chinese-miners-worried-about-a-user-activated-fork-propose-synthetic-fork/
→ 出典: https://docs.com/jiang-johny/3602/synthetic-fork

2．プラットフォーム分野

- エンタプライズ向けethereum開発へ
- JPモルガンによるエンタプライズ版Ethereum、Quorum
- Enterprise Ethereum Alliance（EEA）
- Chain、Confidential Assetsプロトコル発表
- Corda、オープンソースとして公開

エンタプライズ向けETHEREUM開発へ

- ethereumの技術をベースにしたpermissioned版とすることにより、PoCではないMVP開発への移行を促す。
- これまでもBlockApps STRATO、Hydrachain、Quorum等がプライベート版ethereumを提供してきたが、可搬性やコードベースのフラグメンテーション、ベンダーロックイン等が課題だった。
- 現行のethereumスケーリングロードマップに載せて、互換性や相互運用性を維持。

→ 出典: https://media.consensys.net/the-birth-of-enterprise-ethereum-in-2017-ebe7f7abed92#.rdv3j7185
→ 出典: https://www.ethnews.com/enterprise-ethereum-a-private-blockchain-for-corporate-businesses

JPモルガンによるエンタプライズ版ETHEREUM、QUORUM

- 既知の参加者によるパーミッショングループ内におけるプライベートトランザクション処理において高いスループットを実現するもの。
- ビジネス要件にカスタマイズ可能な、「トランザクションレベルのプライバシー」と「ネットワークレベルの透明性」を両立。
- スループットは秒間数十から数百トランザクションのレベルであり、投票ベースのQuorumChainコンセンサスアルゴリズムを利用。
- パーミッション管理は当初は手動だが、今後スマートコントラクトベースのガバナンスツールを含むものへアップデート予定。

→ 出典：https://www.jpmorgan.com/country/US/en/Quorum

ENTERPRISE ETHEREUM ALLIANCE (EEA)

- セキュリティ、プライバシー、スケーラビリティおよび相互運用性にフォーカスしてethereumをドライブするコラボレーションに向けた取り組み。
- パブリックethereumとプライベートethereumの双方をまたぐハイブリッドなアーキテクチャも探索。
- コンパチビリティがキーテーマ。
- 現在、JP MorganによるQuorumがMicrosoft Azure上で利用可能（EEA上のファーストインプリ）。
- 2017年中にEntEth1.0の仕様を定めるとあわせ、EntEth2.0構築ロードマップ策定予定。（プロダクトは作らず、仕様策定に注力）

- 出典: http://entethalliance.org/
- 出典: https://www.ethnews.com/enterprise-ethereum-alliance-officially-launches
- 出典: https://event.webcasts.com/starthere.jsp?ei=1137845
- 出典: https://bobsummerwill.files.wordpress.com/2017/02/enterprise-ethereum-technical-roadmap-slides-final.pdf
- 出典: http://entethalliance.org/wp-content/uploads/2017/02/EEA.pdf
- 出典: https://www.reddit.com/r/ethereum/comments/5wo6hy/ethereum_enterprise_alliance_live_updates/

CHAIN、CONFIDENTIAL ASSETSプロトコル発表

- Confidential Transactionsを拡張し、トランザクション数量のみでなく、アセットタイプとアセット数量を隠蔽することにより、複数アセットの取引におけるプライバシーを改善。
- 単一チェーン上でconfidential/non-confidentialの双方を取り扱う、選択的ディスクロージャーも可能。

→ 出典：https://blog.chain.com/hidden-in-plain-sight-transacting-privately-on-a-blockchain-835ab75c01cb#.xoa330hpv

CORDA、オープンソースとして公開

- ノード間で互いをできるだけ信用しない分散データベースシステム。
- トランザクション一意性検証を行う公証インフラ機能（タイムスタンプや二重支払防止）。
- ビットコイン同様のUTXOトランザクションモデル。
- CorDappsと呼ばれる分散アプリ向けプラットフォーム。
- データは知る必要がある者のみで共有され、全トランザクションがブロードキャストされることが無い。
- ノードは認証されたP2Pネットワークであり、全てのコミュニケーションはダイレクトで行なわれる。
- ブロックチェーンは無く、トランザクションの競争は公証システムを用いて行なわれる。
- 現在テストネット構築中。
- 公証システムは現在Raftベースだが、今後BFTプロトコルにする予定。

→ 出典: https://github.com/corda/corda/blob/master/README.md
→ 出典: https://vimeo.com/192757743/c2ec39c1e1
→ 出典: https://docs.corda.net/_static/corda-technical-whitepaper.pdf
→ 出典: https://docs.corda.net/
→ 出典: https://docs.corda.net/consensus.html
→ 出典: https://docs.corda.net/data-model.html#rationale-for-and-tradeoffs-in-adopting-a-utxo-style-model
→ 出典: https://www.corda.net/2016/11/30/the-road-ahead/

トピックリスト①

- Catapult、秒間4000トランザクション超達成
  - https://www.sakura.ad.jp/press/2016/1220_blockchain/
  - http://jp.techcrunch.com/2016/12/20/mijins-next-generation-core-catapult-records-4142-tps/
- Catapult、ホワイトペーパー発表
  - https://www.nem.io/catapultwhitepaper.pdf
- Ethereumの開発者イベントedconがパリで開催
  - https://edcon.io/
- EthereumのR&Dラウンドアップ（Zcashチームとのコラボやzk-snarksの実装など）
  - https://blog.ethereum.org/2017/02/14/ethereum-rnd-roundup-valentines-day-edition/

トピックリスト②

- Etheremへのトラストライン導入アイデア、Raiden Networkから発表
  - http://www.ibtimes.co.uk/introducing-trustlines-original-ripple-idea-ethereum-1607226
- Enterprise Ethereumへ向けたプロジェクトにJP Morganなど参画
  - http://www.coindesk.com/jp-morgan-santander-said-join-enterprise-ethereum-blockchain-group/
- 独自コンセンサスアルゴリズムBKF2によるmiyabi
  - https://bitflyer.jp/pub/bitFlyer_miyabi-press_ja.pdf

個別サービス①

名称	サービス概略	URL
NTumbleBit	TumbleBitの実装	→ https://medium.com/@nicolasdorier/tumblebit-tumbler-mode-ea44e9a2a2ec
Grin	MimbleWimbleの実装	→ https://github.com/ignopeverell/grin/blob/master/README.md
Stratis	NTumbleBitプロジェクトを発表	→ http://stratisplatform.com/2016/12/07/anonymous-transactions-coming-to-stratis/
	Tumblebit実装のBreezeウォレット開発	→ https://stratisplatform.com/2017/03/02/stratis-breeze-wallet-redefines-financial-privacy-for-blockchains/

個別サービス②

名称	サービス概略	URL
Zeke	ethereumベースのAIプロジェクト	→ http://zeke.ai/
Qtum	UTXOベースのPoSスマートコントラクト	→ https://qtum.org/whitepaper/
Difinity	分散型クラウド	→ https://dfinity.network/
iEx.ec	分散型クラウドコンピューティング	→ http://iex.ec/
Tezos	独自ブロックチェーンによるスマートコントラクト	→ https://tezos.com/
ox	ethereum上の分散取引所向けオープンプロトコル	→ https://www.0xproject.com/

3. ライフスタイル分野

① ゲーム、投票、ポイントむけ応用
② 自動車関連分野の応用
③ 21 incはメールサービスへピポッド
④ オンライン広告産業むけプラットフォームadChain
⑤ オンライン広告産業むけプラットフォーム
Basic Attention Token
⑥ ロイヤリティポイントやギフトカードの生成・管理むけプラットフォームChain of Points
⑦ デジタルフリーカルチャーの登録・認証・流通プロジェクト
Creativechain

ゲーム、投票、ポイントむけ応用

- SoG、ソフトローンチ
  - https://bitcoinmagazine.com/articles/spells-of-genesis-soft-launch-pairs-enhanced-gameplay-with-advantages-of-blockchain-tech-1481321040
- The rock and roll of fame、最大規模のブロックチェーンベースのファン投票
  - http://bitcoinist.com/rock-roll-hall-fame-blockchain-vote/
- テックビューロと日立ソリューションズ、ポイント管理への適用検証
  - http://mijin.io/ja/789.html
- IndieSquare、セレスと提携して位置情報とトークンを活用した「モッピーGO」提供
  - http://host211006211247.stockdatabank.jp/tdnet/data/20170210/140120170210496251.pdf

自動車関連分野の応用

- テスラの自動車からスマートコントラクト起動しetherの支払を行うProject OakenのM2M価値移転プラットフォーム
  - https://www.ethnews.com/tesla-on-the-blockchain-an-interview-with-project-oaken
- ダイムラー、Mercedes Pay開発に向けビットコイン決済サービス会社を買収
  - http://www.coinspeaker.com/2017/01/19/daimler-acquires-bitcoin-services-company-paycash-develop-mercedes-pay/
- Bosch、Cisco、Foxconn等がコンソーシアム設立
  - https://www.ibtimes.co.uk/bosch-cisco-foxconn-join-blockchain-iot-consortium-1603508
- Oxigen Initiative、Share&Chargeと協業でEV充電むけウォレット
  - http://oxygeninitiative.com/blockchain-4-charging-stations/

21 INCはメールサービスへピポッド

- 21 inc、paid emailプラットフォーム立ち上げ
  - https://news.bitcoin.com/21-incs-new-venture-email-that-pays-recipients-in-bitcoin/

- 21 inc、ビットコインを使った有料linkedinサービス21 lists立ち上げ
  - https://medium.com/@21/get-replies-from-vcs-and-ceos-with-21-lists-663f2a8d8b9e

オンライン広告産業むけプラットフォームADCHAIN

- オンライン広告産業では、既存の問題点として、①はデータがサイロ化し標準が限られているため不正行為の特定が困難であり、②業界全体としても共通言語がなく協調して不正排除が難しい。

- adChainは、ConsenSysと協業によってEthereumプラットフォーム上に構築されたものであり、共有台帳を用いて広告のサプライチェーンに透明性をもたらす。

- 広告配信の検証に加えて、皆が理解し信用できる共通言語とデータセットを提供し、全参加者がアクセスして不正を排除できるとしている。

- デジタル広告におけるスマートコントラクトベースのアプリケーションは、大勢が共有のプラットフォーム上で協調・競争することから、ブロックチェーンに適したユースケース。

→ 出典：http://www.prweb.com/releases/2017/01/prweb14009259.htm

オンライン広告産業むけプラットフォーム
Basic Attention Token

- アテンションベースのEthereumトークンを用いて、デジタル広告における非効率性を、メディア・広告主・ユーザ間の新たな交換単位を作ることによって改善する。
- BraveブラウザとBasic Attention Token（BAT）を組み合わせ、分散化された透明性あるデジタル広告のプラットフォームとする。

- Braveブラウザが匿名でユーザアテンションをモニタリングし、メディアに対してBATに従って報酬を与える。

- ユーザはアテンションに大してBATで報酬を受け取ることができる。
- メディアはユーザアテンションに基づきBATを受け取る。
- 不正や仲介人が減るため、メディアはより多くの広告収入を得ることができる。
- 広告主はより高いROIを獲得し、よりターゲティングされた不正のない広告が可能になる。

→ 出典：https://basicattentiontoken.org/

ロイヤリティポイントやギフトカードの生成・管理むけプラットフォームCHAIN OF POINTS

- POINTトークンを用いて、マーチャントから顧客、顧客同士、マーチャント同士の価値移転を行う。
  - マーチャントは、発行したPOINTトークンがどのように換金されるかを、リカーディアン・スマートコントラクトを用いてカスタマイズできる他、ロイヤリティプログラムの条項を執行可能。

- 「リカーディアン・コントラクト」は裁判における正当化を意図したスマートコントラクト
  - リカーディアン・コントラクトは人間にとって可読性があり、マシンによってコンパイル可能であり、マシンと人間の双方によってコントラクトがどのように実行されるかを合意できることを目指す。
  - POINTトークンを使う条項がJSONベースのプログラム中に記載されている。
  - これらの法的文書がハッシュを通じてスマートコントラクトへリンクされる。
  - 本プロジェクトでは、リカーディアン・コントラクトを実装するための分かりやすい言語を用いて汎用的な法的契約を生成しているため、Solidityのように特別な技術知識なく、ユーザが使いやすいAPIを以ってPOINTトークンの条項を設計できる。

→ 出典: https://chainofpoints.com/cop_whitepaper.pdf
→ 出典: https://www.smithandcrown.com/chain-points-blockchain-solutions-customer-loyalty-industry/

デジタルフリーカルチャーの登録・認証・流通プロジェクトCREATIVECHAIN

- 中間介在人無しに知財の認定・流通をサポートするインフラ
  - ネットワーク上へコンテンツを作家が登録すると、著作権やライセンス情報などがブロックチェーンへ記録
  - 登録されたデジタル作品の知財を認定するタイムスタンプを提供
  - プラットフォーム上の暗号通貨Creativecoinを用いたP2Pのコンテンツ流通システム

- クリエイターはプラットフォーム上で様々な方法でマネタイズ可能
  - 著作権移転、ロイヤリティ、クラウドファンディング、限定版発行など。

- 様々なライセンス形態をスマートコントラクトに組み込み、アサイン合意や販売・流通流通手段に基づくコントラクト
  - ライセンスフリーの写真に関するロイヤリティフィー
  - 投資参加として配当の配分。小規模投資家へ自動配布

→ 出典: http://creativechain.org/wp-content/uploads/2017/03/Whitepaper-Creativechain-1.2.pdf
→ 出典: https://bitcointalk.org/index.php?topic=1809920.0
→ 出典: https://www.smithandcrown.com/creativechain-token-sale-ico-marketplace-intellectual-property/

個別サービス

名称	サービス概略	URL
LaborX	短期求人リクルートサービス	→ http://blockchain-finance.com/2017/01/20/blockchain-solution-for-recruitment-sector/
Acronis Notary	デジタルコンテンツの公証サービス	→ http://www.acronis.com/ja-jp/personal/blockchain-data-authentication/
dotblockchain Music	音楽の権利・ペイメントサービス	→ http://dotblockchainmusic.com/
BlockLog	分散型ブログ	→ http://blocklog.xyz/
Love Chain	バレンタインデー向けメッセージ	→ http://lovechainproject.com/
BlockPhase	VRコンテンツ流通プラットフォーム	→ https://www.blockphase.com/

個別サービス

名称	サービス概略	URL
GameCredit	ゲーム向けペイメント	→ https://gamecredits.com/
Livepeer	ライブビデオブロードキャスト	→ https://livepeer.org/
Blocktix	イベントホスティングサービス	→ https://blocktix.io/
Trekmiles	トークンリワードによるフィットネスアプリ	→ http://www.trekmiles.com/p/what-is-trekmiles.html
LegendsRoom	会員制クラブへのメンバーシッププログラム	→ http://legendsroomlv.com/
NYIAX	広告契約のトレードプラットフォーム	→ https://nyiax.com/
Xhai Studio	XEMとトークン相互交換するモバイルゲーム	→ http://xhaistudios.com/
MetaX	デジタル広告のサプライチェーン	→ https://metaxchain.com/

4.サプライチェーン系

- トラッキング分野での応用
- ロジスティクス・貿易金融分野への応用

トラッキング分野での応用

- Everledger、ワインボトルのトラッキング
  - http://www.pymnts.com/blockchain/2016/everledger-tracks-provenance-of-a-wine-bottle-thanks-to-blockchain/
  - https://www.finextra.com/pressarticle/67381/everledger-secures-the-first-bottle-of-wine-on-the-blockchain
- LUXTAG、NEMブロックチェーンを用いた真正性証明
  - https://drive.google.com/file/d/0B02d77LKZwnsUUd0cVI3dWJiU28/view
- マイクロソフトによるプロダクトトラッキングManifestプロジェクト発表
  - https://www.ethnews.com/microsoft-project-manifest-blockchain-product-tracking

ロジスティクス・貿易金融分野への応用

- HSBC等によるDigital Trade Chainコンソーシアム
  - http://www.ibtimes.co.uk/deutsche-bank-hsbc-five-other-big-banks-form-digital-trade-chain-consortium-1601259
- ロッテルダム港、ABNアムロやデルフト大学とコンソーシアムを結成
  - http://btcnews.jp/SO3JTD9I10299/
- IBM、インドのマヒンドラグループとサプライチェーン向けブロックチェーンのテスト
  - http://www.coindesk.com/ibm-blockchain-mahindra-supply-chain/
- IBM、ドバイの税関当局や貿易当局と協力し導入推進
  - http://www.prnewswire.com/news-releases/ibm-launches-blockchain-initiative-with-dubai-government-agencies-and-enterprises-on-ibm-cloud-300403183.html
- Hyperledger Fabric用いた綿花取引のコンソーシアム発足
  - https://www.ethnews.com/cotton-blockchain-consortium-formed-with-ibm

個別サービス

名称	サービス概略	URL
AccuAudit IO	無線タグによる監査証跡サービス	→ http://blockchain-finance.com/2017/01/26/blockchain-verified-database-for-securing-sensitive-items/
Co Tricity	ソーラーエネルギー向けローカルマーケットプレイス	→ https://co-tricity.com/en/about-co-tricity/#
Sun Exchange	太陽エネルギーのクラウドファンディング	→ https://thesunexchange.com/silicon-based-economy-financing-solar-cells-bitcoin

5. シビックテック系

① 行政分野への応用
② 本人認証・証明分野への応用
③ ヘルスケア・テレコム分野への応用
④ 不動産分野への応用
⑤ 不動産所有権をデジタル化するREIDAO

行政分野への応用

- Georgia共和国、ButFuryと土地登記プロジェクト
  - https://medium.com/@BitFuryGroup/the-bitfury-group-and-government-of-republic-of-georgia-expand-historic-blockchain-land-titling-4c507a073f6b
- アリゾナ州、契約として成立したスマートコントラクトに対して拘束力持たせる法案HB2417提出
  - https://legiscan.com/AZ/text/HB2417/id/1497439
- ハワイ州、ツーリズムへのユースケース探るワーキンググループ設立
  - https://legiscan.com/HI/text/HB1481/2017
- AntwerpのDigipolisにおける電子行政実験でmijin採用
  - https://antwerpen.digipolis.be/nl/blog/8279c5f3-5e33-4a1f-8c19-1200d01f4f26

本人認証・証明分野への応用

- GMOグローバルサイン、本人認証サービス
  - https://www.gmo.jp/news/article/?id=5536

- ジュリアン・アサンジ氏、ビットコインの最新ブロックハッシュ値を生放送して生存証明
  - http://www.coindesk.com/julian-assange-just-read-bitcoin-block-hash-prove-alive/

ヘルスケア・テレコム分野への応用

- DeepMind、ヘルスケアデータ管理にブロックチェーン関連技術利用
  - https://www.cityam.com/255023/googles-deepmind-using-blockchain-related-technology/
  - https://news.bitcoin.com/deepmind-healthcare-ai-blockchain/

- Sprint、Softbankおよび米TBCASoft、テレコム業界のキャリアシステム向け技術開発
  - http://www.tbcasoft.com/news.html

不動産分野への応用

- Deloitte、ロッテルダムで不動産リース取引
  - https://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/for-the-first-time-lease-agreements-are-recorded-in-blockchain.html

- ABN Amroの企業不動産取引
  - http://bravenewcoin.com/news/abn-amro-launches-pilot-blockchain-application-for-commercial-real-estate/

不動産所有権をデジタル化するREIDAO

- 不動産価格高騰によって、個人投資家は不動産投資の機会が限られる
  - この問題を解決し、不動産市場を投資に関心を持つ人々へ広く開かれたものにする
  - Ethereumブロックチェーンを用いて、分散自律組織（DAO）の方法をとることによって、所有権トークンを各参加者・オーナーに対して発行

- 不動産をトークン化し、不動産保有に関わるメンバーへ配布
  - トークンは物理的な不動産に裏づけられているため、その価値が保持される
  - 予算に応じて不動産所有権の一部を保有することを可能にする
  - DAOモデルに基づき、DAOトークンを使って、トークン保有者は不動産に関する戦略上の論点に関して投票を行うことが出来る
  - クリプトアセットはERCトークンスタンダードに準拠し、Ethereumブロックチェーン上の他サービスとのインテグレーションも可能

→ 出典：http://www.reidao.io/
→ 出典：http://reidao.io/whitepaper.pdf

個別サービス

名称	サービス概略	URL
landstead	NEMブロックチェーンによる土地登記	→ http://landstead.atraurablockchain.com/#!/
Procivis	ブロックチェーンベースの電子政府appStore	→ https://procivis.ch/
Hashed Health	ヘルスケア向けコンソーシアム	→ https://hashedhealth.com/
Ethlance	フリーランスと雇用主を結ぶ分散マーケットプレイス	→ http://ethlance.com/#/
AnonymousVoting	投票者のプライバシー重視の投票プラットフォーム	→ https://eprint.iacr.org/2017/110.pdf
Lunyr	クラウドソースによるウィキペディア	→ https://lunyr.com/
REX	不動産リスティングサービス	→ http://rexmls.com/
Decentraland	バーチャルリアリティ上の土地所有権管理	→ https://decentraland.org/

6.金融機関系の動き

① ペイメント分野
② 証券・投信分野
③ ゴールド・原油
④ 中国の動き
⑤ 日本国内の動き

ペイメント

- Royal Bank of Canada、パブリックチェーンベースのペイメントシステム検討
  - http://www.coindesk.com/royal-bank-canada-sees-role-public-blockchains-secure-payments/

- UBS、電気自動車の充電代金をethereumベースで自律支払可能なCar eWalletプロジェクト発表
  - http://www.ibtimes.co.uk/ubs-collaborates-blockchain-wallets-cars-1599055
  - https://www.ethnews.com/car-ewallets-your-vehicle-pays-its-own-way

- BNPパリバ、リアルタイムペイメント
  - https://group.bnpparibas/en/press-release/bnp-paribas-completes-real-time-blockchain-payments/amp

証券・投信

- Winklevoss兄弟のビットコインETF、米SECによる承認ならず
  - https://99bitcoins.com/winklevoss-bitcoin-etf/
  - https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf
- DTCC、クレジットスワップ取引システムのリプレイスに向けてIBM・R3・AXONIをパートナーに選定
  - http://www.dtcc.com/news/2017/january/09/dtcc-selects-ibm-axoni-and-r3-to-develop-dtccs-distributed-ledger-solution
- ドイツ取引所グループ、送金プラットフォームのコンセプト発表
  - http://deutsche-boerse.com/dbg-en/media-relations/press-releases/Deutsche-Boerse-presents-blockchain-concept-for-risk-free-cash-transfer/2883236
- ドイツ中央銀行、証券取引向けブロックチェーンプロトタイプ構築
  - https://news.bitcoin.com/central-bank-germany-blockchain/
  - https://www.bundesbank.de/Redaktion/EN/Downloads/Press/Pressenotizen/2016/2016_11_28_blockchain_prototype.pdf

ゴールド・原油

- Euroclearのゴールドセツルメント
  - https://www.ethnews.com/euroclear-and-paxos-implement-blockchain-solution-for-gold-settlement
- 英国王立造幣局、ゴールドトレード商品Royal Mint Goldを開発
  - https://fintechonline.jp/archives/101141
- INGとSociete Generale、原油トレードのEasy TradING Connect
  - https://m.youtube.com/watch?v=RLyiIXLEqg4

中国の動き

- 中国人民銀行、デジタルマネーYuanCoinのテスト実施
  - http://bitcoinist.com/china-trials-bitcoin-suck/
- ChinaLedger、ホワイトペーパー発表
  - https://bitcoinmagazine.com/articles/chinaledger-white-paper-outlines-industry-blockchain-standards/

日本国内の動き

- 日銀、欧州中央銀行と分散台帳技術の調査へ
  - http://www.boj.or.jp/announcements/release_2016/rel161207a.htm/
- 金融庁より「銀行法施行令等の一部を改正する政令等（案）」が公表
  - http://www.fsa.go.jp/news/28/ginkou/20161228-4.html
- 税制改正大綱が公開、仮想通貨への消費税非課税とすることに
  - https://jimin.ncss.nifty.com/pdf/news/policy/133810_1.pdf
- SMBC、貿易分野の実証実験
  - http://www-03.ibm.com/press/jp/ja/pressrelease/51685.wss
- 東京短資とHAW、Open Assets Protocolを貸金貸借市場へ応用
  - http://www.coindesk.com/blockchain-startup-haw-reveals-bitcoin-lending-market-concept/
  - http://www.boj.or.jp/announcements/release_2017/data/rel170227a3.pdf

8.金融系スタートアップの動き

① Circle、Stellar、SETL
② AIヘッジファンドNumerai向け暗号トークン、Numeraire
③ ブロックチェーンアセットむけヘッジファンド、
④ Polychain Capital
⑤ トークンのアセットファンド、TaaS

CIRCLE、STELLAR、SETL

- Circleがピボット
  - https://bitcoinmagazine.com/articles/beyond-bitcoin-circle-pivots-to-next-gen-blockchain-enabled-social-payments-1481223358
- Stellar、フィリピン、インドやアフリカで提携して事業展開へ
  - https://www.stellar.org/blog/global-partnerships/
- SETL、デロイトが出資
  - http://www.coindesk.com/deloitte-invests-first-blockchain-startup/

B E D

AIヘッジファンドNUMERAI向け暗号トークン、NUMERAIRE

- Numeraiは、データサイエンティストのネットワークをベースとしたヘッジファンド
  - データサイエンティストは統計学や機械学習や人工知能のエキスパートで、予測モデルを構築。
  - 金融データをデータサイエンティストのネットワークによる機械学習むけ問題に変換。
  - データサイエンティストに株式市場データを提供し、機械学習アルゴリズムで予測構造を発見。
  - データサイエンティストがどのようなアルゴリズムを用いるかをNumeraiが知ることはなく、データサイエンティストは結果をアップロードするのみであり、知的財産はデータサイエンティストに留保。
  - Numeraiとデータサイエンティストの間のトラストレスな関係を、暗号や匿名性が支える構造。
  - データサイエンティストは自身が何者か述べる必要なく、ビットコインの支払を受ける。

- ヘッジファンドのネットワーク効果を高め、協調を動機付けるためデータサイエンティスト達にクリプトトークンNumeraireを発行
  - 過去のパフォーマンスに基づき12000人のデータサイエンティスト達に対して発行された
  - データサイエンティストは予測を提示すると、予測に対してNumeraireの持分を得る。
  - もし予測が正確であったなら、Numeraireトークンを持つデータサイエンティストはそれを使ってマネーを得ることができるが、予測がプアであった場合はそのトークンは破棄される。
  - Numeraireトークンを用いて、オークションメカニズムを採用することによって、予測の過剰適応を経済的に合理性が成り立たないようにすることを狙うもの。

→ 出典: https://numer.ai/
→ 出典: https://numer.ai/whitepaper.pdf
→ 出典: https://medium.com/numerai/a-new-cryptocurrency-for-coordinating-artificial-intelligence-on-numerai-9251a131419a

ブロックチェーンアセットむけヘッジファンド
Polychain Capital

- ブロックチェーンアセットのポートフォリオをアクティブに管理することを通じて高い投資リターンを狙うヘッジファンド。
- アプリ層ではなく、プロトコル層への投資を通じて、機関投資家むけバリューを生み出すことを望んでいる。
- そのため、ウォッチしている種類のベンチャーとしては、EthereumやIPFS、Tezos、Rchain、PolkaDot、Difinity、Cosmos等になっている。
- ビットコイン・ブロックチェーンについては、イノベーションのジレンマにさいなまれており、マーケットシェアを減じる傾向が続くほか、同ブロックチェーン上でのアプリケーションが生まれにくいと、同社ファウンダーのOlafは述べている。
- Polychain Capitalには、a16z、USV、Boostなどが投資している。

→ 出典: https://dailyfintech.com/2017/03/28/polychain-capital-a-hedge-fund-investing-at-the-protocol-layer-of-web-3-0/
→ 出典: http://btcnews.jp/4f569md510397/
→ 出典: http://polychain.capital/

トークンのアセットファンド
TaaS (Token As A Service)

- クローズドエンドなクリプトアセットファンド
  - ファンドのメンバシップトークンを販売
  - トークンはファンドの利益の５０%を保有者に還元
  - プロフィットシェアリングのEthereumスマートコントラクトを用いて支払

- ファンドはビットコインを含む暗号アセットへの投資で構成
  - １０%～３０%がビットコイン

- Cryptographic Audit
  - トークン保有者はファンドのパフォーマンスをモニタリング可能
  - 取引履歴やポートフォリオの残高を容易に誰もが検証できるモニタリングツール
  - 投資家が取引活動を自動的に人間の介入なしにモニタリングできる
  - 参照限定APIを用いて誰もが取引所の口座残高を確認でき、ポートフォリオ残高はEthereumブロックチェーンへ一日二回ハッシュ記録され過去の活動を変更不可とし、安全なコールドストレージに保管された投資の所有権証明を提供

→ 出典: https://taas.fund/
→ 出典: http://taas.fund/media/presentation.pdf
→ 出典: https://www.smithandcrown.com/sale/taas/

その他の個別サービス①

名称	サービス概略	URL
XBRL	ConsenSysと、ブロックチェーントークンの標準化へ向けて提携	→ https://dcebrief.com/xbrl-and-consensys-partner-to-create-blockchain-token-standards/
Axoni	R3脱退のGoldman SachsとJP Morganが出資	→ https://dcebrief.com/goldman-sachs-jpmorgan-among-group-funding-axoni-startup/
LendingRobot	自律的な投資ヘッジファンド管理サービス	→ https://www.lendingrobot.com/
TokenMarket	ICOむけデジタルアセットプラットフォーム	→ https://tokenmarket.net/
Quantum Resistant Ledger	量子コンピューター攻撃を軽減すべく設計された台帳	→ http://theqrl.org/whitepaper/QRL_whitepaper.pdf
Orebits	金の所有権証明	→ http://orebits.io/
Humaniq	Unbanked層むけモバイルバンキング	→ https://humaniq.co/

その他の個別サービス②

名称	サービス概略	URL
Alice.si	寄付プログラム	→ http://alice.si/
SIMS	スタートアップ向けパートナーシッププログラム	→ http://ico.maincoin.org/wp-content/uploads/2016/12/Whitepaper-MCN-eng.pdf
Omise Go	Ethereum/Raiden networkによるunbanked向けeWallet	→ https://omg.omise.co/
StabL	トークン向けデリバティブ	→ https://medium.com/stabl-blog/stabl-bringing-stable-tokens-and-derivative-products-to-the-ethereum-blockchain-df4d5eba89d9
Bancor	トークンのコンバージョン・プロトコル	→ https://www.bancor.network/
Vega Fund	分散型トークンベース・クラウドファンディング・ファンド	→ http://www.vega.fund/
Internet of Coin	チェーン横断のアセット交換	→ https://coinstorm.net/en

その他の個別サービス③

名称	サービス概略	URL
Aragon	組織マネジメントプラットフォーム	→ https://aragon.one/
EquiChain	キャピタルマーケット向けプラットフォーム	→ http://www.equichain.com/
GiveTrack	寄付のトラッキング	→ https://bitgivefoundation.org/bitcoin-charity-2-0-initiative/
Lukke	クリプトアセット交換プラットフォーム	→ https://lykke.com/leadership.php
TokenCard	デビットカード・トークンバンキングプラットフォーム	→ http://monolith.ventures/tokencard.html
Blockchain Capital	自身のトークン発行するベンチャーキャピタル	→ http://blockchain.capital/
Lendroid	デジタルアセットのレンディングプラットフォーム	→ https://lendroid.com/
DAO IPCI	カーボンマーケット	→ http://ipci.io/

9.参考資料リンク集

- 技術トピックリスト

トピックリスト①

- litでマイクロペイメントを行ったレポート
  - http://www.unitedbitcoiners.com/blog/mit-dci-lit
- Lightning Networkを使ったクロスチェーン取引
  - https://bitcoinmagazine.com/articles/atomic-swaps-how-the-lightning-network-extends-to-altcoins-1484157052
  - http://techmedia-think.hatenablog.com/entry/2017/01/13/184906
- Micropayment channel と HTLCを組み合わせてリアルタイムトランザクション実装
  - https://prtimes.jp/main/html/rd/p/000000005.000016959.html
- NEMアポスティーユ上での借用証書取りかわしレポート
  - http://godtanu.hateblo.jp/entry/2017/02/08/041416

トピックリスト②

- Tumblebit論文輪読会レポート
  - http://www.unitedbitcoiners.com/blog/tumblebit
- Segwitが依然進まない中、TumbleBitに注目
  - https://hackernoon.com/understanding-tumblebit-part-2-the-endgame-instant-anonymous-scaleable-payment-system-on-top-479e7eb9ca24#.v0ybq7gh7
- SegWitのメリット・デメリット
  - https://bitcoincore.org/en/2016/01/26/segwit-benefits/
  - https://bitcoincore.org/en/2016/10/28/segwit-costs/
- SegWitに対するDigital Currency Group意見とそれに対する反論
  - https://medium.com/@DCGco/scaling-bitcoin-reflections-from-the-dcg-portfolio
  - https://hackernoon.com/the-dcg-is-not-bitcoin-you-are-bitcoin

トピックリスト③

- New Context Conference 2016 San FranciscoでのAdam Backプレゼン動画など公開
  - https://m.youtube.com/watch?v=iDMNQlUnz2g
  - https://m.youtube.com/watch?v=O3HYObvgS18
- Blockchain Protocol Analysis and Security Engineering 2017 (1/26-27 2017, Stanford University)
  - https://cyber.stanford.edu/blockchainconf
- MIT Bitcoin Expo 2017
  - https://m.youtube.com/watch?v=0mVOq1jaR1U&sns=tw
  - http://diyhpl.us/wiki/transcripts/mit-bitcoin-expo-2017/
  - https://m.youtube.com/watch?v=sQDa5jSGFOk
- イリノイ大学のビットコイン関連講座資料集
  - http://soc1024.ece.illinois.edu/teaching/ece598am/fall2016/

トピックリスト④

- Top 10 Mistakes in Enterprise Blockchain Projects
  - http://www.gartner.com/smarterwithgartner/top-10-mistakes-in-enterprise-blockchain-projects/
- Why Bitcoin suceeded and “blockchain industry” failed so far
  - https://medium.com/@pavelkravchenko/why-bitcoin-suceeded-and-blockchain-industry-failed-so-far-7fc66c7dc0ef
- 仮想通貨法の解説資料
  - https://drive.google.com/file/d/0B1ih8RdU5yywV3lmbE9XS2NaZTg/view
- ブロックチェーン理解記事
  - http://coinandpeace.hatenablog.com/entry/newspicks_blockchain_experts

トピックリスト⑤

- Chain Interoperability (Vitalik Buterin)
  - https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf
- ブロックチェーンのPrivacy & Confidenciality保護技術まとめ
  - https://www.r3cev.com/blog/2017/3/8/survey-of-confidentiality-and-privacy-preserving-technologies-for-blockchains
- zkSNARKs in a nutshell
  - https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/

トピックリスト⑥

- Ledger誌の初回号が発行
  - The Bitcoin Mining Game
  - BIX Certificates: Cryptographic Tokens for Anonymous Transactions Based on Certificates Public Ledger
  - Governance in Blockchain Technologies & Social Contract Theories
  - Game Channels for Trustless Off-Chain Interactions in Decentralized Virtual Worlds
  - Ring Confidential Transactions
  - Gaming Self-Contained Provably Fair Smart Contract Casinos
  - Autonocoin: A Proof of Belief Cryptocurrency
  - Subchains: A Technique to Scale Bitcoin and Improve the User Experience
  - A Probabilistic Analysis of the Nxt Forging Algorithm
  - Bitcoin Market Volatility Analysis Using Grand Canonical Minority Game

→ 出典: http://www.ledgerjournal.org/ojs/index.php/ledger/issue/view/2/showToc