

BITCOIN & BLOCKCHAIN概況

2017.07 by SATO

「Bitcoin2.0概況」「Blockchain2.0概況」から改題

過去9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)** : 今回

第10回の臨時構成

- これまでの各回のトピックふりかえり
- 第一部:通常編成で各分野の動向トピック
- 第二部:各分野ユースケースの系譜ふりかえり

第1回(2014年10月): 2014年7月～9月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">• Colored Coins• Counterparty• MaidSafe• Storj• Swarmによるクラウドファンディング• Overstock
Ethereum	<ul style="list-style-type: none">• 7月23日から42日間、「Ether」の販売
Ripple	<ul style="list-style-type: none">• ゲートウェイ• XRP• スマートコントラクトのプロジェクトCodius

第2回(2015年1月): 2014年10月～12月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">• Factom• Sidechain• OpenBazaar• BitNation• アーティスト暗号通貨TatianaCoin• 分散取引所(DEX) Coinffeine• 暗号通貨建ての資金調達ICOが話題になりはじめる• GEMS – GetGems• La'Zooz• Synereo• トークンエコノミーが話題になりはじめる
Ethereum	<ul style="list-style-type: none">• Dapps
Ripple	<ul style="list-style-type: none">• 独Fidor銀行に続き、米国CBW銀行・Cross River銀行が導入

第3回(2015年5月): 2015年1月～4月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">• クラウドファンディングプラットフォームKoinify• Coinbaseが7500万ドルの資金調達を実施• Spells Of Genesis
Ethereum	<ul style="list-style-type: none">• Augur• IBMが、サムスンとの提携におけるIoTデバイスの開発に、Ethereumを活用した「ADEPT」概念実証
Ripple	<ul style="list-style-type: none">• SymbiontがCounterpartyと連携したRippleゲートウェイの作成を発表• 元ホワイトハウス顧問・Yahoo重役の招聘、IFPA参画• ウェスタンユニオン(WU)とのパートナーシップ
NEM	<ul style="list-style-type: none">• 2015年3月31日にローンチ
金融機関	<ul style="list-style-type: none">• UBSがブロックチェーン研究ラボをロンドンに開設• ゴールドマンサックスがCircleに出資• Blythe Masters氏がDigital Asset Holdingsへ

第4回(2015年8月): 2015年5月~7月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">• Lightning Network• 2way pegged Sidechain• Bitcoinへのアンカリングを用いたEverledger• Streamium• Colored coinベースのデジタルアセットColu• Sidechain Element (Confidential Transactions)
Ethereum	<ul style="list-style-type: none">• Ethereum Frontier版をリリース・稼働開始• Dapps開発プラットフォームEris
Ripple	<ul style="list-style-type: none">• スマートコントラクトプラットフォームCodiumを中止• 6月後半より本人確認を導入
金融機関	<ul style="list-style-type: none">• Nasdaqが未公開株取引パイロットプロジェクト• クロスボーダー決済向けCitiCoin• スペインSantander銀行、“Fintech 2.0”レポート
プライベート チェーン	<ul style="list-style-type: none">• Digital Asset HoldingsがHyperledgerを買収• MITメディア・ラボのEnigma

第5回(2015年11月): 2015年8月～11月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">取引所間サイドチェーンLiquid21 Inc.からBitcoin Computer発表8MBにブロックサイズを拡張し、8GBに達するまで2年毎に倍増させるBIP-101Gavin AndresenとMike HearnがリリースしたBIP-101入りのBitcoin XTクライアントは早々にリジェクトコミュニティはブロックサイズ動的変更のBIP-100支持モンリオールでScaling Bitcoinワークショップ開催
Ethereum	<ul style="list-style-type: none">DEVCON1がロンドンで開催
NEM	<ul style="list-style-type: none">MosaicとNamespaceをテストネットリリース
Ripple	<ul style="list-style-type: none">Interledger(ILP)をリリース
金融機関	<ul style="list-style-type: none">R3CEVを中核とした銀行系コンソーシアムNasdaq、未公開株式取引システムLinq発表
プライベートチェーン	<ul style="list-style-type: none">mijinOrb

第6回(2016年4月): 2015年12月～2016年4月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">• 香港で「Scaling Bitcoin」フェーズ2開催• 香港ラウンドテーブルでSegWitと2MBのハードフォークを合意
Ethereum	<ul style="list-style-type: none">• Slock.it、TheDAOのホワイトペーパーを発行• Homestead版がリリース
金融機関	<ul style="list-style-type: none">• R3のコンソーシアム、具体的な実験の動き始まる• UBSの「Utility Settlement Coin」• Goldman Sachsの証券決済システムSETLcoin• 国内金融機関で実証実験が相次いで開始• 仮想通貨の規制法案が閣議決定
プライベートチェーン	<ul style="list-style-type: none">• The Linux FoundationのHyperledger Project• R3、金融サービスむけの分散台帳プラットフォームCordaを発表• J.P. Morgan、独自にJunoプロジェクトを公開• Mijin、実証実験での適用を開始

第7回(2016年7月): 2016年12月～2016年7月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">• 2度目の半減期を迎える
Ethereum	<ul style="list-style-type: none">• TheDAO、クラウドセールで150億円相当を調達• TheDAOへの攻撃、そしてEthereumハードフォーク
NEM	<ul style="list-style-type: none">• mijin新型コアエンジンCatapult、NEMと共通採用へ
Ripple	<ul style="list-style-type: none">• クロスボーダー送金ネットワークへの参画金融機関として7社を公表
プライベート チェーン (金融機関含む)	<ul style="list-style-type: none">• Barclays、R3のCordaプラットフォームを用いてスマートコントラクトを使ったデリバティブ取引を実験• Digital Asset Holdings、Digital Asset Modeling Languageを発表• Chain、金融機関むけブロックチェーン「Open Standard 1」を発表• ミャンマーのマイクロファイナンスBC Finance社、勘定データ移行テストをmijinで実施

第8回(2016年12月): 2016年8月～2016年11月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">ミラノで「Scaling Bitcoin」フェーズ3開催Tumblebit、Mimblewimble、Zcash
Ethereum	<ul style="list-style-type: none">DEVCON2が上海で開催マイクロペイメント向けRaiden Network銀行口座とEthereumのブリッジを構築するCashEth
NEM	<ul style="list-style-type: none">アップデート可能な公証・タイムスタンプサービス、「NEMアポステューユ」仮想通貨やトークンの発行支援サービス「Zaica」ビットガールズ、ICOプランとしてトークン売り出し
Ripple	<ul style="list-style-type: none">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「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
プライベート チェーン (金融機関含む)	<ul style="list-style-type: none">JP MorganのプライベートEthereum「Quorum」R3コンソーシアム、トレードファイナンスでプロト開発DAH、「Global Synchronization Log」発表

第9回(2017年3月): 2016年12月～2017年3月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">• Bitcoin Unlimitedのブロックサイズ提案• SegWitへむけたUser Activated Soft Fork提案
Ethereum	<ul style="list-style-type: none">• Enterprise Ethereum Alliance (EEA)
NEM	<ul style="list-style-type: none">• LUXTAG、NEMブロックチェーンによる真正性証明• Landstead、NEMブロックチェーンによる土地登記
プライベート チェーン (金融機関含む)	<ul style="list-style-type: none">• Corda、オープンソースとして公開• Catapult、ホワイトペーパー発表• 独自コンセンサスアルゴリズムBKF2によるmiyabi• ChinaLedger、ホワイトペーパー発表• DTCC、IBM・R3・AXONIをパートナーにクレジットスワップ取引システムのリプレイスへ

第10回(2017年7月): 2017年4月～2017年7月の動き

分類	トピック
Bitcoin	<ul style="list-style-type: none">• トランザクション渋滞と手数料高騰• Segwit2Mbに基づくハードフォークへむけたNY合意• BIP148によるUASF• Bitmain、UASF(BIP148)対抗弁としてUAHF計画• サイドチェーンプロジェクトDrivechain
Ethereum	<ul style="list-style-type: none">• ICOブームでether価格高騰・トランザクション数急伸
NEM	<ul style="list-style-type: none">• 日本円に対して為替が安定した仮想通貨を志向したデジタルトークン社会実験において「Zen」の発行開始
Ripple	<ul style="list-style-type: none">• ILPのビットコイン向けプラグイン、Paychan
プライベート チェーン (金融機関含む)	<ul style="list-style-type: none">• 全銀協「ブロックチェーン連携プラットフォーム」にmijin製品情報提出• Hyperledger Fabric1.0リリース• R3のCorda ベータリリース

TABLE OF CONTENTS

➔ 今回は、2017年4月～2017年7月の動きを中心に整理

1. ビットコインのテクニカル分野
2. プロトコル改善へむけた動向
3. プラットフォーム分野
4. ライフスタイル分野
5. サプライチェーン分野
6. シビックテック分野
7. 金融機関の動き
8. 金融系スタートアップの動き
9. 参考資料リンク集

1. ビットコインのテクニカル分野

- スケーリング紛争
- トランザクション渋滞・手数料高騰
- Segwit・BigBlock以外のスケーリングソリューション
- LightningNetwork関連動向
- 秘匿性ソリューション動向
- BIP動向
- その他トピック

1-1. スケーリング紛争

- ① BU (Bitcoin Unlimited) のテクノロジートピック
- ② AsicBoost
- ③ BitmainのマイニングハードウェアにバックドアAntbreed
- ④ DCG、Segwit2Mbに基づくハードフォークへむけたNY合意を発表
- ⑤ UASF(User Activated Soft Fork)
- ⑥ BIP148:UASF関連のリスク対処
- ⑦ Bitmain、UASF(BIP148)対抗弁としてのUAHFプランを提示
- ⑧ 中国でラウンドテーブルが開催されNY合意サポートを表明
- ⑨ Bitmain、UAHF : UASF (BIP148)コンティンジェンシープランを発表
- ⑩ Segwit2xベータ版リリースとLukeによるレビュー
- ⑪ The Future of Bitcoin ConferenceでのJihan Wu氏による主張
- ⑫ Craig Wright氏、nChain設立
- ⑬ LitecoinがSegwit支持

BU (BITCOIN UNLIMITED) のテクノロジーピックアップ

- Adjustable Block-size Cap (ABC):
 - ノードオペレーターがノード再起動やソースコードからのリコンパイル無く容易にノードの受け入れブロックサイズを調整可能。
 - 同様にマイナーも再起動・リコンパイル無しに大きなブロック生成可能。ブロックサイズ選好をネットワークに対してシグナルできる。
- Xtreme Thin Blocks (Xthin):
 - トランザクションがノードに二回受信される非効率性を改善。
 - テストではブロック伝播を5.6倍改善したとのこと。
- Parallel Validation:
 - 従来、ノードが新しいブロックを受信するとブロックを受け入れるか拒否するか検証する間、新しいトランザクションをリレーせず競合ブロックを検証することもないフリーズ状態になるため、悪意あるエンティティが検証に極度に時間のかかるブロックをマイニングしてネットワークをフリーズさせる攻撃がある。
 - そこでノードが同時に一つ以上のブロックを検証できるようにしたもの。

→ 出典: <https://www.bitcoinunlimited.info/technologies/>

ASICBOOST

- Gregory Maxwellから、PoW機能の欠点を突いた秘密の攻撃を抑制するための改善提案がなされた。
- その中で、ASICマイニングチップに、特許出願中の技術として、マイナーのマイニング効率を20-30%高めるAsicBoostが秘密裏に使われていることがAsicのリバースエンジニアリングで判明したと示した。
- 昨年夏、KnCMinerが「中国のマイナーは何か秘密の利点を抱えている」と指摘していた。
- AsicBoostは、ASIC内のSHA256ハッシュエンジンの新しい設計、Asic外のソフトウェアとして追加のプレプロセッシングステップを組み込んで、マイニングスピードを高める。
- AsicBoostは、Timo Hanke がSergio Lerner と共同で開発して特許出願中。LernerはRSK Labsの開発者でもある。
- AsicBoostはSegwitソフトフォークとコンパチブルではないが、Extension Blockとはコンパチブル。
- Bitmainは、テスト利用はしたもののmainnetでの利用はしないと否定。

→ 出典: <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-April/013996.html>

→ 出典: <https://www.asicboost.com/patent>

→ 出典: https://media.wix.com/ugd/e74c41_ac889bc947914d3fa26ffe437bfd9cd.pdf

→ 出典: http://211.157.104.77:8080/sipo_EN/search/

→ 出典: <https://medium.com/@WhalePanda/asicboost-the-reason-why-bitmain-blocked-segwit-901fd346ee9f>

→ 出典: <https://blog.bitmain.com/en/regarding-recent-allegations-smear-campaigns/>

→ 出典: https://medium.com/@samcole_74219/asicboost-655a73d48ae4

参考 EXTENSION BLOCK

- BIP141(Segwit)の拡張。BIP141とコンパチブルではなく追加ルールを必要とする。
- アップグレードしていないノードの既存UTXOセットへの干渉を避けるため、extension blocksは自身のUTXOセットを持つ。
- アップグレードしていないノードに、既存UTXOセットが期待通りに振る舞っていると信じ込ませる。
- ビットコインに直接結びつけられたサイドチェーンとも言える。
- 問題点は、フルノードに二種類のクラスを作ることになるリスク。

BITMAINのマイニングハードウェアにバックドア ANTBREED

- BitcoinおよびLitecoinむけマイニングハードウェアに発見された、ファームウェアの欠陥。
- 定期的な周期で操作されるセントラルサービスを用いてチェックするもの。
- このチェックが起動するたびに情報がマイナーからサーバーに移動し、それにはデバイスのシリアル番号やMACアドレスおよびIPアドレスなどが含まれる。
- この情報はマシンと特定ユーザーを紐付けるに十分なものとされ、リモートサービスにて、Antminerのマイニングオペレーションを停止できるため、Bitmainがハッシュレートをシャットダウン可能であることが問題視された。

→ 出典: <https://bitcoinmagazine.com/articles/bitmain-can-remotely-shut-down-your-antminer-and-everyone-elses/>

→ 出典: <https://themerple.com/what-is-antbleed/>

DCG、SEGWIT2MBに基づくハードフォークへむけた合意を発表(NY合意:NYA)

- Segwitのアクティベート対ブロックサイズ増加という政治的コンフリクト解消を目指したビットコインにパッチをあてようというもので、新しい解決策ではないが少なくとも共通の基準を見いだそうとする提案。
- Segwitのアクティベート（マイナーの95%のシグナリング）を実現することを条件に、Segwitと2MBブロックサイズを組み合わせるハードフォークする。
- Segwitを即時アクティベートし、2MBハードフォークのカウントダウンを開始するというコンセンサスへのサポートを95%のマイナーが行うという提案。
- スプリットを回避し、ビットコインコミュニティの再統合を図ることが狙いとした「妥協案」。
- Segwit2MBはRSK Labsからの提案だが、RSK LabsはBitmainから出資をこの3月に受けたばかり。

UASF(USER ACTIVATED SOFT FORK)

- 特定の日付をもってフルノードによってアクティベートされるソフトフォークの仕組み。
- 過去には、P2SHソフトフォーク(BIP16)の際に成功した試みがある。
- 今回はSegwit(BIP148におけるマイナーアクティベートのソフトフォーク:MASF)との組み合わせ。

→ 出典: <https://segwit.org/user-activated-soft-forks-the-bip-148-alternative-28e87ffdb76f>

→ 出典: <http://www.uasf.co/>

BIP148:UASF関連のリスク対処①

- 8/1を以ってBIP148 (UASF) が起動。
- BIP148がハッシュレートで少数のサポートしか得られない場合、チェーンはフォークすることとなるため、自身のBIP148サポート是非によらず影響を被る。
- たとえば、支払い当事者の彼我がフォークにより分断されるなど。
- チェーン分断後、BIP148サイドはSegwitがアクティベートされる。
- こうした分断は、BIP148サポートが多数派（95%ではなく51%で充分）となることによって回避可能であるし、或いは8/1以前にSegwitがロックイン（ハッシュレートの95%）すればBIP148はキャンセルされる。
- または、8/1以後にBIP148サポートが上回るというシナリオにより分断が解消されるということも考えられる。
- より多くの人々がBIP148ノードを動かすことにより、皆のリスクが軽減出来る。

BIP148:UASF関連のリスク対処②

- 8/1を以ってチェーンがスプリットする可能性がある。
- ビットコインユーザーのあるセグメントが、BIP148に記載されたUASF (User Activated Soft Fork) をアクティベートすることをコミットしたおり、SegWitをサポートすることをシグナリングしてないビットコインブロックをリジェクトするとしている。
- もし8/1までにSegWitサポートをシグナリングするマイナーが過半数に届かない場合に、ビットコインのブロックチェーンは二つにスプリットすることになる。
- そのために考慮しておくべきポイントは以下の三つ。
 - 自分の秘密鍵をコントロールすること。
 - 安全面を考慮して、8/1からしばらく（長さは事態による）はトランザクションを控えること。
 - なおも二つのチェーンが残る場合は、自分のコインを違うウォレットに分けること。

→ 出典: <https://bitcoinmagazine.com/articles/bitcoin-beginners-guide-surviving-bip-148-uasf/>

→ 出典: <https://bitcoinmagazine.com/articles/beginners-guide-surviving-coin-split/>

→ 出典: <https://github.com/bitcoin/bips/blob/master/bip-0148.mediawiki>

BITMAIN、UASF(BIP148)対抗弁としてのUAHFプランを提示

- BIP148により定義されたUASFへの対抗として8月に「コンティンジェンシープラン」と題したハードフォークをローンチする可能性に言及。
- Bitcoin UnlimitedやSegwit2xに続く、ハードフォークの提案にあたる。
- UAHFと表されているものの、正確にはBitmain単体によりアクティベートできるとされる。
- UAHFはUASF成功時にのみローンチされるものだが、ビットコインの履歴を共有する新たなコインであるため「Bitmain's Bitcoin」と言われる。

→ 出典: <https://blog.bitmain.com/en/uahf-contingency-plan-uasf-bip148/>

→ 出典: <https://bitcoinmagazine.com/articles/bitmain-responds-uasf-another-hard-fork-announcement/>

中国でラウンドテーブルが開催され NYコンセンサス(SEGWIT2X) サポートを表明

- OKCoin、Huobi、BTCCPool、Bitmain、F2Poolなどが署名。
- 八割以上のビットコインハッシュレートを抱える中国マイナーが改めてSegwit2xのサポートを表明したということ。
- UASFに先立ち7/31にSegwi2x実装。

BITMAIN、UAHF： UASF (BIP148)コンティンジェンシープランを発表

- BIP148によるUASFに対するUAHFコンティンジェンシープランとして、ニューヨーク合意（NYA）を支持するBitmainから発表されたもの。
- ソフトウェア自体は7/1までに予定されており、それまでにtestnetに公開されるとしている。
- BIP148アクティベート時には同日にUAHFも有効となる。
- ロードマップとしては、2017/8に2MB、2017/9に4MB、2018/4に約6MB、2018/8に約8MB、2019/4に約12MB、2019/8に約16MBを予定。

SEGWIT2Xベータ版リリースとLUKEによるレビュー

- "Segwit2MBハードフォーク"のネットワークアップグレードにフォーカスしたbtc1 Core 1.14.3のベータリリース。
 - btc1は、Bitcoin Core 0.14.2ではなく0.14.1をベースとしており、ネットワークアップグレードシーケンスは、bits4 Segwitアクティベーションおよび144*90ブロック。
 - btc1はBIP91を含みSegwitアクティベートの閾値をbits4上で80%に下げることに加え、20%のハッシュレートを持つマイナーに拒否権を与えるもの。
 - ハードフォークに関しては、8MB最大ブロックサイズリミットを含む（コード上では2MBに見えるようになっている）。
- 実際にはハードフォークはbits4を使わず、Segwitアクティベート（BIP148などどのような方法でアクティベートされたにせよ）の90日後にbtc1はハードフォークする。
 - Segwit2xの本当の目的はSegwitを遅らせることにあるように見える。
 - BIP148の代わりにBIP91とSegwit2xを進めることによってマイナーがやりたいことは拒否権を手にすることでありBitmainが最後に全てをブロックすること以外に目的は無い。
 - 8/1迄にBIP148へのアップグレードが出来ない場合にはBitmainにchain split攻撃の機会を与えることになり、そうした中での唯一の解決策はBIP148を8/1迄に広めること。
 - BIP148はSegwit2xを禁じたりSegwitサポートを求めたりするものでもなく、ただSegwit適用をマイナーが止めようとする事ができなくするもの。

→ 出典: <https://github.com/btc1/bitcoin/releases/tag/v1.14.3>

→ 出典: <https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-May/000000.html>

→ 出典: <https://medium.com/@lukedashjr/the-segwit-2x-beta-review-and-thoughts-ca480694a8c7>

THE FUTURE OF BITCOIN CONFERENCEでの JIHAN WU氏による主張

- “Why Multiple Implementations are Quite Important for Bitcoin.”と題しての発表。
 - ハロー効果やバンドワゴン効果を挙げた上で、暗号通貨エコシステムを取り囲むオーソリティへの服従心理について説いた。
 - 暴君や独占者によるハイジャックの問題を解決するために、コミュニティは複数の実装を必要とすると述べている。
- スマートコントラクト、フルノードやステークホルダーへの経済的インセンティブ、ビットコインに実験的機能をもたらすための拡張ブロック使用の必要性を強調した。
 - ビットコインはスマートコントラクトや分散取引所やICOの機会を逃しているとする。
 - 分散アプリケーションを開発できる複雑なスクリプト言語が必要と述べ、スマートコントラクトの文脈でBitmainがサイドチェーンのRSKに投資したことも触れた。
- コミュニティとしてはビットコインがこれらのイノベーションに少し遅れをとっていると述べた。
 - コインの長期保有者やフルノード運営への経済的インセンティブについてはEthereumがPoWからPoSへの移行を予定していることに言及。
 - ビットコインについてはプロトコル開発にまつわる単一文化に起因して多くのアイデアを試せてないとした。
 - 拡張ブロックによりビットコインにもたらされる機能として、スマートコントラクトおよびMimblewimbleを挙げた。

CRAIG WRIGHT氏、NCHAIN設立

- nChainをBlockstreamの対抗軸として位置付けている模様。
- まず第一弾として、ノードのブロック伝播を高速化可能とするSDKをリリース予定。
- nChainはBitcoin Coreと互換性をもち、この点で BUとの差別化を強調している。

→ 出典: <http://www.coindesk.com/craig-wrights-new-company-developing-bitcoin-core-alternative/>

→ 出典: <https://nchain.com/news/>

JON MATONIS氏とCRAIG WRIGHT氏によるFUTURE OF BITCOINでの”SHINSEIKI EVANGERION”講演

- ビットコンネットワークは現在キャパシティおよびトランザクションスループットのボトルネックに直面しており、それが成長を抑制している。
 - ビットコインは、スケールしなければ生き残ることが出来ず、そのために複数のソリューションが利用可能だが、Blockstreamエンジニアチームと多くが重複するコア開発者グループによるコントロール下にある。
 - 彼らはオンチェーンでのスケーリングに対抗し、多くのオリジナルビットコインスクリプト機能やOP_CODEを利用不能あるいは削除している。
- ビットコインには次の3つのインセンティブが内在している。
 - (1)経済およびゲーム理論システムを用いることによりセキュリティを生み出している
 - (2)タイミングモデルおよび設定の最適化
 - (3)CPUあたり一票の投票は、一人あたり一票の投票ではない
- 「皆がSegWitを求めている」「全ての有能なビットコインエンジニアがSegwitが必要だと考えている」というのは誤り。
 - SegWitでは各トランザクションはより多くの帯域を必要とするスケールしない。
 - シンプルなブロック増加のほうが、より効率的にスケールすることが出来る。

JON MATONIS氏とCRAIG WRIGHT氏によるFUTURE OF BITCOINでの”SHINSEIKI EVANGERION”講演

- ムーアの法則が我々の味方となる。
 - 2009年以来、システムは50倍の成長をパワーにおいて経験してきたが、ビットコインは1MBのまま。
 - オリジナルの方法論はFloodコントロールであったが、これは価値が高ければうまく機能するもの。
 - 2010年においてビットコインは0.01米ドルであり、このレベルではFloodコントロールはうまくいかないものだったが、今やビットコインの価値は大きく高まっている。
- ビットコインは経済システムである。
 - SidechainやLNを追加することはBlockstreamを利することになるが、その一方でそれはマイナーむけの手数料を下げ、システムセキュリティが低下することになる。
 - そのため、マイナー収入は減り、価値がビットコインから失われるだろう。
- nChainがとろうとするUnlimitedブロックサイズ戦略は、以下の3つである。
 - (1)共有およびトランザクションのためのやりとりを容易にするプラットフォーム
 - (2)生産者・消費者双方のグローバルな参加者をひきつけるプラットフォーム
 - (3)取引所を成長させ、価値を共に創造することができるプラットフォーム

JON MATONIS氏とCRAIG WRIGHT氏によるFUTURE OF BITCOINでの”SHINSEIKI EVANGERION”講演

- このための戦術は、以下の5つである。
 - (1) Unlimited Uncapped Blockへ向けたサポートおよび価値上昇
 - (2) Block Capを除去してCoreコードをFixする取組
 - (3) マイニングコミュニティへのサポート強化
 - (4) 非Segwitプールのデプロイ
 - (5) Floodベースフィーのデプロイ
- 新たな変数追加を通じて、フィーベースのレートコントロールを追加する。
 - $nStdFee$ = 次の10000トランザクションのためのものであり、0.005米ドルレートにおけるトランザクションの大半を網羅。
 - $nMaxFee$ = ブロック中の他トランザクションのためのものもあり、Floodのリミット。渋滞時に支払いたいユーザが0.05米ドルのレートで即時にトランザクションを送付できる。
- 将来のノード収入は、以下の2つとなるだろう。
 - (1) トランザクション収入 = 高速なバリデーションプロセス手数料、コインミキシングによる匿名化手数料、ブロック伝播リレー手数料
 - (2) カストディアン収入 = トークン化保険・管理手数料、スマートコントラクトのスクリプト作成手数料、エスクローおよび保険手数料

BITCOIN UNLIMITED 事務局長 PETER RIZUN 氏による FUTURE OF BITCOIN での講演

- SegwitによってマイニングされるSegwit coinは、従来のビットコインとは異なる定義であり、異なる特質を与えるものであるため、ビットコインとは言えない。
- Segwit coinは、ビットコインと異なり、以前の所有者のデジタル署名を確認すること無しに、マイナーは自身のUTXOセットを更新することができる。
- マイナーはフィーの請求にあたりそれらを必要とすることがないため、以前の所有者のデジタル署名は、ビットコインと比べてSegwit coinむけマイナーによって価値の少ないものとなる。
- ビットコインでは全マイナーが以前の所有者のデジタル署名を確認することによって安定的なナッシュ均衡が存在するのに対して、Segwit coinではそれが存在しない。
- 以上より、Segwit coinはビットコインと比べてセキュリティの弱いモデルである。

参考リンク集

- 【図説】8月1日にUASFが実行されると、ビットコインに何が起こるのか
 - <http://btcnews.jp/bkb0bu4c11459/>
- 【図解】Bitcoin Scalabilityに関する議論のタイムライン ~Bitcoin XTからUnlimited、Segwit2xまで
 - <http://btcnews.jp/25eopxo011571/>
 - <http://btcnews.jp/infographics-timeline-history-of-bitcoin-scalability-debateenglish-ver/>
- Segwit Support
 - https://en.bitcoin.it/wiki/Segwit_support
 - コア開発者やマイナー等事業者によるSegwitやそのデプロイおよびハードフォークに対するサポート有無の一覧

1-2. トランザクション渋滞・手数料高騰

- ① Mempoolのトランザクションキューが記録更新
- ② Mempool渋滞とトランザクション手数料高騰
- ③ ビットコインスケーリング紛争の行き詰まりがアルトコインバブルを招く一因に
- ④ Mempoolサイズが縮小/トランザクション渋滞緩和

MEMPOOLのトランザクションキューが記録更新

- ビットコインネットワーク上に155000件のunconfirmed transactionがあり、85BTC相当のフィーが決済待ちとなっている。
- mempool size増大とともに、トランザクションフィーも上昇しており、トランザクションあたり1.0～1.5ドルになっている。
- 21 incのfee calculatorによれば、現在の最速・最安トランザクションフィーはバイトあたり280satoshiであり、トランザクションサイズの間値226バイトを考慮すると、63280satoshiなので約0.98ドルに相当。

MEMPOOL渋滞とトランザクション手数料高騰

- 3日もすればトランザクションはconfirmされるか或いはウォレットに再び現れるが、トランザクションの手数料が低すぎる場合はフルノードのmempoolに残ったまま、期限切れを迎えるかマイナーがピックアップしてブロックに含めるのを待つことになる。
- 現時点ではトランザクションサイズのバイトあたり20satoshiが最低限必要なので、191バイトのトランザクションであれば3820satoshi（およそ0.00004BTCすなわち約5セント）の手数料が必要。
- 手数料がこれを満たさない低水準の場合、フルノード中のトランザクションはmempoolに期限切れまで留まるが、Bitcoin Core 0.12においてexpiration timeは72時間のため、冒頭のように3日が基準となる。
- しかし、expiration timeは実装毎に変更可能であり、誰もがトランザクションを再ブロードキャスト可能なため、ノードをセットアップして低水準な手数料で時間切れまで再ブロードキャストを続けるような攻撃も可能とも考えられる。

ビットコインスケーリング紛争の行き詰まりが アルトコインバブルを招く一因に

- ビットコインのスケーリング論争の行き詰まりにより、ネットワーク上のトランザクションがキャパシティ一杯。
- これがこの二ヶ月のアルトコインバブルをもたらしている、という分析が示された。
- アルトコイン価格が8倍となる中でビットコイン自身の価格も2倍以上に。

MEMPOOLサイズが縮小。トランザクション渋滞緩和でビットコイン手数料が低下

- ビットコインのmempoolがこの一か月で九割近く縮小。
- 未処理のトランザクションのバックログ数も減少傾向。
- ネットワークパフォーマンス改善に加え、手数料も低減中であり、先日450satoshi/byteを記録した手数料は330satoshi/byteに。
- 一方、Ethereumも、ICOブームに押され、一日あたりトランザクション数がビットコインに並んだ。
- 七日間移動平均で約300kトランザクション弱。

- 出典: <https://digitalminer.net/bitcoin-mempool-drops-90-despite-localbitcoins-records/>
- 出典: <https://blockchain.info/charts/mempool-size?timespan=30days>
- 出典: <https://bitinfocharts.com/comparison/transactions-btc-eth-sma7.html>
- 出典: <https://jochen-hoenicke.de/queue/#all>
- 出典: <http://btcnews.jp/2cs8tnsi11647/>

LITECOINがSEGWIT支持

- LitecoinおよびBitcoin双方でSegwitを支持することの意義は、BitcoinのLNトランザクションの方がLitecoinのLNトランザクションに比べ高コストであり、経済的な観点からLNからみてLitecoinから出てBitcoinに戻すLNトランザクションとするのが理にかなう。
- またBitcoinに比べてLitecoinの方がトランザクションの渋滞がゆるい。LightningNetworkは双方の高速道路をつなぐ架け橋として機能するのが、トランザクションコストやトランザクション渋滞の観点から有意義。
- 加えて、LNを通じて双方間のアトミックなクロスチェーントランザクションを実現することができれば、BTCとLTCを即時にリスクなくトレードすることができ、効果的な分散取引所も可能となる。
- このようにBitcoinとLitecoinは将来のトランザクション需要において並存し、BitcoinをゴールドとたとえるならLitecoinをシルバーとたとえることが出来るだろう、とする。

1-3. Segwit・BigBlock以外のスケーリングソリューション

- ① サイドチェーンプロジェクトDrivechain
- ② BIP: OP_BRIBVERIFY
- ③ Segwitやビッグブロックを必要としないMoonbeam

ビットコインスケーリングの解決策サイドチェーンとしてのDRIVECHAIN

- ビットコインエコシステムにsidechainを提供しようとするプロジェクト。
 - Bloq社のエコノミストPaul Sztorcが推進する。
- ビットコインのスケーリングとしてsidechainを用いるというオプションもあると主張。
 - 各チェーンが自身のブロックスペースを持ち、理論的にはブロックサイズリミットを排除できる。
 - ラージブロックのビットコインが欲しい人は自分のBTCをそうしたネットワークに移せば、自分のトランザクションはBitcoin Coreにインパクトを与えない。
- Sztorcは、DCGの提唱するSegwit2xよりも優れたスケーリングソリューションだと主張。
 - 例えばSegwit2xはハードフォークを必要とするが、サイドチェーンでは必要とされないため、2MBへのブロックサイズ拡張のためにハードフォークするのはコストに見合わないとする。
- サイドチェーンの利点を活かすことを意図しているプロジェクト
 - Hivemind（P2P予測市場）、Mimblewimble（ブロックチェーンを劇的に圧縮するトランザクションシステム）、Rootstock（ビットコインベースのスマートコントラクト）、Siacoin（P2Pドロップボックス）、Blockstream Elementsなどがある。

→ 出典: <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-May/014364.html>

→ 出典: <https://themerkle.com/what-is-drivechain/>

→ 出典: <http://www.drivechain.info/projects/index.html>

→ 出典: <http://www.drivechain.info/faq/index.html>

→ 出典: <http://www.coindesk.com/are-sidechains-a-better-solution-for-bitcoins-scaling-debate/>

BIP: OP_BRIBVERIFY

- DrivechainのBMM (Blind Merged Mining) に必要となるオペコードの提案。
- BMMは、Coinbaseトランザクションのアウトプットにハッシュ値を含めるようにユーザーがマイナーを仕向ける (フィーによるbribe) ことが出来るようにするもの。
- 既存のオペコードNOP4を再定義して、ビットコインのマイナーに余分なリソースで負荷をかけることなしに、ビットコインのサイドチェーンがビットコインに対してMerged Mining出来るようにする。
- これによりコミュニティの分派が、ビットコインブロックチェーンと相互運用性ある自分のブロックチェーン上で自身のビジョンを実現し、ビットコインを自分のネットワークのReserve Currencyとして使うことが出来るようになる。

→ 出典: <http://www.mail-archive.com/bitcoin-dev@lists.linuxfoundation.org/msg05722.html>
→ 出典: <http://www.truthcoin.info/blog/blind-merged-mining/>
→ 出典: <http://drivechains.org/what-are-drivechains/what-is-merged-mining/>

SEGWITやビッグブロックを必要としないビットコイン スケーリングソリューション、MOONBEAM

- Lightning Networkと異なりSegwitを通じたトランザクション展性解決を必要とせず、またビッグブロックも不要なため即時デプロイ可能な点が特徴のスケーリングソリューション。
- 取引所や決済プロセッサといった複数ユーザーを抱えるビットコインプラットフォームが標準化された一方向決済チャネルを互いに開くことで、ビットコインネットワークの負荷軽減を可能とする。
- それらのマルチユーザープラットフォームのトランザクションをオフチェーンとすることにより、mempool上の混雑を緩和してトランザクションフィーを低減すること。

→ 出典: <https://bitcoinmagazine.com/articles/moonbeam-scaling-network-semi-decentralized-scaling-solution/>

→ 出典: <https://github.com/luno/moonbeam/blob/master/docs/overview.md>

1-4. LightningNetwork動向

- ① BIP-199 (Hashed Time-Locked Contract: HTLC)
- ② Ind v0.2 alpha
- ③ Lightning Network Faucet
- ④ ビットバンク、Indのfaucetを公開
- ⑤ ACINQ、Litecoin上でLightningNetworkのテスト成功
- ⑥ Litecoin、LNDをサポートへ
- ⑦ Lightning Networkの軽量クライアント、Litがv0.1アルファリリース
- ⑧ LitecoinのMainnet上でZurich～SanFrancisco間の支払い

BIP-199

(HASHED TIME-LOCKED CONTRACT: HTLC)

- 汎化されたオフチェーンのコントラクトにおけるネゴシエーションに関するBIP。
- HTLCでは、売り手がハッシュのプリイメージ（原像）を公開することでコインを消費でき、また買い手はプリ公開のタイムアウト到来時にはコインを取り戻すことができるもの。
- まず、買い手と売り手は公開鍵を交換して、タイムアウトの閾値に合意する。
- 売り手はハッシュダイジェストを提供する。すると、両者はHTLCのスクリプト及びP2SHアドレスを生成。
- 買い手はそのP2SHアドレスにコインを送付。
- 売り手はトランザクション中で買い手に原像を公開して、コインを消費できる。
- 或いは、タイムアウト閾値到来後に買い手がコインを取り戻すことができる。

LND V0.2 ALPHA

- BOLTの仕様に準拠したLndのマイナーリリース。
- マルチホップルーティングで用いられるSphinx packetの生成・処理に使うshared secretの修正。
- 候補となるペイメントパス選定に、「Yenのアルゴリズム」の改良版を応用。
- 以前のLndではグラフ内でアナウンスされる全ての辺および頂点の認証を検証している訳ではなかったが、今回のリリースではアナウンスにおける全ての辺および頂点を検証して、有効チャンネル認証やノードアナウンス証明を生成。

LIGHTNING NETWORK FAUSET

- ビットコインテストネットに実装されたTeatnet Lightning Faucet(TLF)。
- 直接ユーザーにオンチェーンでビットコインを送るfausetではなく、対象ユーザー向けにペイメントチャンネルを開設。
- 現在はIndとのみコンパチブルであり、他のLightning実装であるlit、eclairやc-lightningなどとは今後対応。

ビットバンク、LNDのFAUCETを公開

- テストネットによるLightning Network Faucet。
- lnd (Lightning Network Daemon)は、Lightning Networkノードの実装であり、ビットコインテストネットワークであるtestnet4に現在デプロイされている。チャンネルの生成・クローズ、チャンネル状態管理、認証・検証済みチャンネルグラフ保持、経路探索のほか、オニオンルーティングペイメントが可能となっている。

→ 出典: <https://lnd-faucet.bitbank.cc/>

→ 出典: <https://github.com/lightningnetwork/lnd/blob/master/README.md>

ACINQ、LITECOIN上で LIGHTNINGNETWORKのテスト成功

- Litecoin上でLightningソリューションEclairを用いてテストを行った。
- Eclairは、Scala言語を用いて記述されている。

LITECOIN、LNDをサポートへ

- Litecoinにおいて、今後二週間ほどでSegwitをアクティベート予定。
- これによりLitecoin上にLightningのデプロイが可能になる。
- あわせて、LitecoinのテストネットでLndをサポート。
- サポートにあたり、btcdをフォークしItcdを構築。
- Itcdは、Litecoinの独立したフルノード実装で、CSVやSegwitソフトフォークをサポート。
- 現在のItcdはシングルチェーンのみ対応だが、将来はマルチチェーン対応予定。
- マルチチェーン上のチャネル管理により、オフチェーンによる分散取引所や、オフチェーンによるクロスチェーン支払、クロスチェーンのatomic swapなどの実装にあたる前提が整備される。
- Yours Networkが、Litecoin環境への移転を表明

→ 出典: <http://lightning.community/release/software/lnd/lightning/2017/05/03/lightning/>

→ 出典: <https://news.bitcoin.com/yours-network-litecoin-full-launch/>

LIGHTNING NETWORKの軽量クライアント、LITがv0.1アルファリリース

- ウォレット内蔵とすることにより、フルノードを必要としないLightning軽量クライアント「Lit」のv0.1アルファリリースを公開。
- LNを構築するチャンネルは同じブロックチェーンにある必要はない。複数のアルトコインがSegwitアクティベートしてテストネットワークを提供している中、Litは同時に複数ネットワークに接続してそれぞれ独立したチャンネルを構築可能。これにより集中型の両替を伴うことなくコイン交換をネットワーク上のピアに直接接続して行うことができる。
- LNによって、トランザクションのconfirmationに10分待つことが不要になるだけでなく、このように、別のブロックチェーン間でペイメントチャンネル構築し、クロスチェーンのアトミックスワップを行うことができる点が、他のLN実装と違い、ウォレットを持ちフルノード不要。
- フルノードはセキュリティやプライバシーを提供するがギガバイト単位のデータダウンロードなどセットアップコストが高いのに対して、Litはローカルフルノードに接続してテストが可能。
- Bitcoinのtestnet3およびLitecoinのtestnet4といった複数ブロックチェーン上で稼働するほか、regnet環境（テストイベントに応じて即時にブロック生成したり、実価値を伴わないプライベートsatoshiを生成することができるローカルテスト環境）もサポート。

→ 出典: <https://medium.com/mit-media-lab-digital-currency-initiative/introducing-lit-lightweight-lightning-network-software-2e1078f26368>

→ 出典: <https://news.bitcoin.com/lightweight-lightning-network-client-lit-ready-testing/>

LITECOINのMAINNET上でLIGHTNINGを用いて ZURICH～SANFRANCISCO間のペイメント

- Blockstreamが、LitecoinにおけるTestnetではないMainnet上でLightningの実装を行ったもの。
- LitecoinでのSegwitアクティベートから2時間後に1.3米ドル相当のLightningチャネルをZurich/SF間に開設し、0.00000001LTC分を送金。

→ 出典: <https://www.blockstream.com/2017/05/11/lightning-on-litecoin.html>

→ 出典: <https://m.youtube.com/watch?v=baHHMNA8yf4>

1-5. 秘匿性ソリューション動向

- ① Confidential Assets
- ② TumbleBitをサポートするフルブロックSPVウォレットHiddenWallet
- ③ MoneroブロックチェーンのLinkability
- ④ Grin、MimbleWimbleの実装プロジェクト
- ⑤ Rust言語によるzk-snarks構築ライブラリ、Bellman
- ⑥ ZECC、JP MorganのQuorumプラットフォームにゼロ知識セキュリティ導入

CONFIDENTIAL ASSETS

- Confidential Transactionsがトランザクション中のビットコイン額を隠蔽するのに対して、所有権やIOUのようなブロックチェーン上のアセットに同種のプライバシーレベルを提供する。
- 金額およびアセットタイプを隠蔽したマルチアセットトランザクションを生成可能。
- Blockstreamの既存sidechainであるLuiquidの他、Digital Garageとのコラボレーションにてデプロイが見込まれている。

→ 出典: <http://fc17.ifca.ai/bitcoin/papers/bitcoin17-final41.pdf>

→ 出典: <https://bitcoinmagazine.com/articles/confidential-assets-brings-privacy-all-blockchain-assets-blockstream/>

→ 出典: <http://techmedia-think.hatenablog.com/entry/2017/04/05/183321>

参考論文概要: CONFIDENTIAL ASSETS

- ビットコインではそのコインをUTXOセットに従い流通し、またトランザクションはこのセットへの変更を記述する。
 - 全てのUTXOは金額および署名検証鍵と組み合わせられ、使用可能な量およびそれが可能と認証されたエンティティを表す。
 - トランザクションはUTXOを破壊した上で新たに同額もしくはそれ以下の金額のUTXOを生成し、破壊されたUTXOと紐付いた鍵により署名される。
 - このモデルによりペイメントプロセッサを信頼することなくトランザクションの正しさを検証できる。
- 台帳は分散され公に検証可能なため、全てのUTXOおよび変更履歴は永遠に保存され、公に利用可能で全ユーザーの支払履歴の分析に利用できる。
 - この履歴は直接ユーザーと結びつくものではないものの、たとえ少額でも個人を特定可能な情報があれば完全にユーザーのプライバシーは破られる。
 - さらにコインの履歴トレースは「クリーンな」コインが向けマーケットを作ることに繋がり、アセットのfungibilityを害する。
 - トランザクション構造を不明瞭なものとする方法として、トランザクションを相互に組み合わせでどのインプットがどのアウトプットに紐付くか不明瞭にするCoinJoinがある。
 - しかしトランザクションの金額が見えてしまっているため、全アウトプットの金額が同じでない限りは区別されグルーピングされてしまう。

参考論文概要：CONFIDENTIAL ASSETS

- 当論文では、全UTXOの金額を隠蔽しつつも公なトランザクション検証可能性は保持するスキームであるConfidential Transactionsについて記載（Elements Alphaサイドチェーンにデプロイ済）。
 - このスキームはトランザクショングラフから金額を取り除きプライバシーおよびfungibilityを改善する。
 - 各UTXOの金額を準同型コミットメントにより置き換える。これらの金額は整数セットではなく有限環の上で準同型なため、オーバーフローに関連した攻撃を避けるべく各アウトプットにrangeproofを付与。
 - さらにこれを、単一のブロックチェーンベースの台帳で、単一トランザクション内において、複数のアセットタイプをトラッキングできるConfidential Assetsへと拡張する。
- Confidential Transactionを、金額のみでなくアセットタイプの隠蔽へと拡張することにより、全アセットのプライバシーおよびFungibilityを改善するもの。
 - マルチアセットのブロックチェーンは過去に言及されたことがあったが、アセットの機密性がサポートされておらず、トランザクションのインプット・アウトプットにおける金額やアセットタグが公に参照可能だった。
 - またColored coinsを用いてビットコイン上でアセットを保証するサポートもあり、個々のコインをそれぞれのアセットタイプを表すものとして識別可能だが、ビットコインの不完全なfungibilityに拠っている。
 - Ethereumでもスマートコントラクトを用いてアセットのトークンを保証することをサポートしているが、同様にアセットタイプや数量の不明瞭化には取り組んでいない。
 - Zcashはトランザクションのインプット・アウトプットに関する特定情報を隠蔽しているが、マルチアセットをサポートしていない。またzk-SNARKsを用いるなどプライバシー保持に大きなコストを要し、ゼロ知識証明は計算がかなり遅い。

参考論文概要: CONFIDENTIAL ASSETS

- Confidential Assetsでは、ランダムオラクルモデルである楕円曲線離散対数に基づく。
 - Confidential TransactionsのベースとなるPedersenコミットメントとは、離散対数に基づく無衝突関数を用いたビットコミットメントスキーム（ビットコミットメント=立会い人無しにbit(手番)を委託する方法。ビットを封じるコミットフェーズと公開するオープンフェーズの二段階）。
 - ランダムオラクルカードモデルにおいて、アセットタグは一様なランダムカーブポイントであり、その離散対数は他のアセットタグに関して既知ではない。
 - あるアセットの数量へのPedersenコミットメントは同時にアセットタグの同量へのPedersenコミットメントであると考えられる。さらに、blinding factorおよび或るgeneratorに関するオープニング情報を知る者は、他のgeneratorに関するオープニング情報を決定できる。そうしたPedersenコミットメントは、数量だけでなくアセットタグもコミットすると考える。
- Confidential Assetsでは、マルチアセットトランザクションを、複数のシングルアセットトランザクションとして取扱う。
 - それぞれのアウトプットにアセットタイプを識別するasset tagを付与し、検証者は単一アセットタイプのみを持つトランザクションサブセットの検証方程式をチェック。
 - また、アウトプットアセット間の関係性が分からないように全てのアセットタグは隠蔽され、個々のトランザクションで使われる特定アセットが何かというプライバシーを保護するため、たとえ少量でもその利用だけでユーザーを特定されるようなアセットにおいて有益。
 - ランダムなアセットコミットメントをトランザクションアウトプットに付与し、マッピングを開示することなくインプットとアウトプットを紐付ける方法が必要であり、インプットコミットメントからアウトプットコミットメントへのasset surjection proof(ASP)を導入。

TUMBLEBITをサポートするフルブロック SPVウォレットHIDDENWALLETがテストリリース

- ブロックチェーンは格納せずブロックのvalidateも行わないで、Merkle proofを用いて他のSPVウォレット同様にトランザクション有効性を検証する。
- 一方でSPVウォレットと異なりフルノード同様にフルブロックをダウンロード。ブロックチェーン分析業者もSPVウォレット間のアドレスのリンクを再構成することが不可能であり、プライバシーの問題を改善。
- プライバシー問題解決にあたりフルノードは対案ではあるが全ブロックチェーンのダウンロードが必要であった。
- そこでフルブロックダウンロードのSPVウォレットとしたもの。

→ 出典: <https://hackernoon.com/introducing-hiddenwallet-full-block-spv-tumblebit-wallet-testing-release-1054a15a9bb1>

→ 出典: <https://news.bitcoin.com/tumblebit-hiddenwallet-released/>

MONEROブロックチェーンのLINKABILITY

- Moneroのプライバシーについて、特に2017年2月以前のトランザクションが問題視されている。
- ビットコインと異なり、Moneroではトランザクション間のリンクが攪乱されており、各トランザクションインプットはmixinと呼ばれるおとりリンクを含むことになり、原理上はmixinのうちどれが本物かを誰も分からない。
- しかし、調査において、mixinがうまく出来ておらずリンク可能なことが判明したとのこと。
- MoneroLinkのブロックエクスプローラを用いるとMoneroトランザクションで隠蔽されたリンクが判明可能。
 - <http://hackingdistributed.com/2017/04/19/monero-linkability/>
 - <http://monerolink.com/>

→ 出典: <http://hackingdistributed.com/2017/04/19/monero-linkability/>

→ 出典: <http://monerolink.com/>

MONEROブロックチェーンのLINKABILITYに関する 参考論文

- An Empirical Analysis of Linkability in the Monero Blockchain
 - Moneroは、使用する本物のコインと併せてmixinと呼ばれる屑コインを含めることによって、ユーザーがトランザクショングラフを見えなくすることが出来るプライバシー特化型の暗号通貨。
 - 本論文では、Moneroのmixinサンプリング戦略における二つの弱点について実験的に評価している。
 - まず、mixin中の62%のトランザクションインプットが、chain-reaction分析（本物のインプットが推測可能）に対して脆弱。また、mixinは、本物のコインとageにより容易に区別可能な形でサンプリングされる（本物のインプットは通常は最新のインプット）。
 - ひとつ以上のmixinを持つトランザクションにつき80%の正確さで本物のインプットを推測できると見積もっている。前者の脆弱性はRingCTより前のソフトウェアに適用されるが、後者の脆弱性は最新のバージョンにも当てはまる。
- A Traceability Analysis of Monero's Blockchain
 - Moneroは2014年4月ローンチ以来急速に人気を得ており、この成長の源泉はビットコインなどの他の暗号通貨に勝るプライバシー特性にある。
 - この論文では、Moneroブロックチェーンを分析し、Moneroの追跡不可能性（あるトランザクションインプットが与えられたときに本物のアウトプットを他のアウトプット中で匿名とする）を検証している。
 - 87%のケースにおいて、本物のアウトプットを確信を持って特定できる。
 - また、Monero RingCT（トランザクション値も隠蔽する第二世代Monero）にも拡張可能とする。

GRIN、MIMBLEWIMBLEの実装プロジェクト

- Mimblerwimbleは高度なスケーラビリティやプライバシーおよびフンジビリティを提供するブロックチェーンのフォーマットおよびプロトコル。
- GrinはMimblerwimble実装のオープンソースプロジェクトであり、以下を主な目的・特徴とする。1) デフォルトで完全なフンジビリティを提供する高度なプライバシー性能。2) トランザクション数ではなくユーザー数でスケールし、スペースの大幅節約。3) Asic耐性あるマイニングアルゴリズムCuckoo cycleによるマイニング分散化促進。4) 強固で実証済みの楕円曲線暗号。
- Mimblerwimbleトランザクションが依拠する特徴は次の二つ。
 - ゼロサム検証
 - アウトプットからインプットを引いた合計は常にゼロであり、トランザクションが新たに資金を作り出してないことを実際の金額を明かすことなく証明。
 - 秘密鍵所有
 - 他の暗号通貨同様、トランザクションアウトプットの所有権は楕円曲線暗号による秘密鍵所有により保証されるが、あるエンティティが秘密鍵を持つことの証明はトランザクションに直接署名することだけでは満たされない。

RUST言語によるZK-SNARKS構築ライブラリ、 BELLMAN

- zcashの次期バージョンsaplingへ向けたセキュリティやパフォーマンス面の改善。
- より効率的にメモリ消費を抑えてZk-snarksを構築することを目的としたBLS12-381楕円曲線の実装を含む。

ZECC、JP MORGANのQUORUMプラットフォームに ゼロ知識セキュリティを導入へ

- Zcashを開発したZECCがJP Morganとの協業を発表。
- JP MorganのエンタプライズブロックチェーンプラットフォームQuorumへの技術供与により、Quorumのプライバシー保護を拡張し、分散台帳上でのデジタルアセットのプライベートなセトルメントを、中間介在無しに可能とする。
- Quorumは、JP Morganにより進められている、オープンソースによるグローバルファイナンス向け分散台帳技術であり、ethereumプロトコルをベースとするもの。
- これにより、Quorumは分散台帳プラットフォームの中で最初にゼロ知識セキュリティレイヤーを搭載することになる。

→ 出典: <https://z.cash/blog/zsl-quorum.html>

→ 出典: <http://www.zcashfans.com/posts/916>

1-6. その他のトピック動向

- ① Bitcoin Covenants
- ② クロスチェーンアトミックスワップをサポートする分散取引プロトコル、Enigma Catalyst
- ③ RSK、テストネットをローンチしオープンベータ版へ
- ④ Liquid Betaのデモンストレーション
- ⑤ ILPのビットコイン向けプラグイン、Paychan
- ⑥ Bitcoin Proof-of-Work Upgrade Initiative
- ⑦ Proof of existence、ASICメーカーにより買収

BITCOIN COVENANTS

- コインの消費を制限するScript。
- どのアドレスでどれだけの金額を消費できるかをロックできるもの。
- Scriptにはトランザクションデータの読み込みを許可するようなオペレーションを含まないため、理論的にはCovenantsを利用することができないが、トランザクションデータとやりとりする上での方法として、署名検証を行うCHECKSIGを使うことにより、Covenantsをサポートできる。

クロスチェーンアトミックスワップをサポートする 分散取引プロトコル、ENIGMA CATALYST

- 双方向ペイメントチャネル及びHTLC上に構築されたオフチェーンペイメントネットワークの拡張として運営される。
- アルゴリズムトレードマネージャーの指示のもとに、HTLCを用いたクロスチェーンアトミックスワップを行う方法を提供するもので、これによりアセット保護ならびに取引アルゴリズムの秘匿性を保持できる。
- 低遅延スワップをサポートするために、ハブ&スポークを構成する既存ペイメントネットワークの子グラフとして運営。
- トレーダーはstate-channelを用いて複数取引所とチャネルを開くため、取引所横断の裁定機会を作り流動性を高める。
- HTLCおよび経済的インセンティブを用いてファンドの持ち逃げを防ぐ他、仲介役への信頼必要なしに高速で価値移転が可能。
- 様々なクリプトアセットのクロスチェーンアトミックスワップのサポートにあたり、両当事者間のラウンドトリップでルーティングを行う循環state-channelペイメントを構築。
- 長期的ゴールをICOトークンのライブトレーディングサポートとしているため、ethereumスマートコントラクト間のオフチェーン価値移転を行うRaiden Networkと完全互換予定。

RSK、テストネットをローンチしオープンベータ版へ

- Rootstockを提供するRSK Labsは、ビットコインとethereum版のサイドチェーンを用いてスマートコントラクトを可能とすることを目指しており、パブリックテストネットGingerをローンチすることを発表した。
- テストネット用コインなどを用いて、RSKのサイドチェーン上でビットコインネットワークへのethereumスマートコントラクトを試行できる。
- Gingerを用いて、トランザクション圧縮プロトコルLuminoによる秒間2万トランザクションでのスマートコントラクトが可能。
- 同じタイミングで、Blockstreamからもサイドチェーン Liquidのベータプログラムが発表された。

→ 出典: <https://github.com/RSKSmart>

→ 出典: <https://news.bitcoin.com/sidechain-juggernauts-rsk-labs-launches-ginger-testnet-after-3-5m-in-new-funding/>

→ 出典: <https://www.docdroid.net/QHJX8MI/luminotransactioncompressionprotocolltcp.pdf.html>

LIQUID BETAのデモンストレーション

- Consensus2017で発表されたデモの紹介。
- 初めてのfederated sidechainであるLiquidをまたいだトランザクション。
- ビットコインのメインチェーンにペグされたコインを、Liquidに参加する取引所間において数秒で送金。
- またLiquidの将来像として、トークン化された法定通貨をモバイルウォレット間のsidechainをまたいで秘密裏に送金するデモも紹介された。

ILPのビットコイン向けプラグイン、PAYCHAN

- Rippleによりオープンソースとして発表された、ILP向けビットコインプラグイン。
- CHECKLOCKTIMEVERIFY (CLTV) を実装した一方向ビットコインペイメントチャネルを用いている。
- ビットコインの他、エンタープライズ向けプラットフォームであるChainにもプラグインが発表された。
- Berlinで行われたデモでは、パブリックチェーンやプライベートチェーン、中央集中台帳、従来型ペイメントチャネルなど七つの台帳を横断した単一トランザクションが行われた。

→ 出典: <https://github.com/interledgerjs/ilp-plugin-bitcoin-paychan/blob/master/README.md>

→ 出典: <http://www.coindesk.com/interoperability-boost-ripple-sends-blockchain-transaction-across-7-different-ledgers/>

BITCOIN PROOF-OF-WORK UPGRADE INITIATIVE

- ビットコインのPoW向けに分散型アルゴリズムの研究・テスト・実装を求める取り組み。
- Bitcoin CoreやBlockstreamとは無関係としている。
- 現在ほとんどのマイニングパワーが直接的・間接的に一つの組織体によりコントロールされていることへの問題提起。
- 個人ユーザが実質的にビットコインをマイニングできないため、PoWを変革したビットコインのCPU/GPUマイニングの機会を再び可能にしようというもの。
- 単一政府の司法管轄権下へのマイニングの集中な政治的な操作や検閲に対するリスクとなるという問題意識。
- ビットコインがスケーリングソリューションをなかなか実装できない状況にある中、PoWを変革してスケーリングへの門戸を開こうとするもの。

PROOF OF EXISTENCE、ASICメーカーにより買収

- 買収するのは北京のCanaan社で、Avalonminerなどを製造するAvalonグループのメーカー。
- Proof of existenceは2013年にローンチされ、ブロックチェーン上でドキュメントそのものや自身を明かすことなく情報所有を証明するサービスの先駆け。
- 同種のタイムスタンプサービスにはStamperyやBlock Notary、Eternity Wall、Verisart、Opentimestampなどがある。
- 創業者のManuel Araozはこの他に2015年にライブストリーミングStreamiumを開発し、現在はブロックチェーンベースのVRプロジェクトDecentralandに従事。

→ 出典: <https://news.bitcoin.com/bitcoin-mining-manufacturer-canaan-acquires-proof-of-existence/>

→ 出典: <https://canaan.io/2017/05/21/canaan-acquires-proof-of-existence/>

2. プロトコル改善にむけた動向

- ① 暗号通貨へのルーティング攻撃対策
- ② マイニング報酬のバラつきを縮小し公平性を高めるマイニングプロトコルの見直し
- ③ Permissionlessなビザンチンコンセンサスによるセルフイッシュマイニング軽減
- ④ ビットコインブロックチェーンの非効率性
- ⑤ 分散型匿名マイクロペイメント
- ⑥ Confidential Transactionへの安全な切替を可能とするSwitch Commitments
- ⑦ 汎用化PoAによるハイブリッドコンセンサス
- ⑧ 非同期ネットワークにおけるブロックチェーンプロトコル
- ⑨ スマートコントラクト向けデータフィード
- ⑩ 量子コンピュータ耐性あるブロックチェーン開発
- ⑪ ISOにおけるブロックチェーン技術検討

暗号通貨へのルーティング攻撃対策

- インターネットのルーティング基盤を用いて、悪意あるISPがネットワークの攻撃が可能。
 - 13のISPでビットコインネットワークの30%をホストしており、60%のビットコイントラフィックが3つのISPを通過しているため、悪意あるISPがトランザクションをインターセプトできる。
- インターネットルーティング攻撃の効率性やビットコインネットワークの集中を背景として、Partition攻撃及びDelay攻撃がルーティングアタックとして今日可能とされる。
 - Partition攻撃はIPプリフィクスをハイジャックすることによりISPがビットコインネットワークを分断するもの。パラレルブロックチェーンを作ることが可能となり、攻撃終了後、小さい方のコンポーネントでマイニングされたブロックはそこに含まれるトランザクションやマイナー収益とあわせ破棄される。
 - Delay攻撃はノード間のトラフィックを伝えるISPがブロック伝播を20分ほど遅延させるもの。犠牲者がマーチャントであれば二重使用、マイナーであれば計算リソース空費、一般ノードであれば伝播によるネットワーク貢献への被害となる。
- これら攻撃はマイナーの収益を下げるほか、二重使用などの嫌疑をもたらすもの。
 - 個々のノードを標的とした小規模攻撃、ネットワーク全体を標的とした大規模攻撃の双方が考えられるため、長短期での対策を急ぎ講じることが必要であるという提言。

➔ 出典: <http://hackingdistributed.com/2017/05/01/bgp-attacks-on-btc/>

➔ 出典: <http://hackingdistributed.com/2017/05/01/bgp-attacks-on-btc/>

➔ 出典: https://btc-hijack.ethz.ch/files/btc_hijack.pdf

マイニング報酬のバラつきを縮小し 公平性を高めるマイニングプロトコルの見直し

○ FruitChains: A Fair Blockchain

- ブロックチェーンプロトコルに公平性を導入し、ある比率の計算パワーを持つプレイヤーが少なくとも一定のブロックを獲得できるようにするもの。
- ブロックチェーン上にトランザクションレコードを記録する代わりにfruitsを記録し、fruitsが一定のfruits困難度を伴うPoWの解を要求することで、チェーン中のブロック（fruitsを記録したブロック）からfruitsを「もぎとる」もの。ここではfruitsがブロックのような役割を果たす。
- 各ラウンドにおいてプレイヤーはfruitとブロックの双方のためにマイニングを行う。
- マイニング報酬やトランザクション手数料がマイナーに一律に配分され、マイニング報酬のバラつきを縮小するとともに、マイニングプールの必要性を小さくすることが出来るという提案。
- マイニング報酬はバラつきが大きく、これがマイナーが集まり報酬を分け合うマイニングプールを作る動機にもなっており、マイニングプールの副作用としてシステムの分散性を損なうことに繋がっている。
- FruitChainプロトコルではマイニング困難度を独立した2つのパラメータ（block困難度とfruit困難度）で規定することにより、decentralizedな方法でマイナー報酬のバラつきを縮小する。
- 現在典型的なソロマイナーは報酬獲得に2年ほど要するが、これを数日にまで短縮可能とし、マイニングプールを不要にできる。

PERMISSIONLESSなビザンチンコンセンサスによる セルフフィッシュマイニング軽減

- Solidus: An Incentive-compatible Cryptocurrency Based on Permissionless Byzantine Consensus
 - ビットコインの課題として、confirmation timeの長さやトランザクション・スループットの低さが挙げられるが、他の課題として、プロトコル中の情報伝播インセンティブ不足のためトランザクションの保留やセルフフィッシュマイニング等の懸念をもたらす点がある。
 - 合理的なマイナーは他マイナーから得た複数の情報タイプを保留し、ネットワークから最近のブロックを選択的に隠蔽するセルフフィッシュマイニングにより自身の報酬を増やそうとする。
 - これら課題に対処するため、Permissionlessなビザンチンコンセンサスにおける分散暗号通貨Solidusを提案する。Solidusにおけるコア技術は、PoWを用いてリーダー選挙を行うことでPBFTをPermissionlessな環境に適用すること。またインセンティブ互換とし、セルフフィッシュマイニングを軽減。
 - SolidusではPoWのチェーンを構築せず、代わりにPoWをリーダーのランクとして使うことで、シビル攻撃回避だけでなくコンセンサスを駆動するための一意なリーダーを保証する。
 - ビットコインではPoWをブロックチェーン構築のために用いて、それがpermissionlessなコンセンサスを提供する。これに対して、SolidusではPoWをpermissionlessなコンセンサス解決のために用いて、それがブロックチェーンを構築する。
 - PBFTをpermissionlessな環境に適用することでトランザクションスループットを改善するほか、ビザンチンコンセンサスがコミットされればトランザクションのconfirmationもビットコインより早くできるとする。
 - Solidusの構成要素はインセンティブコンパチブルであり、コミット者をトランザクション検証を動機付けているため、これら動機により参加者の多数が合理的であり連合を組まない場合に、分散システムにsafety（安全性:常に成り立つ）およびliveness（生存性:有限時間内に成り立つ）を提供。

ビットコインブロックチェーンの非効率性

○ Blockchain Inefficiency in the Bitcoin Peers Network

- ビットコインのネットワークにおけるブロックやトランザクションの動態をモニタリングすると、トランザクションの43%が一時間経過後もブロックチェーンに含まれていない他、トランザクションの20%は30日経過後も含まれていないなど、ビットコインのシステムにおける重大な非効率性が明らかになった。
- しかし、これらの「忘れられたトランザクション」のほとんどは金額が小さいため、送金額で見ればトランザクションの93%が三時間以内にブロックチェーンに含まれており非効率ということもない。
- これはブロックサイズが1MBに制限されていることが理由ではなく、なぜなら平均ブロックサイズが0.8MBであり0.99MB超はブロックの3%に留まるほか、また幾つかのブロックはトランザクションを含まないことからネットワーク起因でないと言える。
- 相当の比率のトランザクションがタイムリーに処理されていないということは、信頼できるタイムスタンプという目的でもビットコインのブロックチェーンの利便性に深刻な疑念を投げかけることになる。
- P2Pで中間介在人を必要としないシステムが効率的トランザクション記録を促進する上で導入すべき正しいインセンティブシステムについて議論が必要。

分散型匿名マイクロペイメント

○ Decentralized Anonymous Micropayments

- ビットコインのマイクロペイメントでは、トランザクションフィーの高額化、Confirmation timeの遅さ、および匿名性の無さがあり、それぞれZerocashなどの解決策が提案されている。
- 目指すゴールは、マイクロペイメントとして分散型で・匿名性があり・オフラインでレスポンスが早いこと。
- 分散型の匿名マイクロペイメントのスキームを提案するものであり、参加者は台帳にアクセスしてオフラインで確率的ペイメントを直接かつプライベートに行うことができる。
- Zerocashのスキームを拡張して新たな確率的ペイメントスキームを取り入れたもの。
- 二者間での確率的メッセージ移送を可能とするため、Fractional message transfer (FMT: 断片的メッセージ移送) を提案している。
- FMTにより、断片的隠蔽・断片的関連付けを可能とし、プライバシー面の問題であるLinkabilityに対して半透明性を導入するもの。

CONFIDENTIAL TRANSACTIONへの安全な切替を可能とするSWITCH COMMITMENTS

- Switch Commitments: A Safety Switch for Confidential Transactions
 - セキュリティ上の疑念が生じたときに異なるアルゴリズムに切り替える俊敏性について、暗号通貨ではブロックチェーン上に状態が永続的なものとなるため実現が難しい。
 - たとえば採用している署名スキームが安全でない場合には異なるスキームに切り替えることで可能なのは、将来のトランザクションアウトプットを保護することのみで、既にブロックチェーンに記録されたトランザクションアウトプットは解決されず、盗難のリスクに晒される。
 - こうした状況はConfidential Transactionのように準同型コミットメントによりトランザクション量を隠蔽してプライバシーを保護する場合に深刻となる。
 - もし攻撃者がコミットメントをブレイクした場合に通貨を真空から生み出すことができ通貨全体のセキュリティを脅かす。
 - そこでこの論考では、switch commitmentsを導入し、セキュリティ上の疑念が生じた場合に計算的な暗号から統計的な暗号へと、既存のコミットメントを切り替えることを可能とできると述べている。

汎用化PoAによるハイブリッドコンセンサス

- Forking-Free Hybrid Consensus with Generalized Proof-of-Activity
 - PoWは効率性に課題がある他、計算パワーの集中化の動機となる可能性をはらみ、本来の目的である分散化を損なう。
 - その後にPoSが提案されたが、PoWとPoSはそれぞれ異なる利点・欠点があるため、PoA(Proof of Activity)が双方の仕組みの組み合わせとして提案されている。
 - 一方でハイブリッド・コンセンサス・プロトコルは効率性を改善することを目的に、コミット者のローテーションを動的に維持しているが、Selfish miningやFair committee electionといった課題が残っている。
 - そこで本論考では、PoWを一般化した変化形を考察した後、汎用PoWを用いてForking-freeなハイブリッドコンセンサスを構築し、通常のハイブリッドコンセンサスが直面する課題へのアプローチを提示。
 - さらに、Forking-freeなハイブリッドコンセンサスメカニズムをPoSに組み合わせるとPoAを一般化。
 - PoAと比べて、汎用PoAは効率性に優れ、PoWとPoSの柔軟な組み合わせをもたらすことが出来るコンセンサスキームとなっている。

非同期ネットワークにおける ブロックチェーンプロトコル

- Analysis of the Blockchain Protocol in Asynchronous Networks
 - 従来のブロックチェーン・コンセンサス・プロトコルに関する分析は、単純化した仮定をおき、ネットワークチャンネルを完全に同期型（例えばメッセージが即時に遅延なく届けられる）としたものだった。
 - この論考では、ブロックチェーンのコンセンサス・プロトコルが非同期型ネットワークにおいて、強い形態の整合性（consistency）および進行性（liveness）を満たすことを証明した。
 - 関連する論考としては、インセンティブ互換性に関するものとして「Fruit Chain」、高速 confirmationに関するものとして「Hybrid Consensus」などがある。

スマートコントラクト向けデータフィード

- Town Crier: An Authenticated Data Feed for Smart Contracts
 - スマートコントラクトには信用に足るデータフィードが不可欠。
 - Town Crier(TC)はスマートコントラクトと、非ブロックチェーンサービスに信用された既存ウェブサービスのブリッジとして、認証済みデータフィードとする提案。
 - スマートコントラクトを信用するために、ブロックチェーンのフロントエンドを信用されたバックエンドと接続。
 - TCはまたプライベートデータの機密性もサポート。
 - TCはインテルのSGXによるTrusted hardwareを用いて、データをethereumブロックチェーンに提供することにより、データフィードの信用度を確保している。
- Discreet Log Contracts
 - スマートコントラクトのスケールビリティやプライバシー問題に対処しつつ、外部データをスマートコントラクトに提供するoracleに対する信頼を最低限とすることを目指したもの。
 - このコントラクトでは、外部の観察者がトランザクション中にコントラクトの存在を検知することができないように考慮されている。

量子コンピュータ耐性あるブロックチェーン開発

- ロシアの科学者（Russian Quantum Center）が世界で初めて量子コンピュータ耐性のあるブロックチェーンを開発し、銀行（Gazprombank）がテストを行い量子コンピュータによりハッキングされないことを示した。
- デジタル署名を用いず、その代わりに光子による量子暗号を用いて認証を行う。
- またネットワーク中のノード間をQKD（量子鍵交換）リンクを用いて接続。
 - 第一階層はQKDネットワークでブロックチェーンユーザ間の認証を行う。
 - 第二階層のメッセージデータ移送ではToeplitzハッシュアルゴリズムに基づく認証タグを利用。
- QKDはワンタイムパッド（OTP）暗号むけに安全な型で鍵を共有するものであり、OTP暗号は量子コンピュータにも破られないものとして数学的には証明されている。
- QKDネットワークはスマートコントラクトや高度に機密性の高いデータ移送に使われていくとされるがブロックチェーンに採用されたのは初めて。

参考論文：量子暗号時代への対応（1/4）

- Post-quantum cryptography---dealing with the fallout of physics success
 - 大規模な量子コンピューターにより可能となるRSAやECC（楕円曲線暗号）の危殆化や攻撃を仮定して、安全性を維持する量子暗号システムの研究が進んでいる。
 - RSAは素因数分解の難しさに依拠しているが、1994年に「Shorのアルゴリズム」により素因数分解の解を量子アルゴリズムで高速に見つけることが出来ている。また、同様のアルゴリズムによりECCも破ることができる。このアルゴリズムを用いてRSAやECCを破るには、数千の論理量子ビット上で数十億回のオペレーションが必要だが、これらの攻撃可能性への防御策は必要。
 - また1996年に発表された「Groverのアルゴリズム」は、スケーラブルな量子コンピューターでShorのアルゴリズムが稼働すれば不要だが、小規模で高速な量子ビット操作で十分な場合に128ビットAES鍵に有効であり、今のうちに256ビットAES鍵に切り替えることが推奨されている。
 - Code-based暗号、Lattice-based暗号、Lattice-based署名、Multivariate-quadratic-equation署名、Hash-based署名などの新たな暗号・署名が研究・提案されている。
 - 暗号システムのデプロイにもまたコストとして、時間やエネルギーが必要となる。今日の多くのユーザーによる暗号のデプロイはユーザーの予算にフィットしたという事実により支えられている。
 - また同じ暗号システムを導入していくためには標準化も前提となる。IETFがhash-based署名の標準化を推進している他、NISTが標準化にむけて候補を受け付けている。
 - 未だ若い分野であり、暗号の利便性や柔軟性などが主な課題とされる。

参考論文：量子暗号時代への対応（2/4）

○ Quantum-secured blockchain

- <https://arxiv.org/abs/1705.09258>
- ネットワーク上での量子鍵交換（QKD）を用いて安全な認証を可能とすることにより、量子コンピュータへのハッキング耐性を持たせるとするもの。
- 複数参加者のネットワークを介した量子の状態を直接伝達する技術は、量子耐性あるブロックチェーンのみでなく、量子コンセンサスや量子デジタル署名など、量子技術ベースのコンセンサスアルゴリズムなど、量子技術時代の分散台帳セキュリティに有効。

参考論文：量子暗号時代への対応 (3/4)

- Post-quantum RSA
 - <https://eprint.iacr.org/2017/351>
- Quantum Information Set Decoding Algorithms
 - <http://eprint.iacr.org/2017/213>
- XOR of PRPs in a Quantum World
 - <http://eprint.iacr.org/2017/356>
- Post-Quantum Key Exchange on ARMv8-A -- A New Hope for NEON made Simple
 - <http://eprint.iacr.org/2017/388>
- Quantum Authentication and Encryption with Key Recycling
 - <https://eprint.iacr.org/2017/102>

参考論文：量子暗号時代への対応（4/4）

- Quantum Authentication with Key Recycling
 - <https://eprint.iacr.org/2017/119>
- 10-qubit entanglement and parallel logic operations with a superconducting circuit
 - <https://arxiv.org/abs/1703.10302>
 - <http://m.economictimes.com/news/science/worlds-first-quantum-computing-machine-made-in-china/articleshow/58492628.cms>
- Quantum-secured blockchain
 - <https://arxiv.org/abs/1705.09258v1>
- Post-Quantum Cryptography: S381 Cyclic Subgroup of High Order
 - <https://arxiv.org/abs/1704.07238>

ISOにおけるブロックチェーン技術検討

- 四月にシドニーに30ヶ国が集まり、ブロックチェーンおよび分散台帳に関するグローバル標準にむけた研究活動について討議が行われた。
- ISOのテクニカルコミッティにおいて五つのスタディグループが組成された。(Reference Architecture, Use cases, Security, Identity, Smart Contracts)

3. プラットフォーム分野

① 個別サービスリスト

個別サービス①

名称	サービス概略	URL
iEx.ec	クラウドコンピューティング・プラットフォーム	→ http://iex.ec/
Zeronet	ビットコインの暗号と、BitTorrentを使ったオープンネットワーク	→ https://zeronet.io/
Minebox	ディスク容量を貸出しSiacoinを稼げる分散クラウドストレージ	→ https://minebox.io/store
Agrello	法的・ITスキル不要でAIベースにスマートコントラクト生成するインターフェース（AIを用いたコントラクトジェネレーター）	→ https://www.agrello.org/
Mysterium	ブロックチェーンベースのVPN	→ https://mysterium.network/
Aragon	分散型組織マネジメントツール	→ https://github.com/aragon/aragon/releases
Prism	Shapeshiftがローンチを予定しているスマートコントラクトで構築	→ https://prism-launch.com/
BOScoin	トラストコントラクトを特徴とするプラットフォーム	→ https://boscoin.io/en/home/
Ivy Playground	Chainによるスマートコントラクト	→ https://chain.com/docs/1.2/ivy-playground/tutorial

個別サービス②

名称	サービス概略	URL
Tezos	DAOガバナンスによるブロックチェーン	→ https://tezos.com/
SONM	ネットワークマイニングによる分散型スパコン	→ https://sonm.io/
Aeternity	トラストレスステートチャネルを備えたスマートコントラクト	→ https://www.aeternity.com/ja
TrustedChain	European Trust Service Providersによるブロックチェーン	→ https://trustedchain.it/en/
CompCoin	トレーディングコンピュータの分散ネットワーク	→ https://compcoin.com/
Postchain	Chromaway社によるコンソーシアムデータベース	→ https://chromaway.com/products/postchain/
Swap	ethereumの分散型トレードプロトコル	→ https://swap.tech/
ConsenSys Diligence	ethereumエコシステム内のセキュリティベストプラクティス	→ https://medium.com/@c.diligence/
DIMCOIN	Data Interchange ModuleとしてNEM上エコシステムを目指す	→ https://www.dimcoin.io/

4. ライフスタイル分野

- ① 2017 第一四半期の動向
- ② 個別サービスリスト

2017 1Qの動向

- OpenAssetProtocolを用いて個人の株式に見立てたトークンをトレードする、VALU
 - 個人が株式会社のように模擬株式に見立てた「VA」を発行し、自分の価値として好きな価格をつけて、ビットコインによって他人との売り買いができる。
 - SNSのフォロワー数・友達数に応じて自身の時価総額を自動的に算出。
 - 各ユーザーは株主（VALUER）に向けてイベント参加権や優待を設定可能。
 - ビットコイン・ブロックチェーンの技術を用いて開発。
 - <https://valu.is/>
 - <http://jp.techcrunch.com/2017/06/01/valu/>
 - <https://readyfor.jp/projects/valu>
- AT&T、車内支払いに続きホーム加入者サーバー（HSS）領域で特許
 - 携帯電話の通信ネットワークを利用するために必要なユーザー情報を管理するデータベースとして認証・認可・配信を行うHSSにブロックチェーンを用いて「分散型セキュアホーム加入者サーバー」とすることにより、送信ノードを分散化することでマルチメディア配信ネットワークのセキュリティを向上させる。
 - <http://www.coindesk.com/att-awarded-patent-bitcoin-powered-subscriber-server/>
 - <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetacgi%2FPTO%2Fsearch-adv.htm&r=1&f=G&l=50&d=PTXT&p=1&S1=blockchain&OS=blockchain&RS=blockchain>

個別サービス①

名称	サービス概略	URL
Voise	分散ミュージックプラットフォーム	→ https://voise.it/
Zimrii	ミュージックプラットフォーム	→ http://www.zimrii.com/
DigitalGarage	クレディセゾン・Blockstreamとロイヤリティポイント	→ https://cointelegraph.com/news/bitcoin-blockchain-to-help-collect-customers-activate-consumption-in-japan
Global Miles	マイレージプログラム	→ http://www.globalmiles.com/en/
Civil	分散ジャーナリズム	→ http://joincivil.com/
Charitychain	チャリティファンドレイジング	→ https://github.com/charitychain-io/v0/blob/master/Charitychain.sol
Curation Markets	トークンによるキュレーション・コラボレーション	→ https://docs.google.com/document/d/1VNkBjjGhcZUV9CyC0ccWYbqeOoVKT2maqX0rK3yXB20/mobilebasic
Babel	分散型eコマースプラットフォーム	→ https://billh93.github.io/babel/
Aventus	イベントチケット	→ https://aventus.io/
SkinCoin	ゲームアセットのマネタイズ向け分散マーケット	→ https://skincoin.org/

個別サービス②

名称	サービス概略	URL
Indorse	分散型ソーシャルネットワーク	→ http://www.indorse.io/
Status	モバイルメッセージング	→ https://status.im/
Kin	チャットプラットフォームKikむけのERC20ベース暗号通貨	→ https://kin.kik.com/
Qrator	Synereoによるアテンションエコノミーアプリ	→ https://blog.synereo.com/2017/04/03/synereo-announces-qrator-the-first-liberated-attention-economy-application/
District0x	分散マーケットコミュニティのネットワーク	→ https://district0x.io/
AdEx	分散ウェブ広告マーケット	→ https://www.adex.network/adex/AdEx-Whitepaper-v1.4.pdf
21 inc	マイクロコンサルティングを可能にする21 lists	→ https://21.co/lists/

5. サプライチェーン系

- ① 2017 第一四半期の動向
- ② 個別サービスリスト

2017 1Qの動向 (1/3)

- トヨタ、将来の自動車開発に向けたブロックチェーン利用をMIT Media Lab他と共同で行うことを発表
 - MITの他、Oaken Innovations、Gem、Commuterz、BigchainDBと共同で利活用の可能性を研究する。
 - ブロックチェーンのインパクトとして、データ共有、カーシェアリングおよび利用ベース保険の三領域に着目。
 - 自動車所有者からのデータ蓄積・共有を通じて、自動運転技術の安全性や利便性向上につなげるとしている。
 - また空きシートやトランクスペースなどのリソースのシェアリングを通じてクルマのオーナーがマネタイズしやすくなる。
 - クルマのセンサーが溜めたドライブデータをブロックチェーンへ格納して不正の無い安全運転度合いに応じて保険料を安くするなどを検討。
 - <http://corporatenews.pressroom.toyota.com/releases/toyota+research+institute+explores+blockchain+technology.htm>

2017 1Qの動向 (2/3)

- Share&Charge、ethereumベースの充電ステーションアプリ開発
 - ドイツのエネルギーコングロマリットRWE社の子会社Innogy SEが数百箇所規模の充電ステーションをスマートモビリティスタートアップShare&Chargeと協働で立上げると発表。
 - ペイメント向けクリプトユーロを用いてシームレスな電気自動車充電をEthereum上で行う。
 - パブリックEthereumブロックチェーンをトランザクション層として活用することにより、スマートモビリティ向けシェアリングエコミーサービスを立ち上げる。
 - Share&Chargeは3つのタイプのスマートコントラクトを使用。
 - ①LibManager: コントラクトによって他コントラクトを参照し、既存コントラクトをバグフィックス時にアップデート可能とする
 - ②MobilityToken: 残高を保持し、規制面のフレームワークを可能とするERC20トークン。充電代金の支払はユーロにより裏づけられドイツ法による規制対応したデジタルトークンであり、Share&Chargeのアプリを通じて購入可能なMobilityTokenを用いて行われる。
 - ③ChargingPoles: 充電代金の登録簿として充電ステーションでの開始・停止オペレーション処理に必要なロジックを搭載。
 - <https://bitcoinmagazine.com/articles/innogy-charges-new-electric-car-fleet-using-ethereum-blockchain/>
 - <https://play.google.com/store/apps/details?id=com.shareandcharge.app>
 - <https://shareandcharge.com/sharecharge-smart-contracts-technical-angle/>

2017 1Qの動向 (2/3)

- TeneT、エネルギーグリッド管理を蘭・独で試行
 - TenneT、sonnen、VandebronおよびIBMが、オランダ・ドイツにおける電力グリッド管理向けブロックチェーン開発にむけて協働。
 - 分散エネルギーデバイスのパフォーマンス値の検証・記録プロセスは、IBMがHyperledger Fabricを用いて開発し、小規模バッテリーおよび電気自動車のトランザクションの検証可能性および透明性を確保する。
 - <https://www.tennet.eu/news/detail/tennet-unlocks-distributed-flexibility-via-blockchain/>

個別サービス

名称	サービス概略	URL
FreightWaves	トラック輸送のサプライチェーン	→ https://www.freightwaves.com/news/truck-fleets-and-blockchain
CreditStorage	CreditEaseによるサプライチェーン	→ http://www.coindesk.com/lending-giant-creditease-launches-blockchain-supply-chain-service/
PassLfix	小包のP2P宅配サービス	→ http://pacifics.org/
Foodblockchain	食品のサプライチェーントラッキング	→ http://www.foodblockchain.xyz/
GridX	ConsenSysが開発中の分散エネルギーマーケット	→ https://medium.com/gridx/gridx-the-future-of-energy-markets-da104c285363

6. シビックテック系

- ① 2017 第一四半期の動向
- ② 個別サービスリスト

2017 1Qの動向 (1/4)

- Nayuta、兵庫県とデータ流通マーケットの実験
 - ブロックチェーンを用いたデータ流通インフラシステムのプロトタイプを使って、売買を行う者同士の直接データ取引を実施。
 - 大型放射光施設「SPring-8」内の兵庫県放射光ナノテク研究所において、ブロックチェーン技術を使ったデータ流通の実験を行ったもの。
 - 兵庫県では、企業が持つSPring-8での測定データの有効活用を図り、企業の次世代材料開発を促進させるため、企業間で測定データとそれに付随する情報を流通させる新たな仕組みを検討中。
 - 各社がブロックチェーンノードをもち、データは所有者が自分で保持。
 - データを販売したい会社はハッシュ値・データ内容・データ価格などをブラウザで入力。
 - マーケットに上がっているデータ内容はサーバレスでリスト表示される。
 - 購入支持により、データが暗号化され転送、同時に支払が行われる仕組み。
 - [https://prtimes.jp/main/html/rd/p/000000007.000016959.html](https://prt看imes.jp/main/html/rd/p/000000007.000016959.html)
- Keychain、IoT認証セキュリティプラットフォーム開発へNEDOの支援
 - <http://www.jiji.com/sp/article?k=000000005.000021131&g=prt>

2017 1Qの動向 (2/4)

- 国連プロジェクトサービス機関（UNOPS）、利活用に向けた情報提供依頼を発出
 - <https://www.unops.org/ApplyBO/File.aspx/UNOPS-2017-RFI-Blockchain-001-2%20.pdf>
- 国連、ヨルダン資金援助むけにethereum用いて大規模試行
 - <http://www.coindesk.com/the-united-nations-just-launched-its-first-large-scale-ethereum-test/>
- 国連WFP、一万人のシリア難民へバウチャーを配布
 - <http://www.coindesk.com/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain/>
- UNHCR、難民むけに生体認証でのethereumペイメントシステム
 - <https://www.ethnews.com/un-integrates-irisguards-ethereum-payment-platform-for-refugees>

2017 1Qの動向 (3/4)

- ドバイ、英ObjectTechと協業で生体認証を組み合わせたデジタルパスポート計画
 - <http://www.coindesk.com/dubai-plans-gate-less-airport-security-using-blockchain-tech/>
- カナダのTransUnionとEquifax、ブロックチェーンアイデンティティネットワークの試行
 - <https://www.ethnews.com/blockchain-identity-network-being-tested-in-canada>
- Accenture、Microsoftと難民むけデジタルアイデンティティシステム開発
 - <https://www.cryptocoinsnews.com/accenture-microsoft-develop-global-ethereum-blockchain-digital-id/>
 - <http://www.bbc.com/news/technology-40341511>
- uPort、スイスZugでデジタルIDのパイロット利用を9月に実施
 - <https://www.ethnews.com/uport-announces-zug-digital-ethereum-id-pilot>
 - <http://cryptocurrencymagazine.com/?p=12638>

2017 1Qの動向 (4/4)

- MS Office、ドキュメント検証むけにStamperyのアドイン
 - Stamperyは、EthereumおよびBitcoinのブロックチェーンを用いてドキュメントの認証・検証を、API/ウェブページを介して行う。
 - ドキュメントのハッシュをパブリックブロックチェーンへ送ると、ハッシュデータはパブリックブロックチェーンに記録され、ドキュメントはハッシュを無効化せずに変更できない。
 - <https://news.bitcoin.com/microsoft-office-bitcoin-blockchain-upgrade/>
 - <https://www.microsoft.com/reallifecode/2017/04/10/stampery-blockchain-add-microsoft-office/>
- 広東省仏山市、公共サービスのトライアル
 - http://www.gov.cn/xinwen/2017-06/23/content_5204956.htm
- ウクライナ、BitFuryとeガバナンスで提携
 - <https://dcebrieff.com/ukraine-and-bitfury-group-partner-for-egovernance/>

個別サービス

名称	サービス概略	URL
AmPLY	子供むけデジタルアイデンティティ	→ http://amply.tech/
Zonafide	個人のアクティビティを証明	→ https://www.zonafide.net/
Civic	Rootstockと生体認証を組み合わせ、ビットコインブロックチェーンでアイデンティティ情報保護	→ https://www.civic.com/
Sovrin Foundation	アイデンティティ管理ツールIndy	→ https://www.sovrin.org/about/ → https://www.hyperledger.org/category/hyperledger-indy
Sphere	Airbitzと提携したアイデンティティ	→ http://www.sphre.co/
Nottar	ethereum上でドキュメント公証	→ https://nottar.io/
NuArca	投票や所有権記録むけ TransactChainを開発	→ http://nuarca.com/solutions
Patiantory	ethereumブロックチェーンへの医療記録ストレージ	→ https://patientory.com/
Factom Harmony	Factomによるモーゲージソリューション	→ https://www.factom.com/products/harmony
Resilience	分散型ベーシックインカム	→ https://gist.github.com/anonymous/541ed0bb4a7cbc66b499c04bd8352f68

7.金融機関系の動き

① 2017 第一四半期の動向

2017 1Qの動向 (1/6)

- イタリアの銀行コングロマリット、OpenTimestamps用いて取引データ検証
 - イタリアの銀行コングロマリットであるIntesa Sanpaoloは、トレーディングデータの検証を行うべく、データのレコードキーピングをブロックチェーンで試行。
 - DeloitteおよびEternity Wallと昨年から協業してテストしているが、このプロジェクトのコアはオープンソースのOpenTimestampsプロトコル（Peter Todd により開発され、Eternity Wallにより実装された）。
 - ビットコインブロックチェーンを用いてトランザクションのnotarizeを行い、参照用に記録の証跡を残す。
 - OpenTimestampsは、一つのビットコイントランザクション中に無数のタイムスタンプを組み合わせたことができる他、ビットコインのconfirmationを待たずに一秒ほどで第三者検証可能なタイムスタンプを生成可能。
 - <http://www.coindesk.com/intesa-sanpaolo-trade-data-bitcoin-blockchain/>
- BlockchainCapital、VCとして初めてトークン株式発行
 - <https://blockchaincapital.tokenhub.com/>
- 米DTCC、クレジットデフォルトスワップシステムをIBMと構築へ
 - <https://www.ethnews.com/dtcc-develops-blockchain-solution>

2017 1Qの動向 (2/6)

- 英Royal Mint、BitGoとブロックチェーンシステム開発
 - 2016年11月に、Royal MintとCME Groupが、インフラとしてブロックチェーンを用いたデジタルゴールド商品であるRoyal Mint Goldを発表。
 - このためのブロックチェーンの設計・開発にあたり、CMEはBitGoを選定。
 - ブロックチェーンはアルファテスト中であり、RMGむけトレーディングプラットフォームはAlphaPoint社の技術をベースとし、ローンチ間近とされる。
 - このデジタルアセットはRoyal Mintによりリザーブされた純金。
 - <https://blog.bitgo.com/building-the-blockchain-for-royal-mint-gold-cecb4ff6f329>
 - <http://www.royalmint.com/rmg>
- JPモルガン他、代理人投票システム構築
 - <https://www.ethnews.com/major-finance-companies-complete-blockchain-based-proxy-vote-solution>
- 全銀協、ブロックチェーン連携プラットフォーム基本構想を発表
 - <https://www.zenginkyo.or.jp/news/detail/nid/8042/>

2017 1Qの動向 (3/6)

- Bank of Canada、Jasperプロジェクトの結果を発表
 - R3 Cordaを用いてホールセールペイメントシステムを構築したフェーズ2について。
 - 分散型台帳により現行の中央集中システムに匹敵する便益を提供することは、現行バージョンの分散台帳技術ではできない。
 - クロスボーダートランザクションなどの金融市場インフラのエコシステムとの相互作業の中から今後メリットが見えてくるかもしれない、との結論づけ。
 - 六月末に詳細なホワイトペーパーが発行される予定。
 - <http://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf>
- カンボジア中央銀行、ペイメントインフラをHyperledger Iroha用いて開発
 - <http://www.econotimes.com/National-Bank-of-Cambodia-Soramitsu-partner-to-co-develop-Hyperledger-Iroha-blockchain-project-654992>
- JP Morgan Chase、GSやMorgan Stanleyに続きR3コンソーシアム脱退
 - <http://mobile.reuters.com/article/idUSKBN17T2T4>

2017 1Qの動向 (4/6)

- Citi、CitiConnect for Blockchainをローンチ
 - このサービスを用いた最初の接続先はNasdaqのプライベートマーケットエクステンジ。
 - Citi Treasury and Trade Solutionsを通じて、法人顧客むけにシームレスなペイメントサービスを提供する。
 - ChainのChainCoreは、CitiおよびNasdaqで稼働しており、今回の例は共有台帳上での業界横断ネットワーク構築を示すもの。
 - <https://blog.chain.com/chain-takes-citi-to-production-2c618e43375d>
- シンガポールMAS、デジタルシンガポールドルの検証プロジェクトUbinを完了
 - フェーズ1は、シンガポールドルをトークン化して、プライベートethereum上で銀行間送金するもの。
 - デジタルSGDの実装においては、クレジットリスクおよび流動性リスクを指摘。
 - <http://www.mas.gov.sg/~media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf>
- ロシア中銀、EthereumフォークのMasterchainのテスト準備へ
 - <http://www.coindesk.com/russian-central-bank-group-prepares-masterchain-ethereum-fork-testing/>

2017 1Qの動向 (5/6)

- Thomson ReutersのOracleサービス、BlockOne IQ
 - Smart Oracleを通じてマーケットデータを提供するもの。
 - OracleはウェブベースAPIとブロックチェーンを繋ぐアダプター機構。
 - このOracleを使うことで、ブロックチェーンアプリがThomsonReutersのデータにアクセスして自動処理に利用できる。
 - 現時点ではEthereumおよびCordaとのみ互換で、EEAやR3メンバー向けにリリース予定。
 - <https://www.thomsonreuters.com/en/press-releases/2017/june/thomson-reuters-releases-blockone-iq-into-blockchain-developer-community.html>
 - <https://blockoneiq.thomsonreuters.com/>
- IBM、欧州Digital Trade Chainコンソーシアムむけに中小企業トレードファイナンスシステム開発
 - <https://www-03.ibm.com/press/us/en/pressrelease/52706.wss>
- Daimler、プライベートEthereumで社債発行
 - <https://www.daimler.com/investors/refinancing/blockchain.html>

2017 1Qの動向 (6/6)

- 中国人民銀行、暗号通貨の研究ラボ開設し独自デジタル通貨のテスト
 - <http://bit-finance.com/pboc-opens-new-cryptocurrency-research-institute/>
 - <https://www.technologyreview.com/s/608088/chinas-central-bank-has-begun-cautiously-testing-a-digital-currency/>
- ABN AmroやING、Cordaによるコマーシャルペーパープロトタイプ
 - <http://www.coindesk.com/r3-completes-dlt-commercial-paper-prototype-bank-partners/>
- Swift、TownCrierオラクル用いたスマートコントラクトのトライアル完了
 - <http://www.coindesk.com/swift-completes-blockchain-smart-contracts-trial/>

8.金融系スタートアップの動き

- ① 2017 第一四半期の動向
- ② 個別サービスリスト

2017 1Qの動向

- BCCC、日本円に対して為替が安定した仮想通貨を志向した デジタルトークン社会実験において「Zen」の発行を開始
 - 対日本円為替安定した仮想通貨を作ることができるかに関する社会実験。
 - 時価1円に対応する1Zenを発行、発行時市場価格で日本円に交換して銀行口座保管。
 - 取引所ではZenを法定通貨・他仮想通貨と交換可能。
 - 発行先は提供サービス・製品にZen建てで価格を付けて取引可能。
 - http://bccc.global/ja/articles/20170410_jpyz.html
 - <http://bccc.global/ja/articles/20170705.html>
- テックビューロ、全銀協「ブロックチェーン連携プラットフォーム」にmijin製品情報提出
 - <http://mijin.io/ja/868.html>
- Colu、金融機関がデジタル通貨発行するためのオープンソースプロトコルをローンチ
 - <http://kabutan.jp/disclosures/pdf/20170627/140120170627417418/>
- インフォテリア、株主総会の議決権行使における実証実験完了
 - <http://kabutan.jp/disclosures/pdf/20170627/140120170627417418/>

個別サービス①

名称	サービス概略	URL
EquiBit	P2Pのエクイティ管理	→ http://www.livebitcoinnews.com/equibit-development-corporation-plans-launch-blockchain-based-mainstream-investment-products/
Fundchain	ファンド流通のバリューチェーン	→ http://fundchain.lu/ → http://www.thefundschain.com/
Blocksure	ethereumベースの保険	→ https://www.blocksure.com/
Sikoba	IOUベースの分散マネープラットフォーム	→ http://www.sikoba.com/
Exscudo	マルチカレンシーペイメントとチャット	→ https://channels.exscudo.com/
Bext360	Stellarを用いたロボットペイメント	→ https://techcrunch.com/2017/04/11/bext360-is-using-robots-and-the-blockchain-to-pay-coffee-farmers-fairly/
Provachain	Royal Mint Goldなどコモディティ商品トレードむけ分散台帳	→ https://www.provachain.com/#home
KYC chain	金融機関むけKYC	→ http://kyc-chain.com/

個別サービス②

名称	サービス概略	URL
BitcoinHivemind	予測市場スマートコントラクト	→ http://bitcoinhivemind.com/
BitCAD	分散トレードエンジンTectum	→ http://bitcad.me/
Bancor	セルフトレーディング型のスマートトークン	→ https://bancor.network/static/Bancor_Protocol_Whitepaper_en.pdf
Cofound.it	ICONOMIが立ち上げたスタートアップインキュベーター・プラットフォーム	→ https://cofound.it/en/
Swap	ethereum上でのトークントレーディングプロトコル	→ https://swap.tech/whitepaper
KYCstart	KYCチェック向けブロックチェーン	→ https://www.finextra.com/pressarticle/69173/deloitte-develops-blockchain-proof-of-concept-to-mutualise-kyc-checksleft
NVO	分散型取引プラットフォーム、New Venture Opportunities	→ https://nvo.io/
VALU	OpenAssetProtocolを用いて個人の株式に見立てたトークンをトレード	→ https://valu.is/

個別サービス③

名称	サービス概略	URL
Prism	Shapeshiftによるトラストレスなポートフォリオマーケットプラットフォーム	→ https://blog.prism.exchange/blog/introducing-prism-the-worlds-first-trustless-asset-portfolio-platform/
OmiseGo	ethereumベースの分散型取引所・ペイメントネットワーク	→ https://cdn.omise.co/omg/whitepaper.pdf → https://omg.omise.co/
dharma	ethereumベースのP2Pレンディング	→ https://dharma.io/
Vault	DappsやDAOむけ自律ペイメントスマートコントラクト	→ http://vaultcampaign.giveth.io/
Cofound	分散型VCエコシステム	→ https://cofound.it/
Omega One	取引所間トレードの分散自律実行プラットフォーム。取引所間の分散自動取引を通じた流動性提供サービス	→ https://omega.one/
TIX	トレードファイナンスプラットフォーム	→ https://tradeix.com/
Impak	ソーシャルインパクト向けトークンバンキング	→ https://impakfinance.com/home/

個別サービス④

名称	サービス概略	URL
Proveq	クラウドセールでの不正防止ソリューション	→ https://proveq.io/
Harbour	トークンアセット管理を目的としたクラウドセール投資むけDAO	→ https://harbour.tokenate.io/#Project
Seglos	分散自律トレーディングプラットフォーム	→ http://www.seglos.com/
Swarm Fund	分散投資プラットフォーム	→ https://www.swarm.fund/
Bankbox	ColuによるColored Coinを用いたデジタル通貨発行管理プラットフォーム	→ https://github.com/Colored-Coins/BankBox/blob/master/README.md
Istanbul BFT	台湾AMIS Trchnologiesが開発したQuorumむけEthereumコンセンサスアルゴリズム	→ https://github.com/ethereum/EIPs/issues/650

9. 参考資料リンク集

① 個別トピックリスト

トピックリスト①

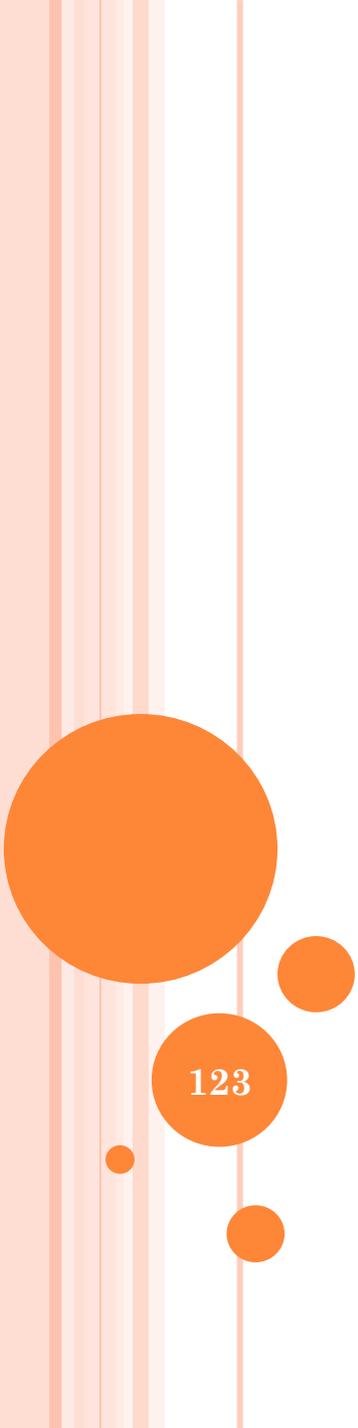
- 改正資金決済法リーフレット
 - <http://www.fsa.go.jp/common/about/20170403.pdf>
- Cryptocurrency Growth
 - <http://insight.jbs.cam.ac.uk/2017/cryptocurrency-growth/>
- Financial Crypto2017
 - <http://fc17.ifca.ai/bitcoin/schedule.html>
- "Rebooting the Web-of-Trust" イベント
 - 次世代の分散型web-of-trustベースのアイデンティティシステムを作ることを目指して、第4回DesignShopイベントが開催された。
 - <https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2017/tree/master/topics-and-advance-readings>
- プリンストン大学のコースシラバス
 - <http://www.cs.princeton.edu/courses/archive/spr17/cos518/syllabus.html>

お役に立てば嬉しいです

○ BTCアドレス

16ApP6FaD3CzzEBhK9PvSGVY1aafz6hciF





BITCOIN & BLOCKCHAIN概況

2017.07 by SATO

123

「Bitcoin2.0概況」「Blockchain2.0概況」から改題

第二部：ユースケースの系譜

過去9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
- **第9回 (2017年3月)** : 2016年12月～2017年3月の動き

201410

201501

201505

201508

201511

201604

201607

201612

201703

201707

TABLE OF CONTENTS

→ 今回は、第1回から全10回分の適用事例の系譜を再掲

1. プラットフォーム分野
2. ライフスタイル分野
3. サプライチェーン分野
4. シビックテック分野
5. 金融機関の動き
6. 金融系スタートアップの動き

1. プラットフォーム分野

2014/10紹介分

名称	サービス概略	URL
Ethereum	ブロックチェーンによるDapps開発基盤	→ https://www.ethereum.org/
Counterparty	ブロックチェーン上でフリーP2Pマーケットや金融機関のP2Pトレーディングを可能にするオープンソースソフト	→ https://counterparty.io/
MaidSAFE	分散クラウドストレージサービス	→ https://maidsafe.net/
Storj	分散クラウドストレージサービス	→ https://storj.io/

2015/01紹介分

名称	サービス概略	URL
Factom	<p>ブロックチェーンに記録されたデータを格納するための分散的なハッシュテーブルを利用する独自ノードの独立したネットワーク。</p> <p>ブロックチェーン上に、改変不可能なデータ記録のレイヤーを構築。文書・議事録・特許・公文書・契約書などが、間違いなくその時に作られて、あとから改ざんされていない、その時にあったことを証明する役割を、電子的に行う。</p>	<p>→ http://factom.org/</p> <p>→ http://www.factom.jp/</p>
Zennet	分散型コンピューティングネットワーク	→ http://www.zennet.sc/

2015/05紹介分

名称	サービス概略	URL
nem	PoIアルゴリズム (Proof-of-importance) によるP2Pのクリプトプラットフォーム	→ https://www.nem.io/
ADEPT	IoTのプラットフォーム作りにブロックチェーン技術を活用	→ https://www.ibm.com/services/us/gbs/thoughtleadership/internetofthings/

2015/08紹介分

名称	サービス概略	URL
BlockCypher	ブロックチェーンのAWSを標榜し、マイクロランザクションのAPI等を提供	→ https://www.blockcypher.com/
Sidechain Element	Sidechain Elementのソースコードとテスト環境を提供することで、新しい銀行システムに向けたプロトタイプ作り（ビットコインの機能拡張や、ブロックチェーンのアプリケーション）を促すもの	→ https://www.elementsproject.org/
Eris	Dapps開発プラットフォームとして、開発ツールを提供	→ https://monax.io/
Enigma	MITメディア・ラボが発表した、プライバシーを保証した分散コンピューティング	→ https://www.media.mit.edu/projects/enigma/overview/
21.Inc	ネット接続端末に組込可能な、Bitcoinマイニング専用チップ	→ https://21.co/buy/

2015/11紹介分

名称	サービス概略	URL
Blockstack.io	エンタープライズ・ブロックチェーン・プラットフォーム目指しソフトウェアスタックを提供	→ https://blockstack.io/
Multichain	ビットコインコアのフォークをベースとした、ユーザがPermittedユーザのリストを設定可能なPermissionedチェーン	→ https://www.multichain.com/
HydraChain	Ethereumベースの「Permissioned Distributed Ledger」	→ https://github.com/HydraChain/hydrachain
Tierion	ブロックチェーンへのデータ記録エンジン	→ https://tierion.com/chainpoint
Metaco	Colored Coinを用いたスマート・フィアットのブローキングおよびトレーディングのプラットフォームを開発	→ https://metaco.com/
Interledger (ILP)	銀行とブロックチェーンを繋ぐネイティブトークン無しのプロトコル	→ http://interledger.org/interledger.pdf
ConsenSys	Ethereumにフォーカスしたベンチャープロダクションスタジオ	→ https://consensys.net/about/

2015/11紹介分

名称	サービス概略	URL
mijin	「2018年までに金融機関のインフラコストを1/10未満に削減すること」をミッションとして、プライベートネットワークに特化したオリジナルコード。	→ http://mijin.io/
Orb	ブロックチェーン認証の分散クラウドコンピューティング	→ https://imagine-orb.com/
Deals4	カレンシーポートによる、ブロックチェーンを扱うときに使いやすいフレームワーク部分を提供するサービス	→ http://www.ccyport.com/
AIRA	DAOのマネジメントプラットフォームをEthereumベースでAIと組み合わせ提供	→ http://aira.life/
RootStock	Ethereumの世界とBitcoin Blockchainの世界をSidechainで繋ぐ	→ http://www.rsk.co/

2015/11紹介分

名称	サービス概略	URL
Tau-Chain	分散型P2Pネットワーク	→ http://tauchain.org/
Elliptic	ブロックチェーン上のトランザクションの出元と宛先を高いレベルで正確に特定し、マネロン対策を提供。グラフ画像解析および機械学習を用いた不正取引検出「THE BITCOIN BIG BANG」を運営。	→ https://www.elliptic.co/
Coinalytics (現在はSkry)	ブロックチェーンインテリジェンスツール「Blockstem API」を開発。ブロックチェーンの状態監視やトランザクション追跡。パターン認識や機械学習を用いたトランザクション承認アルゴリズム。	→ https://skry.tech/
Colony	DAOのプラットフォーム	→ http://colony.io/
Otonomos	「会社をアナログからデジタルへ」を標榜し、Online Formation、P2P Funding、スマートコントラクトによるAutomated Governanceを提供。	→ http://www.otonomos.com/

2015/11紹介分

名称	サービス概略	URL
Blocknet	<ul style="list-style-type: none">・異なるブロックチェーン上のノード間でP2Pサービスを可能に。・ブロックチェーンのインターネットを標榜。	→ http://blocknet.co/
BlockChainGroup.io	ブロックチェーンの分析を容易かつ情報量豊かなものにすべく、①BlockSearch、②BitRank、③Bitalyticsを提供	→ http://blockchaingroup.io/
Hawk	スマートコントラクトシステム。取引プライバシー保護すべくトランザクションをブロックチェーン上に格納せず、プライベート・スマートコントラクトを記述可能。	→ https://eprint.iacr.org/2015/675.pdf
Etherparty	スマートコントラクトの管理・実行向けPaaS	→ http://etherparty.io/

2016/04紹介分

名称	サービス概略	URL
Hyperledger Project	The Linux Foundationによるオープンソースの分散レジスターフレームワークの構築	→ https://www.hyperledger.org/
ロックオン	mijinを用いたEC用受注エンジンの実証実験	→ http://prtmes.jp/main/html/rd/p/000000013.000012906.html
OKWAVE	mijinを用いて知財販売の決済やユーザー認証、サポートキュー開発	→ http://www.okwave.co.jp/news/press_log/2016/0104.html
フィスコ	mijinを用いて情報配信の実証実験	→ http://mijin.io/ja/481.html
GMOインターネット	mijinを用いてゲーム用バックエンドエンジンを開発	→ http://mijin.io/ja/525.html
Intelの“Sawtooth Lake”	TEE (trusted execution environments) 上に構築する分散台帳プラットフォーム	→ https://intelledger.github.io/introduction.html
21 Marketplace	クレジットカード等なしにビットコインを用いて50以上のAPIを購入可能なマーケットプレイス	→ https://21.co/mkt/

2016/04紹介分

名称	サービス概略	URL
Guardtime	データセキュリティスタートアップ。 エストニアのeHealth Foundationと提携し、ヘルスケア記録のセキュリティを確保。 英国Future Cities Catapultと提携し、原発などの重要インフラ向けサイバーセキュリティソリューションの開発。	→ https://guardtime.com
MetaLair	分散システムセキュリティコンサル	→ http://www.metalair.org/
BlockSeer	ブロックチェーン分析	→ https://www.blockseer.com/
Chainalysis	ブロックチェーン分析	→ https://chainalysis.com/
TradeBlock	ブロックチェーン分析	→ https://tradeblock.com/

2016/04紹介分

名称	サービス概略	URL
Tradle	KYCを中心としたコンプライアンス	→ http://tradle.io/
UniquID	アイデンティティ・アクセス管理	→ uniquid.co
GNOSIS	予測市場	→ https://gnosis.pm/
Eternity Wall	メッセージ記録	→ https://eternitywall.it/
BigchainDB	スケーラブルなブロックチェーンDB	→ https://www.bigchaindb.com/
Cryptid	オープンソースのIDシステム	→ http://cryptid.xyz/
Lisk	分散アプリケーション開発プラットフォーム	→ https://lisk.io/

2016/07紹介分

名称	サービス概略	URL
Bloq	Blockchain Operating System (BOS) として BloqEnterpriseを発表	→ http://bloq.com/bloq-launches-bloqenterprise,-a-comprehensive-blockchain-operating-system-%28bos%29.html
Stratis	ブロックチェーン開発プラットフォーム	→ http://stratisplatform.com/
Microsoft	Azureの能力を活用して、オープンで独立性の高いブロックチェーンの構成要素を実現する「Bletchley」プロジェクト	→ https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md
Acronis	データタイムスタンプのプロトタイプ公開	→ http://www.acronis.com/en-sg/
ChainAchor	MITが検討している、検証可能だが匿名担保するアイデンティティ	→ http://connection.mit.edu/wp-content/uploads/sites/29/2014/12/Anonymous-Identities-for-Permissioned-Blockchains2.pdf
BTC Relay	Ethereumベースのネットワークを可能にするオープンソースプロジェクト	→ https://consensys.net/static/BTCRelay.pdf

2016/07紹介分

名称	サービス概略	URL
IPDB (Interplanetary Database)	BigchainDBが発表した、パブリックのブロックチェーンデータベース	→ https://ipdb.foundation/
Tierion (Hash API)	ブロックチェーンのデータにアンカリングするフリーAPIを公開 データプライバシーを維持しながら 監査証跡を生成する	→ https://tierion.com/blog/tierion-launches-free-api-to-anchor-data-in-the-blockchain/
Wings	ChainLabによるDAOむけプラットフォーム	→ https://wings.ai/

2016/12紹介分

名称	サービス概略	URL
Chronicled	EthereumベースのIoTレジストリ	→ http://chronicled.org/
ProofLog	ログストレージ	→ http://www.fina-sol.com/news/102485.html
Antshares	中国市場にフォーカスしたデジタルアセットプラットフォーム	→ https://www.antshares.org/zh-CN/Blog/Details/31
NEMアポステリーユ	アップデート可能な公証・タイムスタンプサービス	→ http://www.trendstream.net/bitcoin/nem-apostille-whitepaper-japanese-3171/
Zaica	仮想通貨やトークンの発行支援サービス	→ https://corp.zaif.jp/info/2807/
Raiden Network	Ethereumを用いたマイクロペイメント	→ http://raiden.network/

2016/12紹介分

名称	サービス概略	URL
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	→ http://www.coindesk.com/bitcoins-lightning-network-now-digital-asset-compatible/
ZRelay	ZCashとEthereumのリレー	→ https://github.com/ConsenSys/Project-Alchemy/blob/master/README.md
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	→ http://cloud.watch.impress.co.jp/docs/news/1025608.html
Onchain	Alibaba向けeメールエビデンスレポジトリ	→ https://coinreport.net/onchain-framework-alibaba-blockchain/
スイス国鉄	券売機でビットコイン販売	→ http://cryptocurrencymagazine.com/swiss-rail-operator-sbb-bitcoins
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	mijinの電子マネー分野への適用実証実験	→ http://knowledge.sakura.ad.jp/knowledge/6450/

2016/12紹介分

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/new-s-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	

2016/12紹介分

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/

2016/12紹介分

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=%2Fnetacgi%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/
Polkadot	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/

2017/03紹介分

名称	サービス概略	URL
NTumbleBit	TumbleBitの実装	→ https://medium.com/@nicolasdori er/tumblebit-tumbler-mode-ea44e9a2a2ec
Quorum	JPモルガンによるエンタプライズ版 Ethereum	→ https://www.jpmorgan.com/country/US/en/Quorum
Grin	MimbleWimbleの実装	→ https://github.com/ignopeverell/grin/blob/master/README.md
Catapult	一般的クラウド上で秒間3000以上を安定処理可能な高性能ブロックチェーンコア	→ https://www.nem.io/catapultwhitepaper.pdf
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/

2017/03紹介分

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/
Dfinity	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/
miyabi	独自コンセンサスアルゴリズムBKF2によるブロックチェーン	→ https://bitflyer.jp/pub/bitFlyer_miyabi-press_ja.pdf

2017/07紹介分

名称	サービス概略	URL
iEx.ec	クラウドコンピューティング・プラットフォーム	→ http://iex.ec/
Zeronet	ビットコインの暗号と、BitTorrentを使ったオープンネットワーク	→ https://zeronet.io/
Minebox	ディスク容量を貸出しSiacoinを稼げる分散クラウドストレージ	→ https://minebox.io/store
Agrello	法的・ITスキル不要でAIベースにスマートコントラクト生成するインターフェース（AIを用いたコントラクトジェネレーター）	→ https://www.agrello.org/
Mysterium	ブロックチェーンベースのVPN	→ https://mysterium.network/
Aragon	分散型組織マネジメントツール	→ https://github.com/aragon/aragon/releases
Prism	Shapeshiftがローンチを予定しているスマートコントラクトで構築	→ https://prism-launch.com/
BOScoin	トラストコントラクトを特徴とするプラットフォーム	→ https://boscoin.io/en/home/
Ivy Playground	Chainによるスマートコントラクト	→ https://chain.com/docs/1.2/ivy-playground/tutorial

2017/07紹介分

名称	サービス概略	URL
Tezos	DAOガバナンスによるブロックチェーン	→ https://tezos.com/
SONM	ネットワークマイニングによる分散型スパコン	→ https://sonm.io/
Aeternity	トラストレスステートチャネルを備えたスマートコントラクト	→ https://www.aeternity.com/ja
TrustedChain	European Trust Service Providersによるブロックチェーン	→ https://trustedchain.it/en/
CompCoin	トレーディングコンピュータの分散ネットワーク	→ https://compcoin.com/
Postchain	Chromaway社によるコンソーシアムデータベース	→ https://chromaway.com/products/postchain/
Swap	ethereumの分散型トレードプロトコル	→ https://swap.tech/
ConsenSys Diligence	ethereumエコシステム内のセキュリティベストプラクティス	→ https://medium.com/@c.diligence/
DIMCOIN	Data Interchange ModuleとしてNEM上エコシステムを目指す	→ https://www.dimcoin.io/

2. ライフスタイル分野

2015/01紹介分

名称	サービス概略	URL
TatianaCoin	初めてのアーティスト暗号通貨	→ http://tatianamoroz.com/tatiana-coin/
GetGems	独自コインのウォレットを組み込んだメッセンジャーアプリ	→ http://www.getgems.jp/
La'Zooz	分散型ライドシェアリング	→ http://lazooz.org/
Synereo	“Proof of attention”コンセプトに基づく暗号通貨ベースのSNS。ユーザーのプライバシーを極限まで尊重しつつ、ネットワーク参加へのインセンティブを生み出す新しいタイプのSNS	→ http://www.synereo.com/

2015/05紹介分

名称	サービス概略	URL
Augur	分散型の予測市場サービス	→ http://www.augur.net/
Spells Of Genesis	Counterpartyプラットフォームを利用し、ゲームと仮想通貨の融合を実現させるモバイルトレーディングカードゲーム	→ http://www.spellofgenesis.com/

2015/08紹介分

名称	サービス概略	URL
Streamium	分散型ストリーミングプラットフォームによる、ビットコイン版ライブチャット課金サービス	→ https://streamium.io/
Colu	Colored coinベースのブロックチェーンによるデジタルアセット管理	→ http://coloredcoins.org/
PopChest	アーティストへのリワード・マイクロペイメント	→ popchest.com
PeerTracks	ブロックチェーンを取引トランザクションに用いて、ストリーミングへの支払いに活用	→ http://peertracks.com/
Gyft Block	ギフトカードの交換プラットフォーム	→ https://block.gyft.com/

2015/11紹介分

名称	サービス概略	URL
BlockNotary	ブロックチェーン上に写真のデジタル指紋を格納	→ https://www.blocknotary.com/
Faradam	フリーランス向けマイクロペイメントサービス	→ https://faradam.com/
Bankymoon	アフリカ向けスマートメーター	→ http://bankymoon.co.za/
Ujo	Ethereumブロックチェーンベースの音楽P2Pプラットフォーム	→ https://ujomusic.com/ → https://consensys.net/static/UjoRelease.pdf

2015/11紹介分

名称	サービス概略	URL
UbiMS	消費者の需要シフトへの対応、商品の流れのコーディネートといったロジスティックス	→ http://www.ubims.com/
Etheria	Ethereumベースのゲーム	→ http://etheria.world/
LBRY	分散型コンテンツ流通システム	→ http://www.lbry.io/

2016/04紹介分

名称	サービス概略	URL
FreeMyVunk	ゲーム内アイテムを売買可能なマーケットを提供	→ http://www.freemyvunk.com/
インテル	ファンタジースポーツ分野でプレイヤーにゲーム内通貨“mikels”を付与し、発行したトークンを選手に紐付け、トークン取引（交換・売却）を可能に。	→ http://www.coindesk.com/intel-testing-blockchain-built-fantasy-sports-game/
AIRA	Ethereumスマートコントラクトを使ったドローンコントロールプロジェクト	→ http://aira.life/
MaskNetwork	分散マーケットプレイス	→ http://www.masknetwork.com/
DECENT	P2Pでコンテンツをシェアする分散型パブリッシュプラットフォーム	→ http://decent.ch/decent-whitepaper.pdf
Ampliative Art	アート作品に関する貢献&相互報酬のプラットフォーム	→ http://www.ampliativeart.org/
Mediachain	デジタルコンテンツを保護するアイデンティティ・認証プラットフォーム	→ http://www.mediachain.io/

2016/04紹介分

名称	サービス概略	URL
Satoshi Fantasy	フットボール向け予測市場	→ http://protoblock.com/
MUSE	CCEDKとOpenLedgerによるP2P音楽プラットフォーム	→ http://museblockchain.com/
Genecoin	DNAゲノム情報をブロックチェーン上にバックアップ	→ http://genecoin.me/
IBREA	登記やエスクロー等の不動産分野への応用	→ http://www.ibtcrea.org/
ArtCity	デジタルアートの安全管理	→ http://www.artcity.io/
cointemporary.com	デジタルアート売買プロジェクト	→ http://cointemporary.com/
ikono.tv	アートTVチャンネル。アーティストの権利確認にブロックチェーンを用い、どのアーティストの作品か著作権所有者を管理。	→ http://www.ikonotv.art/

2016/04紹介分

名称	サービス概略	URL
UPROOV	<ul style="list-style-type: none">書類だけでなく、写真・動画・オーディオまで対象とした、公証サービス。タイムスタンプをとってブロックチェーンに記録することで公証。各著作物にコードを付与し、著作物の識別、観覧制限が可能。	→ https://uproov.com/
Plantoid	ビットコインの寄付を使って自らを複製するブロックチェーンベースのロボット作品	→ http://www.plantoidproject.eu/

2016/07紹介分

名称	サービス概略	URL
Capgemini	BigchainDBを用いてロイヤリティプログラムを開発	→ http://bravenewcoin.com/news/capgemini-partners-with-ascribe-to-produce-loyalty-and-rewards-programs/
ドバイ	ドバイのグローバルブロックチェーンカウンシルが発表したパイロットプロジェクト	→ http://www.the-blockchain.com/2016/05/30/loyal-announces-blockchain-based-tourism-program-deal-dubai-future-foundation/
Fermat	P2Pシェアリングエコノミープラットフォーム	→ http://www.fermat.org/
ガイアックス	シェアリングエコノミー分野での応用を目指した本人確認サービスの実証実験	→ http://www.gaiax.co.jp/news/press/2016/04271/
Stem	クリエイターむけコンテンツ&報酬マネジメントプラットフォーム	→ https://stem.is/

2016/07紹介分

名称	サービス概略	URL
LBRY	クリエイターむけコンテンツシェアリングプラットフォーム	→ https://lbry.io/news
Akasha	EthereumとIPFSベースの次世代ソーシャルメディア	→ http://akasha.world/
Steemit	ブロックチェーンベースのソーシャルネットワーク	→ https://steem.io/SteemWhitePaper.pdf
Flip	P2Pリースマーケットプレイス	→ https://flip.lease/
APPII	求職者のキャリアプロフィールの検証を可能とするスマートコントラクト	→ http://www.appii.io/
リクルートテクノロジーズ	ascribeと協力し履歴書公証データベースのプロトタイプ開発	→ http://recruit-tech.co.jp/news/images/20160425_PressRelease.pdf

2016/07紹介分

名称	サービス概略	URL
Sweatcoin	トレーナー購入や運動クラス受講に対応するデジタル通貨	→ http://sweatco.in/
DAISEE	Internets of Energyを目指す	→ http://daisee.org/
Ion	モバイルゲームむけコイン	→ https://ionomy.com/
Paymeabit	ビットコインによるオンラインコンテンツ向けマイクロランザクション	→ http://www.paymeabit.com/
Yope	初期購入時に自転車の所有権台帳を登録するEtehereumベースブロックチェーン	→ http://www.yope.io/
Dot Blockchain Music Inc	ミュージシャンや音楽制作に携わる人がフェアに権利を主張できるプラットフォーム	→ http://dotblockchainmusic.com/

2016/12紹介分

名称	サービス概略	URL
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	→ https://blog.brave.com/introducing-brave-payments/
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	→ https://engineering.yours.network/
Project ORB	ブロックチェーンゲームプラットフォーム	→ http://www.spellsofgenesis.com/play/
ビットガールズ	ICOプランとしてトークン売り出し	→ http://bitgirls.io/ja/

2016/12紹介分

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/
SingularDTV	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/

2017/03紹介分

名称	サービス概略	URL
VALU	OpenAssetProtocolを用いて個人の株式に見立てたトークンをトレード	→ https://valu.is/
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/
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/
モッピーGO	IndieSquareとセレスによる位置情報とトークンの活用サービス	→ http://host211006211247.stockdatabank.jp/tdnet/data/20170210/140120170210496251.pdf

2017/03紹介分

名称	サービス概略	URL
Project Oaken	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
Chain of Points	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	→ https://chainofpoints.com/cop_whitpaper.pdf
Creativechain	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	→ http://creativechain.org/wp-content/uploads/2017/03/Whitepaper-Creativechain-1.2.pdf
21 lists	ビットコインを使った有料linkedinサービス	→ https://medium.com/@21/get-replies-from-vcs-and-ceos-with-21-lists-663f2a8d8b9e
adChain	オンライン広告産業むけプラットフォーム	→ http://www.prweb.com/releases/2017/01/prweb14009259.htm
Basic Attention Token	オンライン広告産業むけプラットフォーム	→ https://basicattentiontoken.org/

2017/03紹介分

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/

2017/07紹介分

名称	サービス概略	URL
VALU	OpenAssetProtocolを用いて個人の株式に見立てたトークンをトレード	→ https://valu.is/
Voise	分散ミュージックプラットフォーム	→ https://voise.it/
Zimrii	ミュージックプラットフォーム	→ http://www.zimrii.com/
DigitalGarage	クレディセゾン・Blockstreamとロイヤリティポイント	→ https://cointelegraph.com/news/bitcoin-blockchain-to-help-collect-customers-activate-consumption-in-japan
Global Miles	マイレージプログラム	→ http://www.globalmiles.com/en/
Civil	分散ジャーナリズム	→ http://joincivil.com/
Charitychain	チャリティファンドレイジング	→ https://github.com/charitychain-io/v0/blob/master/Charitychain.sol
Curation Markets	トークンによるキュレーション・コラボレーション	→ https://docs.google.com/document/d/1VNkBjjGhcZUV9CyC0ccWYbqeOoVKT2maqX0rK3yXB20/mobilebasic
Babel	分散型eコマースプラットフォーム	→ https://billh93.github.io/babel/
Aventus	イベントチケット	→ https://aventus.io/

2017/07紹介分

名称	サービス概略	URL
Indorse	分散型ソーシャルネットワーク	→ http://www.indorse.io/
Status	モバイルメッセージング	→ https://status.im/
Kin	チャットプラットフォームKikむけのERC20ベース暗号通貨	→ https://kin.kik.com/
Qrator	Synereoによるアテンションエコノミーアプリ	→ https://blog.synereo.com/2017/04/03/synereo-announces-qrator-the-first-liberated-attention-economy-application/
District0x	分散マーケットコミュニティのネットワーク	→ https://district0x.io/
AdEx	分散ウェブ広告マーケット	→ https://www.adex.network/adex/AdEx-Whitepaper-v1.4.pdf
AT&T	ホーム加入者サーバー (HSS) 領域で特許	→ http://www.coindesk.com/att-awarded-patent-bitcoin-powered-subscriber-server/
21 lists	マイクロコンサルティングを可能にする21 incのサービス	→ https://21.co/lists/
SkinCoin	ゲームアセットのマネタイズ向け分散マーケット	→ https://skincoin.org/

3. サプライチェーン系

2015/01紹介分

名称	サービス概略	URL
OpenBazaar	分散型マーケットプレイス	→ https://openbazaar.org/

2015/05紹介分

名称	サービス概略	URL
Provenance	ブロックチェーンを用いて商品のサプライチェーンをトラッキング。ビデオ・イメージを通じて、プロダクトのストーリーを伝えるプラットフォーム。	→ https://www.provenance.org

2015/08紹介分

名称	サービス概略	URL
Ascribe	アート作品などの著作権管理にブロックチェーンを適用	→ https://www.ascribe.io/
Everledger	ダイヤモンドの所有権証明・トランザクション履歴証明	→ http://www.everledger.io/
Verisart	アート作品の証明にビットコインを用いる	→ https://www.verisart.com/
BlockVerify	偽造薬の撲滅を通じサプライチェーン上の偽物を防ぐ	→ http://blockverify.io/

2015/11紹介分

名称	サービス概略	URL
Filament	ブロックチェーンのパブリック台帳上にデバイスのユニークIDを保持する分散IoTソフトウェアスタックを提供	→ https://filament.com/
Tilepay	ユーザがIoTデバイスのデータにアクセスコントロールできるマイクロペイメントプラットフォーム	→ http://www.tilepay.org/
Slock.it	スマートコントラクトを用いた金庫で資産を貸出・売却・共有 • スマホを通じてコントロール可能な「スマートロック」を提供 • EthereumベースのIoTプラットフォーム・IoTデバイス	→ http://slock.it/

2016/04紹介分

名称	サービス概略	URL
Tradechain	<ul style="list-style-type: none">台湾のDigital Treasury Corporation (DTCO) が発表。デジタル署名や取引の透明性確保にブロックチェーンを利用する「green enterprising certification service」。農業や医薬品をターゲット。	→ https://tradechain.co/
tallysticks	<ul style="list-style-type: none">インボイス・リコンサイル	→ https://tallysticks.io/
Cargochain	<ul style="list-style-type: none">国際貿易における輸出入業者・海運会社・税関むけ情報をEthereum上で実施。	→ https://github.com/domschiener/cargochain
OpenBazaar	<ul style="list-style-type: none">特定のサーバが存在しない分散マーケット	→ https://openbazaar.org/
Chronicle	<ul style="list-style-type: none">スニーカー収集における存在証明	→ http://www.chronicle.com/

2016/04紹介分

名称	サービス概略	URL
Warranteer	<ul style="list-style-type: none">Coluを使った製品ワランティ	→ http://www.warranteer.com/
Wave	<ul style="list-style-type: none">B/Lによる輸入手続きといった国際貿易分野への応用貿易書類のペーパーレス化	→ http://wavebl.com/
Skuchain	<ul style="list-style-type: none">IoTむけブロックチェーンリサーチのChain of Thingsと提携IoTをトレードファイナンスに活用することによって、温度センサーがSkuchainへ信号情報を伝達し、スマートコントラクト上のイベントを起動することを可能に。	→ https://skuchain.com/

2016/04紹介分

名称	サービス概略	URL
BlockCharge	<ul style="list-style-type: none">ドイツの大手電力会社RWEとSlockの電気自動車のチャージステーション実証実験	→ http://www.coindesk.com/german-utility-company-turns-to-blockchain-amid-shifting-energy-landscape/
Nayuta	<ul style="list-style-type: none">使用权コントロール可能な電源ソケットのプロトタイプ	→ http://nayuta.co/wp-content/uploads/pressrelease20151228.pdf
IOTA	<ul style="list-style-type: none">IoTむけマイクロトランザクション暗号トークン分散合意形成のコンセプトは引き継ぐものの、ブロックチェーンは使わない軽量Tangle構造（非循環有向グラフ）	→ https://iota.org/

2016/07紹介分

名称	サービス概略	URL
SingularDTV	<ul style="list-style-type: none"> ConsenSysと提携し、フィルム向け権利管理プラットフォームを構築。 	<ul style="list-style-type: none"> → https://singulardtv.com/update/consensyspartnership → https://consensys.net/static/Singular.pdf
Artprice	<ul style="list-style-type: none"> アートマーケット向けブロックチェーンプロジェクトを発表。 	<ul style="list-style-type: none"> → http://www.prnewswire.com/news-releases/bpi-labelled-artprice-announces-its-blockchain-project-for-the-art-market-578785081.html
ArtTracktive	<ul style="list-style-type: none"> Deloitteによるアート業界向けユースケース。 アート作品の来歴を管理することで、作品のライフサイクル全般の記録およびトラッキングを可能に。 	<ul style="list-style-type: none"> → https://www2.deloitte.com/lu/en/pages/technology/articles/blockchain-proof-concept-solve-traceability-issues-art.html
Emercoin	<ul style="list-style-type: none"> ロシアの時計メーカー向けの偽造防止プラットフォーム。 時計のほか、車両番号、不動産登記、ソフトウェアライセンスキーなどへの適用。 	<ul style="list-style-type: none"> → http://blockchain-finance.com/2016/06/08/emercoin-provides-blockchain-platform-to-russian-watch-factory-to-fight-counterfeiting/

2016/07紹介分

名称	サービス概略	URL
米郵政公社	配送乗務に用いるトラックの追跡にブロックチェーンを用いる事で監視を行い問題検出	→ https://www.uspsaig.gov/sites/default/files/document-library-files/2016/RARC-WP-16-001.pdf
Kouvola市	インテリジェント・コンテナ「SmartLog project」	→ https://www-304.ibm.com/events/tools/interconnect/2016ems/REST/presentations/PDF/InterConnect2016_7271.pdf

2016/12紹介分

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
FreshTurf	宅配荷物のトラッキングを行うストレージロッカー	→ 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	→ https://www.finextra.com/pressarticle/66661/walmart-to-apply-blockchain-to-supply-chain
ISID	GuardTimeと地方創生を支援する研究プロジェクト立上	→ 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	→ http://www.autobacs.co.jp/images/data/news/2016/11/16/2ohL28.pdf

2016/12紹介分

名称	サービス概略	URL
Marin Transport 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
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/
CryptoSeal	Chronicledが開発した暗号 化密封	→ http://www.chronicled.com/download/CryptoSeal-Datasheet.pdf

2017/03紹介分

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
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
Manifestプロジェクト	マイクロソフトによるプロダクトトラッキング	→ https://www.ethnews.com/microsoft-project-manifest-blockchain-product-tracking
Digital Trade Chain	HSBC等によるトレードファイナンスコンソーシアム	→ http://www.ibtimes.co.uk/deutsche-bank-hsbc-five-other-big-banks-form-digital-trade-chain-consortium-1601259

2017/07紹介分

名称	サービス概略	URL
FreightWaves	トラック輸送のサプライチェーン	→ https://www.freightwaves.com/news/truck-fleets-and-blockchain
CreditStorage	CreditEaseによるサプライチェーン	→ http://www.coindesk.com/lending-giant-creditease-launches-blockchain-supply-chain-service/
PassLfix	小包のP2P宅配サービス	→ http://pacifics.org/
Foodblockchain	食品のサプライチェーントラッキング	→ http://www.foodblockchain.xyz/
GridX	ConsenSysが開発中の分散エネルギーマーケット	→ https://medium.com/gridx/gridx-the-future-of-energy-markets-da104c285363
TeneT	エネルギーグリッド管理を蘭・独で試行	→ https://www.tennet.eu/news/detail/tennet-unlocks-distributed-flexibility-via-blockchain/
Share&Charge	ethereumベースの充電ステーションアプリ	→ https://shareandcharge.com/
トヨタ	将来の自動車開発に向けたブロックチェーン利用をMIT Media Lab他と共同で行うことを発表	→ http://corporatenews.pressroom.toyota.com/releases/toyota+research+institute+explores+blockchain+technology.htm

4. シビックテック系

2015/01紹介分

名称	サービス概略	URL
BitNation	政府サービスをdecentralizedな方法によって、アイデンティティやベーシックインカムをブロックチェーンベースで提供。 土地権利などの記録や、婚姻・遺言・出生届などの契約を記録。	→ https://bitnation.co/

2015/05紹介分

名称	サービス概略	URL
Blockchain Health	電子カルテ（EMR : Electronic Medical Record）の記録 処方箋などのドキュメント公証人 サービス デジタル・ヘルス・ウォレット	→ https://blockchainhealth.co/

2015/08紹介分

名称	サービス概略	URL
OneName	ブロックチェーンベースのIDサービス、PassCardを提供	→ https://onename.com/
ShoCard	ブロックチェーンベースのアイデンティティ証明	→ https://shocard.com/
Factom	ホンジュラスで土地登記に活用	→ http://cryptocurrencymagazine.com/factom-honduras-partnership
GroupCurrency	メンバーにベーシックインカムや、グループのファンドに関する投票権を提供する暗号通貨	→ https://groupcurrency.org/
Neutral Voting Bloc (Flux)	投票参加者による投票結果に基づき政治行動を行うPoliticalアプリ	→ http://nvbloc.org/

2015/11紹介分

名称	サービス概略	URL
Alexandria	The People's Library (An open-source decentralized library) を目指す、Blocktech社のプロジェクト	→ http://blocktech.com/ → https://github.com/dloa/alexandria-docs
Follow My Vote	オンライン投票	→ https://followmyvote.com/
The World Table	評価コメントシステム	→ https://www.worldtable.co/
米コネチカット州	Tierionと共に政府調査の記録にブロックチェーン活用	→ http://www.coindesk.com/connecticut-non-profit-uses-blockchain-tech-for-government-project/
Tradle	KYC要件への対応	→ https://tradle.io/
Funderbeam	スタートアップ向け投資プラットフォーム (Colored Coinを用いたトレードプラットフォーム)	→ https://www.funderbeam.com/marketplace

2015/11紹介分

名称	サービス概略	URL
Sia	分散クラウドストレージ	→ http://sia.tech/ → http://www.sia.tech/sia.pdf
Stampery	ドキュメント公証人サービス	→ https://stampery.com/
TransActive Grid	近隣住民に再生可能エネルギーの相互売買を可能にするプラットフォーム	→ http://transactivegrid.net/

2016/04紹介分

名称	サービス概略	URL
エストニア	Bitnationとコラボレーションし、パブリックノタリーサービス	→ https://bitnation.co/blog/pressrelease-estonia-bitnation-public-notary-partnership/
エストニア	Guardtimeと提携し、100万人規模の健康記録データの管理に利用	→ http://www.ibtimes.co.uk/gem-prescribes-blockchain-solutions-healthcare-sector-1548862
Flux	ブロックチェーン投票による直接民主制を目指す	→ https://voteflux.org/
Factom	中国におけるスマートシティの権利管理、監査、公証サービス	→ http://www.factom.com/ancun-and-factom-inc-announce-a-mou-for-the-integration-of-blockchain-technology-and-traditional-notarization-services-in-china/
ウクライナ	Ethereumベースの「E-VOX」を用いた投票プラットフォーム	→ http://forklog.net/elections-in-ukraine-may-run-on-ethereums-blockchain/

2016/04紹介分

名称	サービス概略	URL
Open Trade Docs (OtDocs)	書類に書きこまれたデータの改ざん防止	→ http://otdocs.com/
Arcade City	ライドシェアリングサービス。 Ethereumを用いて暗号エクイティを発行することによって、ドライバーが会社所有者になることが可能に。	→ https://arcade.city/
Grid Singularity	新興国のソーラーエネルギーのPay-as-you-goを目指し、エネルギートランザクション認証を実験中	→ http://gridsingularity.com/

2016/07紹介分

名称	サービス概略	URL
Gem Health Network	GemがPhilips Blockchain Labと共同でヘルスケア向けブロックチェーン	→ https://gem.co/health
ケンブリッジ大学	新薬の開発における臨床試験データの修正防止	→ http://www.eurekalert.org/pub_releases/2016-05/fo1-dub051116.php
ドバイの通信会社 Du	ヘルスケア向けID認証システム	→ http://themerple.com/major-dubai-telecom-company-du-experiments-with-blockchain-technology/
米デラウェア州	法人登記プロセス向上に活用	→ https://www.cryptocoinsnews.com/delaware-governor-announces-plan-to-embrace-blockchain-in-public-and-private-ventures/
米バーモント州	ブロックチェーン上でタイムスタンプされた文書を、通常のビジネス文書と同様に扱う法案	→ http://dcebrief.com/vermont-breaks-new-ground-in-cryptocurrency-technology/

2016/07紹介分

名称	サービス概略	URL
Bitland	ガーナで土地登記システム	→ http://www.prnewswire.com/news-releases/new-blockchain-initiative-bitland-is-putting-land-on-the-ledger-in-ghana-300269491.html
スウェーデン	不動産登記情報の登録・記録	→ http://chromaway.com/landregistry/
SITA Digital Traveler Identity App	ShoCardと協業でデジタルアイデンティティのPoCを開発	→ http://www.sita.aero/solutions-and-services/solutions/sita-smart-path
Microsoft	ConsenSysおよびBlockstack Labsとオープンソースのアイデンティティシステム	→ https://azure.microsoft.com/en-us/blog/what-does-identity-mean-in-today-s-physical-and-digital-world/
MITメディアラボ	ビットコインブロックチェーンを使って学位認定	→ http://certificates.media.mit.edu/
MIT	文化遺産保護のため暗号学的遺産を提唱	→ http://www.newsbtc.com/2016/04/24/mit-explores-cryptographic-heritage-solutions-bitcoin-blockchain/

2016/07紹介分

名称	サービス概略	URL
米国防高等研究 計画局 (DARPA)	ブロックチェーンをベースとした暗号 化メッセージアプリに関心	→ http://www.coindesk.com/darpa-seeks-blockchain-messaging-system-for-battlefield-back-office-use/
英国連邦	クロスボーダー犯罪捜査における コラボレーション促進および証拠 収集	→ http://thecommonwealth.org/media/press-release/commonwealth-announces-new-app-fight-cross-border-crime
英国政府	ブロックチェーン活用による税収効 率化	→ https://zuoonline.com/archives/105326
英国政府	社会福祉ペイメントとして GovCoin	→ http://www.financemagnates.com/cryptocurrency/news/uk-tests-blockchain-based-social-welfare-payments-govcoin/
ウクライナ	政府発行ライセンスや、不動産な どを対象とした世界初のブロック チェーンオークショ	→ http://www.newsbtc.com/2016/07/04/ukraine-host-worlds-first-blockchain-based-auction/?platform=hootsuite
スイスZug	公共サービスむけ支払いにビットコ インを受入れ	→ http://cryptovalleyzug.net/

2016/07紹介分

名称	サービス概略	URL
Bitland	アフリカガーナにおける土地登記	→ http://www.bitland.world/ → http://www.bitland.world/wp-content/uploads/2016/03/Bitland_Whitepaper.pdf
Bitsoko	アフリカガーナにおける土地登記およびデジタルガバメントペイメント。Bill & Melinda Gates Foundationからも注目されている送金プラットフォーム。	→ http://bitsoko.com.gh/
Clipperz	ブロックチェーン上で知財管理・保護	→ https://clipperz.is/
ProofOfYou	契約や法律関連文書の作成・締結を行うEthereumベースのプラットフォーム（エストニア）	→ http://www.proofofyou.com/
MedRec	患者のヘルスケアデータを管理する、ヘルスケアプロバイダー横断の医療レコード管理システム	→ http://www.pubpub.org/pub/medrec
Hullcoin	ポジティブなソーシャルアクション（ボランティア）に対してリワードを与え、ローカル経済をサポート	→ http://www.theguardian.com/cities/2016/apr/22/hullcoin-bitcoin-volunteers-new-way-pay

2016/07紹介分

名称	サービス概略	URL
DNA.bits	<ul style="list-style-type: none">イスラエルの医療データ向け Permissionedブロックチェーンサービス。安全性・真正性・匿名性を担保しつつ医療情報をタグ付け・トラッキング・クロスレファレンス。	→ http://socialm1.wix.com/dnabits
IBREA (International Blockchain Real Estate Association)	不動産向けブロックチェーン適用を検討	→ http://www.ibtcrea.org/
Flip	ビットコインのブロックチェーンに不動産リース契約レポートを格納	→ https://flip.lease/
REX	Ethereum上で分散型P2P不動産プラットフォーム	→ http://www.rexmls.com/blog/ → http://rexmls.com/
BrikShares	不動産プロジェクト向けのファンド構築プラットフォーム	→ http://www.brikshares.com/
Prescrypt	慢性疾患患者が処方箋を安全入手。REshape Center for Innovationが、SNS Bank および Deloitteと協業	→ http://prescrypt.com/

2016/07紹介分

名称	サービス概略	URL
Cleverent	Multichainを用いて不動産リースや購入のリーガルドキュメントのタイムスタンプ・検証を行う、フルサービス不動産サービスアプリ	→ http://cleverent.com/
D-Cent	分散型民主主義を目指すプラットフォーム	→ http://dcentproject.eu/
Backfeed	分散型組織むけソーシャルオペレーティングシステム	→ http://backfeed.cc/
Helperbit	P2Pによる自然災害むけ援助	→ http://www.helperbit.com/
WISeKey	デジタルアイデンティティの認証プラットフォーム	→ https://www.wisekey.com/
Distributed ID (DIID)	IDの「Verification」「Notarization」「Retrieval & Authentication」および「Hash Checks」を行う	→ http://devpost.com/software/distributed-id-diid
Borderless.Tech	DappsプラットフォームのExpanseによる分散型ガバナンスサービス。市民権、アイデンティティ、公証、婚姻などに適用可	→ http://www.expanse.tech/ → http://www.borderless.tech/docs/BorderlessWhitepaper.pdf

2016/12紹介分

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/

2017/03紹介分

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/#/
Anonymous Voting	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/
ButFury	Georgia共和国で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

2017/03紹介分

名称	サービス概略	URL
Digipolis	Antwerp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
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/
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://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
ABN Amro	企業不動産取引	→ http://bravenewcoin.com/news/abn-amro-launches-pilot-blockchain-application-for-commercial-real-estate/

2017/03紹介分

名称	サービス概略	URL
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
REIDAO	不動産所有権をデジタル化	→ http://www.reidao.io/

2017/07紹介分

名称	サービス概略	URL
国連	ヨルダン資金援助むけに ethereum用いて大規模試行	→ http://www.coindesk.com/the-united-nations-just-launched-its-first-large-scale-ethereum-test/
国連WFP	一万人のシリア難民へ Ethereumを用いてバウチャーを 配布	→ http://www.coindesk.com/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain/
UNHCR	難民むけに生体認証での ethereumペイメントシステム	→ https://www.ethnews.com/un-integrates-irisguards-ethereum-payment-platform-for-refugees
Nayuta	兵庫県とデータ流通マーケットの 実験	→ https://prtnews.jp/main/html/rd/p/000000007.000016959.html
Keychain	IoT認証セキュリティプラットフォーム開発へNEDOの支援	→ http://www.jiji.com/sp/article?k=000000005.000021131&g=prt

2017/07紹介分

名称	サービス概略	URL
Microsoft	MS Office、ドキュメント検証むけにStamperyのアドイン	→ https://news.bitcoin.com/microsoft-office-bitcoin-blockchain-upgrade/
広東省仏山市	公共サービスのトライアル	→ http://www.gov.cn/xinwen/2017-06/23/content_5204956.htm
ウクライナ	BitFuryとeガバナンスで提携	→ https://dcebrieff.com/ukraine-and-bitfury-group-partner-for-egovernance/
ドバイ	生体認証を組み合わせたデジタルパスポート計画	→ http://www.coindesk.com/dubai-plans-gate-less-airport-security-using-blockchain-tech/
TransUnionとEquifax	ブロックチェーンアイデンティティネットワークの試行	→ https://www.ethnews.com/blockchain-identity-network-being-tested-in-canada
Accenture	Microsoftと難民むけデジタルアイデンティティシステム開発	→ http://www.bbc.com/news/technology-40341511
uPort	スイスZugでデジタルIDのパイロット利用	→ http://cryptocurrencymagazine.com/?p=12638

2017/07紹介分

名称	サービス概略	URL
AmPLY	子供むけデジタルアイデンティティ	→ http://amply.tech/
Zonafide	個人のアクティビティを証明	→ https://www.zonafide.net/
Civic	Rootstockと生体認証を組み合わせ、ビットコインブロックチェーンでアイデンティティ情報保護	→ https://www.civic.com/
Sovrin Foundation	アイデンティティ管理ツールIndy	→ https://www.sovrin.org/about/ → https://www.hyperledger.org/category/hyperledger-indy
Sphere	Airbitzと提携したアイデンティティ	→ http://www.sphre.co/
Nottar	ethereum上でドキュメント公証	→ https://nottar.io/
NuArca	投票や所有権記録むけ TransactChainを開発	→ http://nuarca.com/solutions
Patiantory	ethereumブロックチェーンへの医療記録ストレージ	→ https://patientory.com/
Factom Harmony	Factomによるモーゲージソリューション	→ https://www.factom.com/products/harmony
Resilience	分散型ベーシックインカム	→ https://gist.github.com/anonymous/541ed0bb4a7cbc66b499c04bd8352f68

5.金融機関系の動き

2015/05紹介分

名称	サービス概略	URL
Bank of England	銀行間取引のインフラ、中央銀行発行の法定デジタル通貨として発行手段として	→ http://www.bankofengland.co.uk/research/Documents/onebank/discussion.pdf
米メロン銀行	行内の報酬プログラムとしてのコイン発行で実験	→ https://coinreport.net/bank-new-york-mellon-experimenting-bitcoin/

2015/08紹介分

名称	サービス概略	URL
エストニアLHV銀行	ColoredCoinによる送受金可能なウォレットプラットフォームCuber	→ http://cryptocurrencymagazine.com/estonia-lhv-bank
Citi	クロスボーダー決済向けCitiCoin	→ http://www.ibtimes.co.uk/codename-citicoin-banking-giant-built-three-internal-blockchains-test-bitcoin-technology-1508759

2015/11紹介分

名称	サービス概略	URL
UBS	金融機関どうしのPostトレード決済に使われるUtility Settlement Coin	→ http://www.ibtimes.co.uk/clearmatics-robert-sams-talks-about-ubs-backed-settlement-coin-aversion-tokens-1519263
UBS	多くの債券チェーン・デリバティブチェーンが出た先を見据えたSidechainもちいたマルチアセットチェーンの構想	→ http://www.ibtimes.co.uk/ubs-reveals-its-interest-sidechains-well-ethereum-1519706
Rabobank	Ethereumを用いたスマートキャッシュウォレットにより、コインやロイヤリティポイント・クーポンのやりとりをするグループペイメント実験	→ http://www.ibtimes.co.uk/ubs-reveals-its-interest-sidechains-well-ethereum-1519706
Nasdaq	未公開株式取引システムLinq	→ http://www.nasdaq.com/press-release/nasdaq-announces-inaugural-clients-for-initial-blockchainenabled-platform-nasdaq-linq-20151027-00986
VISA	駐車場や自動車保険、カーリースのような従量課金サービスを、ブロックチェーンを用いて管理する新サービスのプロトタイプアプリ	→ http://www.coindesk.com/visa-docusign-car-lease-proof-of-concept-bitcoin/

2016/04紹介分

名称	サービス概略	URL
R3	サードパーティーのクリアリングハウスやセトルメントハウス無しに4大陸横断の銀行間セトルメント	→ http://r3cev.com/press/2016/1/20/r3-brings-eleven-major-global-financial-institutions-together-on-a-cloud-based-distributed-ledger
R3	40行との間で債券の発行・トレード・償還におけるスマートコントラクト	→ http://www.nytimes.com/reuters/2016/03/02/business/02reuters-banking-blockchain-bonds.html
住信SBIネット銀行	NEMおよびMijinを利用し、将来の基幹・業務システム構築を目的とした実証実験	→ https://www.netbk.co.jp/wpl/NBGate/i900500CT/PD/corp_news_20151216
東京三菱UFJ銀行	行内通貨「MUFGコイン」を開発中との報道	→ http://www.asahi.com/articles/ASJ1W4RWKJ1WULFA012.html
みずほFG	カレンシーポートと協働でシンジケートローン業務を対象に実験	→ http://www.mizuho-fg.co.jp/release/pdf/20160216release_jp.pdf
みずほFG	Open Assets Protocolを利用したクロスボーダー証券取引	→ http://www.fujitsu.com/global/about/resources/news/press-releases/2016/0308-01.html

2016/04紹介分

名称	サービス概略	URL
日本取引所グループ	低トランザクション市場を想定した場合の、技術的な限界や可能性について評価	→ http://www.jpx.co.jp/corporate/news-releases/0010/20160407-01.html
静岡銀行とORIX	Orbを利用して、海外送金や各種決済サービスの検証	→ http://btcnews.jp/nttdata-orb-start-poc-for-banking/
ふくおかフィナンシャルグループ	ハウインターナショナルが協力し、ポイント交換や各種決済サービスなどの新たな金融サービスへの適用可能性に向けた検証	→ https://www.fukuoka-fg.com/news_pdf/20160315_block.pdf
Goldman Sachs	暗号通貨による証券決済システム「SETLcoin」	→ http://www.nasdaq.com/article/goldman-sachs-files-setlcoin-patent-what-it-is-and-what-it-means1-cm551600
J.P. Morgan	Digital Asset Holdingsと融資資金の流動性ミスマッチ解決	→ http://reuters.com/article/idUSKCNOV9115
Bank of America	暗号通貨へ一旦交換した上で銀行間送金を行う“Crypto Wire Transfer”	→ http://www.coindesk.com/bank-of-america-cryptocurrency-wire-transfer-patent/

2016/04紹介分

名称	サービス概略	URL
ドイツ銀行	スマートコントラクトを用いた社債の発行・償還	→ http://www.efinancialnews.com/story/2015-12-04/deutsche-bank-reveals-blockchain-corporate-bond-successful
UBS	既存の顧客向けロイヤリティポイント制度“KeyPoints”をモデルに実験	→ http://www.finews.ch/news/english-corner/19873-ubs-loyalty-program-fintech-experiment-crypto-currency
SWIFT	ブロックチェーンによるグローバル決済イニシアチブを発足	→ http://www.swift.com/about_swift/shownews?param_dcr=news.data/en/swift_com/2015/PR_global_payments_innovation_initiative.xml
DBSとStandard Chartered	貿易金融向け分散台帳プロジェクト	→ http://www.coindesk.com/dbs-and-standard-chartered-developing-distributed-ledger-for-trade-finance
ソフトバンク	コンセンサス・ベイス支援のもと、援国際募金プラットフォームのプロトタイプを開発	→ http://www.softbank.jp/corp/group/sbm/news/press/2016/20160106_01/

2016/04紹介分

名称	サービス概略	URL
BNP Paribas	SmartAngelsと提携してクラウドファンディングのパイロット	→ http://securities.bnpparibas.com/news/smartangels-revolutionise-financ.html
Barclays	Circleと提携してペイメントサービスを立ち上げ、英米間国際送金	→ http://www.forbes.com/sites/laurashin/2016/04/06/circle-launches-its-social-payment-service-in-the-uk-partners-with-barclays/#3d50ce8fd66a
DTCC	ポストトレードのライフサイクルイベントの管理をテスト	→ http://www.dtcc.com/en/news/2016/april/07/successful-blockchain-test-completed
ロンドン大学	即時決済や小口決済を可能で、中央銀行によるコントロールが可能な中央銀行向け「RSCoin」を開発	→ http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf
チュニジア	Monetasと組んでeDinarをブロックチェーンバージョンへ	→ http://bitcoinist.net/monetas-unifies-edinar-and-blockchain-technology-in-tunisia/

2016/07紹介分

名称	サービス概略	URL
TradeSafe	DBSのトレードファイナンス向け分散台帳	→ https://govinsider.asia/smart-gov/singapore-government-builds-blockchain-system-to-protect-banks/
ベルギー-KBC	中小企業向けトレードファイナンス Digital Trade Chain	→ https://www.finextra.com/newsarticle/29159/kbc-develops-blockchain-based-app-for-cross-border-sme-trade
MUFG	Chainと約束手形のPoCを構築	→ http://blog.chain.com/post/142485528836/chain-partners-with-japans-largest-financial
Allianz	自然災害向けスワップ取引のパイロットプロジェクト	→ http://blockchain-finance.com/2016/06/15/allianz-nephila-announce-successful-pilot-of-blockchain-tech-for-cat-swap/
仏Credit Mutuel Arkea	Hyperledger blockchainを用いたKYCプロセス	→ http://www.coindesk.com/ibm-completes-blockchain-trial-french-bank-credit-mutuel/
Barclays	Smart Contract Templatesを使ったデリバティブ取引	→ http://www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-trade-derivatives.html

2016/07紹介分

名称	サービス概略	URL
BNY Mellon	貸付証券(securities lending)の資産の取引および移動	→ http://www-03.ibm.com/press/us/en/pressrelease/49632.wss
ロシアのNational Settlement Depository	e-proxy voting systemを対象にNXTプラットフォーム上で開発・試験	→ https://www.nsd.ru/en/press/ndcnews/index.php?id36=628973
シドニー証券取引所	パブリックブロックチェーンを用いて決済システム	→ https://www.cryptocoinsnews.com/sydney-stock-exchange-building-public-blockchain-system/
Nasdaq	NasdaqのLinqブロックチェーンサービスを用いて太陽光発電認定（電力証書）を売却	→ http://www.coindesk.com/nasdaq-blockchain-solar-power-market/
欧州の7金融機関	スモールビジネスむけポストトレードサービス	→ http://www.coindesk.com/fis-post-trade-blockchain-small-businesses/

2016/07紹介分

名称	サービス概略	URL
The Central Bank of Canada	カナダドルのデジタル版をテスト開発	→ http://www.coindesk.com/bank-canada-demos-blockchain-based-digital-dollar/
Bank of England	リアルタイムグロスセツルメント (RTGS) システム等への適用を意図	→ http://www.bankofengland.co.uk/publications/Pages/speeches/2016/914.aspx
オランダ中央銀行	DNBCoinの実験	→ http://www.dnb.nl/binaries/Speech%20Ron%20Berndsen_tcm46-342846.pdf
Deloitte	RippleプロトコルとTemenosコアバンキングソフトの統合	→ http://www.financemagnates.com/cryptocurrency/education-center-2/deloitte-integrates-ripple-banking-software-international-transfers/
Santander	Rippleを英国ではじめてクロスボーダーペイメントに採用	→ http://www.coindesk.com/nasdaq-blockchain-solar-power-market/
カナダATB Financial	RippleおよびSAPと協業して国際送金	→ https://news.bitcoin.com/canadian-ripple-sap-first-blockchain/
みずほFG	SBIホールディングス、R3CEVとRippleを用いて国際送金実験	→ http://www.mizuho-fg.co.jp/release/20160719release_jp.html

2016/12紹介分

名称	サービス概略	URL
Utility Settlement Coin	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	→ http://www.ibtimes.co.uk/devcon2-santander-ethercamp-building-bridges-between-bank-accounts-ethereum-1582242
CashEth	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	→ http://www.coindesk.com/santander-vies-become-first-bank-issue-digital-cash-blockchain/
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	→ https://newsroom.accenture.com/content/1101/files/Cross-FSBC.pdf
VISA	Chainと協業で国際B2Bペイメントソリューション	→ http://www.coindesk.com/visa-blockchain-payments-service/
PwC	デジタルアセットサービスVulcan	→ https://www.vulcandas.com
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	→ https://webforms.ey.com/ch/en/newsroom/news-releases/news-release-ey-switzerland-accepts-bitcoins-for-payment-of-its-services

2016/12紹介分

名称	サービス概略	URL
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	Keystone Capitalと提携し初のブロックチェーンエクイティ発行	→ 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/

2016/12紹介分

名称	サービス概略	URL
JP Morgan	プライベートEthereum	→ https://drive.google.com/file/d/0B42vMkapQi1MSEVaa2tuVEtXZXM/view
Six-securities	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/
中国の全国社会保障基金理事会	社会保障の支払い	→ 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	→ 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/

2016/12紹介分

名称	サービス概略	URL
HSBC	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	→ 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/

2016/12紹介分

名称	サービス概略	URL
Visa Europe	SatoshiPayと提携しマイクロペイメントの試行	→ http://www.coindesk.com/visa-europe-bitcoin-micropayments/
Deloitte	ethereum ベースのアイデンティティプラットフォームSmart ID	→ 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	→ 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	→ https://www.finextra.com/newsarticle/29400/barclays-executes-live-letter-of-credit-transaction-using-distributed-ledger-technology

2016/12紹介分

名称	サービス概略	URL
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
R3	15行でトレードファイナンス分野のプロトタイプ開発	→ 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/

2016/12紹介分

名称	サービス概略	URL
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
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	→ http://www.coindesk.com/bank-tokyo-use-blockchain-contract-management-2018/
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	企業内コイン「OOIRI」の検証	→ http://cryptocurrencymagazine.com/kabu-com-ooiri-coin

2017/03紹介分

名称	サービス概略	URL
DTCC	IBM・R3・AXONIとクレジットスワップ取引システムのリプレイス	→ 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	→ 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	→ https://news.bitcoin.com/central-bank-germany-blockchain/
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	→ http://www.ibtimes.co.uk/ubs-collaborates-blockchain-wallets-cars-1599055
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-

2017/03紹介分

名称	サービス概略	URL
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/
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	HAWと協働でOpen Assets Protocolを貸金貸借市場へ応用	→ http://www.boj.or.jp/announcements/release_2017/data/rel170227a3.pdf
中国人民銀行	デジタルマネー-YuanCoinのテスト	→ 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/
Euroclear	ゴールドセツルメント	→ https://www.ethnews.com/euroclear-and-paxos-implement-blockchain-solution-for-gold-settlement
Royal Mint	英国王立造幣局が開発したゴー	→ http://www.royalmint.com/rmg

2017/07紹介分

名称	サービス概略	URL
Intetesa Sanpaolo	OpenTimestamps用いて取引データ検証	→ http://www.coindesk.com/intesa-sanpaolo-trade-data-bitcoin-blockchain/
BlockchainCapital	VCとして初めてトークン株式発行	→ https://blockchaincapital.tokenhub.com/
JPモルガン	代理人投票システム構築	→ https://www.ethnews.com/major-finance-companies-complete-blockchain-based-proxy-vote-solution
Bank of Canada	R3 Cordaを用いてホールセール ペイメントシステムを構築	→ http://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf
カンボジア中央銀行	ペイメントインフラを Hyperledger Irohaで開発	→ http://www.econotimes.com/National-Bank-of-Cambodia-Soramitsu-partner-to-co-develop-Hyperledger-Iroha-blockchain-project-654992
CitiConnect for Blockchain	法人顧客むけにシームレスなペイ メントサービスを提供	→ https://blog.chain.com/chain-takes-citi-to-production-2c618e43375d

2017/07紹介分

名称	サービス概略	URL
シンガポールMAS	デジタルシンガポールドルの検証プロジェクトUbin	→ http://www.mas.gov.sg/~media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf
ロシア中銀	EthereumフォークのMasterchainのテスト準備	→ http://www.coindesk.com/russian-central-bank-group-prepares-masterchain-ethereum-fork-testing/
BlockOne IQ	Thomson ReutersのOracleサービス	→ https://blockoneiq.thomsonreuters.com/
Digital Trade Chain	中小企業トレードファイナンスコンソーシアム	→ https://www-03.ibm.com/press/us/en/pressrelease/52706.wss
Daimler	プライベートEthereumで社債発行	→ https://www.daimler.com/investors/refinancing/blockchain.html

2017/07紹介分

名称	サービス概略	URL
中国人民銀行	暗号通貨の研究ラボ開設し独自デジタル通貨のテスト	→ http://bit-finance.com/pboc-opens-new-cryptocurrency-research-institute/
ABN AmroやING	Cordaによるコマーシャルペーパープロトタイプ	→ http://www.coindesk.com/r3-completes-dlt-commercial-paper-prototype-bank-partners/
Swift	TownCrierオラクル用いたスマートコントラクトのトライアル完了	→ http://www.coindesk.com/swift-completes-blockchain-smart-contracts-trial/

6.金融系スタートアップの動き

2014/10紹介分

名称	サービス概略	URL
Swarm	仮想通貨によるファンディングプラットフォーム	→ http://www.swarm.fund/
Ripple	XRPという仮想通貨を発行し、Rippleネットワークを通じた送金・受金	→ https://ripple.com/
Stellar	他通貨間との送受金むけ分散プロトコル	→ https://www.stellar.org/
Overstock (TØ.com)	暗号証券による株式市場の再構築	→ https://tzero.com/
BitShares	分散型のcrypto-equityとして、bitsharesを保有する株主とのコミュニティを通じて、銀行・証券取引所のような機能を実現することを目指す	→ https://bitshares.org/

2015/01紹介分

名称	サービス概略	URL
Bitreserve (Uphold)	リアルタイムで検証可能な支払能力の証明(Proof of solvency)を行う世界初の金融サービスを目指す。	→ https://bitreserve.org/
Coinffeine	ビットコインを預からない分散型のP2Pビットコイン取引プラットフォーム	→ http://www.coinffeine.com/

2015/05紹介分

名称	サービス概略	URL
Digital Asset Holdings	株・住宅ローン・融資などの取引の決済と記録管理に利用	→ https://www.digitalasset.com/

2015/08紹介分

名称	サービス概略	URL
Symbiont	Counterparty創業者によって設立され、スマート証券のプラットフォームを目指す	→ https://symbiont.io/
Abra	イスラムの送金システムHawaraをブロックチェーンで実現	→ https://www.goabra.com/

2015/11紹介分

名称	サービス概略	URL
SETL	マルチ貨幣・マルチ資産の取引・決済	→ http://www.setl.io/
Clearmatics	OTC市場むけクリアリング	→ http://www.clearmatics.com/about/
Liquid	Blockstreamが開発したSidechainによる初のプラットフォーム	→ https://blockstream.com/2015/10/12/introducing-liquid/
Riskebiz	マイクロ損害保険	→ http://www.riskebiz.com/#!about/c136u
Tierion	ブロックチェーンレシート	→ https://tierion.com/
Uphold	Bitreserveが、オーバホールされリブランド	→ https://uphold.com/ → http://www.coindesk.com/bitreserve-overhauls-platform-rebrands-as-uphold/

2015/11紹介分

名称	サービス概略	URL
Manifold	Manifold Technologyによる、プライベートチェーンプラットフォーム	→ http://manifoldtechnology.com/
AlphaPoint	AlphaPointによる、金融向けブロックチェーンプロトコル	→ https://alphapoint.com/
InsurETH	ethereumのスマートコントラクトを用いたP2P保険 (SMART FLIGHT INSURANCE)	→ http://insureth.mkvd.net/ → http://mkvd.s3.amazonaws.com/apps/InsurEth.pdf
MoneyCircles.com	Uphold(旧BitReserve)のブロックチェーン上で銀行なしに貯蓄・貸付・借入	→ http://www.moneycircles.com/
OpenCharity	チャリティ・寄付のスマートコントラクトで資金トラッキング	→ http://www.opencharityuk.org/
String	ブロックチェーンとスマートコントラクトによる金融クラウド	→ http://string.technology/
Blockchain Clearing Corporation	T+0清算・決済	→ http://blockchainclearing.com/

2016/04紹介分

名称	サービス概略	URL
R3	金融関連の同意事項を金融機関同士で記録・管理・同期するための分散台帳プラットフォーム Corda	→ http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services
ConsenSys	金融スワップツール：eTRS (Ethereum Total Return Swap)	→ http://www.coindesk.com/ethereum-swaps-microsoft-blockchain-toolkit/
Kynetix	コモディティマーケットにおける所有権移転コンソーシアム	→ http://www.finextra.com/news/fullstory.aspx?newsitemid=28166
KPCB Edge	ファウンダーむけインターナルブロックチェーン「Edgecoin」	→ http://www.coindesk.com/kleiner-perkins-is-using-blockchain-tech-to-incentivize-its-founders/
WeiFund	EthereumのDappsによる分散型クラウドファンディング	→ http://weifund.io/
KYC-Chain	KYCドキュメントの認証ゲートキーパー	→ http://kyc-chain.com/
DigixDAO	EthereumベースのDAOプラットフォーム	→ https://sale.digix.io/

2016/04紹介分

名称	サービス概略	URL
Wirex	ビットコインウォレットとデビットカードの双方向サービス	→ https://wirexapp.com/ja/
Block Notary	P2Pローンアプリ	→ http://www.blocknotary.com/
The DAO	ICOに類似した分散オーナーシップの仕組み。支持者が一時的な褒賞に留まらずに投資できて株主になることができる	→ https://slock.it/dao.html
Equibit	ブロックチェーンベースの店頭市場 ・CORE：オープンソースマイナー ・INVESTOR：ウォレット ・ISSUER：株式ユニット作成	→ https://equibitgroup.com/
BTL Group LTD	送金技術「InterBit」を発表	→ http://btl.co/interbit/
DiQi	マルチカレンシー&スマートプロパティのデジタルアセット管理	→ https://diqi.us/ → http://diqi.us/static/whitepaper_en.pdf
AlgoRythmix	信用情報レーティング、KYCプラットフォーム	→ http://algorythmix.in/

2016/04紹介分

名称	サービス概略	URL
Digital Asset Holdings	ゴールドマンサックスとIBMが出資	→ http://www.finextra.com/news/fullstory.aspx?newsitemid=28415
	JPモルガンやDTCC等から5000万ドルを調達	→ http://digitalasset.com/press/digital-asset-closes-funding-exceeding-50-million.html → http://digitalasset.com/press/asx-selects-digital-asset.html
	DTCCとポストトレード分野(レポ取引のクリアリング)で実証実験	→ http://www.coindesk.com/dtcc-use-digital-asset-tech-blockchain-post-trade-trial/
ChromaWay	LHV銀行のCuberウォレット開発をサポート	→ http://chromaway.com/
Overstock (TØ.com)	自社株の公募をブロックチェーンで	→ http://investors.overstock.com/
Tradeblock	Permissioned LedgerとしてAxoniをローンチ	→ https://tradeblock.com/ → https://tradeblock.com/blog/axoni-launches-to-provide-permissioned-ledger-technology → https://axoni.com/updates/icap-announces-completion-of-a-blockchain-proof-of-technology-with-axoni-2

2016/07紹介分

名称	サービス概略	URL
Digital Asset Holdings	Digital Asset Modeling Languageを発表	→ http://digitalasset.com/press/introducing-daml.html
EdgeVerve Systems	銀行むけブロックチェーンプラットフォームEdgeVerve Blockchain Framework	→ https://www.edgeverve.com/finance/edgeverve-blockchain-framework-financial-services/
Chain	金融機関むけブロックチェーン「Open Standard 1」を発表	→ https://chain.com/docs/1.2/protocol/papers/whitepaper
Chain	ウォールストリートでデジタルキャッシュに関するシークレットミーティング	→ http://www.bloomberg.com/news/articles/2016-05-02/inside-the-secret-meeting-where-wall-street-tested-digital-cash
String Labs	Ethereumパブリックチェーン上におけるファイナンスシステム(Open Chain Financeプロジェクト)	→ http://string.technology/
Vault OS	ブロックチェーンベースの銀行業界むけオペレーティングシステム	→ https://www.thoughtmachine.net/

2016/07紹介分

名称	サービス概略	URL
PwC	レジューレスと企業間資金流通の透明性向上、経理業務の効率化を図る新規サービスを共同開発	→ http://www.pwc.com/jp/ja/japan-press-room/press-release/2016/companies-remittance160513.html
Dragonfly Fintech	NEMのブロックチェーン技術を利用した海外送金	→ https://www.finextra.com/pressarticle/64928/dragonfly-fintech-selected-to-implement-blockchain-based-remittance-platform
Kompany.com	KYC/KYBむけに企業情報登録台帳の開発	→ https://www.finextra.com/pressarticle/64421/kompany-to-move-company-records-to-a-blockchain
ObjectChain Collab	分散型の個人IDを構築	→ http://www.objectchain-collab.com/about

2016/07紹介分

名称	サービス概略	URL
BC Finance	ミャンマーのマイクロファイナンスにおいて、勘定データ移行テストをmijinで実施	→ http://itpro.nikkeibp.co.jp/atcl/news/16/061601748/
Dynamis	Insurance DAOを通じてP2P失業保険を提供	→ http://www.dynamisapp.com/
LenderBot	ビットコインブロックチェーンを用いてシェアリングエコノミー向けマイクロ保険	→ https://www.finextra.com/pressarticle/65264/stratumn-and-deloitte-unveil-blockchain-based-micro-insurance-poc
itBit	Euroclearと組んで金市場のセトルメントを対象としたソリューション	→ https://www.euroclear.com/en/news-views/news/press-releases/2016/2016-MR-07.html

2016/07紹介分

名称	サービス概略	URL
Quelupa	ブロックチェーンベースの保険 (ラテンアメリカ)	→ http://allcoinsnews.com/2016/04/10/quelupa-plans-bringing-blockchain-based-insurance-to-latin-america/
EtherEx	暗号通貨取引およびトークン発行	→ http://www.ibtimes.co.uk/etherex-looks-beyond-cryptocurrency-trading-towards-tokenised-future-ethereum-1555211
Teambrella	P2P保険	→ https://news.bitcoin.com/teambrella-p2p-insurance-bitcoin/
Consuelo	移民むけマイクロ保険。健康保険・生命保険むけのマイクロ保険 (メキシコ)	→ http://consuelo.mx/ → http://cointelegraph.com/news/consuelo-offers-blockchain-powered-microinsurance-to-migrant-workers

2016/07紹介分

名称	サービス概略	URL
Tramonex	クロスカレンシーペイメント	<ul style="list-style-type: none">→ http://www.the-blockchain.com/2016/04/29/tramonex-scoops-250k-uk-grant-blockchain-based-cross-currency-payments/→ http://www.coindesk.com/uk-government-awards-250000-develop-cross-border-blockchain-prototype/
ECHO	暗号化されたプライベートチャット およびインスタント送金	→ http://my-echo.com/
AMoney	AMoneyプロトコル、ブロックチェーン、Rippleプロトコル、Stellarプロトコルの4本を連結したクロスボーダーペイメントでアフリカにおけるウォレットを統合	<ul style="list-style-type: none">→ https://myaconect.com/fintech/→ http://cointelegraph.com/news/blockchain-revolution-3-african-startups-to-watch-in-2016
The Sun Exchange	太陽エネルギーに投資したい人とそれにアクセスしたい人を繋ぐP2Pレンディングプラットフォーム	→ http://www.thesunexchange.com/

2016/07紹介分

名称	サービス概略	URL
Taqanu Bank	移民・難民むけにデビットカードや小切手口座などブロックチェーンベースの銀行サービスを提供（ノルウェー）	→ http://www.taqanu.com/#overview
WONE	スマートコントラクトを用いて同じモバイルウォレットアプリを使ってないユーザ同士のペイメントを可能とするP2Pモバイルペイメント（フィンランド）。	→ http://wone.io/
ChainThat	分散型再保険	→ http://chainthat.com/insurance/
SafeShare	ロンドンのCornerstone Insurance Brokers Limitedによるシェアリングエコノミーをベースとした保険	→ http://www.safeshareinsurance.com/
HEAT	クラウドファンディングプラットフォーム	→ http://heatledger.fi/
DPactum	スマートコントラクトによるデリバティブの清算・管理	→ http://www.dpactum.com/#/home

2016/07紹介分

名称	サービス概略	URL
Common Accord	リーガルドキュメントを分散台帳を介して移動できるグローバルテキストコードを開発中。 BNP ParibasのFinTechアクセラータプログラムで選抜。	→ http://www.commonaccord.org/ → http://p2pfoundation.net/Common_Accord → https://github.com/CommonAccord/Cmacc-Org
SETL	セトルメント向けの初の商用ブロックチェーンとして「OpenCSD」プラットフォームを発表	→ https://setl.io/opencsd/
Wall Street Blockchain Alliance (WSBA)	分散台帳技術 (DLT) の認定プログラムを、Positrust LLCとの協働で発表	→ http://www.wsba.org/Licensing-and-Lawyer-Conduct/Member-Tools-and-Information/Status-Certificates
Abra	P2Pペイメントサービスとしてローンチ。米国のユーザがスマホアプリをダウンロードし、銀行口座から入金して電話番号を入力するだけで他ユーザへ無料送金可能。	→ http://www.businessinsider.com/mobile-payment-company-abra-launches-with-blockchain-technology-in-us-2016-6
Ant Financial	Alipayのペイメントにブロックチェーン適用へ。まず最初にAlipayの寄付支払から。	→ http://coinjournal.net/ant-financial-blockchain-tech/

2016/12紹介分

名称	サービス概略	URL
Digital Asset Holdings	台帳間の同期化ログ「Global Synchronization Log」	→ http://digitalasset.com/static/documents/The_Global_Synchronization_Log.pdf
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	→ 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	Deloitte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 (t0)	自社の株式取引をブロックチェーンで開始	→ https://www.coin-portal.net/2016/10/31/14279/
インドUnocoin	クロスボーダーペイメントAPI	→ http://www.ibtimes.co.uk/unocoin-releases-api-power-bitcoin-economy-india-1590196

2016/12紹介分

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/57bda2fdebdbd1acc9c0309b2/1472045822585/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/

2017/03紹介分

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/xbri-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/

2017/03紹介分

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	チェーン横断の資産交換	→ https://coinstorm.net/en
Aragon	組織マネジメントプラットフォーム	→ https://aragon.one/

2017/03紹介分

名称	サービス概略	URL
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/
Numeraire	AIヘッジファンドNumerai向け暗号トークン	→ https://numer.ai/
Polychain Capital	ブロックチェーンアセット向けヘッジファンド	→ http://polychain.capital/
TaaS	トークンのアセットファンド	→ https://taas.fund/

2017/07紹介分

名称	サービス概略	URL
EquiBit	P2Pのエクイティ管理	→ http://www.livebitcoinnews.com/equibit-development-corporation-plans-launch-blockchain-based-mainstream-investment-products/
Fundchain	ファンド流通のバリューチェーン	→ http://fundchain.lu/ → http://www.thefundschain.com/
Blocksure	ethereumベースの保険	→ https://www.blocksure.com/
Sikoba	IOUベースの分散マネープラットフォーム	→ http://www.sikoba.com/
Exscudo	マルチカレンシーペイメントとチャット	→ https://channels.exscudo.com/
Bext360	Stellarを用いたロボットペイメント	→ https://techcrunch.com/2017/04/11/bext360-is-using-robots-and-the-blockchain-to-pay-coffee-farmers-fairly/
Provachain	Royal Mint Goldなどコモディティ商品トレードむけ分散台帳	→ https://www.provachain.com/#home
KYC chain	金融機関むけKYC	→ http://kyc-chain.com/

2017/07紹介分

名称	サービス概略	URL
BitcoinHivemind	予測市場スマートコントラクト	→ http://bitcoinhivemind.com/
BitCAD	分散トレードエンジンTectum	→ http://bitcad.me/
Bancor	セルフトレーディング型のスマートトークン	→ https://bancor.network/static/Bancor_Protocol_Whitepaper_en.pdf
Cofound.it	ICONOMIが立ち上げたスタートアップインキュベーター・プラットフォーム	→ https://cofound.it/en/
Swap	ethereum上でのトークントレーディングプロトコル	→ https://swap.tech/whitepaper
KYCstart	KYCチェック向けブロックチェーン	→ https://www.finextra.com/pressarticle/69173/deloitte-develops-blockchain-proof-of-concept-to-mutualise-kyc-checksleft
NVO	分散型取引プラットフォーム、New Venture Opportunities	→ https://nvo.io/

2017/07紹介分

名称	サービス概略	URL
Prism	Shapeshiftによるトラストレスなポートフォリオマーケットプラットフォーム	→ https://blog.prism.exchange/blog/introducing-prism-the-worlds-first-trustless-asset-portfolio-platform/
OmiseGo	ethereumベースの分散型取引所・ペイメントネットワーク	→ https://cdn.omise.co/omg/whitepaper.pdf → https://omg.omise.co/
dharma	ethereumベースのP2Pレンディング	→ https://dharma.io/
Vault	DappsやDAOむけ自律ペイメントスマートコントラクト	→ http://vaultcampaign.giveth.io/
Cofound	分散型VCエコシステム	→ https://cofound.it/
Omega One	取引所間トレードの分散自律実行プラットフォーム。取引所間の分散自動取引を通じた流動性提供サービス	→ https://omega.one/
TIX	トレードファイナンスプラットフォーム	→ https://tradeix.com/
Impak	ソーシャルインパクト向けトークンバンキング	→ https://impakfinance.com/home/

2017/07紹介分

名称	サービス概略	URL
Proveq	クラウドセールでの不正防止ソリューション	→ https://proveq.io/
Harbour	トークンアセット管理を目的としたクラウドセール投資むけDAO	→ https://harbour.tokenate.io/#Project
Seglos	分散自律トレーディングプラットフォーム	→ http://www.seglos.com/
Swarm Fund	分散投資プラットフォーム	→ https://www.swarm.fund/
Bankbox	ColuによるColored Coinを用いたデジタル通貨発行管理プラットフォーム	→ https://github.com/Colored-Coins/BankBox/blob/master/README.md
Istanbul BFT	台湾AMIS Trchnologiesが開発したQuorumむけEthereumコンセンサスアルゴリズム	→ https://github.com/ethereum/EIPs/issues/650

2017/07紹介分

名称	サービス概略	URL
Zen	日本円に対して為替が安定した 仮想通貨を志向した デジタル トークン	→ http://bcc.global/ja/articles/20170705.html
Colu	金融機関がデジタル通貨発行す るためのオープンソースプロトコルを ローンチ	→ http://kabutan.jp/disclosures/pdf/20170627/140120170627417418/
インフォテリア	株主総会の議決権行使における 実証実験完了	→ http://kabutan.jp/disclosures/pdf/20170627/140120170627417418/

お役に立てば嬉しいです

○ BTCアドレス

16ApP6FaD3CzzEBhK9PvSGVY1aafz6hciF

