BLOCKCHAIN2.0概況

2015.08.14 by SATO

※「Bitcoin2.0概況」から改題

今回の位置づけ

- **過去３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**
  - **2014年10月、2014年7月～9月の動きを整理**
    - http://www.digitalmoney.or.jp/wp-content/uploads/2014/10/20141003_BTC2.0.pdf
  - **2015年1月、2014年10月～12月の動きを整理**
    - http://www.digitalmoney.or.jp/wp-content/uploads/2015/01/20150116_BTC2.03.pdf
  - **2015年５月、2015年1月～４月の動きを整理**
    - http://www.digitalmoney.or.jp/wp-content/uploads/2015/05/20150508_BTC2.0.pdf
  - **（臨時：2015年６月、金融分野のトピックに絞って整理）**
    - http://www.digitalmoney.or.jp/wp-content/uploads/2015/06/20150619_BlockChain2.0_FI_v4.pdf

- **今回は、2015年５月～７月の動きを中心に整理したもの**

おさらい：初回（2014年10月）

- **2014年7月～9月の動きを中心に整理**
  - **イントロダクション**
  - **Webの進化**（Ethereum, Web3.0）
  - **スマートコントラクト＆スマートプロパティ**（Codius, Counterparty）
  - **組織・意思決定**（DAC, DAO, Eris）
  - **ファンドレイジング**（MaidSafe, Storj, Swarm）
  - **金融プラットフォーム①：ゲートウェイ**（Ripple, Stellar）
  - **金融プラットフォーム②：交換所インフラ**
    （NXT, Overstock, BitShares）
  - **クロージング**

おさらい：第2回（2015年1月）

- **2014年10月～12月の動きを中心に整理**
  - **イントロダクション**
  - **Bitcoin2.0のアーキテクチャ**　（Factom, Sidechain等）
  - **多様な価値流通**　（OpenBazaar, Zennet等）
  - **金融関連分野**　（Bitreserve, Overstock-Medici等）
  - **パブリック分野**　（Bitnation等）
  - **ライフスタイル関連分野**（GetGems, La'Zooz, Synereo）
  - **新たな経済圏**　（Dapps, トークンエコノミー等）
  - **クロージング**

おさらい：前回（2015年5月）

- **2015年1月～4月の動きを中心に整理**
  - **イントロダクション**
  - **金融系**　（Fidor, Ripple, Bitreserve, Swarm, BitGold）
  - **基盤系**　（Factom, NEM, IoT, AI）
  - **生活系**　（Synereo, Augur, SoG, Bitnation等）
  - **外部機関**　（IDEO, MITメディアラボ）
  - **クロージング**

TABLE OF CONTENTS

➔ 今回は、2015年5月～7月の動きを中心に整理したもの

イントロダクション
- カテゴリーマップ（私案）
- ブロックチェーンのユースケース

1．金融機関の動き

2．金融分野におけるスタートアップ動向

3．金融機関とスタートアップの協業動向

4．サプライチェーン分野
- IoT決済
- 所有権トラッキング
- 来歴管理・偽物防止

5．ライフスタイル分野
- マーケットプレイス
- 動画・アートへのリワード
- ギフト・プリペイド・ポイントカード
- ゲーム
- コミュニケーション
- マイニング×日常生活

6．シビックテック・公共分野
- ID証明
- バーチャル国家プラットフォーム
- 宇宙開発
- 小額貯蓄・進学サポート
- 土地登記
- 予算可視化
- ベーシックインカム
- 政治投票

7．イノベーション推進エコシステム

8．ブロックチェーン2.0サービス開発の考察

9．基盤関連

10. テクニカルセクションメモ
- Blockchain2.0系の実装技術まとめメモ
- Permissioned Distributed Ledger
- Sidechain
- Lightning Network

イントロダクション

- ブロックチェーンの応用対象
- カテゴリーマップ（私案）
- ブロックチェーンのユースケース

ブロックチェーンの応用対象

Blockchain＝Trustless・不可逆・書換不能・透明性・転々流通性の高いインフラ

金融資産	証券取引（Overstock、Symbiont、Bitshares、Mirror、Hedgy）
著作権や書類などの記録	土地登記（Factom）
	認証（BlockVerify）
	タイムスタンプ（Ascribe）
	医療情報（BitHealth）
	来歴管理（Provenance）
	投票（Neutral Voting bloc）
イベントチケットや商品券・ギフトカードなどの所有権	所有権証明（Everledger）
	書類・契約のデジタル化、所有権証明（Colu）
	デジタルコンテンツの所有権証明（Ascribe）
	ゲーム資産（Spells of Genesis、Voxelnauts）
	ギフトカード（GyftBlock）
セキュアなID	デジタルID（ShoCard、OneName）
分散化	予測市場（Augur）
	マーケットプレイス（OpenBazaar）
	クラウドストレージ（Storj）
	バーチャル国家（BitNation、Spacechain）
トークンエコノミー	メッセンジャー（GetGems）
	ライドシェア（La'Zooz）
	SNS（Synereo、Reveal）
	アーティストトークン（PeerTracks）
ペイメント・リワード	IoT決済（Adept）
	ストリーミング（Streamium）
	アーティストリワード（PopChest）

カテゴリーマップ（分野・取組内容ベース）

金融

- 為替・送金
- ﾋﾞｯﾄｺｲﾝの法貨連動
- ｸﾗｳﾄﾞﾌｧﾝﾃﾞｨﾝｸﾞ
- 法定通貨とペグ付け
- 金保管
- 株式
- デリバティブ
- 分散取引所
- ｽﾏｰﾄｺﾝﾄﾗｸﾄ
- ｿｰｼｬﾙﾊﾞﾝｷﾝｸﾞ
- 取引所
- ｲｽﾗﾑの送金ｻｰﾋﾞｽ
- ｲｽﾗﾑのｼｬﾘｱ遵法ｻｰﾋﾞｽ
- スマート証券
- 決済
- 移民むけ送金

サプライチェーン

- 商品由来ﾄﾗｯｷﾝｸﾞ
- ﾊﾞﾘｭｰﾁｪｰﾝ即時決済
- IoT・決済
- アート作品所有権
- ダイヤモンド
- アート作品証明
- 偽薬・偽物防止

ライフスタイル

- メッセンジャー
- SNS
- ライドシェアリング
- マーケットプレイス
- 予測市場
- ストリーミング
- ｱｰﾃｨｽﾄ向けﾘﾜｰﾄﾞ
- ギフトカード交換
- ｱｰﾃｨｽﾄｴｸｲﾃｨ取引
- プリペイドカード
- リワードトークン
- ﾄﾚｰﾃﾞｨﾝｸﾞｶｰﾄﾞｹﾞｰﾑ
- ｹﾞｰﾑ上の資産管理
- SNS
- マイニングチップ
- マイニング電球

シビックテック

- ヘルスケア情報
- デジタルID証明
- デジタルID証明
- バーチャル国家
- 宇宙開発
- 送金・貯蓄
- 土地登記等の公証
- 市政予算可視化
- 政治投票
- ベーシックインカム

プラットフォーム

- Dapps開発基盤
- Dapps開発ﾌﾟﾗｯﾄﾌｫｰﾑ
- 台帳管理システム
- ﾏﾙﾁﾌﾞﾛｯｸﾁｪｰﾝﾈｯﾄﾜｰｸ
- トークン発行
- P2Pプラットフォーム
- 分散ｸﾗｳﾄﾞｽﾄﾚｰｼﾞ
- 分散ｸﾗｳﾄﾞｽﾄﾚｰｼﾞ
- 分散ｸﾗｳﾄﾞｺﾝﾋﾟｭｰﾃｨﾝｸﾞ
- API提供
- 分散ｺﾝﾋﾟｭｰﾃｨﾝｸﾞﾈｯﾄﾜｰｸ
- 分散型AIシステム

カテゴリーマップ（名称ベース）

金融	サプライチェーン	ライフスタイル	シビックテック
Ripple	Provenance	GetGems	Bithealth
Bitreserve	Factory Banking	Synereo	OneName
Swarm	Adept	La'ZooZ	ShoCard
BitShares	Ascribe	OpenBazaar	BitNation
BitGold	Everledger	Augur	Spacechain
Overstock	Verisart	Streamium	Stellar
Hedgy	BlockVerify	PopChest	Factom
Coinffeine		GyftBlock	MayorsChain
Mirror		PeerTracks	Neutral Voting Bloc
ROSCA		BuyAnyCoin	GroupCurrency
itBit		Ribbit Rewards	
Abra		Spells Of Genesis	
Blossoms		Voxelnauts	
Symbiont		Reveal	
SETL		21 Inc.	
Toast		BitFury	

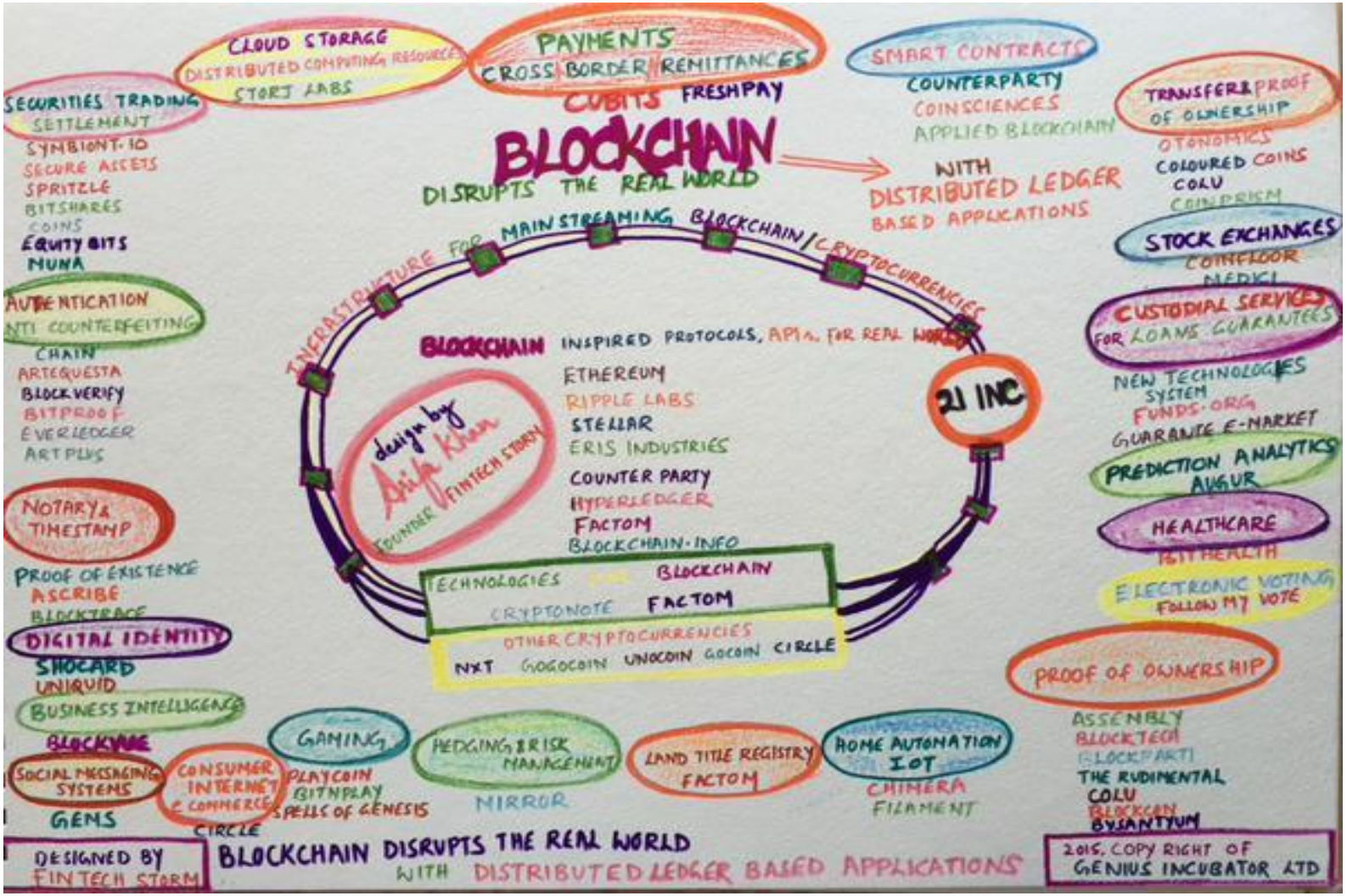
プラットフォーム

Ethereum	Sidechain	Maidsafe	BlockCypher
Eris	Counterparty	Storj	ZENNET
Hyperledger	NEM	Enigma	Sapience AIFX

ブロックチェーンのユースケース①

→ 出典：http://letstalkpayments.com/blockchain-use-cases-comprehensive-analysis-startups-invoved/

ブロックチェーンのユースケース②



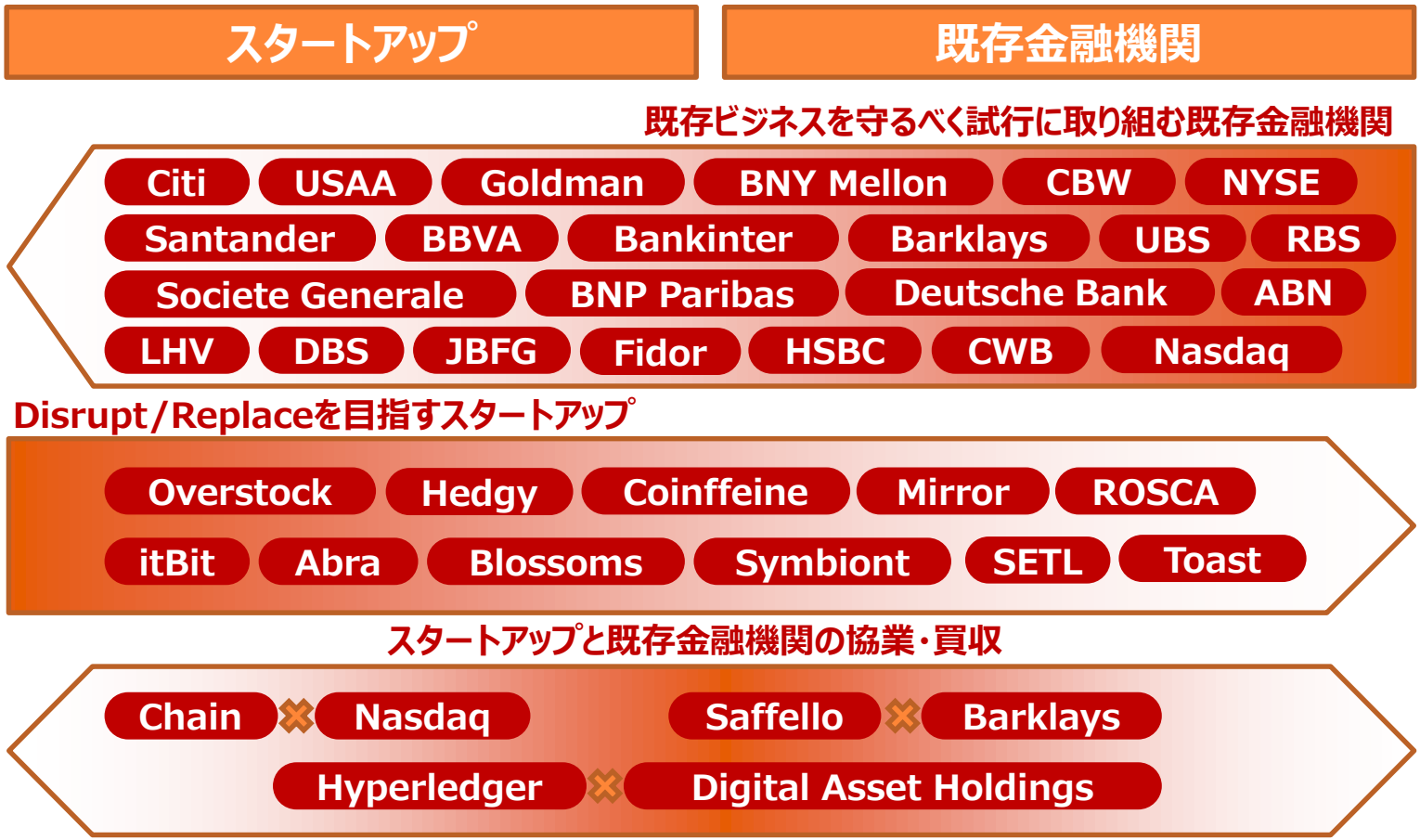
出典：https://twitter.com/GeniusIncubator/status/630343149639102464/photo/1

１.金融機関の動き

- Blockchain2.0的な取組みを進める海外金融機関
- 米USAA、ブロックチェーン研究チーム立ち上げ
- 米NASDAQ、未公開株式市場向けの導入検討
- エストニアLHV銀行、ウォレット開発
- 元JPモルガン：ブライス･マスターズが語る
- スペインSantander銀行、“Fintech 2.0”レポート
- Citiのクロスボーダー決済向けCitiCoin
- 欧州銀行協会（EBA）の暗号通貨技術に関するレポート

概略チャート

- Disrupt/Replaceを目指すスタートアップの攻勢と既存ビジネスを守るべく取り込みを図る既存金融機関



BLOCKCHAIN2.0的な取組みを進める海外金融機関

- **米国系と欧州系の各行が先行する中、アジア系も出てきた。**

	名称	取組み
米国	Citi	ブロックチェーンでCitiCoin開発。 「MobileChallenge」で “Most Visionary Social Media Solution”にGetGemsを選出。
米国	USAA	研究チーム立上げ
米国	Goldman Sachs	Circle出資
米国	BNY Mellon	社内でBKコインを試行
米国	VISA	ビットコインやRippleなど暗号通貨技術の研究開発。 ブロックチェーンの研究開発チームを設立。
欧州	Santander	Fintech2.0レポート発行, Ripple
欧州	BBVA	Coinbase出資
欧州	Bankinter	Coinffeine提携
欧州	Barklays	Saffelloと競業
欧州	UBS	ラボ開設, スマート債券, リーガソン開催
欧州	Societe Generale	暗号通貨スペシャリスト・インターンを募集
欧州	BNP Paribas	ブロックチェーンや分散台帳への見方表明
欧州	Deutsche Bank	ブロックチェーン技術調査に着手し、応用可能性についてレター
欧州	ING Bank	セキュリティ対応でブロックチェーン認証を実験
欧州	LHV	Colored coinを使ったウォレット開発
アジア	DBS	ブロックチェーンハッカソン開催
アジア	JBフィナンシャルグループ	Fintechイベントで、ブロックチェーンIDサービスのCoinPlugが優勝

出典：http://cointelegraph.com/news/114889/10-big-banks-that-are-seriously-looking-into-blockchain-technology

BLOCKCHAIN2.0的な取組みを進める海外金融機関

- **国際送金、証券取引などにおける取組みも進展。**

	名称	取組み
国際送金	ABN Amro	Rippleクローン開発（ABN Trade）
国際送金	Fidor Bank	Krakenと協業, Ripple
国際送金	HSBC	Ripple
国際送金	RBS	Ripple
国際送金	CBW	Ripple
国際送金	CommonWealthBank	Ripple
国際送金	Westpac	Ripple，Coinbaseへの戦略的出資
証券取引	NYSE	Coinbase出資、ビットコインindex立上げ
証券取引	Nasdaq	未公開株市場試行、Chainとの競業
他	SWIFT	研究資金拠出
他	Digital Asset Holdings	Blythe Mastersの合流、Hyperledger買収

→ 出典：http://cointelegraph.com/news/114889/10-big-banks-that-are-seriously-looking-into-blockchain-technology

BLOCKCHAIN2.0的な取組みを進める海外金融機関

- **個別金融機関だけでなく、中央銀行も意見・関心を表明。**

名称	取組み
シンガポール金融管理局	投資計画表明
ドイツ中央銀行	研究必要性表明
イングランド中央銀行	ビットコインフォーラムメンバーに
EBA（欧州銀行協会）	ブロックチェーン関連レポート公開
イギリス政府	デジタル通貨研究への投資表明

→ 出典：http://cointelegraph.com/news/114889/10-big-banks-that-are-seriously-looking-into-blockchain-technology

米USAA、ブロックチェーン研究チーム立ち上げ

- **軍関係者を顧客層とする中、先進的なサービスを展開してきた大手行**
  - アメリカの元・現役軍人、軍属およびその家族のみを対象とした銀行・保険業。
  - バンク・オブ・アメリカに次ぐ大手行（1100万を超える顧客、2100億ドルの残高）
  - 軍関係者を対象としているため、遠隔地で任務を遂行する軍関係者が口座にアクセスしやすいよう、早期からダイレクトバンキングやスマホ対応を進めてきた。
  - 2013年にはバーチャルアシスタントサービス（Siriのように音声で指示をすると口座残高や当該週のクレジットカード利用総額などがスマートフォン上に表示）を展開したりと、常に先進的なサービスを展開。
  - 2015年1月に行われたCoinbaseの7500万ドルのシリーズCにも投資。
- **行内バックオフィス業務の効率化を目的とした利活用を模索**
  - 仮想通貨を直接使用するのではなく、あくまでブロックチェーンのみを利用することに焦点を当てている。
  - 技術開発部門マネージングディレクターであるアレックス・マルケス氏は、「企業や銀行、保険、投資会社がブロックチェーン技術を利用することで、バックオフィス業務の分散化に役立てることができるだろう」と述べている。

→ 出典：http://btcnews.jp/us-usa-usaa-bank-research-blockchain-technology/
→ 出典：http://jp.forexmagnates.com/2015/05/11/%E3%83%86%E3%82%AF%E3%83%8E%E3%83%AD%E3%82%B8%E3%83%BC/20749

米NASDAQ、未公開株式市場向けの導入検討

- **未公開株市場むけにブロックチェーン技術のテスト開始**
  - 未公開株式市場向けのインフラ技術にブロックチェーンを導入することを最終目標とするブロックチェーン技術イニシアティブを発足。
  - ブロックチェーン技術を活用して元帳を分散化した有価証券が、所有権移動・ガバナンス・監査能力・整合性といった面で、効果的な機能を提供することを重要視。
  - 2015年後半までに最初のアプリケーションが完成するとしており、未公開株式市場の株式管理機能の強化にまずは用いられるとしている。
  - 将来的には、未公開企業の有価証券発行や管理・取引を効率的に実施可能に。
- **証券市場との親和性**
  - ビットコイン関連企業は、①証券市場を視野に置いたもの（ブライス・マスターズ率いるDigital Asset Holdings、バリー・シルバート率いるBIT、Noble Markets、Geminiなど）、②銀行システムを目的としたもの（Coinbase、Circle、Xapo、itBitなど）、③決済に焦点を当てたもの（BitPay、Bitnetなど）に分化しつつある
  - 証券市場への応用に勢いがあり、ブロックチェーンを利用した高効率な証券市場が構築されようとしている。

→ 出典：http://cryptocurrencymagazine.com/nasdaq-try-blockchain-technology

エストニアLHV銀行、ウォレット開発

- **ColoredCoinによる送受金可能なウォレットプラットフォームCuberを開発**
  - カラードコインによる送受金可能なウォレットプラットフォームCuber。
  - The Cuber Walletアプリは手数料無料でユーロの受取・送金が可能。
  - ウォレットはカラードコイン上に構築され、ブロックチェーンをDBとして利用。
  - Cuberプラットフォームはオープンソースで、顧客の巻き込みやチケット発行など新たな機能を実装していける仕組みになっており、今後の拡張にも期待。
  - 実験的にデジタル証券の開発にも取り掛かっていることもアナウンスしている。

- **LHV銀行は2009年設立の新しい銀行**
  - ネット・モバイル・チャットなど顧客コミュニケーションに注力しており、昨年にはCoinbase、今春にはCoinFloorとも提携するなど、ビットコインに友好的な銀行。
  - 今回のCuberの開発は銀行傘下の子会社Cuber社にて。
  - 「Cuber」はCryptographic Universal Blockchain Entered Receivablesの略とのこと。このLHV銀行のブロックチェーン活用への真剣度が伺われる。
  - スウェーデンのChromaWay社がカラードコイン技術のサポート。

→ 出典：http://cryptocurrencymagazine.com/estonia-lhv-bank

元JPモルガン：ブライス・マスターズが語る「金融機関がブロックチェーンに取り組むべき理由」

- **Singularity Universityの“Exponential Financeカンファレンス”で、ブロックチェーンについて語った。**
  - 金融機関は時間を割いて、ブロックチェーンの理解・可能性の探索に取り組むべき。
  - 分散化された台帳を通じて金融取引の透明化・効率化・安全に資する。
  - 金融業界に破壊的インパクトがあるばかりでなく増力化できる可能性も。
  - 我々は金融機関や政府の存在しない世界を考えている訳でない。
  - ブロックチェーンで取引速度やセキュリティを改善できる。
  - それゆえ金融分野での応用が大いに考えうる。
  - 既に多くの大手金融機関がブロックチェーンの学習に着手。
  - ブロックチェーン開発者と金融機関の橋渡しをしたい。
  - 両者をつなぐことができれば革命的インパクト。
  - ブロックチェーンは1990年代初頭のインターネットと同規模のBigDeal。

→ 出典：http://www.cnbc.com/id/102726305
→ 出典：https://www.youtube.com/watch?v=PZ6WR2R1MnM&feature=youtu.be
→ 出典：https://bitcoinmagazine.com/20686/financial-blockchain-applications-will-measured-trillions-says-blythe-masters-exponential-finance-2015/

スペインSANTANDER銀行、“FINTECH 2.0”レポート

- **ベンチャーキャピタル子会社が“The Fintech 2.0 Manifesto”を発表**
  - 金融サービスとITを融合させたFinTech1.0（UXやペイメントの改善）ではなく、金融サービスを「再起動」する可能性を秘めた次フェーズへの移行を見据える。
    - ひとつは海外送金。遅い上に手数料が高い海外送金ネットワークをバイパス
    - もうひとつはスマートコントラクト。シンジケートによる協調融資など。
  - モノのインターネット（IoT）やブロックチェーン活用によるBigger Pictureを展望。
  - IoTと金融取引の融合、ビッグデータ解析による業務効率化、分散型元帳による業務コストの削減など。
- **革新を起こすには銀行から歩み寄る必要がある**
  - ブロックチェーンの分散型元帳技術は、2022年までに銀行業務にかかるコストを150億ドル～200億ドル程度削減できる可能性がある。
  - 銀行が得意とする分野、スタートアップが得意とする分野、両者の協業が不可欠。
  - 自分たちだけでFintech2.0を実現できないまま終わるくらいなら、協調すべき。
  - Santander銀行はRipple導入を検討中との報道も。

→ 出典：http://www.finextra.com/finextra-downloads/newsdocs/fintechmanifesto.pdf
→ 出典：http://btcnews.jp/santander-fintech2-0-reports/
→ 出典：http://cryptocurrencymagazine.com/santander-hsbc-are-interested-in-ripple

CITIのクロスボーダー決済向けCITICOIN

- **クロスボーダー決済むけにビットコイン・ブロックチェーンを研究中**
  - ビットコインとブロックチェーンの技術を確かめるため、自身で3つのブロックチェーンを作成して内部でテストをしている模様。（コードネーム：CitiCoin）
  - 世界展開しているシティグループにとっては、国際送金におけるカウンターパーティーリスクへの対応が、Citicoinのユースケースの一つ。
  - 他国の中小銀行と資金のやりとりをする際には担保の差し入れなどが送金にかかる時間やコストを押し上げてしまうが、Citicoinを用いることで即時送金を実現する、という考え。
  - シテイバンクは既に英国政府の求めに応じて「英国もビットコインのような電子マネーを中央銀行が採用すべきだと提言している他、ケニアで銀行口座無しで送金できるシステムを開発したりということも行っている。
  - CitiCoinをM-Pesaのように、銀行口座を持たない層へのサービスに使う構想も。

- 出典：http://www.ibtimes.co.uk/codename-citicoin-banking-giant-built-three-internal-blockchains-test-bitcoin-technology-1508759
- 出典：https://bitcoinmagazine.com/21077/citi-working-citicoin-cross-border-payments
- 出典：https://www.highscore.co.jp/archives/2816
- 出典：http://jp.techcrunch.com/2015/07/08/20150707citibank-is-working-on-its-own-digital-currency-citicoin/
- 出典：paymentnews.infcurion.com/?eid=55

ドイツ銀行の考えるブロックチェーンの応用可能性

- **「ブロックチェーンは新たな産業を生み出し、既存インフラを破壊する可能性がある」と表明**
  - ブロックチェーンが決済・証券・AMLなどに影響を与えるとして検討を推進中。
  - より高速なトランザクションと低コストかつ安定し信頼のおけるシステムモデルであるとその技術を評価。
  - 「Strategy 2020」のプランのひとつとしてブロックチェーン技術に焦点を当てたイノベーションラボの立ち上げを示唆。
  - ブロックチェーン技術が活用可能な領域
    - フィアット通貨の支払い・清算
    - 識別・分割・追跡可能な有価証券の発行および転送
    - 有価証券の利回りや配当などの自動化
    - ポストトレードプロセスをより効率的に行うための決済および清算
    - スマートコントラクトを通じたデリバティブの自動執行および清算の効率化
    - 中央管理機関をバイパスしたアセットレジストリ
    - 顧客のマネーロンダリング監視システム
    - 当局へ透明性の高い情報の提供

→ 出典：http://btcnews.jp/deutsche-bank-reply-esma-blockchain-technology-disrupt-existing-financial-infrastructure/
→ 出典：http://www.coindesk.com/deutsche-bank-letter-touts-expertise-in-blockchain-tech/

欧州銀行協会（EBA）が暗号通貨技術に関するレポートを公開

- **「暗号テクノロジー：重要なITイノベーションかつ変化のための触媒」と題したレポート**
  - EBAは、ユーロ圏の180を超える金融機関が所属する機関であり、銀行や各種サービス・プロバイダがユーロ圏における決済インフラの骨子を構築するための支援を行っている。
- **暗号通貨技術の４区分**
  - 暗号通貨技術を通貨・資産台帳・アプリケーションスタック・資産集約技術の4種のカテゴリに分類してそれぞれを説明し、銀行取引と決済への影響力を多角的に分析している。

通貨 Currency	資産台帳 Asset Registry	アプリケーション スタック	資産集約技術 Asset Centric
• Bitcoin • Peercoin • Litecoin • Dogecoin • Darkcoin	• Counterparty • Colorcoins • Mastercoin	• Ethereum • Eris • NXT • ~~Codius~~	• Ripple • Stellar • Hyperledger • Namecoin

→ 出典：http://btcnews.jp/euro-banking-association-reports-150518/

欧州銀行協会（EBA）が暗号通貨技術に関するレポートを公開

- **レポートにおいては、資産集約技術（RippleやStellar）に深く言及されている。**
- **資産集約技術のユースケースとして、Rippleのゲートウェイ間での為替取引および送金機能。**
  - 例えばユーロのみを取扱うゲートウェイとドルのみを扱うゲートウェイの間で、ユーザー同士のマッチングが成立すれば自然と為替市場が形成される。
  - リップルのトレードシステム上で交換したユーロやドルは、IOU（借用証書）という形で発行されており、それぞれの取扱いゲートウェイ上で出金申請を行い現金を手にすることが可能。
  - 流動性を提供するマーケットメーカーを介すことで、ユーロ→ドル→円などのクロス取引も即時決済することができる。
  - 取引台帳システムはブロックチェーンと同様分散的に管理されており、すべての取引が取引台帳に記録されているが故に、アドレスベースでの取引は非常に簡単に追跡できるという利点がある。
  - この性質を応用することで、現在の荷為替システムに利用することができるというのが、EBAの見解。
- **EBAは3年以内の短期的な目線において、決済領域や銀行取引の分野ではRippleやStellarのような資産集約技術に最も可能性を見ている。**
  - ビットコインやCounterparty、Ethereumについては極めて「破壊的」な技術だということを十分に認識しつつも技術的な制約への直面、および現在の社会制度へ適合できないという点でボトルネックが存在しており、実用レベルに達するには長期の目線で見る必要があるとの見方。

→ 出典：http://btcnews.jp/euro-banking-association-reports-150518/
→ 出典：https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1.0.pdf

欧州銀行協会(EBA)の暗号技術考察レポート

- 大きく1.通貨：Currency, 2.資産台帳：Asset Registry, 3.Application Stack, 4.資産集約技術：Asset Centric Techに区分。
- 金融機関としては、Asset Centric Techへこの1-3年の可能性としてはフォーカス。

	名称	主な例	EBAレポートでの取扱
ブロックチェーン利用	Currency	Bitcoin, その他Altcoin	➢ 法的通貨として認められておらず、**消費者が法的通貨と同等に使えるようなテストが済んでいないとの見方。**
ブロックチェーン利用	Asset Registry	Coloredcoin, Counterparty, Mastercoin	➢ コイン以外の資産をブロックチェーンに登録するもので、ユーザーAからユーザBへの資産移転を可能にするもの。 ➢ 多量の追加データがネットワークパフォーマンスに影響する他、トランザクション検証に追加のプロセッシングパワーを必要とするBlockchain Bloat問題もあり、**銀行向けには限られた用途に留まるとの解釈。**
ブロックチェーン利用	Application Stack	Ethereum, Eris	➢ ブロックチェーン技術を通貨以外の分野に適用して、分散ネットワーク上に構築したアプリの開発・実行するためのプラットフォームと定義。 ➢ AmazonやMS Azureといったクラウドサービスの Decentralized版。 ➢ ユーザーAがインプットしたものをクラウドで処理して、ユーザーBにアウトプット。 ➢ 現時点は銀行向けには未成熟であり、**アプリも今は充分ローンチされていないとの見方。**
ブロックチェーン利用せず	Asset Centric Tech	Ripple, Stellar, Hyperledger	➢ 共有の分散台帳を使ってゲートウェイ間で、通貨・金属，株・債券など既存資産の両替などを行う。共有ではあるがPublicではなくPrivateな台帳であるのが味噌。 ➢ Trustをブロックチェーンやマイニングに依らず、参加者間で直接張る。 ➢ ネットワーク参加者はデジタル資産をネットワーク上にPublishすることにコミットするのに加え、参加者の一部はゲートウェイとしてアセット交換に責任を持つ。 ➢ 用途として、**既存プロセスの自動化がこの1-3年は考えられるとの見方。** **（海外送金、リアルタイムペイメント、荷為替、資産管理サービスなど）**

→ 出典：https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1.0.pdf

本章のまとめ （金融機関の動き①）

- **Blockchain2.0的な取組みを進める海外金融機関**
  - 米国系と欧州系の各行が先行する中、アジア系も出てきた
  - 国際送金、証券取引などにおける取組みも進展
  - 個別金融機関だけでなく、中央銀行も意見・関心を表明
- **米USAA、ブロックチェーン研究チーム立ち上げ**
  - 行内バックオフィス業務の効率化を目的とした利活用を模索
- **米NASDAQ、未公開株式市場向けの導入検討**
  - 未公開株市場むけにブロックチェーン技術のテスト開始
- **エストニアLHV銀行、ウォレット開発**
  - ColoredCoinによる送受金可能なウォレットプラットフォームCuberを開発
- **元JPモルガン：ブライス・マスターズ**
  - Singularity Universityの“Exponential Financeカンファレンス”で、ブロックチェーンについて語る

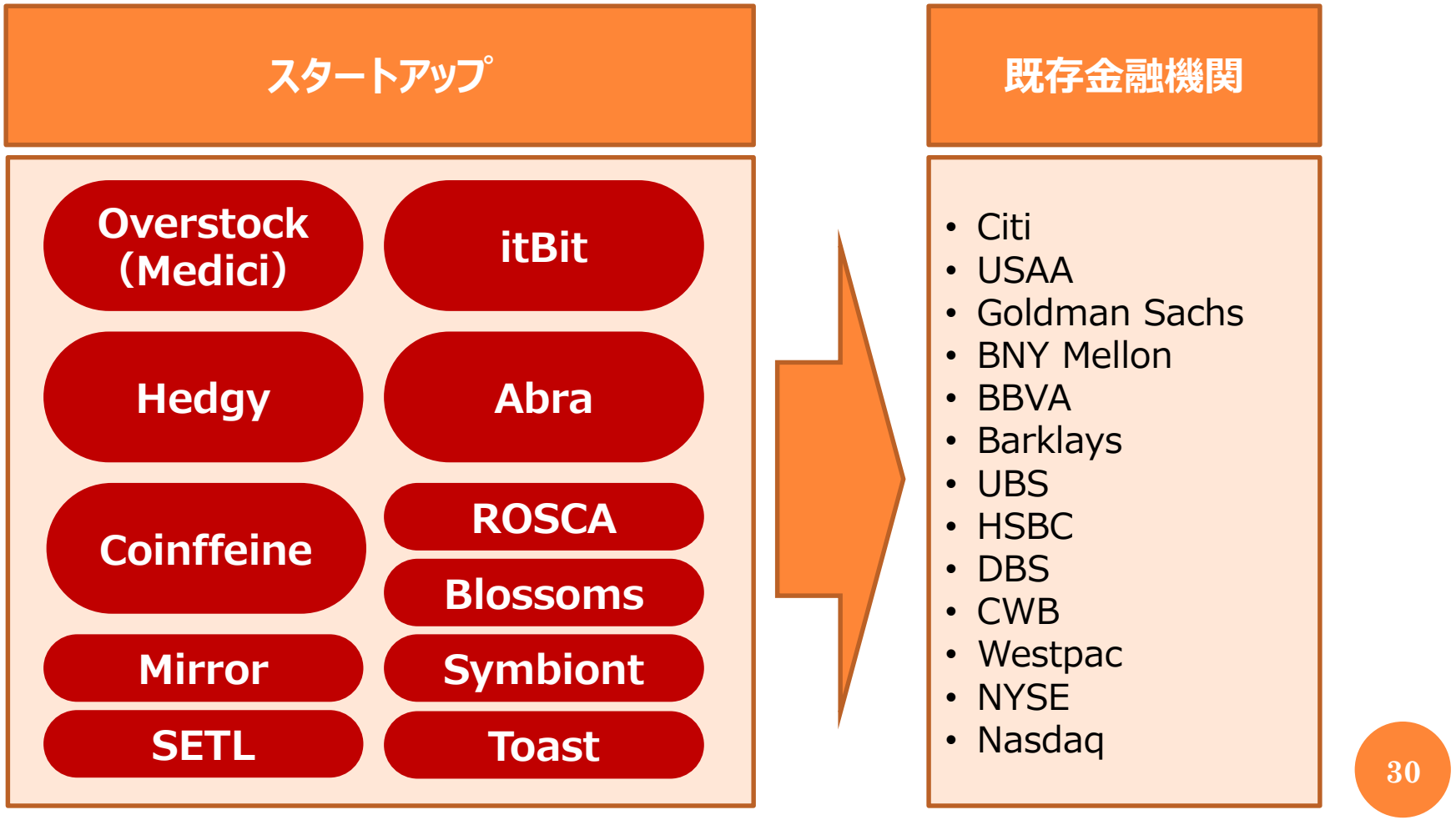
本章のまとめ（金融機関の動き②）

- **スペインSantander銀行、“Fintech 2.0”レポート**
  - ベンチャーキャピタル子会社が“The Fintech 2.0 Manifesto”を発表
- **Citiのクロスボーダー決済向けCitiCoin**
  - クロスボーダー決済むけにビットコイン・ブロックチェーンを研究中
- **ドイツ銀行の考えるブロックチェーンの応用可能性**
  - 「ブロックチェーンは新たな産業を生み出し、既存インフラを破壊する可能性がある」と表明
- **欧州銀行協会（EBA）が暗号通貨技術に関するレポートを公開**
  - 暗号通貨技術を４区分し、特に資産集約技術（RippleやStellar）に深く言及

2.金融分野におけるスタートアップの動き

- OverstockのMediciプロジェクト
- スマート証券のプラットフォームを目指すSymbiont
- スマートコントラクトによるデリバティブ、Hedgy
- イスラムの送金システムHawaraを実現するAbra
- NYDFSが認可、銀行免許を得たBitcoin取引所、itBit
- 分散型ビットコイン取引所、Coinffeine
- 銀行による国際送金利用へ集中するRipple
- その他のサービス

概略チャート


スタートアップ
Overstock（Medici）
itBit
Hedgy
Abra
Coinffeine
ROSCA
Blossoms
Mirror
Symbiont
SETL
Toast
既存金融機関
• Citi
• USAA
• Goldman Sachs
• BNY Mellon
• BBVA
• Barklays
• UBS
• HSBC
• DBS
• CWB
• Westpac
• NYSE
• Nasdaq

OVERSTOCKのMEDICIプロジェクト ブロックチェーンによるデジタル証券市場①

- **暗号化社債（Cryptobonds）2,500万ドル分の売出準備**
  - 米Overstockはブロックチェーンを基盤技術に用いた暗号化証券（Cryptosecurity）取引プラットフォームプロジェクトを推進中。
  - 暗号化社債は、「Medici」の一番最初のプロダクト。
  - 2,500万ドル分の債券を、暗号化社債販売プラットフォーム「TØ.com」上で売出予定。
  - 「TØ」という呼称は、証券取引市場における慣習的な「3営業日の待機期間」を排し、即日取引を行うことができるという意味を込めたもの。
  - TØプラットフォームは、ルール506(c)に基づき、まずは適格機関投資家のみを対象として、しばらくの間稼働する見込み。
  - OverstockのCEO、OpenAssetプロトコルを利用したT0.comプラットフォームで世界初の暗号コーポレート債を50万ドル分購入。

→ 出典：http://btcnews.jp/overstock-launches-offering-of-worlds-first-cryptosecurity/
→ 出典：http://upstart.bizjournals.com/entrepreneurs/hot-shots/2015/06/08/overstock-com-ceo-buys-world-s-first-bond-on.html

OVERSTOCKのMEDICIプロジェクト ブロックチェーンによるデジタル証券市場②

- **暗号証券トレーディングプラットフォームをナスダックで披露**
  - ナスダック本社で開催されたプライベートイベントにおいて、同社が取り組む暗号証券取引所「tØ.com」のプレゼンテーション。
  - tØ.comのコンセプトは「The Trade is the Settlement」。
    - ブロックチェーンの技術を用いることで有価証券の受け渡しを約定した瞬間に行うことが出来る、証券取引の常識を覆すトレードプラットフォーム。
    - 新たな機能として「Preborrow Assured Token」のファンクションを発表。（事前に保証されたトークンを借り受けることで、分散的なプラットフォーム上で空売りが出来る機能を実装）
  - tØ.comはビットコインのブロックチェーンだけでなく、あらゆるブロックチェーンの上で稼働可能になることも示唆。

- 出典：http://btcnews.jp/overstock-tee-zero-platform-disrupt-existing-market/
- 出典：http://blogs.wsj.com/moneybeat/2015/08/05/bitbeat-smart-contracts-land-on-wall-street/
- 出典：http://cryptocurrencymagazine.com/overstock-trading-platform-nasdaq
- 出典：http://www.coindesk.com/smart-contracts-platform-symbiont-issues-its-first-cryptosecurity/
- 出典：http://t0.com

スマート証券のプラットフォームを目指すSYMBIONT

- **Counterparty創業者によって設立**
  - Counterpartyによるスマートコントラクト、トークン発行、トレードネットワークの実現を目指す。
  - 金融マーケットの構造的問題の解決を目指してCounterpartyを設立した創業者が、次のステップへ向けて設立したのがSymbiont。
  - 低コストで透明性・流動性のある金融市場をブロックチェーンテクノロジーを利用し、トレーダーに提供。

- **ブロックチェーンに格納された契約が自己実行されるスマートコントラクトプラットフォームで「スマート証券」を発行**
  - スマートコントラクトによる発行・管理・決済などを行う「スマート証券」のプラットフォームを開発。
  - ブロックチェーンに格納された契約が自己実行されるスマートコントラクトプラットフォームで「スマート証券」を発行。
  - ブロックチェーン上に格納される「スマート証券」発行のプラットフォームを開発し、ウォール街との架け橋を目指す。

→ 出典：http://coinandpeace.hatenablog.com/entry/Counterparty_plus_Ripple
→ 出典：http://counterparty.io/news/announcing-symbiont/

スマートコントラクトによるデリバティブ、HEDGY

- **120万ドルの資金調達と新商品のローンチを発表**
  - Draper Fisher JurvetsonのパートナーであるTim Draper氏やSalesforceのCEOのMarc Benioff氏、Sand Hill Venturesを含む10もの投資家から120万ドルの資金調達。
  - 資金調達完了の発表に際して、マイナーを対象とした新たなビットコイン派生デリバティブ商品をローンチ。
  - この新サービスは、アメリカのビットコインマイニング企業・MegaBigPowerと、ゴールドマンサックス、BNPパリバの旧経営陣によって設立されたビットコインデリバティブ仲介企業・Crypto Facilitiesとの協力の結果、生み出されたもの。
  - このビットコインデリバティブを利用するマイナーは、ブロックチェーン上でスマートコントラクトを利用し取引を完了させ、将来ビットコインを売却する際の価格を事実上固定できる。
  - 同社CEOのMatt Slater氏は、「マイナーが市場でコインを売却しようとするとき、この商品が価格変動における問題の対処に役立つ」と語る。

→ 出典：http://bitcoinmoxy.com/matt-slater-bitcoin-smart-contract-meteor-app-devshop-sf-march-2015-2015-04-08/
→ 出典：https://www.hedgy.co/about.html
→ 出典：http://news.bitflyer.jp/news/hedgy-new-product/

イスラムの送金システムHAWARAを実現する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**
  - 送金分野において「デジタルマネーのUber」を目指す。
  - P2P送金をブロックチェーンベースでやりとりする。
  - 米国では送金業免許無しの送金代行を認めてなかった。
  - Abraはユーザーも代理人もブロックチェーンで自分のカネを保持する仕組み。

- **Abraの送金の流れ**
  - 100ドル必要だとすると、ユーザはAbraのアプリを開き、GPSを使って近くにいるテラーを探す。
  - テラーを見つけたら、どこかで落ち合い、双方ともQRコードをゲットし、取引を認証するためにスキャン。
  - 認証されたら、テラーが送金先へ100ドル送る。
  - テラーは、自身が設定した手数料を得る。（1.5%程度を推奨している）
  - Abraは取引額に対して0.25%の手数料を得る。

→ 出典: https://bitcoinmagazine.com/20951/abra-wants-uber-digital-cash-says-founder-bill-barhydt-exponential-finance-2015/
→ 出典: http://tatsuya1970.com/?p=5679
→ 出典: http://thebridge.jp/2015/04/launch-festival-2015-report
→ 出典: http://www.finextra.com/news/fullstory.aspx?newsitemid=27094

BITCOIN取引所ITBITをNYDFSが認可、銀行免許

- **NYで銀行免許を取得、世界初の公認・銀行グレードのビットコイン取引所が誕生**
  - 信託業務開始の許可を得たことで、itBitは銀行と同様に営業活動を行うことが可能となる。
  - 銀行免許を取得することで顧客の安全性を保証し、アンチマネーロンダリング対策を州の銀行法の下で行うことで、顧客に安心感を与え産業の発展に寄与していくとのこと。

- **大口のビットコイン取引向けに相対取引サービスを提供**
  - 100BTCを超える大口取引専門のOTCトレーディングデスクを開設。
  - 投資家が取引所を介さずに取引可能に。
  - 法人向けOTCトレーディングデスクに匹敵するサービスを提供することで大口投資家の獲得を目指す。

- **招待客限定で"Bankchain Discovery Summit"を7/27開催**
  - Bankchain。itBitの掲げる金融機関向けコンセンサスベースの分散台帳とのこと。

→ 出典：http://bitbitecoin.com/archives/2601
→ 出典：http://btcnews.jp/itbit-receives-first-license-in-new-york-state/
→ 出典：http://thebridge.jp/2015/05/this-is-the-first-bitcoin-exchange-to-be-licensed-in-the-u-s
→ 出典：http://finovate.com/finovate-debuts-itbits-regulated-bitcoin-trading-platform/
→ 出典：http://www.coindesk.com/itbit-to-host-private-blockchain-summit-for-wall-street-elites/
→ 出典：https://bitcoinmagazine.com/21323/itbit-announces-launch-global-otc-agency-trading-desk/
→ 出典：http://jp.forexmagnates.com/2015/07/22/%E4%BB%AE%E6%83%B3%E9%80%9A%E8%B2%A8/21576

分散型取引所『COINFFEINE』がBリリース

- **B版リリース**
  - 2014年11月、スペインのBankinterより支援を受け、今年4月にα版クライアントをリリース。
  - β版リリースによる大きな変更は、testnetからmainnetに変更された以外になし。

- **トレードシステムと資産管理システムを集中化するリスク**
  - 一般的に、サーバ上にビットコインを保管する場合、100%盗まれないような対策は不可能と言われる。
  - 取引所への入金アドレスを書き換えられ、攻撃者のウォレットへ入金するよう誘導するような攻撃や、取引所内部の管理者によるビットコインの持ち逃げのリスクなど、仮想通貨を扱うサービスは様々な問題を抱えている。

- **ビットコインを預からない分散型の取引システム**
  - クライアントにマルチシグウォレットを搭載し、デスクトップウォレットを使って直接トレードを行う。
  - 取引のオファーを出したビットコインを、約定の瞬間まで手元に置いておくことができ、取引所の安全性に疑問を持つユーザーや、すべて分散的な方法で行いたいユーザーの新たな選択肢に。
  - 法定通貨の取扱いが現在OKPayのAPIのみを介して行われているため、OKPay未対応国（アメリカ等）を除く70カ国でのみ利用可能。
  - 現時点ではOKPayアカウントを持っていないと使用できないが、PayPalなどにも対応していく予定。

→ 出典：http://cryptocurrencymagazine.com/no-more-gox-coinffeine
→ 出典：http://btcnews.jp/decentralized-bitcoin-exchange-coinffeine-beta-released/
→ 出典：http://blog.coinffeine.com/2015/07/21/coinffeine-launches-worlds-first-decentralized-bitcoin-exchange-70-countries/

銀行による国際送金利用へ集中するRIPPLE

- **スマートコントラクトプラットフォームCodiusを中止**
  - 理由は「市場が小さく、成熟していない」ため。
- **業界関係者の取り込み**
  - アドバイザーとして元アメリカ合衆国財務省のMichael Barrを迎え入れ。
    - 1月にはオバマ大統領の元経済アドバイザーGene Sperlin、3月に元国務省のAnja Manuelが加入
  - アドバイザーとしてMiranda Partners CEOのDonald Donahueを迎え入れ。
    - Miranda Partnersは金融市場インフラへのリスク関連コンサルティングを行う会社
    - Donald DonahueはThe Depository Trust & Clearing Corporation (DTCC)の前CEO
    - DTCCは昨年1600兆ドルの取引を処理するアメリカの証券およびデリバティブの決済機関
  - 連邦準備制度の委員会に選出。
    - リップルラボのビジネス開発グループ研究リーダーRyan Zagoneが連邦準備制度の Faster Payments Task Force Steering Committeeに選出
    - Ryan Zagoneは前職デロイトではペイメントイノベーションとリテールバンク戦略を担当
- **個人ユーザへの対応**
  - 6月後半より本人確認を導入。8.30が登録期限。
  - 9.1より米国市民ユーザはRipple Tradeにビットコインの入金・出金が禁止される。
  - 金融インフラに革新を起こす即時ボーダーレス送金を実現することに傾注へ。
    - Digital Asset Holdings に買収されたHyperLedgerとも競争

→ 出典: http://cryptocurrencymagazine.com/ripple-labs-elected-to-fed-steering-committee-for-faster-payments
→ 出典: http://cryptocurrencymagazine.com/ripplelabs-discontinues-smart-contract-platform-codius
→ 出典: http://cryptocurrencymagazine.com/ripple-trade-id
→ 出典: http://cryptocurrencymagazine.com/ripple-labs-treasury-official-advisory-board

その他のサービス

名称	取組み
ROSCA	• ソーシャルバンキングを標榜し、分散型のSaving & Lendingの提供を目指す、Ethereum ROSCA Application。
Mirror	• スマートコントラクトプラットフォーム。 • 個人や法人のユーザーがブロックチェーンを使って、金融にまつわる契約を起こしたり交わしたりできる。
Blossoms	• イスラムのシャリア遵法サービスを提供。
SETL	• ヨーロッパの株取引所Chi-Xの創始者が立ち上げた決済サービス。 • 利用者の身元証明を求めるブロックチェーンにしているのが特徴。 • オーナーシップや取引履歴をPermissioned distributed ledgerで維持管理するとのこと。
Toast	• シンガポールのUnbanked 移民労働者むけの送金サービス。

本章のまとめ （金融分野におけるスタートアップの動き①）

- **Overstockのブロックチェーンによるデジタル証券市場**
  - 暗号化社債（Cryptobonds）2,500万ドル分の売出準備
  - 暗号証券トレーディングプラットフォームをナスダックで披露
- **スマート証券のプラットフォームを目指すSymbiont**
  - Counterparty創業者によって設立
  - ブロックチェーンに格納された契約が自己実行されるスマートコントラクトプラットフォームで「スマート証券」を発行
- **スマートコントラクトによるデリバティブ、Hedgy**
  - 120万ドルの資金調達と新商品のローンチを発表
- **イスラムの送金システムHawaraを実現する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

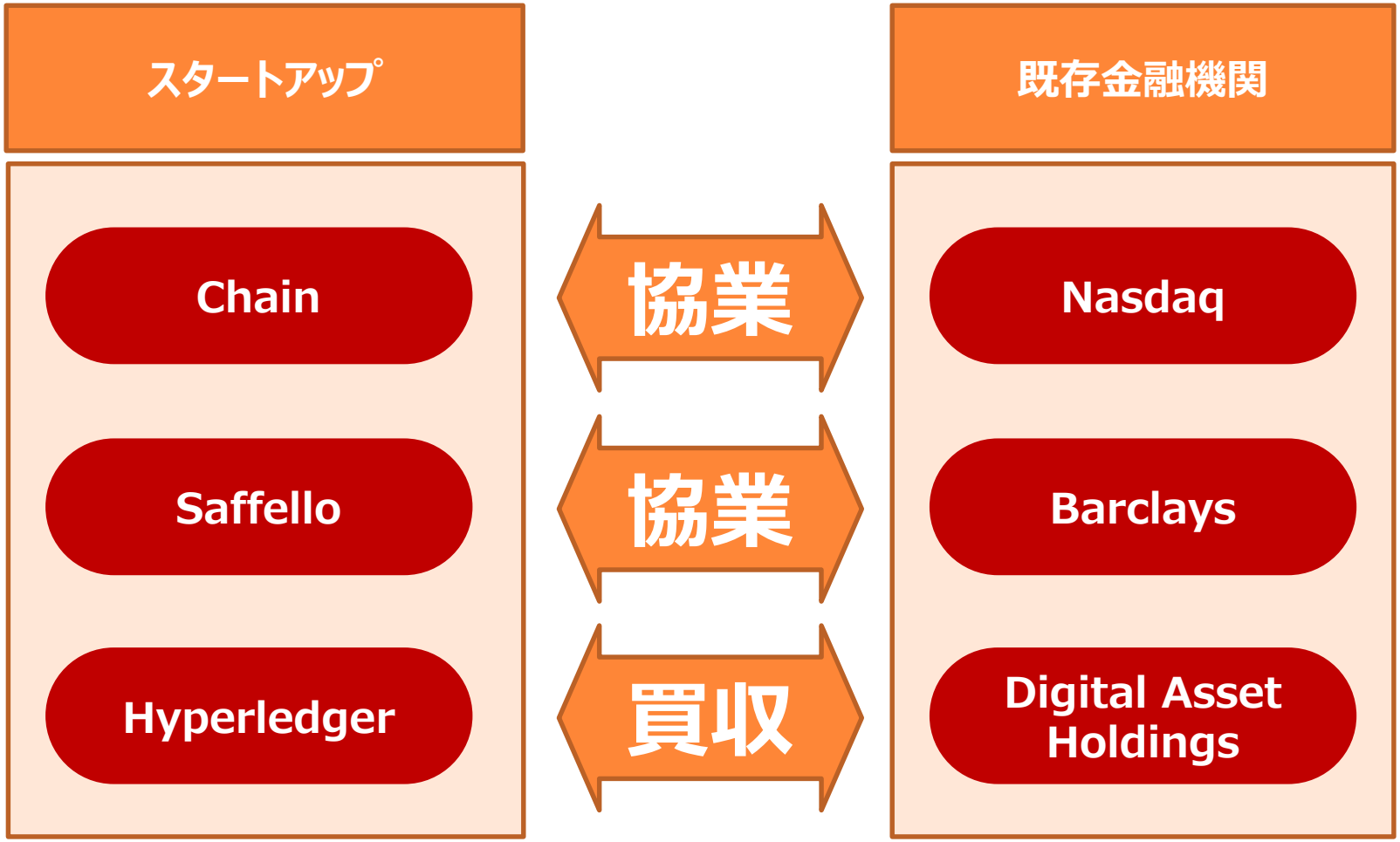
本章のまとめ （金融分野におけるスタートアップの動き②）

- **Bitcoin取引所itBitをNYDFSが認可、銀行免許**
  - 大口のビットコイン取引向けに相対取引サービスを提供
  - 招待客限定で"Bankchain Discovery Summit"を7/27開催
- **分散型取引所『Coinffeine』がβリリース**
  - ビットコインを預からない分散型の取引システム
- **銀行による国際送金利用へ集中するRipple**
  - スマートコントラクトプラットフォームCodiusを中止
  - 業界関係者の取り込みを加速
  - 本人確認など個人ユーザ対応の変質

３.金融機関とスタートアップの協業動向

- Nasdaq･Barclaysの動き
- Digital Asset HoldingsによるHyperledger買収

概略チャート


スタートアップ
既存金融機関
Chain
Saffello
Hyperledger
協業
協業
買収
Nasdaq
Barclays
Digital Asset Holdings

NASDAQ・BARCLAYSの動き

- **Nasdaqが未公開株取引パイロットプロジェクトパートナーにChainを選定**
  - Nasdaqは、ユーザーが資産を独自管理し、同社が提供するトレードプラットフォーム上で簡単に、フィアットあるいはビットコイン、デジタルトークンのペアによる交換をインスタントに行えるような仕組みを目指している。
  - Chainは、Nasdaqのオープン資産プロトコルの構築において、ブロックチェーンへアクセスするための簡易APIを提供することに合意し、分散型未公開株市場のインフラや取引システムの簡素化に貢献していく。
  - Chainは、Gyftとも組んでギフトカードのブロックチェーンベースを発表したばかり。
- **バークレイズがSaffelloとPoC実施へ**
  - UKでのビットコイン利用環境整備を目指すSafello（本社スウェーデン）、バークレイズとの間で金融機関がブロックチェーンをどのように利用できるかのPoC実施へ。
  - Saffelloは、Barclaysのアクセラレータプログラムの出身。
  - ビットコイン用いた資金転送技術の試験を開始。
  - UKの銀行がビットコイン関連企業とPoCに取り組むのは初めて。

→ 出典：http://btcnews.jp/nasdaq-enter-in-partnership-with-chaincom/
→ 出典：http://www.coindesk.com/chain-nasdaq-partnership-pr-stunt/
→ 出典：https://www.cryptocoinsnews.com/bitcoin-spending-platform-safello-deal-barclays-use-block-chain-fintech/

DIGITAL ASSET HOLDINGSがHYPERLEDGERを買収①

- **Hyperledgerの特徴**
  - 多様な台帳を作ることを認めていて、かつ各台帳が異なるコンセンサスルールを持つように設定・構成できる
- **金融機関のニーズへ対応した共有・複製台帳**
  - 多様な資産クラスに対応するため多様な台帳を作らないといけない。
  - 取引をプライベートに保たないといけない。
  - 誰が各ノードをオペレーションし、どこの国の司法管轄権の元にあるか知らないといけない。
  - 誰が台帳上に口座開設できるかコントロールできないといけない。
- **ビルトインされた暗号通貨・トークンを持たない**
  - 規制リスクや技術面のオーバーベッド、そしてボラティリティが少なくて済む。
- **コンセンサス形成アルゴリズム**
  - PBFT(Practical Byzantine Fault Tolerance)を利用
  - PoWを用いることなく秒間一万トランザクションの処理が可能
  - ブロックチェーンを使わずにコンセンサスアルゴリズムを用いて400ミリ秒以下でセツルメントを行う。
  - こうした仕組みをConsensus as a Serviceと称している

- 出典: http://www.coindesk.com/blythe-masters-blockchain-startups-hyperledger-bits-of-proof/
- 出典: http://bravenewcoin.com/news/digital-assets-holdings-reveals-plans-as-it-picks-up-two-blockchain-startups/
- 出典: http://www.digitalasset.com/static/documents/PRESS_RELEASE_Digital_Asset_Acquisitions.pdf
- 出典: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf
- 出典: http://gendal.me/tag/hyperledger/
- 出典: http://www.fifthmoment.com/can-distributed-ledgers-duplicate-m-pesa-story/

DIGITAL ASSET HOLDINGSがHYPERLEDGERを買収②

- **Distributed Ledger Platforms (DLP)として、Rippleとの相違点**
  - Rippleは、シングル台帳・トークン有
  - Hyperledgerは、マルチ台帳・トークン無

- **自分のアセットを作成可能なものとして、Counterpartyとの相違点**
  - Counterpartyはビットコインのブロックチェーン上に構築されたプラットフォームでありウォレットであり、ユーザーがtokenizationを通じてアセットを作成できる。
  - 相違点は、XCPのようなネイティブ通貨を持たないこと、ブロックチェーンではないこと、confirmation timeが数秒で済むこと。

- **Permissionedな仕組み**
  - BitcoinやEthereumはパーミッションレスな暗号通貨で、Ripple・Eris・Hyperledgerはパーミッション必要な分散型台帳システム。
  - そのため、Hyperlegerはビットコイン2.0や暗号通貨2.0という言葉を使っていない。

→ 出典：http://bravenewcoin.com/news/digital-assets-holdings-reveals-plans-as-it-picks-up-two-blockchain-startups/
→ 出典：http://www.digitalasset.com/static/documents/PRESS_RELEASE_Digital_Asset_Acquisitions.pdf
→ 出典：http://www.coindesk.com/blythe-masters-blockchain-startups-hyperledger-bits-of-proof/
→ 出典：http://www.coindesk.com/stellar-ripple-hyperledger-rivals-bitcoin-proof-work/
→ 出典：http://domsteil.com/2014/12/29/distributed-consensus-protocols/
→ 出典：https://mobile.twitter.com/Hyperledger/status/585203807904256001

本章のまとめ （金融機関とスタートアップの協業）

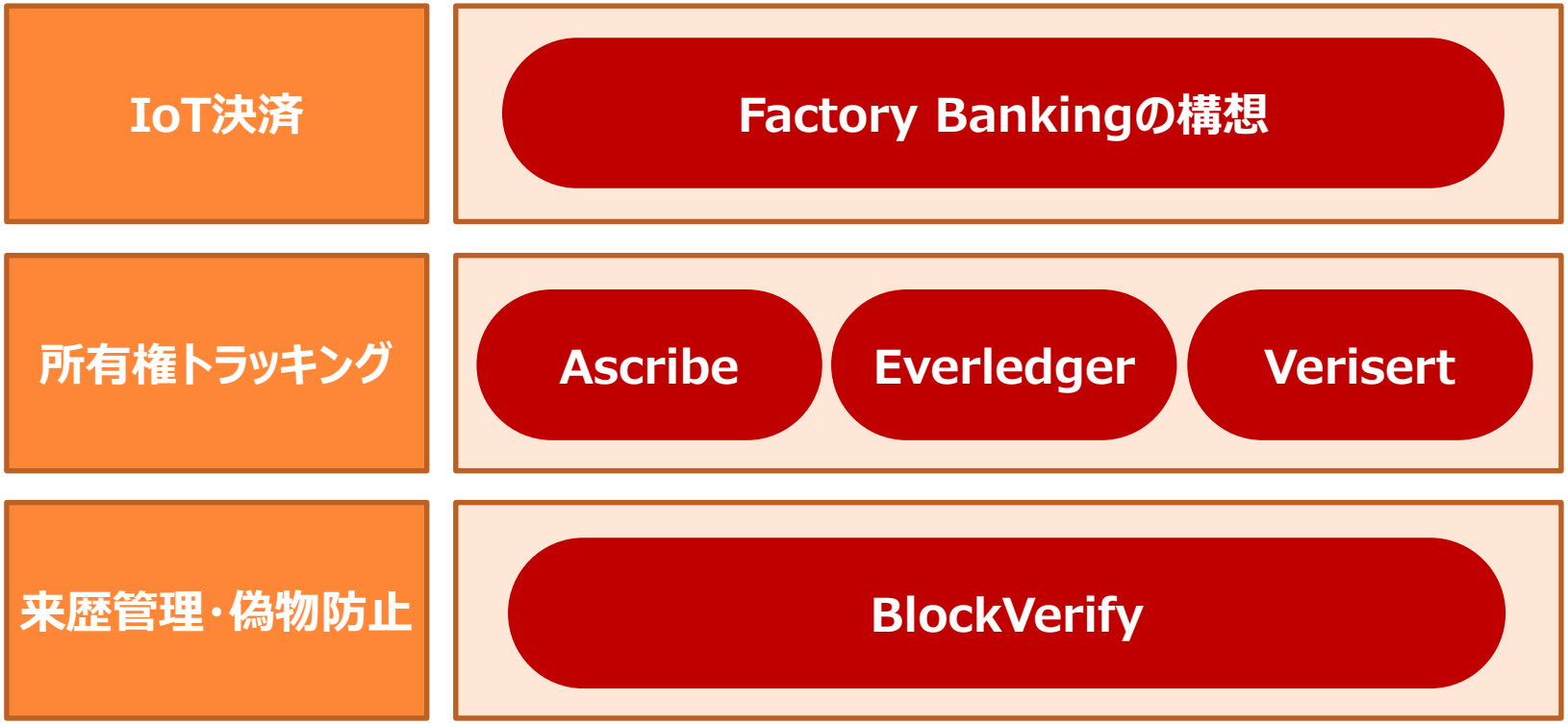
- **Nasdaq・Barclaysの動き**
  - Nasdaqが未公開株取引パイロットプロジェクトパートナーにChainを選定
  - バークレイズがSaffelloとPoC実施へ

- **Digital Asset HoldingsがHyperledgerを買収**
  - 金融機関のニーズへ対応した共有・複製台帳
  - ビルトインされた暗号通貨・トークンを持たない

４．サプライチェーン分野

- IoT決済
- 所有権トラッキング
- 来歴管理・偽物防止

概略チャート


IoT決済
Factory Bankingの構想
所有権トラッキング
Ascribe
Everledger
Verisert
来歴管理・偽物防止
BlockVerify

IoT決済分野へ適用する、Factory Banking

- **バリューチェーン上のプロセスを繋いで自律的に即時決済**
  - ドイツを中心として「インダストリー4.0」と呼ばれるIoTをモノ作りプロセス全体に適用する構想が推進中。
  - スペインBBVAは「IoTでサプライチェーンや消費行動が変わる中で金融も変わる」と述べている。
  - ここにProvenanceといったブロックチェーンによるトラッキングサービスや、ADEPTによるIoT決済サービスが絡まると、IoT時代を迎える上で「次世代の銀行サービス」になる可能性。
  - バリューチェーン上の価値流通プラットフォームとしてIoTへブロックチェーンを適用しIoT時代の次世代銀行サービスを構想する「Factory Banking」。
  - IoTとブロックチェーンを用いて、バリューチェーン上のプロセスを繋ぐことによって、自律的に即時決済する構想。
  - バリューチェーン上を流通する価値・経済を、IoTおよびブロックチェーンを適用したプラットフォームで運用しようと試みるもの。

→ 出典：http://www.dmh.co/wp-content/uploads/2015/05/Introduction-To-Factory-Banking-Daniel-M-Harrison.pdf
→ 出典：https://en.m.wikipedia.org/wiki/Factory_Banking
→ 出典：www.dmh.co/factory-banking/
→ 出典：https://www.bbvaopenmind.com/en/
→ 出典：http://monoist.atmarkit.co.jp/mn/articles/1506/03/news020.html

アート所有権管理のASCRIBE①

- **アート作品などの著作権にブロックチェーンを適用**
  - アーティストがデジタル・アートの作品を登録し、所有権を移転させたり、ブロックチェーンで履歴を確認したり、所有者を確認したりすることができる。
  - Ascribeは、オーナーシップのやりとりを安全に記録するためにブロックチェーンを用いており、後からやりとりをなかったものと否認したり改ざんしたり出来ない。
  - 画像、映像、その他デジタルメディアをアップロードし、作者・製作年・タイトルを登録。
  - Ascribe上に作品をアップロードすると、タイムスタンプを持つ「デジタル証明書」が作られる。
  - この証明書はトレーディングやトラッキングが可能。
  - インターネットのオーナーシップレイヤーを実現し、クリエイターにとってのゲームチェンジャーを目指す。

- **テクニカルアドバイザにDavid Holtzman氏が就任**
  - インターネット黎明期からのパイオニアがアドバイザーに就き、「Webのオーナーシップ層を実現する」という、Ascribeのビジョン達成をサポート。

- 出典：https://www.cryptocoinsnews.com/intellectual-property-ascribe-io-looks-revolutionize-digital-art/
- 出典：doublehash.me/1003
- 出典：https://creativecommons.org/weblog/entry/45612
- 出典：http://www.coindesk.com/blockchain-startup-2-million-intellectual-property
- 出典：https://letstalkbitcoin.com/blog/post/epicenter-bitcoin-78-trent-mcconaghy-ascribe-and-the-internet-of-ownership
- 出典：http://blocktech.com/

アート所有権管理のASCRIBE②

- **デジタル画像の偽造防止システムではない**
  - 画像にコピープロテクトをかけてオリジナリティを保証するのではなく、「作品証明書」の発行・移転。
  - 「作品証明書」をブロックチェーン上に作成し登録することができ、それぞれのエディションごとに、所有権の移転や、貸出、売買などを行うということができる。
  - 一般的な電子透かしシステムと同様に、コンテンツファイルに著作権者情報と紐付くIDを埋め込む。
  - その紐付き関係がP2P上の公開データベースに分散的に記録されるため、ファイル所有者が変わっても著作権者情報が正確に確認できる。

- **Creative Commons Franceとも提携**
  - Ascribeと組んで、フリーカルチャーのためにサイトを立上げ。
  - Ascribeを使い、アーティストが自分の作品を、帰属権を失うことなくシェアできるようにする。

→ 出典：http://doublehash.me/1003
→ 出典：http://hon.jp/news/1.0/0/6602/

ダイヤモンドの所有権証明・トランザクション履歴証明のEVERLEDGER

- **ダイヤモンド等の貴重品の存在証明にブロックチェーンを利用**
  - ダイヤモンドの所有権証明・トランザクション履歴証明に、「不変の元帳」としてブロックチェーン活用。
  - 450億ポンドが保険不正で損失、不正の64%が検知されていないといった問題に着目。
  - 保険をかけた品物が言われたとおり存在することを確認する（出処を明らかにする）ことで保険の不正を防ごうとするもの。

- **これまでに85万のダイヤモンドについてブロックチェーン上に台帳化**
  - シリアル番号やダイヤモンドの4C（カラット数など）の他、ダイヤモンドを構成する40のメタデータをブロックチェーン上に記録。
  - ダイヤ以外にも高価な時計・バッグ・アート等、保険をかけられる全ての貴重品にも使える。将来は家・車にも。

- **パブリックブロックチェーン × プライベートブロックチェーンのハイブリッド**
  - Erisベースのプライベートブロックチェーン（適用しやすい親和性）と、ビットコインベースのパブリックブロックチェーン（高いセキュリティ）を組合せたスマートコントラクト。

→ 出典：http://www.everledger.io/#!smart_contracts
→ 出典：https://www.cryptocoinsnews.com/everledger-uses-block-chain-combat-insurance-fraud/
→ 出典：http://techcrunch.com/2015/06/29/everledger/
→ 出典：http://www.reddit.com/r/Bitcoin/comments/3c6jw7/warning_hackathon_winning_blockchain_based_idea/

アート作品の証明にビットコインを用いるVERISART

- **ブロックチェーンを用いてアート作品の真正性を検証**
  - 来歴をオンライン・リアルタイムに提供。
  - アーティストには無料で提供し、作品管理に役立ててもらう。
  - アート作品の記録を標準的なメタデータと共にブロックチェーンに格納し、透明性が確立されたアート作品の台帳を構築。
  - 売り手・買い手の匿名性や機微情報の安全性確保に、ブロックチェーンのトークン技術が役立つと考えている。
  - ビットコインコア開発者のPeter Toddをボードアドバイザーに招聘。

- **アート作品のP2P流通を促進**
  - アート作品の売買には、ディールのクローズや流動性確保のために仲介人が必要とされる。
  - アート作品がオンライン上で取引されるにつれ、真正性の確認・検証が必要に。
  - アート作品の流通が年間6700億ドル、P2Pへシフト見込。

→ 出典：http://cointelegraph.com/news/114799/verisart-to-use-the-blockchain-to-verify-artwork-signs-bitcoin-core-dev-peter-todd

サプライチェーン上の偽物を防ぐBLOCKVERIFY

- **偽造薬の撲滅を通じた社会インパクトを目指す**
  - ブロックチェーンによる誠実な社会を目指す。偽造品を使うことによる影響が直接的に生じやすい製薬業界から着手している。
  - 偽薬は世界規模で経済的損失をもたらす商品のトップランクに位置づけられている。世界の薬品の1割が偽薬で、ある国では7割に上る。
  - サブサハラや東南アジアで用いられるマラリアの薬の1/3が偽薬であり、偽薬による死亡者が年間70万人におよぶ。
  - これまでも様々な工夫がされてきたものの、中央集権的で透明性が無く成功に至ってない。

- **ブロックチェーンを用いて偽造品・海賊版を防止**
  - 書き換え出来ないデータストアであるブロックチェーンを用いて、購入時にQRコードで真正品かを確認できるようにする。全てのプロダクトを資産とみなしてブロックチェーンに登録し、ユニークなIDを付与。
  - ビットコインのブロックチェーンと併せ、プライベートブロックチェーンも利用。プライベートブロックチェーンに全製品データ、オーナシップの来歴を安全に格納。消費者はプライバシーやプロダクトIDの複製を心配せずに済む。
  - 将来的には、ブランド品の衣服・ジュエリー・ダイヤモンド・家電等も対象とした、流用・盗難・詐欺の防止を目指す。

→ 出典：http://cryptocurrencymagazine.com/block-verify
→ 出典：http://bitcoinist.net/block-verify-turns-bitcoin-life-saving-technology/

本章のまとめ （サプライチェーン分野）

- **IoT決済分野へ適用する、Factory Banking**
  - バリューチェーン上のプロセスを繋いで自律的に即時決済
- **アート所有権管理のAscribe**
  - アート作品などの著作権にブロックチェーンを適用
  - デジタル画像の偽造防止システムではない
- **ダイヤモンドの所有権証明・トランザクション履歴証明のEverledger**
  - ダイヤモンド等の貴重品の存在証明にブロックチェーンを利用
  - これまでに85万のダイヤモンドについてブロックチェーン上に台帳化
- **アート作品の証明にビットコインを用いるVerisart**
  - ブロックチェーンを用いてアート作品の真正性を検証
- **サプライチェーン上の偽物を防ぐBlockVerify**
  - 偽造薬の撲滅を通じた社会インパクトを目指す
  - ブロックチェーンを用いて偽造品・海賊版を防止

5．ライフスタイル分野

- マーケットプレイス
- 動画・アートへのリワード
- ギフト・プリペイド・ポイントカード
- ゲーム
- コミュニケーション
- マイニング×日常生活

概略チャート

マーケットプレイス	OpenBazaar, Augur
動画・アートへのリワード	Streaminum, PopChest, PeerTracks
ギフト・プリペイド・ポイントカード	GyftBlock, BuyAnyCoin, Ribbit Rewards
チケット等のデジタル資産譲渡	Colu
ゲーム	Spells Of Genesis, Voxelnoauts
SNSコミュニケーション	Reveal
マイニング×日常生活	21 Inc., BitFury

分散化マーケットプレイスのOpenBazaar

1. 売り手はクライアントプログラムをダウンロードして、取引したい商品リストを提示価格を添えてネットワーク上に配信。
2. 他ユーザーが検索してヒットしたら、買い手は提示価格を受け入れるか別価格のオファーするかを商品提示した売り手ユーザーへ連絡。
3. 双方が価格に合意したらデジタル署名を交し契約成立して第三者の公証人へ送付。紛争発生時は別に仲裁人が取引に介入。
4. 公証人は契約を確認して、マルチシグ・ビットコイン・アカウント（三者のうち二者の同意でビットコインがリリースされる）を開設。
5. 買い手はマルチシグアドレス宛にビットコインを送付すると通知が売り手に届くので、商品を発送。
6. 買い手が商品受取を確認すると、マルチシグアドレスから売り手へ送金されて取引完了。
7. 買い手が送金した後に、売り手が違う商品を発送したり、商品の状態が良くない場合には、第三者が介入。
   - ✓ マルチシグ口座は、入金されたビットコインを送金先に届けるには三者のうち二者の同意が必要なので、売り手・買い手で合意するか、第三者が対処に合意するまで実際のビットコイン送金は保留。
   - ✓ 第三者の信用担保のために他ユーザーからのフィードバック評価とレーティングの仕組み。

→ 出典：https://blog.openbazaar.org/what-is-openbazaar/

分散型予測市場のAUGUR①

- **Ethereumを基盤として、完全で、P2Pで行うことができることが特徴**
  - 予測市場とは、一種のギャンブル。世の中のある未来について人々が予想を行う。
    - 例）次の米大統領選挙でどちらが勝つか、次のワールドカップでどの国が勝つか、などを対象にして掛ける
  - 集金をしたり、予想結果を仲介するディーラーのような存在がいなくても、ネットワークの参加者だけで、未来を予測し、予測結果を判定し、結果にもとづく報酬の分配ができる。
  - 未来を予測して、その予測が正しければ仮想通貨の形で報酬をもらえる。
  - いわゆるオンラインブックメーカーに近いが、単なるギャンブルの仕組みではない。
  - ブックメーカーと違うところは、オッズがないところと、分散型で胴元がないところ。

- **胴元不在で群衆の叡智による予想**
  - ブックメーカーの場合、勝ち負けのオッズは、胴元が提示する。
  - 予測市場では、オッズ自体を大衆が予想する。掛ける人が多ければ多いほどオッズは高くなる。
  - みんな自分をカネをかけるので、真剣に予想するようになる。
  - 「群衆の知恵」（The wisdom of the crowd）という実験があり、「数名の専門家の意見より、多数の素人の意見の平均値の方が、実際の値や予測値に近い」とされている。
  - Augurは要はこの群衆の知恵を有効に活用し、今までより正確な未来の予測を可能にし、より良い意思決定などに役立たせようというコンセプト。

→ 出典：http://peatix.com/event/90273
→ 出典：http://coinandpeace.hatenablog.com/entry/2015/02/11/112323
→ 出典：http://doublehash.me/tag/augur

分散型予測市場のAUGUR②

- **分散型の予測市場**
  - 賭け事は胴元がつくるのではなく、ユーザーが好きに立ち上げることができる。
  - スマートコントラクトにより、掛け金は、ブロックチェーン上でエクスローされ、結果に応じ、自動分配。
  - 既存の中央集権型の未来予測サービスの問題点
    - 信頼のおける運営体が必要であり、それゆえにそこに富が集中する傾向がある
    - 運営体がSingle Point of Failureになってしまうため、法律的な問題などがあった時などに簡単に潰すことができる
  - Augurは分散型取引所ゆえ、攻撃対象が多数に分散し、潰したり検閲するのが難しくなっている。
- **REPによる運営**
  - 市場に参加するひとの信頼度をトークン化することで、中央の判断者が不要で予測の結果を検証することができる。
  - Reputation（評判）をトレード可能な有限なデジタル資産（仮想通貨）として捉えている。
  - 未来を正しく予想できた人はReputationを受け取り、失敗するとReputationを失う仕組み。
  - Reputationを保有することで、予測の結果が正しかったどうか報告（仲裁）することができる。
  - クラウドセールを8/18～10/2で実施予定
- **P2Pデリバティブ・P2P保険のプラットフォームとしても機能**
  - 暗号通貨において、あらゆる事象におけるデリバティブ契約や保険を作ることが可能。
  - デリバティブはこの予測市場の仕組を金融にしたもの。天候デリバティブや将来の為替予測など。

→ 出典：http://peatix.com/event/90273
→ 出典：http://coinandpeace.hatenablog.com/entry/2015/02/11/112323
→ 出典：http://doublehash.me/tag/augur

分散型予測市場のAUGUR③

予測市場の運営の流れ

- Augurネットワーク上に作られた市場で賭けの対象となるイベントが発生。
- REP保有者がAugurネットワークへ結果をプライベートに報告。
- その１カ月後、 Augurからパブリックに報告が公表される。
- 賭けの参加者に対して、結果に応じた払い戻しが行われる。
- 正直かつアクティブな報告者はREP保有割合に応じてトレーディングフィーを受け取ることが出来る。
  （嘘を報告したりさぼったりするとREPを失い、そのREPは正直・アクティブな報告者へ再配布される）

REPスコアによる動機付けの仕組み

- AugurのREPはそれ自体暗号通貨ではなく、ユーザーのアドレスに紐付くスコアのようなもの。
- REP保持者はAugurの予測市場上でイベントの結果についてレポートできる。
- Augurは、REP保持者に対して、トランザクションフィーの半分をリワードとして報いる。
- REP保持者は8週間おきにレポート期間への参加を求められる。
  - 「はい」・「いいえ」・「分からない」の三択回答
  - レポートは直感的なものを重視しているため、回答にあたり特段のリサーチは不要
- 多くのREP保持者が各イベントの結果についてレポートすることや、ランダムに選択された事項についてレポートすること等から、各イベントの公正なレポートが担保される仕組み。
- 暗号化によって、コンセンサス形成前にREP保持者のレポートが公開されてしまうことを防止。
- REPの持分に応じてトランザクションフィーをキックバックする能力主義により、正確なレポートを促す。

→ 出典：http://www.augur.net/blog/what-is-reputation

分散型ストリーミングプラットフォームSTREAMIUM①

- **ビットコイン版ライブチャットサービス**
  - オープンソースのライブチャットサービスで、仲介手数料ゼロかつ秒単位で課金可能。
  - 間に立つ人は不要で、2者だけで1秒単位での課金を実現。
  - お金を得たい配信者と、お金を払ってでも見たい視聴者のマッチングを、仲介するサーバーや人を一切介さず、手数料ゼロでセキュアな取引を誰でも簡単に体験できる。
  - 動画はVPNを通して配信され、配信者と視聴者だけのあいだでのみやりとりされる。通信の秘密は秘匿される。
  - 配信者はチャネルをつくりライブ動画を配信し、時間あたりの視聴料を任意に設定でき、視聴者はその料金をビットコインで支払う。
  - 但し、現段階のStreamiumは最小限の機能を備えたコンセプトモデル。
- **想定される用途**
  - レッスン（語学や、音楽レッスン、その他個人的な指導）
  - 個人制作映画の配信・オンデマンドムービー（時間単位の課金のコンテンツ配信）
  - コンサルティングやサポート（オンラインのコンサルティング、セラピーや、問題解決、医者、弁護士）
  - 授業（オンライン課金の教育コンテンツの配信）、ポッドキャスト

→ 出典：http://btcnews.jp/the-technology-of-streamium-will-transform-internet-payment/
→ 出典：http://btcnews.jp/bitcoin-live-streaming-service-streamium-beta/
→ 出典：streamium.io/app/#/provider
→ 出典：doublehash.me/1125
→ 出典：https://medium.com/@demibre/a-decentralized-pay-as-you-go-streaming-service-b71ef89cd714
→ 出典：https://bitcoinmagazine.com/20517/5-freelancers-may-use-bitcoin-powered-streamium-cut-middlemen
→ 出典：http://insidebitcoins.com/news/blockchain-technology-and-bitcoin-micropayments-might-prevent-content-piracy/29059
→ 出典：https://github.com/streamium/streamium/blob/master/README.md

分散型ストリーミングプラットフォームSTREAMIUM②

利用手順

- 配信するのにアカウントを作る必要もなく、チャットルーム名と支払を受けるビットコインアドレス、希望課金レートを登録してチャネルを作るとリンクを受け取る。
- 視聴希望者がリンクに接続すると配信者の設定した課金レート、公開鍵、アドレスが分かる。
- 視聴したい時間分のビットコインを、システムが生成したアドレスに対して振り込むことで即座に反映され、入室できる。

秒単位課金

- ビットコイン上で1秒単位のマイクロペイメントが可能。
- 見ただけの時間が課金され、１秒単位の課金が行われる。
- 入室後、視聴者は事前に入金したビットコインから秒単位で課金。
- 放送が期待はずれだった場合は途中退室することも可能で、その場合、消費されていないビットコインの残高は自動的にすべて払い戻される。
- 配信者は視聴者が見た正味時間分の利益のみを、配信終了時に得る。

出典: http://btcnews.jp/the-technology-of-streamium-will-transform-internet-payment/
出典: http://btcnews.jp/bitcoin-live-streaming-service-streamium-beta/
出典: streamium.io/app/#/provider
出典: doublehash.me/1125
出典: https://medium.com/@demibre/a-decentralized-pay-as-you-go-streaming-service-b71ef89cd714
出典: https://bitcoinmagazine.com/20517/5-freelancers-may-use-bitcoin-powered-streamium-cut-middlemen
出典: http://insidebitcoins.com/news/blockchain-technology-and-bitcoin-micropayments-might-prevent-content-piracy/29059
出典: https://github.com/streamium/streamium/blob/master/README.md

分散型ストリーミングプラットフォームSTREAMIUM③

- **マイクロペイメントチャネル**
  - マルチシグネチャを用いた、サーバー型のシステムを必要としない、信用のいらない（trustless）決済用ライン構築技術。
    - Streamiumはマイクロペイメントチャネルを実装した初めてのアプリケーション。
    - BlockCypherによるMicrotransaction API（後述）を利用。
  - 二者間の取引を一時的にシステムによって生成されたマルチシグネチャアドレスに保持し、その間に行われた契約内容に応じてフレキシブルに資産を二者間で分割し、最後に払戻す形で両者へと資産を分割する。
  - Streamiumではビットコインの支払い額を「時間経過」で割っているが、「ページ数」や「再生時間」など他の指数で割ることで、デジタルコンテンツにおけるマイクロペイメントの可能性の幅を広げる可能性。
  - 月額課金サービスや簡易駐車場、レンタルショップ等色々なところにも応用可能。

→ 出典：http://btcnews.jp/the-technology-of-streamium-will-transform-internet-payment/
→ 出典：http://btcnews.jp/bitcoin-live-streaming-service-streamium-beta/

アーティスト向けリワードPopChest

- **アーティストへのリワードをブロックチェーンベースのマイクロペイメントで**
  - コンテンツ購入時にマイクロペイメントを用いて、アーティストに報酬を直接届ける。
  - ブロックチェーン上で監査可能で透明性ある方法で支払いを受けることが可能。
  - YouTubeなどの動画サイトを介さず、アーティストがPopChestのサーバにアップロード。
  - 処理を終えるとPopChestを埋め込まれた動画を受け取り、自身のサイトにアップしたり、PopChestのサイトにリンクしたりできる。
  - 視聴者はビットコインを支払うことで動画のロックを解除できる。

→ 出典：http://insidebitcoins.com/news/micropayments-interview-with-the-popchest-team/33527
→ 出典：popchest.com

アーティストのエクイティ取引システムを検討する 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**
  - リスナーの支払いがダイレクトにアーティストに届く仕組み。
  - アップロードされた曲にはスマートコントラクトを添付され、ファンドを自動分配。

- **アーティストトークンの発行**
  - アーティストがベースボールカードのような、自分の写真と名前の入ったアーティストトークンを作り、トークンの利用可能な総量を決める。
  - トークンはLimited editionであり、一度発行すると追加増量できない。
  - 擬似的な通貨であり、トークンの価値評価額にアーティストのアピールを反映される。

- **トークン価格の変動**
  - トークンの価値は需要と供給で決まる。
  - 名も知らぬアーティストの将来性にかけて安いトークンを購入し、そのアーティストが陽の目をみるために、その作品を購入する、という流れで、アーティストも享受できる仕組み。
  - アーティスト自身も売上やチケット収入などを使ってトークンを買い戻すことが可能で、需要を増してトークン価格に影響を行使できる。

→ 出典：http://www.billboard.com/articles/business/6655915/how-the-blockchain-could-actually-change-the-music-industry?mobile_redirection=false

ギフトカードの交換プラットフォームGYFTBLOCK

- **ブロックチェーン技術を用いて“ギフトカード2.0”構築を目指す**
  - ビットコインによるギフトカードサービスのGyftが、APIデベロッパーのChainと組んで、ギフトカードの交換プラットフォームGyftBlockを開発。
  - ブロックチェーンをギフトカードアセットの次世代プラットフォームに。
  - ギフトカードの発行・送信・交換などをブロックチェーン上で行うもの。
  - Open Assets Protocolを利用。

- **問題解決**
  - 安価ゆえ、大手企業以外にもギフトカード発行の道を拓く。
  - ブロックチェーンを利用して即時送信可能。
  - 店舗内でもアプリやWebなど、どこでも・どのデバイスでも利用可能。
  - ワンタイム利用アドレスにより、セキュリティ対策上も既存の仕組みと比べ優位。
    （スタッフのアクセスコントロール、利用状況のモニタリング）

- **既存のギフトカードを置き換えるだけではない新たな価値提案**
  - ギフトカードやクーポンなどと組合わせ、支払手段を好きに選んだり、ワンタップで償還できたりと、新たなUXも提供。

→ 出典：http://www.coindesk.com/gyft-chain-blockchain-gift-cards/
→ 出典：https://moneyconf.com/news/gyft-block-a-new-partnership-between-gyft-chain-com
→ 出典：http://www.forbes.com/sites/laurashin/2015/06/17/why-the-bitcoin-blockchain-could-make-gift-cards-a-consumer-favorite-even-more-beloved/

暗号通貨のプリペイドカード、BUYANYCOIN

- **暗号通貨のマス・アダプションにむけた課題解決としてのプリペイドカード**
  - マス層がつまずくハードルの一つが、どうすれば購入できるか分からない事。
  - BuyAnyCoinは、暗号通貨をプリペイドカードという物理媒体を以って、マス層に受入れやすくする。
  - 平均的な消費者に暗号通貨というデジタルなものへの物理的なアクセス手段を提供。

- **利用シーン**
  - コンビニ等で、BuyAnyCoinのプリペイドギフトカードを購入できる。
  - クレジット・デビット・現金いずれかで購入後、BACのWebサイトで、どの暗号通貨に変換したいかを選択して使う。

- **変換対象の暗号通貨**
  - 現時点はBitcoin、Litecoin、Rippleのみ対応。
  - 今後Nxt、Dash、Bitsharesなどにも対応予定。

→ 出典：http://cointelegraph.com/news/114576/buyanycoin-a-prepaid-crypto-card-at-your-local-store

リワードトークンのRIBBIT REWARDS

- **Ribbit.meの提供するブロックチェーンベースのリワードトークン**
  - ブロックチェーンを使ってトラッキング可能なリワードクレジット。
  - リワードを商品・サービス・法定通貨・仮想通貨と交換可能。
  - ホテル・薬局など他店舗のポイントで買物できる。

- **類似サービス**
  - ブログ・動画サービスのbitLanders：サイト訪問者へ“bitMiles” というビットコインベースのリワード

- **ブロックチェーン**
  - 最小限の手を加えた、ビットコインコアのクローン。
  - Ribbit Rewardsブロックチェーンを、完了した購買行動を蓄積する元帳として利用。
    （購買行動をトラッキング）

→ 出典：http://blogs.wsj.com/moneybeat/2015/07/02/bitbeat-how-bitcoin-technology-could-shake-up-the-loyalty-points-business/

チケット等のデジタルアセット管理、COLU

- **イスラエル発、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**
  - 開発者むけβ版をローンチ。
  - 暗号通貨だけでなく、鍵・チケット・証書・所有権など様々なトランザクションにブロックチェーンベースの承認をアドオンできる。
- **金融資産から記録、所有権まで様々なデジタルアセットを取扱可能**
  - ビットコインの知識のない人でも株式・債券といった金融資産から著作権や書類などの記録、イベントチケットや商品券・ギフトカードなどの所有権に至るまで様々なデジタルアセットをブロックチェーン上で遣り取りできるプラットフォーム。
  - BitTorrentをデータストレージとして利用。
- **チケット購入における利用シーン**
  - プリントされたチケットを受け取る代わりに数字の羅列からなる暗号化トークンを受け取る。
  - ブロックチェーンに格納されたトークンによって、ユーザがチケット購入したことが確認できる。
  - 同時に秘密鍵を受取り、この鍵を用いてチケット情報にアクセスできる。
  - トークンはQRコードに変換され、ユーザはQRコードをスマホでスキャンして会場へ行けば済む。
- **最初のパートナーとして音楽ビジネスのRecelatorを選択**
  - パートナーシップを組んで両社で権利マネジメントAPIを開発し、デジタルアセットの流通を安全に。
  - インディーズ音楽のセールス・マーケティングインテリジェンス分野のクラウドサービスプロバイダ。

→ 出典：colu.co
→ 出典：http://cointelegraph.com/news/115105/colu-launch-taps-bitcoin-blockchain-to-digitize-assets-starting-with-music
→ 出典：http://venturebeat.com/2015/01/27/colu-raises-2-5m-to-use-the-blockchain-for-something-other-than-bitcoin/

トレーディングカードゲーム、SPELLS OF GENESIS①

- **カードを集めて組み合わせて戦うゲーム**
  - スイス本社のゲーム会社EverdreamSoft社が開発。
  - 10月にβ版リリース予定。
  - ゲームはトレーディングカードゲーム＋アーケードゲームのような作り。
  - モンストのように自分のカードをぶつけて敵を倒すタイプのゲーム。
  - カードは、コミュニティの意向を取り入れ独自のものが考案される。

- **ゲームアイテムをブロックチェーンに記録して所有・トレード可能**
  - ブロックチェーンの機能をつかってトレーディングカードゲームを再現。
  - カードは、Counter Party上のアセットとして作成され、ウォレットに入れることで機能する。
  - アセットはビットコインブロックチェーン上で送受信、交換が可能。
  - Counterpartyで作られたトークン（独自コイン）がビットコインのブロックチェーンに記録されて、プレイヤーが所有・トレードできる。
  - ゲーム会社が没収したり、所有枚数を変えたりすることもできず、ビットコイン同様プレイヤー間でP2Pにセキュアに送受信することができる。
  - Counterpartyには分散トレードの機能が備え付けられており、ゲームアイテムに価格を設定し、他のプレイヤーと直接トレードすることも可能。

→ 出典：togetter.com/li/856513
→ 出典：@tyk97

トレーディングカードゲーム、SPELLS OF GENESIS②

- **ゲーム内通貨BitCrystals**
  - BitCrystalsはカード同様、Counterparty上で作られたトークン。
  - BitCrystalsはゲーム内のプレミアム通貨、およびカードの燃料として使われる。
  - 発行量は1億でロックされており限定流通。
  - 新しいカードがプレイヤーに買われると、その度に相当量のBitCrystalsが燃やされ使用不可能になる。（＝カードが買われるほど、BitCrystalsの総供給量は少しづつ減っていく）
  - カードに人気がでると追加で発行してもうけるというゲーム会社のインチキができない。
  - 発行数・保有者をブロックチェーン上で確認できる。
- **BitCrystalsのクラウドセール**
  - BitCrystalsは、カードを購入するために使われるもので、ゲーム内カードのプレセールにあたる。
  - 1BTC=15000BitCrystalのレートから開始、5日毎にレート上昇。最終日は10000BitCrystal。
  - トークンのセールス結果がゲーム性向上につながる仕組み。
    - 1150BTC集まるとユーザー同士の直接対戦が可能となり、1550BTC集まるとSoGにスマートコントラクトが実装され、運営者・第三者に頼らずにトーナメントやイベントが開催できるようになる
- **BitCrystalsを購入するメリット**
  - BitCrystalsで新しいカードパックを買うと、Appstoreなどを通すより格安でカードを購入できる。
  - BitCrystalsではないと買えないレアカードや、プレイできないステージなども用意される。

→ 出典：togetter.com/li/856513
→ 出典：http://cryptocurrencymagazine.com/more-than-1550-btc-smartcontract
→ 出典：@tyk97

マインクラフト的ゲームのVOXELNAUTS

- **ゲーム上の資産や知的財産権の管理にNXTのブロックチェーンを活用**
  - アイテムの取引・トラッキングや、ユーザが作った通貨やアセット。
  - ユーザがゲーム上で作ったコンテンツのレジストリーとしてブロックチェーンを利用。
  - ゲームユーザが自分のアート作品を作ってゲーム上にインポートできる。（家具・武器・動物など）
  - これらのオーナーシップタイトルをブロックチェーンに記録。
  - ブロックチェーン上でプレイヤーはそれら作品を売買取引可。
  - あたかもBitNationにおいて土地登記をできるように、ブロックチェーン上で自分の財産権を管理。

- **NXTを使って、ユーザ自身の通貨を作ることができるようになる予定**

- **ゲームとブロックチェーンの統合においては、通常の暗号通貨取引同様のチャレンジも**
  - 例えば取引所同様にoff-chainの仕組を導入している。

→ 出典：http://cointelegraph.com/news/114443/voxelnauts-a-minecraft-inspired-game-with-nxt-backed-property-rights-and-drm

SNSのREVEAL①

- **コンテンツを共有して暗号通貨RevealCoinを稼ぐSNS**
  - 五年間の計画は？等、テキストで質問を投稿し、15秒動画で回答。
  - 短編動画を中心に投稿される、Twitterの動画版的なSNS。
    - テキストベースではなく、スマホでの動画や写真の投稿が中心。
    - Reveal(リベール）とは、日本語で「明らかにする」という意味。動画や写真で自分の秘密を明らかにする。
  - インスタのようなティーンズ向けの新しいコミュニケーションツールにと期待される。
  - ソーシャルQ&Aアプリだが、写真・動画と暗号通貨を組み合わせた点が異なる。

- **Stellar上のアセットとしてRevealCoinを運営し、交流の動機づけに**
  - RevealCoin （RVL）というブロックチェーン上の仮想通貨が利用できる。
  - ユーザに参加のリワードとして支払われる暗号通貨RevealCoinを導入。
  - 質問者、回答者共にインセンティブを持たせるApp内独自通貨をStellarを用いて発行
  - RevealCoinはStellarネットワーク上で取引可能。
    - Stellarウォレットを導入した広告料還元型SNS
  - コインの発行総量は決まっており、ユーザ間で広告報酬を配分。
    - アテンション通貨としても機能する。

出典：http://stellar1.blog.fc2.com/blog-entry-32.html
出典：http://www.slashgear.com/reveal-ask-me-anything-an-app-for-teens-to-ask-questions-30391237/
出典：http://dtnoah.blog.fc2.com/blog-entry-181.html
出典：http://www.coindesk.com/review-reveal-mobile-social-network

SNSのREVEAL②

- **RevealCoinを通じた回答インセンティブ設計**
  - 質問への回答報酬としてRevealCoinが移動する事によって、RevealCoinに価値を持たせる。
  - これがインセンティブとなりQ&Aを活性化させ、ユーザーの拡大を狙う。
  - コインを通じ、他ユーザに質問に回答してもらうインセンティブにも。
  - 友人を招待することでコインは増える。
  - 無料の財布を作成することで1000RVLを入手できる
  - ユーザの紹介コードを用いて自身のコンテンツへの「いいね」や友達を招待することでRVLを獲得。（友人招待で10000RVL、いいねボタンで100RVLが提供される）

- **RevealCoinによる広告収入モデル**
  - 広告主はコインで広告費を支払う必要があり、コインを得るにはリアルマネーを支払うことが必要。
  - コインは直接購入することができるが、ユーザからも購入可能。
  - 人気のコンテンツにリワードが支払われ、それがネットワークを拡める動機になり、それが広告主へのアピールを高めることに繋がる、といった好循環を生み出す仕掛け。
  - 将来的に、広告事業主～ユーザ間で独自通貨RevealCoinを用いた経済圏の確立を目指す。

出典：http://stellar1.blog.fc2.com/blog-entry-32.html
出典：http://www.slashgear.com/reveal-ask-me-anything-an-app-for-teens-to-ask-questions-30391237/
出典：http://dtnoah.blog.fc2.com/blog-entry-181.html
出典：http://www.coindesk.com/review-reveal-mobile-social-network

モバイルマイニングチップによりマイニングを可能にする21.INC①

- **ネット接続端末に組込可能な、Bitcoinマイニング専用チップ**
  - 全ての電子機器に組込み、電子機器で発生する電力でマイニングを行えるASICチップを開発
  - スマートデバイスに「BitSplit/BitShare chip」と呼ばれるコアチップを組込むことを計画
  - 世界中にビットコインを普及させるため、ビットコインマイニングを生活の中に取り入れる
  - PC・スマートフォン・USB・ルーター・車・テレビ・冷蔵庫・炊飯器・電子レンジなどのありとあらゆるチップセットにマイニング用ASICを組み込むことで、日常生活の中にビットコインマイニングが溶けこむ未来を描く
  - 「BitSplit/BitShare chip」を搭載したデバイスは、電源をコンセントに差し込んだ時点から省電力なマイニングを開始し、ビットコインを獲得する
  - 採掘したビットコインの分配は、25%がユーザーの利益に、残りの75%が「21」の利益になることが現在計画されている
  - 同社の試算では、チップ１つあたり１日0.72ミリBTC（約20円）の収益が見込めるとのこと（チップ搭載家電を6つ持っていれば、ジュース一本が買える計算）

出典：http://gigazine.net/news/20150519-21-bitcoin-mining-chip/
出典：imgur.com/a/q9cbL
出典：http://btcnews.jp/bitcoin-startup-21inc-paint-a-bright-picture/
出典：http://www.coindesk.com/21-intel-bitcoin-mining-strategy/
出典：https://medium.com/@21dotco/a-bitcoin-miner-in-every-device-and-in-every-hand-e315b40f2821
出典：https://www.cryptocoinsnews.com/breaking-21-inc-releases-new-bitcoin-mining-chip-smartphones/
出典：https://medium.com/@21dotco/a-bitcoin-miner-in-every-device-and-in-every-hand-e315b40f2821
出典：http://blogs.wsj.com/digits/2015/05/18/bitcoin-startup-21-unveils-product-plan-embeddable-mining-chips/
出典：http://www.businessinsider.com.au/bitcoin-startup-21unveils-plan-to-mine-bitcoin-using-your-smartphone-2015-5

モバイルマイニングチップによりマイニングを可能にする21.INC②

- **スマホでモバイルマイニング。マイクロトランザクション絡めたIoT決済の時代へ**
  - ビットコインを市場価格で購入し、手動でビットコインを移動するよりも便利。
  - 「BitSplit/BitShare chip」を標準搭載したデバイスは、秒単位の時間課金等の「継続的な少額供給」を行うことができる画期的なサービスを構築できるようになる。
  - 各端末で生みだされたビットコインを使って、クレジットカード決済で対応しきれないマイクロペイメント(秒単位の時間課金等の超少額決済) など、従来の決済システムでは実現不可能だったサービスを可能に。
    - カフェやバー、レストランなどの席料、公共Wifiの利用に用いる
    - RFIDタグなどと連携し、レジを通さずにその場で決済できる
    - 販売後の利用に関しても課金を行うことができる
  - マイニング機能を埋め込むことによって、ビットコインをCPU・帯域幅・ハードドライブの容量・RAMといった基本的なシステムリソースと同列のものに。
    - 但し、Bitcoinの採掘には相当なエネルギーが必要のため、モバイル端末への搭載が適当かどうかは疑わしい
  - 1億1,600万ドル調達。クアルコムやインテルとも協力。
    - 前財務長官サマーズ氏がアドバイザリーボード就任へ
    - シリコンバレーでホットな7つのFintechの一つに選出

→ 出典: http://btcnews.jp/bitcoin-startup-21inc-paint-a-bright-picture/
→ 出典: http://www.coindesk.com/21-intel-bitcoin-mining-strategy/
→ 出典: https://medium.com/@21dotco/a-bitcoin-miner-in-every-device-and-in-every-hand-e315b40f2821
→ 出典: http://blogs.wsj.com/digits/2015/05/18/bitcoin-startup-21-unveils-product-plan-embeddable-mining-chips/
→ 出典: http://www.businessinsider.sg/fintech-companies-in-silicon-valley-2015-7/6/#.Va5Dtj0azCR
→ 出典: http://www.businessinsider.com.au/bitcoin-startup-21unveils-plan-to-mine-bitcoin-using-your-smartphone-2015-5

マイニング電球のBitFury

- **年内にマイニング電球をリリースへ**
  - 先日のネッカーアイランドでのBlockchain Summitでお披露目。
  - 米商品先物取引委員会長期を務めたDr. James Newsomeを役員会メンバーに招聘。
  - 2000万ドル確保して100メガワット級のデータセンター構築へ。

- **ブロックチェーンへの啓蒙を目指す**
  - ビットコインやブロックチェーンのエコシステムへのアクセス（ウォレット作成や取引利用など）を、電球をひねれば明かりが灯るが如く簡単なものにすることを目指す。
  - BitFuryを用いたアプリ開発に必要なSDKやAPIを提供予定。

- **BitFuryのロードマップ**
  - 第一段階はマイニング電球の市場化アイデア収集
  - 第二段階でプロジェクトを組成
  - 第三段階はアイデア実現チームのサポート方法検討
  - 第四段階でベストプロトを選抜してマスマーケットローンチ

→ 出典: http://www.coindesk.com/bitfury-light-bulbs-mine-bitcoin/
→ 出典: https://www.cryptocoinsnews.com/bitfurys-bitcoin-mining-light-bulb-mainly-education-tool/
→ 出典: https://www.cryptocoinsnews.com/bitfury-adds-bitcoin-heavyweights-advisory-board/
→ 出典: http://bitcoinist.net/bitfury-secures-20-million-funding-building-100mw-data-center/

本章のまとめ （ライフスタイル分野①）

- **分散化マーケットプレイスのOpenBazaar**
  - 取引の流れ
- **分散型予測市場のAugur**
  - 分散型の予測市場
  - REPによる運営、REPスコアによる動機付けの仕組み
- **分散型ストリーミングプラットフォームStreamium**
  - ビットコイン版ライブチャットサービス
  - 秒単位課金、マイクロペイメントチャネル
- **アーティスト向けリワードPopChest**
  - アーティストへのリワードをブロックチェーンベースのマイクロペイメントで
- **アーティストのエクイティ取引システムを検討する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
  - アーティストトークンの発行

本章のまとめ （ライフスタイル分野②）

- **ギフトカードの交換プラットフォームGyftBlock**
  - ブロックチェーン技術を用いて“ギフトカード2.0”構築を目指す
- **暗号通貨のプリペイドカード、BuyAnyCoin**
  - 暗号通貨のマス・アダプションにむけた課題解決としてのプリペイドカード
- **リワードトークンのRibbit Rewards**
  - Ribbit.meの提供するブロックチェーンベースのリワードトークン
- **チケット等のデジタルアセット管理、Colu**
  - 金融資産から記録、所有権まで様々なデジタルアセットを取扱可能
  - 最初のパートナーとして音楽ビジネスのRecelatorを選択
- **トレーディングカードゲーム、Spells of Genesis**
  - カードをあつめて組み合わせて戦うゲーム
  - ゲームアイテムをブロックチェーンに記録して所有・トレード可能
  - ゲーム内通貨BitCrystalsのクラウドセール

本章のまとめ （ライフスタイル分野③）

- **マインクラフト的ゲームのVoxelnauts**
  - ゲーム上の資産や知的財産権の管理にNXTのブロックチェーンを活用
  - NXTを使って、ユーザ自身の通貨を作ることができるようになる予定
- **SNSのReveal**
  - コンテンツを共有して暗号通貨RevealCoinを稼ぐSNS
  - Stellar上のアセットとしてRevealCoinを運営し、交流の動機づけに
  - RevealCoinを通じた回答インセンティブ設計
  - RevealCoinによる広告収入モデル
- **モバイルマイニングチップによりマイニングを可能にする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
  - スマホでモバイルマイニング。マイクロトランザクション絡めたIoT決済の時代へ
- **マイニング電球のBitFury**
  - ブロックチェーンへの啓蒙を目指す

6．シビックテック・公共分野

- 論点出し
- ID証明
- バーチャル国家プラットフォーム
- 宇宙開発
- 小額貯蓄・進学サポート
- 土地登記
- 予算可視化
- ベーシックインカム
- 政治投票

概略チャート

ID証明	OneName, ShoCard		
バーチャル国家プラットフォーム	BitNation	予算可視化	MayorsChain
宇宙開発	Spacechain	政治投票	Neutral Voting Bloc
小額貯蓄・進学サポート	Stellar	ベーシックインカム	GroupCurrency
土地登記	Factom		

パーソナルデモクラシーフォーラム

- **MITメディアラボのデジタル通貨イニシアチブBrian Fordeが講演**
  - ブロックチェーンのシビックイノベーションへの適用がテーマ。

- **Bryan Fordeのメッセージ**
  1. インターネットがメールだけでないように、ブロックチェーンもビットコインといった通貨だけがアプリではない。
  2. ブロックチェーンは、送金・ID管理・評価システム・マーケットといったeBayのフルスタックを包含。資金移動・ID・評価評判の真正証明の手段として活用できる。
  3. ブロックチェーンはオープンデータの未来型になりうる。
     ブロックチェーンをシビックイノベーションに活かすことが可能。
  4. 但し、シビックハッカーを巻き込むには、ソリューションベースではなく問題すべき問題を起点にすることが必須。

→ 出典：http://civichall.org/civicist/pdf15-livestream/

BLOCKCHAIN SUMMIT@ネッカーアイランド

- **メッセージは、"Make the social impact"**
  - 数十億の人々の生活をより良くするためにブロックチェーンをどう使うとよいかという、ソーシャルインパクト（問題解決）の観点で議論が為された。
  - ブロックチェーンを使って「何を出来るか」から「何をすべきか」への変曲点。
- **トピックは、ID・資産所有権・選挙・IoTなどに及んだ**
  - ビットコインコア開発者、エコノミスト、WSJコラムニスト、IoT専門家、天体物理学者、起業家、投資家、法務プロフェッショナルなど多様な分野の46名が参加。
- **論点例**
  1. 資産権利の登録・移転を通じたグローバリゼーション・仲裁。
  2. 数兆のデバイス・センサーの"自身のクラウド"を持つことを可能にするIoT適用
  3. 人身売買やアートの不正取引防止むけデジタルID
- **ID記録手段としてのブロックチェーンの活用例**
  1. ヒューマンIDによる人身売買防止。
  2. メディアIDによるデジタルコンテンツ流通。
  3. 各種デジタル資産流通のDAOを形成・統治するフレームを支えるID。

→ 出典：http://www.virgin.com/richard-branson/launching-a-high-tech-product-is-as-easy-as-screwing-in-a-lightbulb
→ 出典：https://medium.com/@willobrien/the-blockchain-finds-purpose-on-richard-branson-s-necker-island-338013d36ba1
→ 出典：http://www.marc.cn/2015/05/richard-bransons-necker-island-and-the-blockchain-summit-part-1.html

ブロックチェーンベースのIDサービス、PASSCARDを提供するONENAME

- **パスポートや免許証をリプレイスしてゆくデジタルIDサービス**
  - パスワードや、IDカードのみならず、クルマや家の鍵など、各種サービスへのアクセスコントロールに利用。
  - BitNationのDigital Identityと同じくオンラインでのユーザー名/パスワード、或いは身分証明として。
  - KPCB／Boost VC連合の投資候補先として、BlockCypher と並んで挙がっている。
- **Passcardの使い方**
  - 1.ユーザー名を登録。プロフィール情報を入れて身元を確認。
  - 2.プロフィール情報を利用してアクセス可能に。
- **Passcardによる公開API**
  - StamperyやKryptokit等が既に利用。
  - Stamperyは、存在証明(Proof of ownership)や所有権証明(Proof of Existence)サービス。
  - Kryptokitは、ウォレット関連のプラットフォームサービス。
- **Blockchain Name System(BNS)の3階層モデル**
  - DNSに似た仕組み。ブロックチェーンを用いたセキュリティやオーナーシップを保証する分散型のシステム
  - トップレイヤー(Galleries)はデータを取り出してビジュアルフォーマットに変換。
  - 中間レイヤー(Resolver)ではユーザー名からの変換などボトムレイヤーへのアクセス。
  - ボトムレイヤー(Block store)にPasscardに紐付くID情報をKeyValueStore形式で格納。

→ 出典: http://cointelegraph.com/news/112926/onename-raises-seed-funding-to-fuel-decentralized-identity-protocol
→ 出典: http://insidebitcoins.com/news/blockchain-startup-onename-launches-passcard/32545
→ 出典: http://blog.onename.com/onename-api/
→ 出典: onename.com

アイデンティティ証明のSHOCARD

- **ブロックチェーンベースのアイデンティティ証明**
  - アイデンティティ情報をセキュアにブロックチェーン上に格納するモバイルID。
  - モバイルアプリで使えるデジタル身元証明カード。
  - 身元情報をブロックチェーンに格納し、いつでも必要なときに自分の身元を証明できる。
  - フルネーム、生年月日、署名、住所など。ユーザー情報自体をブロックチェーンに格納するのでなく、その情報が正しいという証明を記録。
  - モバイル取引におけるカードホルダの身元確認で、銀行などカード発行者むけ。
  - 同様のものに、OneNameのPasscardや、BitNationのWorld Citizenship Passport。（異分野では、貴重品存在証明のEverledger、アート作品の著作権証明のAscribe）

- **使い方・仕組み**
  - ユーザーはShoCardを作成すると、書類をスキャンして署名を行える。
  - その後アプリケーションが公開鍵と秘密鍵によって厳重に保管する。
  - 書類は暗号化されてビットコインのソフトウェアを使って送信される。

→ 出典：www.shocard.com
→ 出典：http://bitcoinist.net/shocard-identity-bitcoin-blockchain/
→ 出典：http://www.coindesk.com/blockchain-identity-startup-shocard-1-5-million/
→ 出典：http://www.coindesk.com/shocards-quest-secure-identity-blockchain
→ 出典：http://coinsforest.com/p/594/

BitnationのPangeaプラットフォーム

- **Bitnation Pangea Alphaをリリース**
  - Alpha0.1.0は不安定なバージョンであり、すべての機能は使えない。
  - 公証人機能、暗号化メール機能、Dappsライブラリを提供。
  - Dappsライブラリは、Basic income、Spacechain（後述）へのリンク。
  - BitPassport(ID)、BitResolution(紛争解決)、BitLand(土地登記)、BitMarriage(婚姻登録)、BitCorp(会社設立)も計画中。
- **Bitnationの概要**
  - ブロックチェーンベースの世界で最初のヴァーチャル国家を目指すもの。
  - 今までの政府が行ってきた全てのサービスを提供し自由意志での統治を行う。
  - 究極の狙いは、新しい世界を作り出し人々が好きな国家を選ぶことができるという状態。
  - Bitnationに投資することによって暗号株式XBNXを得ることができ、将来的に配当やサービスを受けたりすることができる。(1BTC = 7256 XBNX)
- **Bitnation一周年**
  - Pangeaプラットフォームリリース
  - Citizenship IDなどパイロット試行
  - Horizon他とのパートナーシップ

→ 出典: http://cryptocurrencymagazine.com/blockchain-based-system-bitnation-pangea-alpha
→ 出典: http://cryptonewsday.com/bitnation-releases-proof-of-concept-for-decentralized-government-platform/
→ 出典: http://www.bitnation-blog.com/bitnation%E3%81%AB%E6%8A%95%E8%B3%87/?lang=ja
→ 出典: https://medium.com/@susannetarkowskitempelhof/bitnation-year-1-summary-6a1c40b4ee5a

BITNATIONとSPACECHAINが立ち上げる宇宙関連プロジェクト

- **宇宙開発プロジェクトのオープンソース化・P2P化**
  - 宇宙開発を国家レベルからSpaceXやTeslaのように民間で行えるようになったのをさらに進め、宇宙開発のオープンソース化・P2P化を図るもの。
  - オープンソースで宇宙旅行や技術開発コスト（特に役所仕事）の削減を図る。
  - BitnationとSpacechainのパートナーシップによって行われる。
  - ブロックチェーンの分散技術を用いた計算リソースやアマチュア無線家とのコミュニケーション効率化。

- **５年間ロードマップ**
  - 月面無人探査を経て五年内に有人宇宙飛行目指し、バルーン実験中。
  - 今年の計画は気球を飛ばすことからスタートされる。
  - プロジェクトを応援したい人はビットコインを送ることにより資金提供・投資が可能。

→ 出典: https://www.cryptocoinsnews.com/bitnation-prepares-launch-spacechain-first-decentralized-international-space-program/
→ 出典: http://cointelegraph.com/news/114644/bitnation-spacechain-the-mission-to-decentralize-space-exploration
→ 出典: http://www.spacechain.org/plan20152020.html
→ 出典: http://cryptocurrencymagazine.com/bitnation-spacechain-decentralize-space-exploration

新興国に注力する国際送金手段のSTELLAR

- **国連でStellarとBitpesaがプレゼン**
  - Stellarは、様々な通貨の交換機能を持ち、メールのように価値をネットワーク上で180通貨・３～5秒で転送可能。
  - 国連での演題は「新たな国際送金手段の模索」。
  - プレゼン内容はStellarの概要（仕組み・Gateway・送金など）
  - 「なぜ我々がNPOであるのか？」を強調し「誰かの所有物であってはならない。その為のオープンソースでありNPOである」と強調。
  - Stellarは新興国支援に注目しており、アフリカで少女の少額貯蓄・進学をサポートするなどに取り組んでいる。
  - Stellarのプレゼンに続いて、BitpesaのCFO Amy Ludkum氏によってBitcoinの送金方法の実演が行われた。

- **非営利組織Fast Forwardが提供するアクセラレータープログラムに選出**

- 出典：www.stellar.org/blog/first-year
- 出典：http://dtnoah.blog.fc2.com/blog-entry-167.html
- 出典：https://www.stellar.org/blog/investing-in-the-future-with-vumi/
- 出典：http://webtv.un.org/search/4th-meeting-international-conference-on-migration-and-development-theme-harnessing-migration-remittances-and-diaspora-contributions-for-financing-sustainable-development/4262303412001#full-text

FACTOM、ホンジュラスで土地登記に活用

- **ホンジュラス政府とパートナーを組んでトライアル**
  - ブロックチェーンによる土地登記でホンジュラスとパートナーシップ。
  - ホンジュラス政府とパートナーを組んで新たな土地権利に関する記録を扱う。
  - ホンジュラスは人口800万人の貧しい国であり、国のデータベースがハッキングされてしまうなど土地権利の管理に苦戦してきた。
  - Factomとパートナーを組んで半永久的でセキュアな土地権利記録ができるようブロックチェーンテクノロジーを利用し開発する。
  - Factomの技術を使用して、土地所有権登記所を構築。
  - 公文書がない土地のほぼ60パーセントの所有者に、公式に彼らの資産を登録する
  - 土地所有権の記録は国の活動の基盤であることから、ブロックチェーンが役に立って、国が立ち直っていくことが期待される。

- 出典：http://cryptpark.com/members/admin/activity/9872/
- 出典：http://cryptocurrencymagazine.com/factom-honduras-partnership
- 出典：http://www.coindesk.com/factom-land-registry-deal-honduran-government/
- 出典：https://uk.news.yahoo.com/honduras-build-land-title-registry-using-bitcoin-technology-162701917.html#GSQNCvP

ベーシックインカムを提供するGROUP CURRENCY

- **ベーシックインカムを提供する暗号通貨**
  - 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。
  - 他の暗号通貨と異なり、メンバーの身元が特定される。身元の特定されたメンバーに対してベーシックインカムを提供。

- **グループを形成して資金調達**
  - 学生研究者や教授が学内横断でグループを形成し、研究成果へのアクセスに課金することで資金調達。
  - ゲーム開発者が次のヒット作品に向け、グループを形成し、ゲーム内資産と引換にグループ通貨を受入。

→ 出典：groupcurrency.org
→ 出典：https://www.cryptocoinsnews.com/cryptocurrencies-bring-world-universal-basic-income/

市政予算の可視化を目的にMAYORSCHAIN

- **ロンドン市長選候補者が提唱**
  - 予算・支出をブロックチェーン上で記録・トラッキング。
  - 5%コスト削減目指し、ロンドン市民が改善提案を出せるクラウドソーシングの仕組とセット。

- **ブロックチェーンによる直接民主制を目指す**
  - 予算配分や使途を可視化し、市民による予算管理・監視を協調して行うDecentralized City Governanceモデル。
  - 予算決定に直接携わったり、提案をテーブルに載せたり投票に参加したりなど。投票などの結果もブロックチェーン上に安全かつ永遠に保管し、誰もが参照可能にする。

- **パートナー**
  - 協力しているHorizonとBlocknetは、BitNationともパートナーシップ締結済。
  - StartJOINがクラウドファンディングキャンペーンを主催。

→ 出典：mayorschain.com

ブロックチェーンによる‘Political App’、Neutral Voting Bloc

- **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**
  - 真の民主制を目指してオーストラリアでローンチしたPolitical Appであり且つ政党でもある。選ばれた議員は、参加者によってどのような投票行動をとるべきかを伝えられる。
  - そのため投票参加者は常に議会の議決・投票をコントロールできる。政治活動のアウトプット品質を高めるような批判的環境を育む。
  - 政策ではなくこうした環境にフォーカスすることによって、民主主義をアップグレードすることを目指す。投票はブロックチェーン上に格納される不変の記録を通じ、透明かつオンラインで行われる。
- **中立性確保の追求**
  - 投票は一旦確定すれば皆が参照でき変更できない。特定の政策に肩入れしない他、自身も政策を有することなく中立を保つ。あらゆる政党、オーストラリアのあらゆる選挙民が参加できる。
  - ブロックチェーンにより、いかなる政党も投票を操作したり検閲したりできない。この様に、短期的な政策よりも長期的な中立性を重視。
  - 選ばれた職員との間で統一性を損ねる行動ができないよう厳格に契約で規定するため、投票参加者の権利が損なわれることはない。

→ 出典：nvbloc.org
→ 出典：http://cointelegraph.com/news/114404/true-democracy-worlds-first-political-app-blockchain-party-launches-in-australia

本章のまとめ （シビックテック・公共分野①）

- **パーソナルデモクラシーフォーラム**
  - ブロックチェーンのシビックイノベーションへの適用がテーマ。
- **Blockchain Summit@ネッカーアイランド**
  - メッセージは、“Make the social impact”。トピックは、ID・資産所有権・選挙・IoTなど
- **ブロックチェーンベースのIDサービス、PassCardを提供するOneName**
  - パスポートや免許証をリプレイスしてゆくデジタルIDサービス
- **アイデンティティ証明のShoCard**
  - ブロックチェーンベースのアイデンティティ証明
- **BitnationのPangeaプラットフォーム**
  - Bitnation Pangea Alphaをリリース
- **BitnationとSpacechainが立ち上げる宇宙関連プロジェクト**
  - 宇宙開発プロジェクトのオープンソース化・P2P化

本章のまとめ （シビックテック・公共分野②）

- **新興国に注力する国際送金手段のStellar**
  - 国連でStellarとBitpesaがプレゼン
- **Factom、ホンジュラスで土地登記に活用**
  - ホンジュラス政府とパートナーを組んでトライアル
- **ベーシックインカムを提供するGroupCurrency**
  - ベーシックインカムを提供する暗号通貨
- **市政予算の可視化を目的にMayorsChain**
  - ブロックチェーンによる直接民主制を目指す
- **ブロックチェーンによる‘Political App’、Neutral Voting Bloc**
  - 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

7．イノベーション推進エコシステム

- Dappsのコミュニティ、Corona
- Blockstrapが開発者向けワークショップ
- ブロックチェーン専門VCのBlock26
- 名門VCのKPCBがブロックチェーン進出
- デロイトのイノベーション促進組織Rubix
- ビットコイン・ブロックチェーンに注力するVCリスト

DAPPSのコミュニティ、CORONA

- **Dapps開発に資金面・教育面でサポートする開発ネットワーク**
  - Dapps開発ネットワークのCoronaがビットコイン2.0をプロモート
  - 申込フォームに記入して審査された上で資金融通などを行う。

- **クラウドファンディングも開始**
  - Dappsの開発者ネットワークCoronaによるクラウドファンディングの仕組み - Hybrid Proof of Participation(HPoP)。
  - ビットコイン他、様々な暗号通貨で出資するとCoronazというメンバーシップクレジットを得てDappsへアクセスできる。
  - Bitcoinの他にRipple, NXT, Bitshares, Stellar, NEM, モナコイン, Counterparty, Storjcoinx, Getgems, Swarmなどに対応。

出典: https://bitcoinmagazine.com/20347/decentralized-application-development-network-corona-launches/
出典: http://bitcoinist.net/corona-promotes-bitcoin-2-0-provides-funding-developers/
出典: http://cointelegraph.com/news/114285/decentralization-is-a-market-force-inside-the-corona-dapp-network
出典: http://blog.crypti.me/crypti-corona-announce-strategic-dapp-focused-partnership/
出典: http://www.newsbtc.com/2015/05/29/corona-network-announces-innovative-crypto-crowdfunding-model/
出典: corona.info/#fundraiser
出典: http://www.prweb.com/releases/2015/05/prweb12751582.htm
出典: http://allcoinsnews.com/2015/06/01/corona-developer-network-introduces-multi-cryptocoin-crowdfunding-platform/

BLOCKSTRAPが開発者向けワークショップ

- **ブロックチェーンツールキットのBlockstrapによるワークショップ**
  - Blockstrapは、五月に行われたシンガポールDBSのブロックチェーンハッカソンもサポート。
  - イスタンブール、アムステルダム、バルセロナ、プラハ、ベルリン、ロンドンにて。
  - アムステルダムではBitcoin Embassyがhost。

- **ブロックチェーンのイロハから、トランザクションやマイニング、APIを使ったブロックチェーンアプリの作り方まで学ぶワークショップ**
  - Blockstrapのブロックチェーンワークショップは、ブロックチェーンに関する教育機会・気づきの場を提供した上で、ハッカソンが続く、アクセラレータプログラムの一環とのこと。
  - ブロックチェーンワークショップは受講料無料で、さらに特典としてCoindeskが五月に発行した'Cryptocurrency 2.0 report'（2.0の事例集）を半額提供。

- 出典: http://insidebitcoins.com/news/bitcoin-embassy-amsterdam-to-host-beginners-guide-to-blockchain-technology-event/33302
- 出典: http://allcoinsnews.com/2015/06/18/blockstrap-block-chain-space-accelerator-launch-european-workshops-backed-by-seedcoin-coinsillium/
- 出典: http://blockstrap.com/en/events/blockstrap-barcelona-complete-beginners-guide-blockchain-technology/
- 出典: http://blockstrap.com/en/blog/announcing-european-startingblock-2015-tour/
- 出典: http://blockstrap.com/en/blog/dbs-blockchain-hack-de-brief/
- 出典: http://www.coindesk.com/blockstrap-launches-blockchain-workshop-series-for-beginners/

ブロックチェーン専門VCのBLOCK26

- **ファイナンスだけでなく、サービスの協働開発や、新技術の買収・ライセンシングまで行うVC運営**
  - テクノロジーリサーチのPedram Hasid、ビジネスデベロッパーのNicoel Stark、クリエイティブディレクターのMatt Wignallから成るチーム。
  - ファイナンスやテクノロジー、マーケティング、サプライチェーン等の専門家がブロックチェーンスタートアップを支援するとのこと。

- **投資先**
  - ブロックチェーン専門のBlock26、初の投資はモバイルビットコインウォレットのAirbitzに125万ドル。
  - NYのInsideBitcoinConferenceで1位獲得していたもの。

- 出典：http://www.newsbtc.com/2015/06/23/block26-venture-capital-platform-to-fund-blockchain-startups/
- 出典：block26.com/about/
- 出典：block26.com/team/
- 出典：http://bitcoinvox.com/article/1770/block26-new-blockchain-venture
- 出典：https://www.cryptocoinsnews.com/airbitz-gets-450000-cash-injection-block26/
- 出典：https://play.google.com/store/apps/details?id=com.airbitz

名門VCのKPCBがブロックチェーン進出

- **KPCBの概略**
  - GoogleやUber, Amazonへの投資で知られるVC、Kleiner Perkins Caufield and Byers。

- **ブロックチェーン特化ファンド“KPCB Edge”**
  - ビットコインやブロックチェーン関連スタートアップ特化ファンド立上げ。
  - ブロックチェーンの他、VR、デジタルヘルス、ドローン関連など全6分野に特化したVCファンド。
  - KPCBは投資先の発掘にむけBoost VCとの協業が見込まれる。
  - 現在の投資候補先は、BlockCypher とOneName。

- **提携先Boost.vcの概略**
  - ビットコインおよびデジタルリアリティ（VR/AR）特化のアクセラレーター。
  - Boost VCもビットコインへの注力を発表。
  - Boost VCの昨冬選抜先のTribe5では、CoinPrismやRevealなど。
  - 現在、Tribe6の申込受付中。

→ 出典：https://bitcoinmagazine.com/20957/leading-silicon-valley-vc-firm-shifts-focus-toward-bitcoin/
→ 出典：www.kpcbedge.com/about
→ 出典：http://www.kpcb.com/blog/design-in-tech-report-2015
→ 出典：https://www.slideshare.net/slideshow/embed_code/key/xkFK0gQy5Funvi

デロイトのブロックチェーンやスマートコントラクトによるイノベーション促進組織RUBIX

- **金融仲裁自動化・リアルタイム監査・登記やポイントのデジタル化等を視野**
  - デロイトがトロントでブロックチェーンやスマートコントラクトによるイノベーション促進組織立上げ。
  - 取引先との金融仲裁自動化、決算ステートメントのリアルタイム監査、土地登記・ロイヤリティポイントのデジタル化など。監査の自動化なども構想。

- **デロイトの主張**
  - 金融機関がSidechain, Counterparty, Factom, Ripple, Ethereumの活用を探索しているだけでなく、流通業でもGyftの様にリワードプログラムなどの取組みが進展。

→ 出典：rubixbydeloitte.com

ビットコイン・ブロックチェーンに注力するVCリスト

名称	主な投資先
FuturePerfect VC	Abra, BitPesa, Blockstream
A16Z	Ripple Labs, 21 Inc., Coinbase, OpenBazaar
Digital Currency Group	BitPesa, BitX, Coinbase, Circle, Ripple Labs
RRE Venture	itBit, 21Inc, Mirror, Ripple Labs
Ribbit Capital	Blockstream, Coinbase, Ripple Labs
Union Square Venture	Coinbase, OpenBazaar, OneName
Boost VC	BlockCypher, Reveal
AME Cloud Ventures	Blockstream, Ripple Labs, ShoCard, BlockCypher
IDG Capital Partners	Ripple Labs
Khosla Ventures	21 Inc., Blockstream, Chain

- 出典：http://www.coindesk.com/10-vc-firms-bullish-on-bitcoins-potential/
- 出典：http://www.coindesk.com/future-perfect-vc-blockchain-opportunity/

本章のまとめ（イノベーション推進エコシステムの動向）

- **Dappsのコミュニティ、Corona**
  - Dapps開発に資金面・教育面でサポートする開発ネットワーク
- **Blockstrapが開発者向けワークショップ**
  - ブロックチェーンのイロハ、トランザクションやマイニング、APIによるブロックチェーンアプリ開発迄
- **ブロックチェーン専門VCのBlock26**
  - ファイナンスだけでなく、サービスの協働開発や、新技術の買収・ライセンシングまで行うブロックチェーン専門VC
- **名門VCのKPCBがブロックチェーン進出**
  - ブロックチェーン特化ファンド“KPCB Edge”
  - Boost.vcと提携
- **デロイトのブロックチェーンやスマートコントラクトによるイノベーション促進組織Rubix**
  - 金融仲裁自動化・リアルタイム監査・登記やポイントのデジタル化などを活用の視野に

８．ブロックチェーン2.0サービス開発

- ブロックチェーン2.0サービス開発にむけて思うこと
- ブロックチェーンベースのサービス検討論点試案

1995年～1996年のインターネット界隈

- **2014年～2015年のビットコイン界隈は、1995年～1996年のインターネット界隈に例えられることが多い。**（※VC投資額ベース：State of Bitcoin Q2 2015、P38）
- **では、1995年～1996年はどんな様子だったか？**

1994年	1995年	1996年
• Netscape Navigator • Yahoo!登場 • インターネット接続ホスト数が320万台 • 米ホワイトハウスがホームページを開設 • 首相官邸がホームページを開設 • インプレスがインターネットマガジン創刊	• ソニーがウェブサイトを開設 • 渋谷にインターネットカフェ • インターネット接続ホスト数が820万台 • Amazon.com開始 • Windows 95発売 • 「インターネット」が95年の流行語に選定 • 映画「ザ・インターネット」	• ヤフージャパン、楽天起業 • ソニーが「So-net」を開始 • インプレス、INTERNET Watch正式創刊 • 米Yahoo!が株式上場 • インターネットホスト数が1,000万台 • Windows NT4.0発売 • NTTがインターネット接続「OCN」開始

- **ブロックチェーン界隈でも、インターネットにおけるWindows、Amazon、Yahoo!にあたるようなビジネスモデル・技術を確立していかないといけないステージ**
  - 8月初時点、ビットコインウォレット数は390万に留まる
  - インターネット接続ホスト数でみると1994年10月と同水準

→ 出典：http://i.impressrd.jp/e/2007/08/22/113/
→ 出典：https://blockchain.info/ja/charts/my-wallet-n-users
→ 出典：http://www.infonet.co.jp/ueyama/ip/internet/hosts_tbl.html

実証実験のフェーズは終わった

- **「既存の○○をブロックチェーンで実現」という実証実験（PoC）のフェーズは終わり**
  - なんでもかんでもブロックチェーンに紐付けて考えるのではなく。
- **一般の人たちのニーズに寄り添って、下世話な問題が何で、それをどうすれば解決できるかが最初**
  - MITのBryan Fordeも「シビックハッカー巻込にはソリューションでなく問題解決で」と発言。
  - ネッカーアイランドでのBlockchain Summitでも「ソーシャルインパクト」がキーワード。
- **これからは利用者目線に立ったサービスアイデアがないと次のステージに立てなくなる**
  - 利用者の下世話なニーズ（怒り・不満足・解決すべき課題）に寄り添ったブロックチェーンサービス。

誰のどんな課題に対して解決策を出すか

- **ブロックチェーン応用範囲は広範かつ多様**
  - 下世話な話から、金融ビジネス、ひいては社会インパクト生む壮大な話まで。
  - 日常生活の中の下世話な話
    - Streamium（ストリーム配信）、GetGems　（SNSチャット）
  - 金融ビジネス
    - Swarm　（資金調達）、Medici　（株式市場）
  - 社会インパクト
    - Factom　（新興国の土地登記管理）、Bitnation SpaceChain（宇宙開発）
- **共通するのは、どれも、現状への苛立ち・不満・怒り・矛盾などへの解決手段としてブロックチェーンを使っている点**
  - 客がいない・使ってもらえないことには、1990年代後半から2000年代前半にかけてのインターネットのような、マス・アダプションもない。
- **誰のどんな課題に対してブロックチェーンでこれまでにない解決策を出せるか**
  - 下世話系でいくなら下世話なレベルで何が不満持たれてるのか？
  - 金融ビジネスでいくなら決済やプロセスのどこに課題あるのか？
  - 社会インパクト系でいくなら社会レベルで解くべき課題が何なのか？
  - 現実・現場見据えて課題を特定することが、ブロックチェーンのマスアダプションを果たす近道。

例えば新興国マーケット

- **ビットコイン業界には、1995年頃のインターネット業界並みの資金は入っているものの、技術のフィージビリティ・ビジネスの金脈発見双方、ギャップを埋める必要。**
  - スケール等の課題を抱えつつも試行できる環境で、ブロックチェーンでしか解決できない課題に試行錯誤繰り返すという意味では、金融分野・日常生活いずれも新興国マーケットに着目も一案。
  - 新興国でBitPesaなどスマホ送金のような技術x身近課題や、Factomのホンジュラス試行のように社会課題にアプローチしながら引出していくのはあり。

- **例えば、都市のイノベーション目指してGoogleが設立したSidewalk Labsであれば、都市を巡る非効率の解決にブロックチェーンを使う等。**
  - BitNationのようなガバナンスサービス効率化
  - FactomやAscribeのようなデータ管理
  - GroupCurrencyによるベーシックインカムのような所得配分
  - ADEPTやFactoryBankingのようにIoT絡めたバリューチェーン効率化
  - SAPIENCE AIFXのようにIoTとAI（DeepLearning）絡めたスマートコントラクト、等

ブロックチェーンベースのサービス検討論点試案

ユーザ理解Layer	L1	**ターゲットユーザ** 一般消費者か、金融機関やメーカーなど法人か、もっと広い社会か、等
	L2	**ユーザのGain・Pain** 何が不平不満怒り、嬉しさ・望みだったりするか。（消費者なら下世話な課題、銀行プロセスやサプライチェーンなら業務課題、広く社会にアプローチするなら壮大な社会課題） 例：「ゲームに飽きて次のゲームをやる時に、ポイントやアイテムが引き継げない・・」
提案価値Layer	L3	**ユーザのGainを殖やす・Painを減らすには** 例：「ゲームに飽きたら他人に暗号通貨でトレードすることもできるようにしたら？」
	L4	**サービス内容（そのためにどのユーザに何を提供するか）** 例：「ゲーム内コンテンツと暗号通貨の交換が可能なトレーディングカードゲーム」
仕組みLayer	L5	**ユーザとの関わり方** 対象（トークン、株式、ギフトカード、スコア、通貨など） アクション（上記の対象を、買うなり・稼ぐなり・シェアするなり） **ブロックチェーンの使い方** サービス提供のためにブロックチェーンを何の用途で使うか。（金融分野であれば、資金調達手段・小口決済手段・契約などの証明手段など）
	L6	**ビジネスの収益性** どうやって収益得るか？誰と組むか？（小売とギフトカード、メーカーとサプライチェーン、保険会社とダイヤ保証など） **エンジニアリング実現性** やりたい用途にFitした技術・手段は何か。IoTやID認証の仕掛けをどうするか。 **運営モデルの実効性** AugurのREPのようなインセンティブ付けや、Dapps・DAOのガバナンス・意思決定の仕組をどうするか。

本章のまとめ （ブロックチェーン2.0サービス開発の考察）

- **1995年～1996年のインターネット界隈**
  - 2014年～15年のビットコイン界隈は、1995年～96年のインターネット界隈に例えられることが多い
  - 当時を振返ると、ブロックチェーン界隈でも、インターネットにおけるWindows、Amazon、Yahoo!にあたるようなビジネスモデル・技術を確立していかないといけないステージ

- **実証実験のフェーズは終わった**
  - 「既存の○○をブロックチェーンで実現」という実証実験（PoC）のフェーズは終わり
  - 一般の人たちのニーズに寄り添って、下世話な問題が何で、それをどうすれば解決できるかが最初
  - これからは利用者目線に立ったサービスアイデアがないと次のステージに立てなくなる

- **誰のどんな課題に対して解決策を出すか**
  - ブロックチェーン応用範囲は広範かつ多様だが、共通するのは、どれも、現状への苛立ち・不満・怒り・矛盾などへの解決手段としてブロックチェーンを使っている点
  - 誰のどんな課題に対してブロックチェーンでこれまでにない解決策を出せるか

９．基盤・プラットフォーム関連

- ブロックチェーンのAWSを標榜する、BlockCypher
- 一定期間、情報を暗号化できる、TimeChain
- 開発者むけプラットフォーム、Sidechain Element
- Dapps開発プラットフォーム、Eris
- ブロックチェーンによるDapps開発基盤、Ethereum
- 分散型クラウドコンピューティング技術、Enigma

ブロックチェーンのAWSを標榜するBLOCKCYPHER

- **マイクロトランザクションのAPI等を提供**
  - Transaction API、Microtransaction APIを提供。
  - これらのAPIによって、マイクロトランザクションを用いたブロックチェーンアプリを開発できる。
  - 例えばAppleが30%のフィーを課すなど、従来は1ドル以下の少額決済はトランザクションコストとの見合いで成立しなかった。
  - Microtransaction APIによって、0.5セント相当のマイクロトランザクションが可能となり、ECにインパクトを与える可能性。
  - Microtransaction APIはストリーミングStreamiumで利用。

- **Zero-confirmation Confidence FactorはConfirmationを数秒に短縮**
  - 従来のビットコインのconfirmationで10分要し、売り手にとってリスクだったものを数秒で済ます。
  - Zero-confirmation Confidence Factorは、金の取引所Vaultoroで利用。

→ 出典：http://exponential.singularityu.org/finance/qa-with-blockcypher-ceo-catheryne-nicholson-on-blockchain-technology
→ 出典：https://moneyconf.com/news/pitch-at-moneyconf
→ 出典：https://moneyconf.com/news/pitch-at-moneyconf
→ 出典：http://www.programmableweb.com/news/blockcypher-microtransaction-api-lowers-micropayments-cost/2015/06/10
→ 出典：http://jp.techcrunch.com/2015/01/16/20150114blockcypher-raises-seed-funding-to-be-the-web-services-for-cryptocurrency/

一定期間、情報を暗号化できるTIMECHAIN

- **一定期間、情報を暗号化できるサービス**
  - スマートコントラクトの機能拡張として。
  - 一定期間後にビッドが開封されるオークション、或いはDAC運営などに有効。
  - 取引所やエスクロー、ウォレット、スマートコントラクト等。

- 出典：roberts.pm/timechain
- 出典：http://cointelegraph.com/news/114691/the-timechain-improving-smart-contract-technology-using-time-locks
- 出典：http://www.gwern.net/Self-decrypting%20files
- 出典：https://www.cryptocoinsnews.com/sending-messages-future-timechain-cryptocurrency-security/

開発者むけプラットフォームSIDECHAIN ELEMENT

- **開発者むけプラットフォームSidechain Elementが公開**
  - 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。
  - Sidechain Elementは、現時点ではR&Dレベルのため、製品提供版リリースまでは現実資産に適用しないように強調されている。
  - Sidechain Elementは、ビットコインの持つ分散型でP2Pのネットワークを活かして、中間介在人のいない新たなビジネスモデル（特に金融分野における業務プロセスの破壊的革新）を作りだす上で必要な機能を提供。

- **Sidechain自体の詳細**
  - 後述

出典: www.blockstream.com/developers/
出典: http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
出典: https://github.com/ElementsProject/elementsproject.github.io
出典: https://people.xiph.org/~greg/blockstream.gmaxwell.elements.talk.060815.pdf
出典: http://diyhpl.us/wiki/transcripts/gmaxwell-sidechains-elements/
出典: www.blockstream.com/developers/
出典: http://techcrunch.com/2015/06/13/down-the-blockchain-rabbit-hole/
出典: http://www.coinspeaker.com/2015/06/16/bitcoin-3-0-sidechain-elements-by-blockstream-lightning-network-and-more/
出典: http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/
出典: http://btcnews.jp/blockstream-released-sidechain-elements/

DAPPS開発プラットフォーム、ERIS①

- **Dapps開発プラットフォームとして、開発ツールを提供**
  - 銀行向けのサービスではなく、誰もが知識や同意なしにサーバ仲介不要な分散アプリを開発できるプラットフォームを提供。
  - ブロックチェーンを一連のスマートコントラクトのまとまりにすることを目指す。
  - EPM(Eris Package Manager)とELM(Eris Legal Markdown system)を提供。
    - EPMはスマートコントラクトのコンパイル・デプロイ・テストをまとめて行うもの。
    - ELMは法的契約条項をスマートコントラクトに組み込むもの。

→ 出典：https://blog.erisindustries.com/about%20eris/2014/12/17/eris-what-are-we-building/

DAPPS開発プラットフォーム、ERIS②

- **Erisが提供する開発ツール（データベース、アプリサーバ）**
  - ErisDB：Theloniousはオープンソースのブロックチェーンデザイン。
  - ErisServer：Decerverは分散アプリサーバ。

- **ErisDB：Theloniousはオープンソースのブロックチェーンデータベース。**
  - 単一のブロックチェーンではなく多くのブロックチェーンの集合体。
  - アプリロジックを安全に保持・分散する仕組み。
  - Theloniousはフレキシブルなブロックチェーンであり、セキュリティやコンセンサスのパラメータ設定をコマンドベースで可能。パラメータはブロックチェーン上のハードコーディングでなくGenDougに書き込まれる。
  - GenDougはスマートコントラクトをトラッキングするカーネル。
    - このカーネルによって、マイニングインセンティブやトークン無しにブロックチェーンを安全に保つことが出来る。
    - そのためErisは通貨・トークンをビルトインしていない。

- **ErisServer：Decerverは分散アプリ開発のためのアプリサーバ。**
  - Decerverを使うとBitcoinモジュール・Ethereumモジュール・Theloniousモジュール等、他の分散プロトコル・任意のAPIトークン接続可に。

→ 出典：https://blog.erisindustries.com/about%20eris/2014/12/17/eris-what-are-we-building/

ブロックチェーンによるDAPPS開発基盤 ETHEREUM①

- **分散型アプリケーション（Dapps）の開発プラットフォーム**
  - 誰もが容易に分散ネットワークを使って、ブロックチェーン技術の便益に供することができるようにする
    - 分散ネットワーク上でアプリケーションを構築・稼働できるプラットフォームを構築することによって、インターネットをDecentralizeすることを目指す（ビットコインがペイメントでやっているようなこと）
    - コントラクト（オブジェクト）が作れて、メッセージを送れて、値が保持できる
  - 既存サービスのDecentralize：個人を直接接続し、第三者の介入を取除きコストや手数料を削減
    - 分散型予測市場Augur、分散型IoT基盤Adept、SCMトラッキングProvenanceなど
  - 独自ブロックチェーンを利用
  - チューリング完全なプログラムを動かせる　※ビットコインはLoopを扱えないのでチューリング不完全
  - ハッシュ関数：Dagger/Hashimoto
    - ASICを作ることが極めて困難な仕様（そのためGPUでのマイニングが推奨されている）
- **Frontier版をリリース・稼働開始**
  - Ethereumの公式リリースバージョンの最初のもの
    - 最初のブロックであるジェネシスブロックが作られ、実際にネットワークが稼働
    - Gatecoin、Kraken、Poloniex、ShapeShiftといった取引所で取引開始
    - 開発者むけのリリースバージョン（エンドユーザ向けではなく）
  - 主な制限事項
    - コマンドラインベースで機能。マイニング報酬は通常の1/10（1ブロックあたり5ETH）
    - 手動チェックポイントが設定され、フォーク時にはロールバックされる

- 出典：https://github.com/ethereum/wiki/wiki/%5BJapanese%5D-White-Paper
- 出典：https://blog.ethereum.org/2015/06/21/ethereum-messaging-masses-including-fathers-via-infographic/
- 出典：http://doublehash.me/tag/etherium
- 出典：http://doublehash.me/900
- 出典：http://qiita.com/hshimo/items/20abfc5942d4dd5d3e04

ブロックチェーンによるDAPPS開発基盤 ETHEREUM②

- **今後のリリースプロセス**
  - Frontier版の安定稼働後、Homested版に移行予定
    - Etherのマイニングは通常どおり、チェックポイントは廃止され、完全に自動モードに移行予定。
    - 手動のチェックポイントが外され、自動運航になる
    - マイニング量が通常量に。マイニング報酬が50ETHに
  - Metroporis版で、完全なオフィシャルリリース版
    - コマンドラインだけでなく、一般むけツールが提供され、分散型アプリブラウザ「Mist」が提供される
  - Serenity版
    - 安定版。マイニングが廃止され、PoSに移行。16カ月後を予定。
- **マイニング**
  - 独自PoW、PoS（Ethash）：現在PoWによってマイニング。段階的にPoSに移行。
  - 今後のSerenity版ではマイニングが廃止され、PoSに移行予定。
  - PoSのアルゴリズム候補は、Casper。
    - Security-deposit based Proof of Stakeという新しい概念。
    - POSの認証者になりたいひとは、「デポジット（没収可能性あり）」を積んだ上で、正しい認証を行う。
    - コンセンサスのとれない行動をした場合、デポジットが没収される。

- 出典：https://github.com/ethereum/wiki/wiki/%5BJapanese%5D-White-Paper
- 出典：https://blog.ethereum.org/2015/06/21/ethereum-messaging-masses-including-fathers-via-infographic/
- 出典：https://blog.ethereum.org/2015/03/03/ethereum-launch-process/
- 出典：http://doublehash.me/900
- 出典：http://doublehash.me/1232
- 出典：http://qiita.com/hshimo/items/20abfc5942d4dd5d3e04

ブロックチェーンによるDAPPS開発基盤 ETHEREUM③

- **Ether**
  - Ethereumのネイティブ・トークン（Ethereumのビルトイン通貨）
  - プログラムを動かすための燃料として使われる
    - 誰でも利用料としてEtherを支払うことで、Ethereumを利用できる
  - 分散ネットワークへのリソース貢献者に対する報酬として支払われる

- **金融機関の反応**
  - ロンドンのシティでは、各金融機関がこれから5-10年を見越して、Ethereum による自行アプリ構築が行なわれるようになると見ている模様。
  - UBS、Barclays、BNPパリバがEthereumでもフロントランナーと見られている。
  - UBS や BarclaysがEthereum に関心を示す背景に、Permissioned ledgerなど銀行フレンドリーな別バージョン開発の話も。

→ 出典：http://www.ibtimes.co.uk/bitcoins-smart-sibling-ethereum-only-game-town-banks-build-blockchains-1512726
→ 出典：http://www.ibtimes.co.uk/ubs-barclays-bnp-paribas-are-front-runners-bitcoin-2-0-technology-ethereum-1514138

ブロックチェーンによるDAPPS開発基盤 ETHEREUM④

- **ブロックチェーンの検証方式**
  - ハッシュとコントラクトの実行結果を検証
  - ブロックチェーンを保持するフルノードは、全て同じコントラクトを実行して、結果の正しさを検証

1. マイナーがトランザクション・メッセージを受信
2. マイナーはコントラクトのコードに沿ってメソッドを実行し、実行結果の状態を記録
3. マイナーはマイニングを行う
4. 最初にnonceを見つけたマイナー
   I. ブロックを生成
   II. ブロックにメソッドの実行結果の状態を書き込む
   III. ブロックをブロードキャスト
5. ブロードキャストを受け取ったノード
   I. ブロックのハッシュが正しいか検証
   II. コントラクトのコードに沿ってメソッドを実行し、送られてきたブロックで正しいとされている結果と同じか検証
   III. 問題なければ、ブロックチェーンの末尾にブロックを追加

- 出典: https://github.com/ethereum/wiki/wiki/%5BJapanese%5D-White-Paper
- 出典: https://blog.ethereum.org/2015/06/21/ethereum-messaging-masses-including-fathers-via-infographic/
- 出典: https://blog.ethereum.org/2015/03/03/ethereum-launch-process/
- 出典: http://doublehash.me/900
- 出典: http://qiita.com/hshimo/items/20abfc5942d4dd5d3e04

ブロックチェーンによるDAPPS開発基盤 ETHEREUM⑤

コントラクトの実行方式

- コントラクト
  - メソッドおよびメソッド毎のデータがある
  - コントラクトを識別する固有のコントラクトアドレスが付与される
  - 実行には手数料Etherを支払う必要がある
  - コードの複雑さや長さによって必要なEtherが変わるため、乱用が防げる
  - コードはブロックチェーン上に格納され、検証でき、改ざん不可能
  - データの値もブロックチェーン上に格納される（データの大きさに応じてEtherを支払う）
- トランザクション
  - メソッドへのメッセージ送信。ネットワーク上にトランザクションを流すと、メソッドへメッセージが送信される
  - メッセージを受け取ったコントラクトは、そのメッセージを実行する
  - ブロックチェーン方式のため、メソッドの実行結果は不正・取消・逆戻ができない

●アカウント
・値や情報の直接的やりとりである状態遷移を保持するオブジェクト
・Externally Owned Account (EOA): 秘密鍵により管理される。コードを持たず、トランザクションを生成し署名することでメッセージを送信できる
・Contract Account：自身のコントラクトコードにより管理される

●トランザクション
・EOAから送られたメッセージを貯蔵する署名付きデータパッケージを参照するために使用される
・構成要素
①メッセージの受領人
②送信者を特定する署名
③送信者から受領人へ送られるEtherの量
④オプショナルデータフィールド
⑤STARTGAS値：燃料の上限
⑥GASPRICE値：ステップあたりで払う手数料

●メッセージ
・コントラクトから他コントラクトへ送られるメッセージ
・コントラクトによって生成され、外部で動作しない、という点でトランザクションと異なる
・構成要素
①メッセージの送信者
②メッセージの受信者
③メッセージと一緒に送信されるEtherの量
④オプショナルデータフィールド
⑤STARTGAS値

→ 出典: https://github.com/ethereum/wiki/wiki/%5BJapanese%5D-White-Paper
→ 出典: https://blog.ethereum.org/2015/06/21/ethereum-messaging-masses-including-fathers-via-infographic/
→ 出典: https://blog.ethereum.org/2015/03/03/ethereum-launch-process/
→ 出典: http://doublehash.me/900
→ 出典: http://qiita.com/hshimo/items/20abfc5942d4dd5d3e04

分散型クラウドコンピューティング技術、ENIGMA①

- **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**
  - プライバシーを保証し、他者に明かすことなく個人データの格納・共有・分析が可能。
- **各ノードがデータのプライバシーを完全に守りながら、合同でデータ格納および計算処理を行うP2Pネットワーク**
  - データストレージとしては修正版のDHT(Distributed Hash Table)。
  - 計算処理モデルとしては高度にセキュアに最適化されたMPC(Multi Party Computation)を使用。
  - アクセスコントロールやイベントログとしてブロックチェーンを利用。
- **正確性や公平性を保つインセンティブとして、マイニングでなくデポジットやフィーを利用**
- **ビットコイン同様に第三者への信頼に頼らず、個人データの自律的コントロール可能**
- **プライバシーを暗号化で確保した上で個人データを共有することが初めて可能に**
  - Webは当初Decentralization の急先鋒だったが、近年はその成長がCentralizationと同化し、情報操作・監視・漏洩といった負の側面が露見。
  - こうした中、ブロックチェーンを用いてインターネットアプリケーションをDecentralizedなアーキテクチャーとして構築することが可能になった他、透明性を確保したり、動かぬ証拠を残したりできる。
  - しかし、今のアプリケーションは膨大なデータを扱い、プライベートデータについて重い処理が必要。
  - ブロックチェーンではプライバシーを扱いきれないばかりでなく、プライベートなデータをブロックチェーン上のフルノードにさらすことの問題も。

→ 出典：enigma.media.mit.edu

分散型クラウドコンピューティング技術、ENIGMA②

- **Enigmaのプライベート性**
  - セキュアなMPC(sMPC)を用いて、データは第三者を信用することなく分散的に計算処理される。
  - データは異なるノードに分散格納され、他ノードに漏洩することなくノード間で計算されることが可能。
  - いかなるノードも完全なデータそのものにアクセスできない。
  - プライベート環境（プライバシーを保証できる分散コンピューティング・プラットフォーム）
- **Enigmaのスケーラビリティ**
  - ブロックチェーンと異なり、データ格納や計算処理がネットワーク上の全ノードに複製されない。
  - 冗長性を減じることで計算処理のスケーラビリティに対応している。
- **Enigmaの計算処理の特徴**
  - ローデータ自体にアクセスすることなく計算処理が可能。
  - 例えば、グループで互いの給与にアクセスして、グループの平均給与を計算でき、参加者は各自のグループ内における相対的なポジションを知ることができるものの他メンバーの給与額は知らない。
  - データ共有は不可逆的プロセスであり、一旦データを送ると取り戻しも使用差止もできない。
  - オリジナルのデータオーナー以外はローデータを参照できないのが、Enigmaの相違点。

→ 出典：enigma.media.mit.edu

分散型クラウドコンピューティング技術、ENIGMA③

- **Enigmaとブロックチェーン**
  - 全てのトランザクションはブロックチェーンによって司られ、デジタル署名とパーミッションに基づきアクセスコントロールされる。
  - コードはブロックチェーン(パブリック部分)とEnigma(プライベート部分)の双方の上で実行される。
  - Enigmaの実行はプライバシーと正確性を確保する一方、ブロックチェーンは正確性のみを確保。
  - スマートコントラクトのより強力なバージョンとして、プライバシー情報を扱うことができる「プライベートコントラクト」を扱うことができるDapps向けスクリプト言語が用意される。
  - ブロックチェーン上のコード実行は、全ノードが冗長的に同じコードを実行し同じ状態を保つのに対し、Enigma上ではネットワーク横断で効率的に配分して実行される。
  - コードのパブリック部分はブロックチェーン上で、プライベート部分はEnigma上のoff-chainで実行。
- **Enigmaの応用例**
  - 個人情報を共有しない型で検索エンジンやデータベース、ネットショップ等を構築。
  - プライバシーの確保されたデータマーケット（治験者を探す製薬会社が候補者を探す遺伝子DB）。
  - 顧客データを蓄積してターゲット広告を打つ上で、自社サーバで蓄積・処理してセキュリティリスクを負わなくて済む、プライバシー確保むけバックエンドシステム。
  - 社員のデータ持ち出し等からデータを保護する社内データ管理。
  - 声や顔・指紋などを用いた複数要素認証。
  - IoTによって収集されたデータの格納・管理。

→ 出典：enigma.media.mit.edu

本章のまとめ （基盤・プラットフォーム分野①）

- **ブロックチェーンのAWSを標榜するBlockCypher**
  - マイクロトランザクションのAPI等を提供
  - Zero-confirmation Confidence FactorはConfirmationを数秒に短縮
- **一定期間、情報を暗号化できるTimeChain**
  - スマートコントラクトの機能拡張として、一定期間後にビッドが開封されるオークション等に有効
- **開発者むけプラットフォームSidechain Element**
  - 開発者むけプラットフォームSidechain Elementが公開
- **Dapps開発プラットフォーム、Eris**
  - Dapps開発プラットフォームとして、開発ツールを提供
  - ErisDB：ThelioniousはオープンソースのブロックチェーンDB
  - ErisServer：Decerverは分散アプリ開発のためのアプリケーションサーバ

本章のまとめ （基盤・プラットフォーム分野②）

- **ブロックチェーンによるDapps開発基盤、Ethereum**
  - 分散型アプリケーション（Dapps）の開発プラットフォーム
  - Frontier版をリリース・稼働開始

- **分散型クラウドコンピューティング技術、Enigma**
  - 各ノードがデータのプライバシーを完全に守りながら、合同でデータ格納および計算処理を行うP2Pネットワーク
  - プライバシーを暗号化で確保した上で個人データを共有することが初めて可能に

10. テクニカルセクションメモ

- Blockchain2.0系の実装技術まとめメモ
- Permissioned Distributed Ledger
- Sidechain
- Lightning Network

BLOCKCHAIN2.0系の実装技術まとめメモ

- **トークン発行プラットフォームとして代表的な３点セットである Counterparty、Mastercoin、Open Assets Protocol について、独自通貨・ウォレット・適用例の観点で整理した一覧。**

名称	独自通貨	ウォレット	適用例
Counterparty	XCP	CounterWallet	GetGems・Koinify・Storj・Swarm・LTBcoin
Mastercoin	Mastercoin	OmniWallet	Maidsafe・Factom・La'zooz
Open Assets Protocol (Coloredcoinの流れ)	-	CoinPrizm	GyftBlock・Nasdaq・OverstockのT0

- 出典: http://blog.coinprism.com/comparison-coinprism-counterparty-mastercoin/
- 出典: http://btcnews.jp/counterparty-vs-mastercoin-vs-colored-coin/
- 出典: http://techmedia-think.hatenablog.com/entry/2015/05/03/190805
- 出典: http://siliconangle.com/blog/2015/05/11/nasdaq-gives-blockchain-technology-the-enterprise-treatment/

PERMISSIONED DISTRIBUTED LEDGER (1)

- **主なものはHyperledger、Eris、Ripple、Stellar。**
  - Validator含む参加者はKYC(Know Your Customer)やKYB(Know Your Bank)を通じて互いにKnownな関係。
  - 参加者のアイデンティティがブラック・ホワイトリスト化されている点で既存金融機関と類似。
  - 他の参加者に対して法的・契約上の義務を負う。
- **Permission-less型との違い**
  - このように、参加者との間で契約を通じて安全性を動機づけるため、独自の内部トークンを必ずしも必要としない。
  - また、参加者のアイデンティティの匿名性があるPermission-less型（後述）と違って、参加者に関所が設けられているため、アセットのクリアリングやセツルメントを早く・安く処理可能。

→ 出典: http://www.slideshare.net/MrCollectrix/the-distributed-ledger-landscape
→ 出典: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf
→ 出典: http://domsteil.com/2014/12/29/distributed-consensus-protocols/

PERMISSIONED DISTRIBUTED LEDGER (2)

- **Hyperledger、Eris、Ripple、Stellarについて、内部トークン有無、コンセンサス形成アルゴリズムの観点で整理した一覧。**

	内部トークン有無	コンセンサス形成アルゴリズム
Hyperledger	無し	PBFT
Eris	無し	PoS/PoW
Ripple	XRP	Ripple Ledger Consensus Process
Stellar	STR	SCP (Stellar Consensus Protocol)

- 出典: http://www.slideshare.net/MrCollectrix/the-distributed-ledger-landscape
- 出典: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf
- 出典: http://domsteil.com/2014/12/29/distributed-consensus-protocols/

PERMISSIONED DISTRIBUTED LEDGER (3)

- **一方でPermission-lessなものとしては、ビットコイン、Ethereum、NXT、NEM、Bitshares、Sidechain。**

	内部トークン有無	コンセンサス形成アルゴリズム
ビットコイン	BTC	PoW（Proof of Work）
Ethereum	Ether	独自PoW、PoS（Ethash）
NXT	NXT	PoS（Proof of Stake）
NEM	XEM	PoI（Proof of Importance）
Bitshares	BTS	DPoS（Delegated PoS）
Sidechain	無し	–

- **次頁以降に示すとおり、優劣ではなく、それぞれ向き・不向きがあるので、適材適所で使い分けを考えることが重要。**

→ 出典：http://www.slideshare.net/MrCollectrix/the-distributed-ledger-landscape
→ 出典：http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf
→ 出典：http://domsteil.com/2014/12/29/distributed-consensus-protocols/

PERMISSIONED DISTRIBUTED LEDGER (4)

- **Ethereum ⇔ Sidechain**
  - カナダでトロントのEthereum派とモントリオールのSidechain派という構図があると。トロントはスイス・ロンドン・ベルリンと並ぶEthereumの拠点で、モントリオールはサンフランシスコと並ぶBlockstreamの拠点。ビットコインを使わずブロックチェーンによるアプリ開発を志向するEthereum派と、ブロックチェーントランザクションとしてビットコインとの2way-pegをベースに考えるSidechain派。（出典：dailyfintech ）
- **Ripple ⇔ Hyperledger･Eris**
  - Distributed Ledger Platforms (DLP)としてRipple、Hyperledger、Eris。シングル台帳かマルチ台帳か。自身の通貨を持つか持たないか。シングル台帳・トークン有Rippleとマルチ台帳・トークン無のHyperledger、Eris。（出典： fifthmoment ）
- **Ripple ⇔ Hyperledger & Eris & Sidechain**
  - CitiCoinの話、Rippleなどコンセンサスプロトコル、HyperLegerなど分散台帳、Erisなどと、ブロックチェーンテクノロジー（Sidechainなど）を区別すべし、という記事。（出典：paymentssource）

- 出典: http://dailyfintech.com/2015/07/15/private-blockchains-as-an-it-tool-for-settlement-clearing/
- 出典: http://dailyfintech.com/2015/07/24/canadian-crypto-battle-between-montreal-with-sidechains-toronto-with-ethereum/
- 出典: http://www.fifthmoment.com/can-distributed-ledgers-duplicate-m-pesa-story/
- 出典: http://www.paymentssource.com/news/technology/a-very-public-confluct-over-private-blockchains-3021831-1.html

PERMISSIONED DISTRIBUTED LEDGER(5)

- **Bitcoin ⇔ Sidechain**
  - Sidechainは、ビットコインブロックチェーンと互いに繋がったブロックチェーン。Sidechainはビットコインをグローバル通貨にすることを目指し、より早いconfirmation timeでチェーン同士が価値交換できる手段を提供。Sidechain上の価値・コインは他のSidechainへと移動が可能。（出典：domsteil.com）

- **Counterparty ⇔ Hyperledger**
  - どちらもユーザーが自分のアセットを作成可能な点が共通点。
  - Counterpartyは、ビットコインのブロックチェーン上に構築されたプラットフォームでありウォレット。Counterpartyはユーザーがtokenizationを通じてアセットを作成できる。
  - Counterparty自身の通貨としてXCPがありプラットフォーム上でアセットを作るのに使われる。CounterpartyはXCPをフィーとして実行されるスマートコントラクトを作成可能。
  - 一方Hyperledgerは、分散元帳プラットフォームを作るオープンソース。
  - 両者の相違点はネイティブ通貨を持たないこと、ブロックチェーンではないこと、confirmation timeが数秒で済むこと。
  - Hyperledgerは各分散ノードが別のアセット・別の元帳を持てる。Hyperledgerの元帳はパブリック・プライベートいずれかを選べる。（出典：domsteil.com）

→ 出典：http://domsteil.com/2014/12/29/distributed-consensus-protocols/

PERMISSIONED DISTRIBUTED LEDGER (6)

- **Ethereum ⇔ Eris**
  - どちらもDappsやスマートコントラクトを作るプラットフォーム。
  - Ethereumはスクリプトプラットフォーム。Ethereumはネイティブ通貨etherを持ち、スマートコントラクトの実行時にトランザクションフィーに用いる。
  - 一方Erisは、Ethereum上に構築されたDapps開発プラットフォーム。Erisの各DappsはEthereum上のブロックチェーンを用いる。Erisは各Dapps内でブロックチェーン上のスマートコントラクトをetherを使って実行。（出典：domsteil.com）
- **Ripple ⇔ Eris･Hyperledger**
  - RippleとEris、Hyperledgerの違いは、トークンを持つかどうかと、台帳が一つかどうか。（出典：ofnumbers.com）

→ 出典：http://domsteil.com/2014/12/29/distributed-consensus-protocols/
→ 出典：http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

PERMISSIONED DISTRIBUTED LEDGER (7)

- Blockchain Workshops @ London “Demystifying Blockchains”

	Essence	Core Design			Smart Contract
Bitcoin	Disintermediate banks & currencies	Public	Decentralized blockchain	Virtual machine	✓
Ripple	Replace SWIFT	Private	Transaction network with built-in currency conversions		-
Stellar	Bank the unbanked	Private	Transaction network with built-in currency conversions		-
Hyperledger	Inter-bank clearing	Private	Consensus protocol		-
Ethereum	Public smart contract platform	Public	Decentralized blockchain	Virtual machine	✓
Tendermint	Public smart contract platform	Public	Decentralized blockchain	Virtual machine	✓
Eris	Private smart contracts platform stack	Private	Consensus protocol	Virtual machine	✓

→ 出典: http://www.slideshare.net/_hd/demystifying-blockchains

PERMISSIONED DISTRIBUTED LEDGER (8)

- **プライベートブロックチェーンとパブリックブロックチェーンの共存・棲み分け（By Eris COO Preston Byrne）**
  - ビットコインのようなパブリックブロックチェーンは、企業にレコードが改ざんされてない証拠を安価に示す手段を提供するもの。
  - プライベートブロックチェーンがビットコインを置き換えるのではなく、プライベートネットワーク上のアクティビティーの検証手段としてパブリックブロックチェーンを用いる。
  - プライベートブロックチェーンユーザがこの様にパブリックブロックチェーンを使い棲分け。
  - プライベートブロックチェーンをパブリックな台帳検証メカニズムと組み合わせることによって、スタートアップ企業もデータインフラを安価にコンパクトに構築可能。
  - この様に、パブリックブロックチェーンは、プライベートブロックチェーンの重要なコンポーネント。

→ 出典：http://www.coindesk.com/eris-coo-private-and-public-blockchains-need-to-co-exist/

PERMISSIONED DISTRIBUTED LEDGER(9-1)

- **ブロックチェーン的なデータベースアプリケーションの3区分。（By Vitalik Buterin）**
  - ①パブリックブロックチェーン
  - ②コンソーシアムブロックチェーン
  - ③プライベートブロックチェーン

- **パブリックブロックチェーン**
  - 完全にDecentralizedなブロックチェーンであり、誰もが読込・トランザクション送付・コンセンサスプロセス参加可能。
  - コンセンサスへの影響度合いは暗号経済上のリソース量に比例。
  - PoWやPoSなどの暗号経済メカニズムによって中央集権的トラストを代替。
  - オープンゆえ多くのエンティティに利用されることが出来、ネットワーク効果を享受しやすい。

→ 出典：https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

PERMISSIONED DISTRIBUTED LEDGER (9-2)

- **コンソーシアムブロックチェーン**
  - パブリックブロックの低いトラストとプライベートブロックチェーンの高度なブロックチェーンのハイブリッド。
  - 部分的なDecentralizedなブロックチェーン。
  - 複数金融機関から成るコンソーシアムによる運営など。
  - 予め選択されたノードのセットによってコンセンサスプロセスはコントロールされる。
  - ブロックチェーン読込権限は参加者限定。

→ 出典：https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

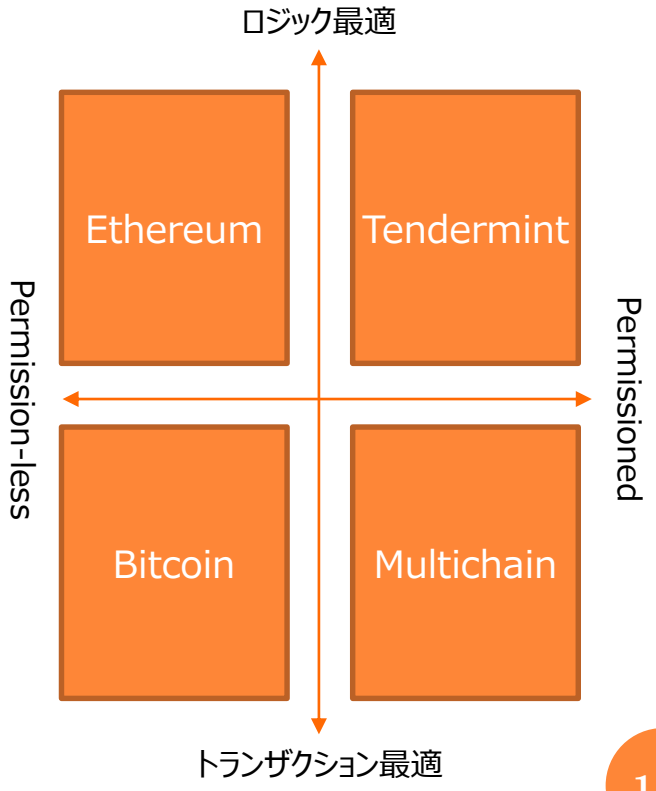
PERMISSIONED DISTRIBUTED LEDGER (9-3)

- **プライベートブロックチェーン**
  - Centralizedなブロックチェーン。
  - 書き込みパーミッションは単一組織に集中。
  - 読込パーミッションはパブリックであったり任意の範囲に制限したり。
  - パブリックな読込・監査は不要な場合に適用。
  - 企業内データベースなど伝統的な中央集権システムを記述。
  - プライベートブロックチェーンを運営する企業やコンソーシアムは必要に応じ容易にブロックチェーンのルール変更可能。
  - 限られたノードのみで検証すれば済むためトランザクションフィーが安く済む。
  - 検証者が知り合いゆえマイナーの共謀による51%攻撃に遭うリスクを回避でき、Confirmationも高速で可能。
  - 読込パーミッションを制限することでプライバシーを提供可能。

→ 出典：https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

PERMISSIONED DISTRIBUTED LEDGER (10)

- **Eris CEOの考えるブロックチェーン四区分マトリクス（By Eris CEO Casey Kuhlman）**
  - 「Permissioned/Permission-less」と「ロジック最適/トランザクション最適」で区分。
  - トランザクション最適はデジタル通貨や金融商品売買の清算(clearing)・決済(settlement)、サプライチェーンの存在証明にProperty Registerとして用いる。
  - ロジック最適なブロックチェーンは複雑なビジネスロジックを記述するスマートコントラクト等にProcess Auditorとして用いられる。
  - Permissionedであるというのは
    - ホワイトリストによるアクセスコントロール。
    - スマートコントラクトの形でブロックチェーンに機能を加えることができるのが誰で、ブロックチェーンと遣り取りできるのが誰かを定める。
    - コンプライアンスリスクを軽減できる。検閲も不可。



- ✓ Tendermint：マイニング不要なコンセンサスプロセスを持ち、Validatorの2/3以上の署名によってブロックの有効性を検証。
- ✓ MultiChain：金融トランザクションむけに、パーミッションに基づくプライベートブロックチェーンを開発・実装できるオープンソースプラットフォーム。

→ 出典：https://db.erisindustries.com/strategy/2015/08/10/how-i-current-explain-blockchains/

SIDECHAIN
①サイドチェーンとは

- **メインのブロックチェーンを分離しつつ、相互運用可能なブロックチェーンを通してビットコインの機能を拡張するもの。**
  - 複数のブロックチェーンの間でアセットを移動・交換できるマルチブロックチェーンのネットワークを可能に。
  - ビットコインを親チェーンとして使うマルチブロックチェーンを通してアセットを交換できる。
  - 親チェーンとなるビットコインからだけでなく、サイドチェーン同士の間でもコインの移動が可能。
  - ビットコインや他のアセットをブロックチェーン間で移動できる。
  - 相互運用可能ではあるが、分離独立しているため、サイドチェーン側で何かあってもダメージはサイドチェーン内に留められる。

→ 出典: http://www.blockstream.com/
→ 出典: http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
→ 出典: http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
→ 出典: http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
→ 出典: http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
→ 出典: http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
→ 出典: http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

SIDECHAIN
②ビットコインとの2WAY-PEGGING

- **2ウェイ・ペグは、コインをチェーン間で移動でき、それをビットコインに裏付けされた固定レートで戻せる仕組み。**
  - 親チェーン～サイドチェーン間で、親チェーンからサイドチェーンへ移した後に最後はオリジナルアセットを保持したまま元の親チェーンへ戻せる。
  - サイドチェーン同士でも、他のサイドチェーンからアセットをインポートした後にまた元のサイドチェーンへ返すことができる。
- **2ウェイ・ペグの意義**
  - チェーン同士を双方向で繋ぐ2ウェイ・ペグにより、自分のビットコインをサイドチェーン上のアセットへ移した後もそのビットコインの価値は保持されるので、サイドチェーン上のアセットと交換したビットコインがオルトコイン市場の価格変動に左右されずに済む。
  - このようにサイドチェーンは複雑に絡み合う分散ネットワークだが、金で裏付けされるドルのようにビットコインで裏付けされていると考えられる。

- 出典: http://www.blockstream.com/
- 出典: http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
- 出典: http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
- 出典: http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
- 出典: http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
- 出典: http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
- 出典: http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

SIDECHAIN
③サイドチェーン誕生の背景

- **ビットコインの抱えるインターバルタイム、スマートコントラクト・スクリプティングの制約、オルトコインの流動性等を回避すること。**
  - ビットコインはブロックインターバルに約10分かかる。
  - ビットコインの所有権移動は出来るが、よりリッチな送信ニーズにはCounterPartyなどがビットコインの更に上にレイヤーを構築したり工夫している。
  - ビットコインのスクリプト言語は限定的なのでスマートコントラクトの実装が難しく、Ethereumの様な工夫がされている。
  - そこで「ビットコインを別のブロックチェーンに送れるとしたら、ブロックインターバルも早く、スクリプト言語もリッチに出来るのでは？」という発想に。

→ 出典：http://www.blockstream.com/
→ 出典：http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
→ 出典：http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
→ 出典：http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
→ 出典：http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
→ 出典：http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
→ 出典：http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

SIDECHAIN
④ビットコインとPEGされたサイドチェーンの意義

- **ビットコインのブロックチェーンの外側に、ビットコインと相互運用可能なブロックチェーンを作る。**
  - ビットコインのブロックチェーンの外側に、ビットコインと相互運用可能なブロックチェーンを作ることで、新たな通貨をサポートすることなく、オルトコイン市場で出来ること同等のことが出来るようにする。
  - 即ちサイドチェーンでは、ユーザーの既に持つアセットを使ってイノベーティブな暗号通貨にアクセスしたり、新しいトランザクション設計やトラストモデル・経済モデルを実験できる。
  - また、オルトコインにまつわる流動性不足・市場変動・断片化・セキュリティ違反などの影響を被ることを防ぐ。

→ 出典: http://www.blockstream.com/
→ 出典: http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
→ 出典: http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
→ 出典: http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
→ 出典: http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
→ 出典: http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
→ 出典: http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

SIDECHAIN
⑤サイドチェーンによる機能拡張（1）

- **プライバシー保護といったセキュリティ面とスクリプト、取扱アセットといった機能パフォーマンス面。**

- **強固なセキュリティとしてのConfidential Transactions**
  - パブリックなトランザクションであるビットコインと違い、送り手・受け手・指定した人、この三者を除く全ての相手からコイン移動量を隠蔽。
  - レギュレーターに対して完全な透明性を提供しつつも、投資家の機微なビジネス情報の開示は守るため、金融機関にとって有用。

- **強力なスクリプト機能**
  - 例えば宝くじのようにランダムに選ばれた受け手に対するペイメント契約などを可能に。

→ 出典：http://www.blockstream.com/
→ 出典：http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
→ 出典：http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
→ 出典：http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
→ 出典：http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
→ 出典：http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
→ 出典：http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

SIDECHAIN
⑤サイドチェーンによる機能拡張(2)

- **Issued Asset**
  - チェーン横断で移動可能な様々なアセットを発行し、他のサイドチェーンと移動したり他のアセットと交換可能。
  - 契約や権利主張、IOUの表現にも応用でき、金融機関が株・債券・デリバティブ・商品券・スマートプロパティなどに応用可能。
  - 或いは、大人数ゲーム、ロイヤリティプログラム、オンラインコミュニティのような組織内の目的限定トークンなども。

→ 出典: http://www.blockstream.com/
→ 出典: http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
→ 出典: http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
→ 出典: http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
→ 出典: http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
→ 出典: http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
→ 出典: http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

SIDECHAIN
⑥サイドチェーンのトランザクション（1）

- **ビットコインの場合**
  1. 移動したい未使用コインを特定し・・・
  2. そのコインを所有し移動する権利があることを鍵発行で証明し・・・
  3. 受け手が受け取る資格あることを証明する手段として秘密鍵のチャレンジを示す。
- **サイドチェーンの場合**
  1. 移動したい未使用ビットコインを特定し・・・
  2. そのビットコインの所有を証明し・・・
  3. 誰かが“サイドチェーン上でもう使われてない”と証明する迄ロックをかける。

- 出典：http://www.blockstream.com/
- 出典：http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
- 出典：http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
- 出典：http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
- 出典：http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
- 出典：http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
- 出典：http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

SIDECHAIN
⑥サイドチェーンのトランザクション(2)

- **親チェーン上でロック ⇒ コインをサイドチェーンへ送る**
  - このように親チェーン上でロックされている間、親チェーンとの更なるやりとりなしに、コインはサイドチェーン上で自由に移動できる。
  - このとき、親チェーンのコインとしてのアイデンティティは保持したままで、自由に元のチェーンに戻ることが出来る。
- **SPV proofによるロック解除**
  - 親チェーン上のコインは、サイドチェーン上の所有権のSPV proofでのみロック解除される。
  - SPVは簡易支払検証の略で、ブロックチェーンのブロック頭部と、取引に関係ある一部の組合せを使って、ブロック全体を取得せずに当該取引がブロックに含まれるかを確認できるのがSPV proof。

→ 出典: http://www.blockstream.com/
→ 出典: http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
→ 出典: http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
→ 出典: http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
→ 出典: http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
→ 出典: http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
→ 出典: http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

SIDECHAIN
⑥サイドチェーンのトランザクション（3）

- **サイドチェーン上でロック ⇒ コインを親チェーンへ戻す**
  - SPV proofを使って当該コインをサイドチェーン上にロックすることで、当該コインがサイドチェーンから消えて（サイドチェーン上で所有していた人のコントロールの下）再び親チェーンで使えるようになる。

- **２つのチェーン間の同期に要する待ち時間**
  - 親チェーン側で待つ時間 ＝ Confirmation Period
  - サイドチェーン側で待つ時間 ＝ Contest Period

→ 出典：http://www.blockstream.com/
→ 出典：http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
→ 出典：http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
→ 出典：http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
→ 出典：http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
→ 出典：http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
→ 出典：http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

SIDECHAIN
⑥サイドチェーンのトランザクション（4）

- **Confirmation Period（親チェーン側での待ち時間）**
  - 親チェーン上でロックをかけてSPV proofを創るのに十分な時間をかけるのが目的。（サイドチェーンのセキュリティのパラメーター）
  - この待ち時間が終わるとともに、SPV proofが作られて、SPV proofが親チェーン上に埋め込まれ、サイドチェーンへ移動できる。

- **Contest Period（サイドチェーン側での待ち時間）**
  - 親チェーンからサイドチェーンへ移動してきたコインが、サイドチェーン上で未だ使えない可能性のある時間。
  - Reorganization期間中に、以前にロックされたコインを移動することによる、「二重消費」を防ぐために設けられた待ち時間。
    - Reorganizationとは、既に受け入れられたブロックチェーンが、よりPoWを持つコンペティターによって覆されると、負けた方のブロックチェーン上のブロックが、コンセンサス履歴から取り除かれること。

→ 出典：http://www.blockstream.com/
→ 出典：http://thebitcoinnews.com/bitcoin-3-0%E2%80%B2-sidechain-elements-by-blockstream-lightning-network-and-more-2/
→ 出典：http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/
→ 出典：http://blogs.wsj.com/moneybeat/2015/06/08/bitbeat-blockstream-unveils-much-awaited-first-sidechain-prototype/
→ 出典：http://blockchainstuff.eu/bringing-new-elements-to-bitcoin-with-sidechains/
→ 出典：http://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
→ 出典：http://gendal.me/2015/06/10/quick-notes-on-sidechains-elements/

LIGHTNING NETWORK ①背景・目的

- **Lightning Networkは、検証可能性やセキュリティを損ねることなくブロックチェーンの外でビットコイントランザクションの大半を処理するもの。**
  - Visaのピークトランザクションは秒間45000で1日換算だと1億トランザクション。一方ビットコインは秒間7トランザクションに過ぎず、それを平均ブロック長300バイト・リミットサイズ1メガバイトで処理している。
  - これをVisa並みにするには10分おきに8ギガバイト、年間換算400ペタバイトが必要となり、ムーアの法則を適用するとしても難しい。
  - そこでVisa並みのトランザクションをさばくには、ビットコインブロックチェーンの外でトランザクションを実行することが必要。

- 出典：http://btcnews.jp/ten-years-later-bitcoin-network-will-collapse/
- 出典：http://cornwarecjp.github.io/amiko-pay/doc/lightning_emulation.pdf
- 出典：http://rusty.ozlabs.org/?p=450
- 出典：http://bitcoin.upper.jp/blockstream-starts-development-on-the-lightning-network/
- 出典：https://en.bitcoin.it/wiki/Scalability

LIGHTNING NETWORK
②ビットコインスケーラビリティへの解

- **Micropayment Channel上でビットコイントランザクションを行い、最後の清算のみをブロックチェーン上で処理。**
  - Lightning Networkはブロックチェーン上の完全な確認に1時間要するビットコインペイメントと違い、トランザクションを即時に処理できる。
  - Lightning Networkにより理論上は最小限のブロックチェーンで1日あたり数十億トランザクションをさばけるため、ビットコインのスケールに寄与すると考えられている。
  - 効率的なマイクロペイメント及び即時に近いトランザクションを可能にするため、ビットコインのスケーラビリティに光明を与えるとされる。

- 出典: http://btcnews.jp/ten-years-later-bitcoin-network-will-collapse/
- 出典: http://cornwarecjp.github.io/amiko-pay/doc/lightning_emulation.pdf
- 出典: http://rusty.ozlabs.org/?p=450
- 出典: http://bitcoin.upper.jp/blockstream-starts-development-on-the-lightning-network/
- 出典: https://en.bitcoin.it/wiki/Scalability

Lightning Network ③Micropayment Channel

- **Micropayment Channel上でトランザクションを行うことにより、カウンターパーティリスクを抑えることが出来る。**
  - Lightning Networkはインターネットパケットのようにマルチポップパスを通じてルーティング可能なので、新たなカウンターパーティ毎にチャネルを作る必要があるが、信頼できる少数の仲介人をチャネルとしてトランザクションすれば済む。
  - Micropayment Channelは、相手が協力しなくなったり、一定期間レスポンスしないといった場合はチャネルを閉じ、トランザクションをブロックチェーンへキックしてそこで決済すればよいので、カウンターパーティリスクも小さい。

- 出典：http://btcnews.jp/ten-years-later-bitcoin-network-will-collapse/
- 出典：http://cornwarecjp.github.io/amiko-pay/doc/lightning_emulation.pdf
- 出典：http://rusty.ozlabs.org/?p=450
- 出典：http://bitcoin.upper.jp/blockstream-starts-development-on-the-lightning-network/
- 出典：https://en.bitcoin.it/wiki/Scalability

LIGHTNING NETWORK
④サイドチェーン開発体制との融合

- **Lightning Network実装上の課題**
  - 但し、Lightning Network実装にはビットコインプロトコルコアに手を加えることが必要。
  - soft forkで済むので既存ブロックチェーンの有効性は維持されるとされる。
- **サイドチェーンの開発体制との融合（Blockstream）**
  - このように、サイドチェーンはメインのブロックチェーンと別に代替ブロックチェーンを作り、Lightning Networkは一部のトランザクションに別場所でトランザクション実行を認めて結果のみをメインブロックチェーンに返す。
  - サイドチェーンとLightning Network、両者には類似点も多いことから、Rusty RussellがBlockstreamに合流してLightning Network開発に携わる等、開発体制も一体化が進んでいる。

- 出典：http://btcnews.jp/ten-years-later-bitcoin-network-will-collapse/
- 出典：http://cornwarecjp.github.io/amiko-pay/doc/lightning_emulation.pdf
- 出典：http://rusty.ozlabs.org/?p=450
- 出典：http://bitcoin.upper.jp/blockstream-starts-development-on-the-lightning-network/
- 出典：https://en.bitcoin.it/wiki/Scalability

本章のまとめ（テクニカルセクションメモ①）

- **Blockchain2.0系の実装技術まとめメモ**
  - トークン発行プラットフォームとして代表的な３点セットであるCounterparty、Mastercoin、Open Assets Protocolについて、独自通貨・ウォレット・適用例の観点で整理した一覧。
- **Permissioned Distributed Ledger**
  - 主なものはHyperledger、Eris、Ripple、Stellar。
  - Hyperledger、Eris、Ripple、Stellarについて、内部トークン有無、コンセンサス形成アルゴリズムの観点で整理した一覧。
  - 一方でPermission-lessなものとしては、ビットコイン、Ethereum、NXT、NEM、Bitshares、Sidechain。
  - 優劣ではなく、それぞれ向き・不向きがあるので、適材適所で使い分けを考えることが重要。

本章のまとめ （テクニカルセクションメモ②）

- **Sidechain**
  - Sidechainは、メインのブロックチェーンを分離しつつ、相互運用可能なブロックチェーンを通してビットコインの機能を拡張するもの。
  - 2ウェイ・ペグは、コインをチェーン間で移動でき、それをビットコインに裏付けされた固定レートで戻せる仕組み。
  - ビットコインの抱えるインターバルタイム、スマートコントラクト・スクリプティングの制約、オルトコインの流動性等を回避することを目指し誕生。
  - ビットコインとPegされたSidechainの意義は、ビットコインのブロックチェーンの外側に、ビットコインと相互運用可能なブロックチェーンを作る。
  - Sidechainによる機能拡張としては、強固なセキュリティとしてのConfidential Transactionsや、強力なスクリプト機能、Issued Assetなど。

- **Lightning Network**
  - Lightning Networkは、検証可能性やセキュリティを損ねることなくブロックチェーンの外でビットコイントランザクションの大半を処理するもの。
  - ビットコインスケーラビリティへの解として、Micropayment Channel上でビットコイントランザクションを行い、最後の清算のみをブロックチェーン上で処理。
  - Micropayment Channel上でトランザクションを行うことにより、カウンターパーティリスクを抑えることが出来る。

カテゴリーマップ（名称ベース）

金融	サプライチェーン	ライフスタイル	シビックテック
Ripple	Provenance	GetGems	Bithealth
Bitreserve	Factory Banking	Synereo	OneName
Swarm	Adept	La'ZooZ	ShoCard
BitShares	Ascribe	OpenBazaar	BitNation
BitGold	Everledger	Augur	Spacechain
Overstock	Verisart	Streamium	Stellar
Hedgy	BlockVerify	PopChest	Factom
Coinffeine		GyftBlock	MayorsChain
Mirror		PeerTracks	Neutral Voting Bloc
ROSCA		BuyAnyCoin	GroupCurrency
itBit		Ribbit Rewards	
Abra		Spells Of Genesis	
Blossoms		Voxelnauts	
Symbiont		Reveal	
SETL		21 Inc.	
Toast		BitFury	

プラットフォーム

Ethereum	Sidechain	Maidsafe	BlockCypher
Eris	Counterparty	Storj	ZENNET
Hyperledger	NEM	Enigma	Sapience AIFX

ブロックチェーンベースのサービス検討論点試案

ユーザ理解Layer	L1	**ターゲットユーザ** 一般消費者か、金融機関やメーカーなど法人か、もっと広い社会か、等
	L2	**ユーザのGain・Pain** 何が不平不満怒り、嬉しさ・望みだったりするか。（消費者なら下世話な課題、銀行プロセスやサプライチェーンなら業務課題、広く社会にアプローチするなら壮大な社会課題） 例：「ゲームに飽きて次のゲームをやる時に、ポイントやアイテムが引き継げない・・」
提案価値Layer	L3	**ユーザのGainを殖やす・Painを減らすには** 例：「ゲームに飽きたら他人に暗号通貨でトレードすることもできるようにしたら？」
	L4	**サービス内容（そのためにどのユーザに何を提供するか）** 例：「ゲーム内コンテンツと暗号通貨の交換が可能なトレーディングカードゲーム」
仕組みLayer	L5	**ユーザとの関わり方** 対象（トークン、株式、ギフトカード、スコア、通貨など） アクション（上記の対象を、買うなり・稼ぐなり・シェアするなり） **ブロックチェーンの使い方** サービス提供のためにブロックチェーンを何の用途で使うか。（金融分野であれば、資金調達手段・小口決済手段・契約などの証明手段など）
	L6	**ビジネスの収益性** どうやって収益得るか？誰と組むか？（小売とギフトカード、メーカーとサプライチェーン、保険会社とダイヤ保証など） **エンジニアリング実現性** やりたい用途にFitした技術・手段は何か。IoTやID認証の仕掛けをどうするか。 **運営モデルの実効性** AugurのREPのようなインセンティブ付けや、Dapps・DAOのガバナンス・意思決定の仕組をどうするか。

お役に立てば嬉しいです

- **BTCアドレス**

  14Ku1wiRFsreeLthxxRxfcE5NmeYRwJAc7

→おしまい