Bitcoin & Blockchain概況

2018.10 by SATO

「Bitcoin2.0概況」「Blockchain2.0概況」から改題

過去14回（＋臨時1回）にわたり、ビットコイン動向とブロックチェーン応用事例トピックを整理

- **第１回（2014年10月）：**2014年7月～9月の動き
- **第２回（2015年1月）：**2014年10月～12月の動き
- **第３回（2015年5月）：**2015年1月～4月の動き
- **臨時（2015年6月）：**金融分野のトピックに絞って
- **第４回（2015年8月）：**2015年5月～7月の動き
- **第５回（2015年11月）：**2015年8月～11月の動き
- **第６回（2016年4月）：**2015年12月～2016年4月の動き
- **第７回（2016年7月）：**2016年12月～2016年7月の動き
- **第８回（2016年12月）：**2016年8月～2016年11月の動き
- **第９回（2017年3月）：**2016年12月～2017年3月の動き
- **第１０回（2017年7月）：** 2017年4月～2017年7月の動き
- **第１１回（2017年10月）：**2017年8月～2017年10月の動き
- **第１２回（2018年2月）：**2017年11月～2018年1月の動き
- **第１３回（2018年5月）：**2018年2月～2018年4月の動き
- **第１４回（2018年8月）：**2018年5月～2018年7月の動き
- **第１５回（2018年10月）：**今回

TABLE OF CONTENTS

➔ 今回は、2018年8月～10月の動きを中心に整理

1. Bitcoinエコシステムの動向

- ECDSAとSchnorr署名
- Lightning Networkとアトミックスワップ
- Sidechain
- Scaling Bitcoinトピック
- Bitcoin Cashのハードフォーク

ECDSAとSchnorr署名

- ECDSAの背景
- ECDSAの署名検証スキーム
- ECDSAの問題点
- Schnorr署名の署名検証スキーム
- Schnorr署名のメリット

ECDSAの背景

- ECDSAは、楕円曲線むけ離散対数問題をベースとしたデジタル署名アルゴリズム。
  - この有限体楕円曲線システムにおいては、乗算が容易だが除算は困難。
  - 秘密鍵はスカラーxとすると、曲線上でP=xGとなる点Pが公開鍵にあたる。
  - もしx（=秘密鍵）を持っていれば、容易にそれが公開鍵となるPを見つけることができる。
  - xから公開鍵Pを求めることは容易だが、反対方向にxを計算するのは困難、という性質を利用。

群と二項演算子
- 2つの元を群からとり加算すると、他の元をその集合の中から得る。
- 全ての元が逆元を持つ。群の中で一つの元に逆元を加算すると相殺。
- 結合性とは(a+b)+cがa+(b+c)と等しいこと。
- 可換性はa+bがb+aと等しいこと。可換性ある群をアーベル群と呼ぶ。

巡回群
- 群の中の全ての元が、何度か自身を加算されたgであるとき、生成元gについて巡回群であるという。

巡回群と公開鍵暗号
- 群の中にPが与えられたとき、xG=Pとなるようなスカラーxがあり、Gを何度か足し合わせることは容易だが、xG=PでPを与えられたときにxが何であるかを知ることは困難。
- 公開鍵暗号に照らすと、xが秘密鍵でPが公開鍵にあたる。
- ビットコインにおいては、有限体上に定義されたsecp256k1を用いる。
- この群から一つの要素を与え、この点を得るために何回Gを加算する必要があるのかを判別することは困難。

楕円曲線
- y^2 = x^3 + ax + bの形状。
- ビットコインでは、secp256k1曲線を用いる。

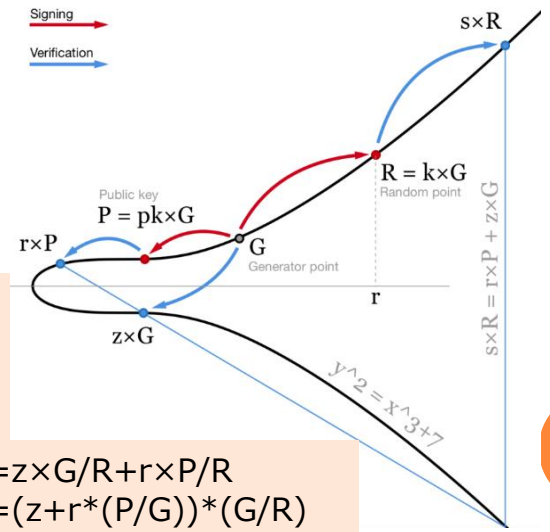
楕円曲線上の点における群演算
- 2つの点を加算するには、点Pをとり、もう一つの点Qを曲線上にとり、それらを加算するには、直線をひくと、それが曲線と接して、それをx軸に対して反転する。そこがP+Qに相当するRである。
- 点を2倍するには、自身を加算すればよい。その点における曲線の接線を見出し、再び曲線に交わる点かX軸に対して反転する。
- 逆数を計算するためには、X軸に対して対称をとる。

離散対数問題とデジタル署名
- 有限体において、ある要素を取り出して何度も乗算した後に、何回乗算したかを知ることは困難。
- こうした非対称性がデジタル署名スキームに組み込まれているのがECDSA。

→ 出典：http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/edgedevplusplus/digital-signatures/

ECDSAの署名検証スキーム

- メッセージmに署名するには、メッセージmをハッシュして、このハッシュを数字として扱って、z=hash(m)とする。
- 乱数kの必要性。
  - 多くの脆弱性が、悪い乱数生成器に関係するので、乱数整数器をトラストしたくない。
  - そのためRFC6979を用いて、秘密および署名するメッセージに基づいて、乱数kを計算する。
- 秘密鍵pkを用いて、rおよびsという２つの数字を含むメッセージmむけ署名を生成。
  - r: ランダムポイントR=k×Gのx座標
  - s: (z+r＊pk)/k　・・・①
- すると、公開鍵P=pk×Gを用いて署名を検証できる。
  - 点Rのx座標がrと等しいことの確認
    - R=(r/s)×P + (z/s)×G のx座標がrと等しいことをチェック
    - s×R= r×P+z×G



●署名（図中の赤矢印）
・生成点がG
・公開鍵はP=pk×G
・ランダムポイントR=k×G
・ランダムポイントRのx座標がr

●検証（図中の青矢印）
・z×Gを計算
・r×Pを計算
・s×R=z×G+r×P
・Rのx座標がrか否か

s=z×G/R+r×P/R
s=(z+r*(P/G))*(G/R)
s=(z+r*pk)/k　と①に戻る

→ 出典：https://medium.com/cryptoadvance/how-schnorr-signatures-may-improve-bitcoin-91655bcb4744

ECDSAの問題点

- 署名検証（R=(r/s)×P + (z/s)×G のx座標がrと等しいことをチェック）に際して、逆数（1/s）および2回の点乗算を含み、計算操作が重い。
  - BTCにおいて各ノードが全てのTXの検証を行わないといけない。
  - TXをブロードキャストすると、数千のコンピュータがあなたの署名を検証する必要あるということ。
  - 検証プロセスをシンプルにしたい。

- 全ノードが全署名を別々に検証する必要がある。
  - m-of-nマルチシグTXにおいて、ノードは同じ署名を複数回検証する必要がある。
  - 例えば、7-of-11マルチシグTXは、7つの署名を含み、全ノードで7～11の署名検証が必要。
  - TXとしてブロックにおいて大きなスペースをとり、その分手数料もかかる。

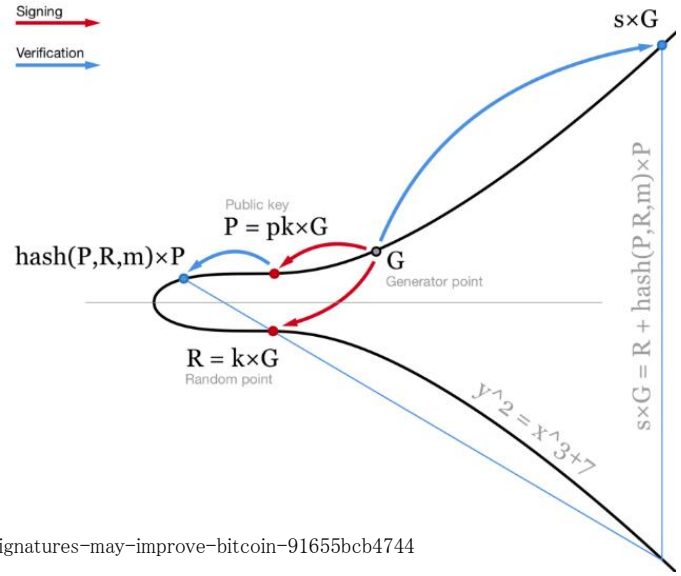
→ 出典：https://medium.com/cryptoadvance/how-schnorr-signatures-may-improve-bitcoin-91655bcb4744

SCHNORR署名の署名検証スキーム

- ECDSAで用いた２つのスカラー(r,s)の代わりに、点Rとスカラーsを用いる。
  - EDCSAと同様に、Rは楕円曲線上のランダムポイントであり、R=k×G
- 署名の残りパートは、ECDSAと異なる方法で計算される。
  - s=k+hash(P,R,m)＊pk　・・・①
    - pkは秘密鍵、P=pk×Gは公開鍵、mはメッセージ
- 署名は、s×G=R+hash(P,R,m)×Pをチェックすることによって検証できる。
  - s×G=R+hash(P,R,m)×pk×G
    - s=R/G+hash(P,R,m)×pk=k×G/G+hash(P,R,m)×pk＝k+hash(P,R,m)×pk　と①に戻ることが確認できる

●署名（図中の赤矢印）
・生成点G
・公開鍵はP=pk×G
・ランダムポイントR=k×G

●検証（図中の青矢印）
・R=k×Gを計算
・hash(P,R,m)×Pを計算
・R＋hash(P,R,m)×P＝s×G



→ 出典：https://medium.com/cryptoadvance/how-schnorr-signatures-may-improve-bitcoin-91655bcb4744

SCHNORR署名のメリット　①バッチ検証

- ビットコインのブロック検証
  - ブロック中の全ての署名が有効であることを確認する必要がある。
  - もしそのうち一つが有効でなければ、それがどの署名かを気にすることなく、ブロック全体を拒否する。
- ECDSAによる検証
  - 全署名を個別に検証する。
    - 検証（R=(r/s)×P + (z/s)×G のx座標がrと等しいことをチェック）に際して、逆数計算 1 回および乗算2回が必要
  - 1000の署名がブロック内にあれば1000の逆数計算と2000の乗算が必要。
  - 合計3000ほどの重い操作。
- Schnorrによる検証
  - 全署名検証を加算を中心として行うことができ、逆数も不要なため、計算パワーを節約できる。
    - s×G=R+hash(P,R,m)×P
  - 例えば、上述の例と同様に、ブロック内に1000TXある場合の検証は、
    - (s1+s2+…+s1000)×G=(R1+…+R1000)
+(hash(P,R,m1)×P1+hash(P,R,m2)×P2+…+hash(P,R,m1000)×P1000)
  - この場合、一塊の加算（計算パワー上ほぼ無料）および1001回の乗算。
    - つまり、ECDSAの場合（重い操作が3000回）と比べて、重い操作の数が 1 ／ 3 で済むということ。

→ 出典：https://medium.com/cryptoadvance/how-schnorr-signatures-may-improve-bitcoin-91655bcb4744

SCHNORR署名のメリット　②集約性

- P2WPKH(P2SH)による2-of-2マルチシグ
  - ２つの署名を使ってTX中に含められる。
- Schnorr署名2-of-2マルチシグ
  - 秘密鍵ペア(pk1,pk2) をつかって、共有の署名を生成でき、これが共有の公開鍵に対応する（P=P1+P2=pk1×G+pk2×G）。
  - この署名を生成するためには、乱数をそれぞれに対して選択して (k1,k2)、ランダムポイントを生成する（Ri=ki×G）。
  - そして、これらを加算して共通ハッシュ（hash(P,R1+R2,m) ）を計算し、デバイス毎にs1 および s2を得る。(si = ki + hash(P,R,m) ＊ pki)
  - すると、これら署名を加算して、ペア (R, s) = (R1+R2, s1+s2)を共有公開鍵Pの署名として用いる。
  - この性質によって、通常のSchnorr署名と区別がつかず、「集約された署名かどうか」の判断がつかなくすることができる点がメリット。

Schnorr署名の署名ペア(R,s)	Schnorr署名によるマルチシグの署名ペア(R,s)
・公開鍵P=pk×G ・ランダムポイントR=k×G ・s=k+hash(P,R,m)＊pk	・共有公開鍵P=P1+P2=pk1×G+pk2×G ・ランダムポイントRi=ki×G ・si = ki + hash(P, R1+R2, m) ＊ pki

→ 出典：https://medium.com/cryptoadvance/how-schnorr-signatures-may-improve-bitcoin-91655bcb4744

LIGHTNING NETWORKとアトミックスワップ

- ペイメントチャネル
- ブロックチェーンへ書き込まれるトランザクション
- ペイメントチャネルとHTLC
- ペイメントチャネルのリバランシングとSplicing
- LNにおけるルーティング
- マルチホップペイメントのアトミックスワップへの応用
- Submarine Swapによるアトミックスワップ
- LNにおける課題と次世代トピック

ペイメントチャネル

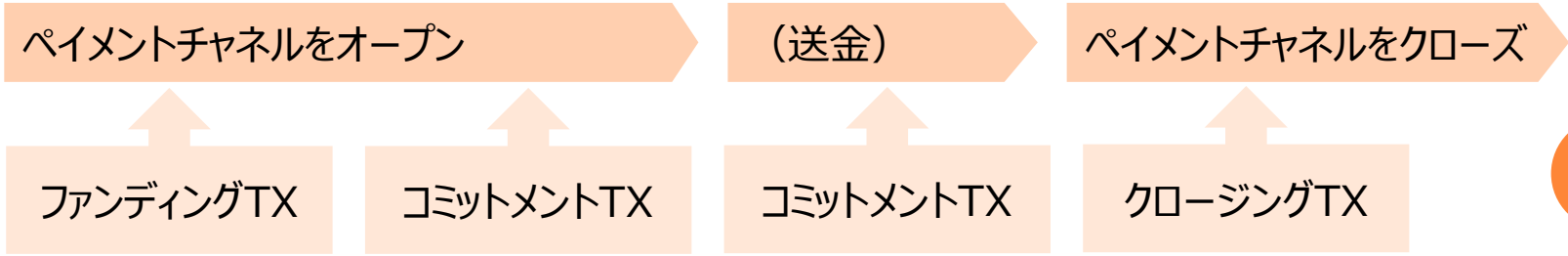
- オフチェーントランザクション
  - アリス～ボブ間でチャネルがあれば、ブロックチェーンへブロードキャストする必要なしに、何度も送金できる。手数料なく即時で可能な点が特徴。
  - チャネルが有効なのは、アリス・ボブの間で複数回トランザクションが発生する場合。
    - チャネルのオープンとクローズは、オンチェーンTXを必要とし、手数料や確認時間の待ちが必要となる。
    - チャネルである間は、ファンドがロックされており、使うことができない。
    - そのため、１回きりのオフチェーンTXを行なうためにチャネルを使うのは、時間とカネの無駄。
- トラストレス性
  - 相手を信頼する必要がない。もし一方が相手を騙そうとすれば、時間もカネも失う。

ペイメントチャネルをオープン	ペイメントチャネルを更新	ペイメントチャネルをクローズ
• ファンディングTXを署名してブロードキャスト • チャネル中にファンドをロック • コミット金額の組み合わせがチャネルのバランス	• 更新には、TXへの署名・合意は必要だが、ブロードキャストは不要 • 但し、送金額は送り手のバランスの範囲内に限定される	• クロージングTXを署名してブロードキャスト • チャネル中のファンドがアンロックされ、所有されるバランスに応じて双方へ付与
アリスとボブがペイメントチャネルをそれぞれ２BTC・３BTCデポジットして開設すると、チャネルバランスは２：３	２：３というバランスのときに、アリスがボブへ１BTC送金すると、１：４のバランスに再配分される	

→ 出典：https://medium.com/muunwallet/rebalancing-the-key-to-the-lightning-network-3da869d4e70d

ブロックチェーンへ書き込まれるトランザクション

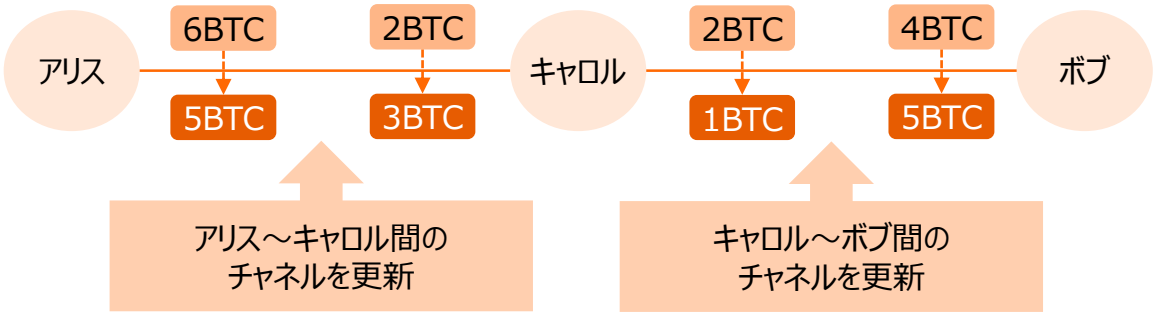
- ファンディング・トランザクション
  - チャネルをオープンする際に使用するトランザクション（送金先＝お互いのマルチシグ）。
  - 後続のファンディングTXやクロージングTXのインプットとなる。
- コミットメント・トランザクション
  - 送金をその場で確定させるべく、いつでもチャネルをクローズしてBTCを配分するTX。
    - チャネルをオープンする際、コミットメントTXを作成することによって、チャネルをオープンし終わる前に相手がいなくなったとしても、ファンディングTXに入っているBTCを取り戻せるようにする。
    - 送金する際、相手が途中で不在になったり異常が起きたりして、チャネルを継続できなくなった場合に、ブロックチェーンに展開するトランザクション。
  - 最新のコミットメントTXをブロックチェーンに展開してクローズすることをUnilateral Closeという。
- クロージング・トランザクション
  - 相手と同意してチャネルをクローズ(Mutual Close)する場合に使用するトランザクション。
  - 他のクローズ方法と比較して手数料が低く、使用できるまでの期間が一番短い。



→ 出典：https://thinkit.co.jp/article/15158
→ 出典：https://thinkit.co.jp/article/14548

ペイメントチャネルとHTLC

- HTLCを用いることによって、ペイメントを行なう当事者同士が直接チャネルを生成する必要なしに、「チャネルの連鎖」を通じて送金が可能になる。
  - 下図において、キャロルがルーティングノード（ペイメントをルーティングする）。
  - アリスがボブへ１BTCを送金したい場合、ルートに関わる全てのチャネルを更新する。



- HTLCのオペレーションはアトミック＆トラストレスに行なわれる。
  - ペイメントの操作自体は「アリス～キャロル」「キャロル～ボブ」と２分割される。
  - しかし、全体としてオペレーションは完全実行されるのか、全く実行されないかのいずれかのみ。
  - 仲介役キャロルは、ボブへのペイメントを意図されたように実行した場合にのみ、アリスからマネーを受け取ることができる。
    - ルーティングノードは、自分のチャネルを「先んじて」ファンドしなければならない。

→ 出典：https://medium.com/muunwallet/rebalancing-the-key-to-the-lightning-network-3da869d4e70d

ペイメントチャネルのリバランシングとSPLICING

- ルーティングノードは、自分のチャネルを先んじてファンドしなければならない。
  - キャロルがルーティングするには、キャロル～ボブのチャネルに十分なバランスが必要。
  - 下図において、アリスがボブへ２BTCを送金したいといっても、バランス不足でルーティング不可。

- ルーティングし続けるためには、キャロルはチャネルを「リバランシング」することが必要。
  - 他方のバランスを減らす(Splice out)ことを犠牲に、一方のバランスを増額する(Splice in)。
  - チャネル開け閉めに伴い、TXのブロードキャストが必要でオンチェーンTX手数料が発生。
- Splice Out
  - チャネルを閉めて新規チャネル開設し、リバランシング差額充当分をアンロック。

- Splice In
  - チャネルを閉めた後に差額充当分を使って再度チャネルを開設しルーティング可能なバランスに。

→ 出典：https://medium.com/muunwallet/rebalancing-the-key-to-the-lightning-network-3da869d4e70d

LNにおけるルーティング

- 直接チャネルを開いていないLNノードに対するルーティング
  - 条件①：送金するLNノードは送金先までのチャネルを知っていること
  - 条件②：送金するBitcoin量＋中継するLNノードへの手数料を保有すること
  - 条件③：中継するそれぞれチャネルに送金するだけのBitcoin量があること
- 送金先までの経路情報の作成
  - データ①：送金者から送金先までの全LNノードとチャネル
  - データ②：各LNノードが相手に支払うBitcoin量
- 経路の暗号化
  - 送金元の人が暗号化する
  - 中継するLNノードは自分が次のLNノードに送金するための情報だけを解読できる
  - 送金経路情報はOnionルーティングプロトコルにより、さらに符号化
  - 次の送金先に関する情報だけが復号できる
- 送金の中継時間制限の目的
  - 中継をしたLNノードが途中で処理を放置しても、タイムアウトすれば送金者に戻ってくるようにするため
  - タイムアウトするまでに送金を終わらせないとBTCを手に入れられないというインセンティブのため

→ 出典：https://thinkit.co.jp/article/14548

マルチホップペイメントのアトミックスワップへの応用

- Lightning Networkにおけるマルチポップペイメントの概略
  - A→B→Cの経路でBを信頼することなくBTC送るもの。
  - まず受け手Cが作った秘密鍵のハッシュを送り手Aに渡し、AはハッシュをBに渡して「対応した秘密鍵あればBTC送る」と伝える。
  - これを受けBはCへハッシュロックしたBTCを送る。
  - するとCは自分が作った秘密鍵でハッシュロック解いてBTC入手でき、同時にBは秘密鍵を知るので、Aのロックしたを入手できる。
- クロスチェーンアトミックスワップへの応用
  - A～B関連のスワップを、1)A→B→Aのマルチポップペイメントと見立てると共に、2)BTC送りLTC返すものと見立てることによって、実現するもの。

参考資料

- HTLCを用いたクロスチェーンスワップの図解
  - https://medium.com/crypto-economics/an-illustrated-primer-on-cross-currency-swaps-in-htlcs-da90a90b60a9
- Lightning のクロスチェーンアトミックスワップPoC
  - https://github.com/ExchangeUnion/Lightning-Swap-PoC-v2/blob/master/README.md

→ 出典：https://yybazaar.com/2018/08/15/crosschain-offchain-atomicswap/

SUBMARINE SWAPによるアトミックスワップ

- Submarine Swapを用いたオンチェーンETHとオフチェーンBTCのアトミックスワップ
  - ユーザーはまずLightningインボイスでオーダーを生成した後、インボイス及びペイメントハッシュ（ハッシュ出力）とあわせてETHをスワップコントラクトへ送付し、オーダーにファンディングする。
  - ファンディングトランザクションを確認できたら、スワップサービス提供者がインボイスに対して支払いを行う。ペイメントが完了すると、ペイメントプルーフ（ハッシュ入力としてのプリイメージ）を提出してスワップコントラクトからファンドを受け取ることができる。
  - ペイメント失敗時には、スワップサービス提供者はペイメントプルーフを取得できず、ファンドを受け取ることが出来ない。
  - 一定期間後、ユーザーはスワップコントラクトへ返金依頼するとETH返金を受け取ることができる。
  - インボイスへの支払いが出来なければ返金してされる点をアトミックと呼び、Ethereumスマートコントラクトにより保証される仕組み。

→ 出典：https://medium.com/@jason.hcwong/atomic-on-chain-eth-to-off-chain-btc-swap-3c959ab22e52

LNにおける課題と次世代トピック　①流動性

- ペイメントが、仲介役を介して複数チャネル横断の担保をまわすことで行なわれる為、アリスがボブに１BTC支払いたいときに、要件は以下２つ。
  - アリスがチャネルルートをボブと自分の間にみつけること。
  - 各チャネルホップが最低１BTCをアリスからボブへの方向で利用可能であること。
- LNは中央のプランナーのいないNWであるため、どれだけ流動性プールが機能するかもあわせて流通経路を予想することは難しい。

トピック	概要
Atomic Multipath Payments	• アリスがボブに１BTC支払いたいが、アリスとボブの間に１BTCをステップ可能な経路が存在しないとする。 • そこでボブへ0.5BTC送るルートのほか、0.3BTCのルート、0.2BTCのルートを見つける。AMPを用いて、支払いを３分割した上で、アトミック（３つとも成功するか全て失敗）に実行可能に。
Splicing	• ユーザがチャネルが消耗したときにチャネルを補充すべく、チャネルバランスの変更（Splice in[チャネルへ資金加算]およびSplice out[チャネル資金の減産]）を、それぞれ１件のオンチェーンTXで可能するもの。
Submarine Swap	• オンチェーンとオフチェーンのファンドをブリッジするもの。 • アリスはボブへオンチェーンTXで支払いでき、これをボブは自分が既に既存チャネル内の支払いとして受け取ることができる。
Channel Factories	• L1とL2チャネル間に中間層を設けることで、チャネルキャパシティ調整を可能に

→ 出典：https://blog.theabacus.io/lightning-network-2-0-b878b9bb356e

LNにおける課題と次世代トピック　②LIVENESS

- LNの様に、カストディをもたないL2スケーリングソリューションにおいては、ライブなインターネットアクセスがあり、他人のペイメントをルーティングしたり自分のペイメントを受けとったりすることができることに加え、そのファンドを安全なものにできることが必要。
- ファンドの安全については、秘密鍵を安全確保するだけでなく、さらにメインチェーンをモニタリングでき、TXを所定タイムスロット内にブロードキャストできる必要がある。

トピック	概要
Watchtowers	• サードパーティノードとして、ユーザーの代わりにチェーンをモニタリングし、必要に応じて取消TXをブロードキャストするもの。
Compact Block Filters for SPV clients	• 通常の軽量SPVクライアントは、自己検証セキュリティをフルノード運営なしに可能とするものであり、TXおよびブロックハッシュのマークル証明を用いて、自分のTXがブロックに含められたことを検証。 • LNにおいて、これと逆に、コンパクトブロックフィルタを用いて、クロージングTXが「無いこと」を証明するもの。
Eltoo	• 古いコミットメントTXを間違って署名しブロードキャストしてしまうリスクに備えるもの。

→ 出典：https://blog.theabacus.io/lightning-network-2-0-b878b9bb356e

LNにおける課題と次世代トピック　③ルーティング

- アリス～ボブ間のペイメントルートについて「どのように増やすかもし無かったらどうするか」を、「①流動性」の項で示した一方、アリスとボブの間にルートがあったとしても、どうやって双方がそれを見つけるかという課題が残る。
- 基本は、インターネットの進化に応じてルーティングメカニズムが進化したように、LNが成長するにつれ、LNのルーティングメカニズムは、結果的にキャパシティ要件を充たすと考える一方、インターネットのようにトラストベースではない点は難しい。

トピック	概要
Flare	• LNにおける状態のスナップショットを、以下４つの動的変数として整理。（①チャネルの存在、②チャネル内のファンディング量、③ルーティング手数料、④ノードのLiveness） • ①（チャネルの存在）は比較的めったに変化しない一方、②～④は高速に変化する。 • そこで、NWステートを維持すべく、①（チャネルの存在）については、能動的に状態を最新にキープ。逆に、②～④は受動的に得られる。 • このハイブリッド戦略を使うことによって、各ノードは自身のルーティングテーブルを構築し、近隣ノード内のノード経路をスコアリングすることができる。 • 加えて、各ノードはランダムにLNのノードからBeaconノードグループを選択し、そこから、近隣の外側にあるネットワークに関する、スナップショットデータを得る。

→ 出典：https://blog.theabacus.io/lightning-network-2-0-b878b9bb356e

SIDECHAIN

- Sidechainの特徴
- Sidechainにおける2Way-Peg
- SidechainにおけるFederationモデル
- ビットコインサイドチェーンLiquid Network
- Liquid SidechainとLightning Networkの違い

SIDECHAINの特徴

- サイドチェーンは、ビットコインのコンセンサスルールの外側でコンセンサス履歴を構築し、任意のコンセンサスルールを持つことが可能。
- 独立したブロックチェーンネットワークであるため、トランザクション検証のためには、自身のマイナーを必要とする一方、マイナーにそのインセンティブが無いことが欠点。

メリット	リスク
• 全く新しいトークンをローンチすることなく新しい機能を実装できるようにする。 • たとえば、即時トランザクションム、プライバシー（秘匿TXや秘匿アセット）、DAG構造、付加機能（EVMベースのRSK）など。 • 後方互換性を必要としない。	• トランザクションの検証のために、自身のマイナーを必要とする。 • サイドチェーンはメインチェーンアセットにペグされるため、マイナーにとってサイドチェーンをマイニングすることのインセンティブはほとんどない。 • マイナーはサイドチェーンを安全なものとするインセンティブがないため、マイナー攻撃に対して脆弱（不正TXやマイナー集中化や51%攻撃など）。 • マイナーインセンティブとして、マージマイニングが一例。マイナーが一つ以上のブロックチェーンを同時にマイニングできるようにするもの。マージマイニングを実装するマイナーは、限定された追加ワーク／エネルギー消費とマイニングフィーを報酬として受け取る。 • そのほかのインセンティブとして、サイドチェーンを破壊するインセンティブのないコンソーシアム企業によって運営するものも。

→ 出典：https://theblockcrypto.com/2018/10/17/crypto-simplified-explaining-sidechains/
→ 出典：http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/sidechains-and-federation-models/
→ 出典：https://theblockcrypto.com/2018/10/17/crypto-simplified-explaining-sidechains/

SIDECHAINにおける2WAY-PEG

- メインチェーンに付属する別のチェーン（サイドチェーン）は、 2WPを通じて、固定レートでメインチェーンアセットに裏づけされたアセットを発行できる。
  - 後述するLiquidの場合、Liquid Bitcoin（LBTC）が１：１でBTCにペグされる
- サイドチェーンのユーザは、自分がペグしようとするアセットを保有していることを証明することを求められる。
  - そのために、アセットをメインブロックチェーンアドレスへ送付。
  - アセットの所有権が検証されると、サイドチェーンはペグされたアセットをユーザに対して発行可。
  - ユーザがサイドチェーンアセットを償還するまでの間、オリジナルのメインチェーンアセットは当該アドレスにロックされ、サイドチェーン上でアンロックされる。
  - サイドチェーンへアセットを償還するとき、逆方向で、ファンドはメインチェーン上でアンロックされ、サイドチェーンにロックされる。
  - この流れは、コントラクトとして考えることができる。

	メインチェーン上の アセットロックアップ		サイドチェーン上の アセットロックアップ
サイドチェーン上アセット発行	ロック	→	アンロック
サイドチェーン上アセット償還	アンロック	←	ロック

→ 出典：https://theblockcrypto.com/2018/10/17/crypto-simplified-explaining-sidechains/

SIDECHAINにおけるFEDERATIONモデル

- Federated ブロック署名者（クローズドな署名者セット）
  - 許可制であり、ブロック署名者セット（ Federation ）に追加・削除するには、オリジナルの署名セットから許可を得ることが必要。
  - m-of-nのマルチシグスキームのように見える。
  - マイナーをトラストすることが必要（固定された既知エンティティのオペレーション上のセキュリティに依存）。
  - Sidechain構築のモデル選択においては、「何を解決しようとしているのか」「誰をトラストするのか（マイナーをトラストするのか・幾つかの企業をトラストするのか・他人をトラストするのか）」のトレードオフに注意。

- Federationによるコントラクト執行
  - FederatedされたウェレットすなわちWatchman達が、ファンドをビットコインブロックチェーンの内外へ移動するのを監視している。
  - Pay-to-contract(p2c)を利用して、ユーザはファンドをFederationウォレットへ直接移すことができる。
  - Segwit前はn-of-15マルチシグFederation中に15の参加者が上限であったが、Segwit後はn-of-67マルチシグとなり、Federation中に67メンバーまで可能に。

→ 出典: https://theblockcrypto.com/2018/10/17/crypto-simplified-explaining-sidechains/
→ 出典: http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/sidechains-and-federation-models/
→ 出典: https://theblockcrypto.com/2018/10/17/crypto-simplified-explaining-sidechains/

ビットコインサイドチェーンLIQUID NETWORK

- BTCと2ウェイペグのL-BTC、Issued Assetsによるトークン化、数量とアセットタイプを秘匿するConfidential Transactionがポイント。
- L-BTCは、BTCがビットコインブロックチェーンへロックアップされると、Liquidサイドチェーン上でのみアンロックされる。
- 2ウェイペグは、Federationメンバーによってのみ執行される。
  - 2ウェイペグを介してBTCをサイドチェーンを送る際には、BTCをマルチシグアドレスへデポジット。
  - 102のConfirmationの後、L-BTCがユーザーに送付される。
- ビットコインブロックチェーンへペグアウトする際には、2 Confirmationのみで済む。
  - L-BTCは2分以内でTXのセツルメント可能
  - L-BTC＆BTC間の即時転換によって、流動性をNWおよび交換所に対して提供可能に
- Liquid Networkのアセット移転は1分間隔でセツルメントされブロック生成。
  - これを地理的に多様なメンバーによるFederationが行う。
- Issued Assetsを提供。
  - ユーザが自身のトークンアセットを生成（コモディティや証券など任意のアセットのトークン）。

→ 出典：https://blockstream.com/2018/10/10/liquid-launch.html
→ 出典：https://twitter.com/blockstream/status/1050943816499384320?s=21
→ 出典：https://twitter.com/blockstream/status/1051497055200468994?s=21
→ 出典：https://twitter.com/blockstream/status/1052671379823386624?s=21
→ 出典：https://cryptoinsider.com/what-is-bitcoins-liquid-sidechain-and-why-does-it-matter/
→ 出典：http://www.datadriveninvestor.com/2018/10/17/how-is-bitcoins-liquid-sidechain-different-from-the-lightning-network/

LIQUID SIDECHAINとLIGHTNING NETWORKの違い

- 既存BTCのブロックチェーンに対してセカンドデータレイヤーのように働く
  - メインBCのデジタルレコードのコピーを保持
    - サイドチェーン上で実行されるTXはメインチェーンのスペースを占有することがなく、ネットワーク手数料を回避
  - 換言すれば、Liquid Networkは代替ルートを全BCTXに対して提供する（＝LN的）
    - BTCネットワークの混雑を回避し、サイドチェーンという代替軽量ソリューションを提供
  - ともにSidechain上で高速TXを提供することによってスケーラビリティ問題を解決するもの
- LNとの違い
  - LNは分散マイクロペイメントソリューションで、ユーザへのリスク軽減のため限定されたキャパシティのもと高速
  - 一方でLiquidは、高ボリューム＆大TXむけ許可型Federation型BCであり、Liquidは大きな金融機関をターゲット（高速で信頼できるTXプロセシングを行なうB2Bむけソリューション）。

共通点	相違点	
	Liquid Network	Lightning Network
• 既存BTCのブロックチェーンに対するセカンドレイヤーとして、代替軽量ルートを提供（スペース・手数料の回避） • 高速TXを提供することによってスケーラビリティ向上	高速で信頼できるトランザクションプロセシングを行なうためのB2Bむけソリューション（高ボリューム＆大TXむけ）	分散マイクロペイメントソリューションとして、限定されたキャパシティのもとに、高速トランザクションを提供

→ 出典：http://www.datadriveninvestor.com/2018/10/17/how-is-bitcoins-liquid-sidechain-different-from-the-lightning-network/

SCALING BITCOINトピック

- Scaling Bitcoin2018の振り返り
- Scaling Bitcoin2018の内容概略

SCALING BITCOIN2018の振り返り （1/3）

- 2016年のMilan・2017年のStanford同様に大学での開催でもあり、参加人数は300人ほどの大教室におさまる規模。
  - 東京開催ということを反映し、日本人参加者は、Milan（数えるほど）, Stanford（20名弱）と比べると徐々に増えており、今回は2割ほどが日本からの参加だった感触。
  - 日本以外のアジア圏からの参加はそれほど多くはなく、参加者の多くを欧米参加者が占めたのは、Milan・Stanfordと同じ傾向。
  - 登壇者にBlockstreamがいない点はStanfordから継続（一部ワークショップのリード参加に留まる）。
  - 登壇者の半分はアカデミア。欧州・米国およびイスラエルからの登壇（バルセロナ自治大、コーネルテック、スタンフォード、ユニバーシティカレッジロンドン、フリードリヒ・アレクサンダー大学エアランゲン＝ニュルンベルク、スイス連邦工科大学ローザンヌ校、ヘブライ大学、チューリヒ工科大学）。
  - 登壇者について、日本からの登壇は、前回に続きDG Labからあったことに加えて、NTTからの登壇と計2セッションと増えたものの、日本開催だった割には存在感はまだ小さい。

→ プログラム: https://tokyo2018.scalingbitcoin.org/#schedule
→ 動画リンク: https://www.youtube.com/channel/UCmwaDulmQtX-H8FOSQTKqMg

SCALING BITCOIN2018の振り返り（2/3）

- 内容面では、プライバシー・フンジビリティに関するセッションは減り明示的なものは１セッションのみとなり（Scriptless Scriptsを除く）、関心事の多様化が進んでいる印象（例えばMilanではTumbleBitやMimblewimbleなど多くがフンジビリティ関連だった）。
  - スケーリング関連の題材についても、セカンドレイヤー・オフチェーン一本槍ではなく、オンチェーンスケーリング関連で３セッションが設定されていた。特に、Forward Block（シャーディングとオンチェーンの組み合わせ）については注目を集めた。（オンチェーンスケーリングへの言及は昨年のStanfordから継続。StanfordではGraphenやギガブロック実験の発表がなされた）
  - セカンドレイヤー関連では、マルチパーティチャネルとしてLightning Factoryのトピックが紹介されたほか、LNのリバランシングインセンティブ、およびLNのベンチマークが紹介された。セカンドレイヤーありきではないものの、随所にHTLCの言及があるセッションが見られ、HTLCがややバズワード化との印象も。
  - セカンドレイヤー以外で多く触れられたトピックとしては、Scriptless Scripts。昨年発表されたものだが、今回３つのセッションが言及するなど、重要なトピックに昇華した印象。
  - シャーディングやDAG、或いはチューリング完全性・Fraud Proof・BLS署名・暗号通貨バックトークンのように、必ずしも今のビットコインで主流となっているトピックに囚われたものではない、幅広なトピックが扱われていたことも特徴的。例えばNTTからは、コンソーシアムチェーンに対するビットコインペイメントを行う仕組みの提案がなされた。
- なお、昨年は翌年東京開催が発表されたが、今年は来年開催地の告知なし。

→ プログラム: https://tokyo2018.scalingbitcoin.org/#schedule
→ 動画リンク: https://www.youtube.com/channel/UCmwaDulmQtX-H8FOSQTKqMg

SCALING BITCOIN2018の振り返り （3/3）

- ちなみに、ScalingBitcoinの内容はアカデミック或いは先進的なものに特化しているため、ビットコイン関連でより実践的な重要技術をおさえる意味では、併せて開催された「Bitcoin Edge Dev++ / BC2 TECHNICAL BOOTCAMP」の内容をフォローするのが有効。
  - 「Bitcoin Edge Dev++ / BC2 TECHNICAL BOOTCAMP」（10/4-10/5 @Tokyo）
    - https://keio-devplusplus-2018.bitcoinedge.org/#speakers
    - http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/edgedevplusplus/

- また、Bitcoin Edge Dev++（実践的重要技術） とScalingBitcoin（先進・アカデミック） の中庸に位置付けられる戦略テーマや方向性を把握する上では、下記の2つが有用。
  - Building on Bitcoin （7/3-7/4@Lisbon）
    - https://twitter.com/build_on_btc/status/1047852453721460736?s=21
  - Baltic Honeybadger Bitcoin Conference 9/22-9/23@Riga）
    - https://youtu.be/PN88h-d09qs

→ プログラム: https://tokyo2018.scalingbitcoin.org/#schedule
→ 動画リンク: https://www.youtube.com/channel/UCmwaDulmQtX-H8FOSQTKqMg

SCALING BITCOIN2018の内容概略(1/9)

セクション	主題	サマリーメモ	資料URL
1. ビットコインの現状	UTXO中のDustに関する分析	• ビットコインコアでは、Dustをフィーにらおける利用に必要となるコストがアウトプットの価値より多くかかるようなアウトプットをDustと定義している。 • 一つのUTXOの価値はサイズに影響しない（大きな価値があるとしても大きなサイズと限らない）。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/an-analysis-of-dust-in-utxo-based-cryptocurrencies.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/analysis-of-dust-in-utxo-based-cryptocurrencies/ ➔ https://eprint.iacr.org/2018/513.pdf
	どれだけプライバシーがあれば充分か	• スケーラビリティは計測可能だがプライバシーは実証的に評価するのが難しい。マイニングされたばかりのコインの方が売却プレミアムあり。 • 交換所は顧客をトランザクション履歴に基づきブロックでき、トランザクショングラフ以上のことを知ることでき、単なる第三者の観察者ではない。ある種のトランザクションタイプ向け顧客を禁止する交換所も。顧客をトラッキングしようとするマーチャントもいる。 • おとりアプローチには限界あり。もし使うなら5でなく500万くらい大規模とし、全ての最近のトランザクションと重複し、注意してサンプリングすること必要。zk証明技術など用いた対数スケーリングも必要。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/how-much-privacy-is-enough.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/how-much-privacy-is-enough/ ➔ https://arxiv.org/pdf/1706.00916.pdf

SCALING BITCOIN2018の内容概略(2/9)

セクション	主題	サマリーメモ	資料URL
2. オンチェーンスケーリング	ビットコインのブロック報酬調整	• ビットコインはエネルギー消費し過ぎかという点についてはセキュリティを落とせというのと同じ。 • ハッシュレートと価値の関係。報酬を半分にすると報酬あたりTHが二倍に。価格上昇は報酬あたりTHを低減。新規ハードウエア登場は報酬あたりTH増加。 • Pay it Forwardスキーム実装にあたり、ブロック報酬減額はソフトフォーク。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/playing-with-fire-adjusting-bitcoin-s-block-subsidy.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/playing-with-fire-adjusting-bitcoin-block-subsidy/
	自己再生を通じたチューリング完全	• トランザクション間の再帰呼び出しを認めることによって、ブロックチェーンのチューリング完全を可能とするもの。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/self-reproducing-coins-as-universal-turing-machine.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/self-reproducing-coins-as-universal-turing-machine/ ➔ https://arxiv.org/abs/1806.10116
	Forward Block	• シャーディングとダイレクトオンチェーンスケーリングを通じて、検閲耐性を改善するもの。 • 集中化のリスクとして、「検証コスト・フルノードバリデータ維持に必要なリソースの増加」および検閲耐性低下をあげている。 • 検閲耐性は、任意ユーザーが公平にブロック採掘可能ということ。規模によらずハッシュレートに比例して採掘成功機会がある。ブロック伝播時間と平均ブロック間隔の比率との間に非線形の関係。 • クロスチェーンヘッダーコミットメントは、フォワードチェーンとコンパチビリティチェーンの双方が他のヘッダーにコミットするもの。 • コンパチビリティチェーンがフォワードブロックヘッダーをロックインすると、トランザクションがプロセシングキューに追加されるとともに、Coinbaseアウトプットがペイアウトキューに追加される。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/forward-blocks-scalingbitcoin-slides.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/forward-blocks/ ➔ http://freico.in/forward-blocks-scalingbitcoin-paper.pdf ➔ http://freico.in/forward-blocks-scalingbitcoin-slides.pdf ➔ https://www.coindesk.com/bitcoin-breakthrough-tech-forward-blocks/

SCALING BITCOIN2018の内容概略(3/9)

セクション	主題	サマリーメモ	資料URL
3. スケーリングセキュリティ	コンパクトマルチシグ	• t-of-nマルチシグについて固定サイズで可能な、アカウンタブル・サブグループ・マルチシグの提案。ランダムオラクルモデルにおいて偽造不可能。 • 1) 公開鍵集約つきペアリングベースマルチシグ（MSP）：署名者と公開鍵の双方を集約できるため、通常のビットコインブロックチェーンと比べて2割以下の容量で済む。加えてバッチ検証をサポートするため高速検証も特徴。また、不正公開鍵攻撃対策でBLS署名をサポート。 • 2) アカウンタブル・サブグループ・マルチシグ（ASM）：n人の参加者セットにおける任意のサブセットSが、合同でメッセージmに署名し、どのサブセットが署名したか証明できる（アカウンタブル）。50-of-100など大きなサイズのt-of-nマルチシグにおける容量節約に有用（1/30の容量で済むとのこと）。 • 3) 離散対数由来マルチシグ（MSDL）：ペアリングベースのベーシックな鍵集約における安全証明を補完すべく、ハッシュ準備ラウンドを組み合わせ。容量節約（通常のビットコインの2割で済む）を保ちながら、離散対数仮定の難しさのもとで安全証明可能に。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/compact-multi-signatures-for-smaller-blockchains.pptx ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/compact-multi-signatures-for-smaller-blockchains/ ➔ https://eprint.iacr.org/2018/483.pdf

SCALING BITCOIN2018の内容概略(4/9)

セクション	主題	サマリーメモ	資料URL
3. スケーリングセキュリティ	Fraud Proof通じたSPVノードの検証セキュリティ改善	• ブロックチェーンを状態遷移システムとして一般化するもの。マークルツリーとして全状態を表現。KVSとして状態を格納。Sparceマークルツリーも利用できる。 • SPVノードはコンセンサスの大半が正直と仮定して無効ブロックを受け入れるため、非中央集権とオンチェーンスケーラビリティの間には大きなトレードオフがある。 • そこでどうすれば不完全な検証を行うSPVノードが無効ブロックを拒否できるか。SPVノードがフルノードをトラストする必要をどうすれば無くせるか。そのために、Fraud Proofとデータ利用可能証明を用いるという提案。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/improving-spv-client-validation-and-security-with-fraud-proofs.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/fraud-proofs/ ➔ https://arxiv.org/pdf/1809.09044.pdf
	RSA Accumulator用いたマークルツリーのリプレイス	• UTXOセットのデータサイズ拡大への対応策として、RSA Accumulatorを用いるもの。 • RSA Accumulatorはinclusion proofのサイズが3000bitで一定なため（ブロックあたり1.5KB）マークルツリーよりベターな他、フルノードストレージ不要な分散ストレージゆえ、ユーザーは自身のUTXOおよびメンバーシップ証明を維持するのみで済む。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/scalable-drop-in-replacement-for-merkle-trees.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/accumulators/

SCALING BITCOIN2018の内容概略(5/9)

セクション	主題	サマリーメモ	資料URL
4. Scriptless Scripts と マルチパーティチャネル	マルチパーティチャネル	• シングルパーティチャネルの場合、2of2マルチシグ用いて共有アカウントをエミュレート。HTLC用いてアトミックな条件付ペイメント。この課題は、(1)資金流れがチャネルのトポロジーにより制約される(2)新しいチャネルを動的にオフチェーンで生成できない(3)各チャネルで単一UTXOが必要。 • マルチパーティチャネルは、これをn:nのペイメントに拡張・一般化するもの。各チャネルに新規UTXOを必要とせず、LN内に動的ルート生成を可能とする。 • 単一コントラクト内に仮想アカウントを持つアカウントモデルと比べてUTXOモデルの利点は容易に新規コントラクトをオフチェーン生成できる点。 • UTXOベースのマルチパーティチャネルは、二重チャネル（ネストされたコミットメント）、Eltoo（バージョンによりコミットメントをリプレイス）、Channel Factory（階層型マルチパーティチャネルフレームワーク）、Lightning Factory（BLS署名用いてコミュニケーション複雑さを軽減）。 • マルチパーティチャネルの方向性として、「Sighash no_input用いた新規ファンド・参加者のSplice in/out」「閾値チャネル監査証明」「ルートトンネリング」「階層プレフィックスアドレシング」「Swaptionによるクロスチャネルスワップ」など。 • マルチパーティチャネルの課題は、(1)MassExit時のオンチェーンフットプリント削減するカットスルー(2)Splice outするためのヘルスチェックプロトコル(3)複雑なマルチステップのスワップを表現できる言語(4)パケットスイッチモデルにおける効率的なタイムロック。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/multi-party-channels-sb-latest.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/multi-party-channels-in-the-utxo-model-challenges-and-opportunities/ ➔ https://eprint.iacr.org/2018/642.pdf ➔ https://eprint.iacr.org/2018/918.pdf

SCALING BITCOIN2018の内容概略(6/9)

セクション	主題	サマリーメモ	資料URL
4. Scriptless Scripts と マルチパーティチャネル	マルチポップロックとECDSAによるScriptless Scripts	• 正直なユーザーがコインをマルチポップペイメントで失わないためのセキュリティツールとして、ハッシュのプレイメージを明かすことによる条件付ペイメント（HTLC）。 • このとき成功裏な完遂から正直なユーザーを排除して手数料を盗むのがワームホール攻撃。経路における同一条件により可能となり（他の仲介者はペイメント失敗と信じ込む）、仲介者が増えるほど攻撃利益増加。 • 現在のペイメントチャネルネットワークは、ワームホール攻撃のほか、誰が誰に支払うかのプライバシー、相互運用には特定ハッシュ関数サポートが条件となることなどが課題。 • 署名自身の中にペイメント条件をエンコードするのがScriptless Scripts。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/multi-hop-locks-for-secure-privacy-preserving-and-interoperable-payment-channel-networks.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/multi-hop-locks/ ➔ https://eprint.iacr.org/2018/472.pdf
	スクリプトレスECDSA	• 現時点のビットコイン向けにSchnorrベースでない、スクリプトレスな2p-ECDSAを提案したもの。ベンチマーク結果では、カギ生成に1票、署名に29ミリ秒。 • 利点としては、現時点でデプロイ可能な以外に、スクリプトやWitnessが小さくフィーが安価で済む点。一方で、正確に実装する上で手間がかかる・モバイルデバイス上でリソース消費・コミットメントトランザクション更新に複数ラウンド必要な点が課題。	➔ https://tokyo2018.scalingbitcoin.org/files/Day1/instantiating-scriptless-2p-ecdsa-fungible-2-of-2-multisigs-for-todays-bitcoin.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/scriptless-ecdsa/ ➔ https://eprint.iacr.org/2018/472.pdf ➔ https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-April/001221.html

SCALING BITCOIN2018の内容概略(7/9)

セクション	主題	サマリーメモ	資料URL
5. アーキテクチャ	OmniLedger	• 分散性とスケールアウトとセキュリティのトリレンマに対する提案。 • 分散乱数用いたシャーディング割当、アトミックなクロスシャードトランザクション（Atomix）、Trust but Verify（二段階検証。低レンテンシモードとスループットモードのオプション）。	➔ https://tokyo2018.scalingbitcoin.org/files/Day2/omniledger-a-secure-scale-out-decentralized-ledger-via-sharding.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/omniledger/ ➔ https://eprint.iacr.org/2017/406.pdf
	GhostDAGプロトコル	• 最長チェーン選択でなくDAG構造における最大k-clusterを選択するよう変更するもの。最大k-clusterを見つけるためのプロトコル提案がGhostDAG。	➔ https://tokyo2018.scalingbitcoin.org/files/Day2/the-ghost-dag-protocol.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/ghostdag/ ➔ https://eprint.iacr.org/2018/104.pdf

SCALING BITCOIN2018の内容概略(8/9)

セクション	主題	サマリーメモ	資料URL
6. Lightning Network	LNにおけるリバランシング	• ルーティングするマネーのロックに際してフィナンシャルコストがかかる。 • LNの全ルーティングノードはリバランシング問題とそのコストに直面する。 • リバランシング問題は(1)ペイメント予測(2)マネー配分最適化(3)リバランシングの小問に分割できる。 • ルーティングノードは正しくペイメントを予測することを通じて経済的に動機付けられる。 • チャネル間のバランス増減を行うリバランシングとしては、Splicingや循環ペイメントなど。リバランシングコストを最小化させながら、如何に多くのペイメントをルーティングするか。	➔ https://tokyo2018.scalingbitcoin.org/files/Day2/rebalancing-in-the-lightning-network-analysis-and-implications.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/rebalancing-lightning/
	再生可能なLightningベンチマーク	• c-lightningを用いたペイメントパフォーマンス。 • アリスからボブへは秒間34ペイメント。 • このときキャロルを介する場合は秒間12ペイメント。	➔ https://tokyo2018.scalingbitcoin.org/files/Day2/reproductible-lightning-benchmark.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/reproducible-lightning-benchmark/ ➔ https://github.com/dgarage/LightningBenchmarks
	ペイメントチャネルネットワークにおけるWatchtowerへのインセンティブ	• Watchtowerへの報酬は、賄賂の動機を減らすため、チャネル価値に相当するものであるべき。	➔ https://tokyo2018.scalingbitcoin.org/files/Day2/incentivizing-payment-channel-watchtowers.pdf ➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/incentivizing-payment-channel-watchtowers/

SCALING BITCOIN2018の内容概略(9/9)

セクション	主題	サマリーメモ	資料URL
7. インターオペラビリティ	HTLCによるアトミックスワップ	• スクリプト言語やScriptless Scripts用いて、秘密とタイムロックによるアトミックスワップ。4トランザクション（条件付送金x2, 償還x2）、条件付ペイメントx2により実装。 • アリスが強欲な場合に支払を行わないという不公平を解決すべく、担保と罰則を導入。	➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/atomic-swaps/
	オフチェーンによるUTXO所有権移転	• Schnorr署名やアダプタ署名やEltooおよびGraftrootを用いて、UTXO所有権をオフチェーンで変更しながらオンチェーン償還を保証するStatechainを構築。 • Bitcoinとコンソーシアムチェーンの連携について。ペイメントチャネルをコンソーシアムチェーン上に構築し、Bitcoinをアトミックに支払う。コンソーシアムチェーンのスマートコントラクトのインプットとして、コミットメントトランザクションを与えるもの。 • 半双方向チャネル向け更新。カスタマーからプロバイダの場合はタイムロックベースの制約。プロバイダからカスタマーの場合はペナルティベースの制約。	➔ http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/statechains/
	ビットコインとコンソーシアムチェーンの相互連携	• ビットコインのペイメントチャネルをコンソーシアムチェーン上に構築。 • コンソーシアムチェーン上のスマートコントラクトのインプットとして、コミットメントトランザクションを用いる。	➔ なし
	暗号通貨バックトークンの相互運用	• トークンがburnされたらビットコインをアンロックする。 • トークンのバックとなるチェーン側でHTLC、トークン発行側で条件付ペイメントで担保化。	➔ https://tokyo2018.scalingbitcoin.org/files/Day2/interoperability-with-cryptocurrency-backed-tokens.pdf

BITCOIN CASHのハードフォーク

- BitcoinABCの提案とnChainによるSVの対立

BitcoinABCの提案とnChainによるSVの対立

- Bitcoin ABCとnChainの対立で、当初予定の現状＋Bitcoin ABCの分岐に加えて、nChainによるBitcoin SVを含めた３本の分岐が11/15に発生可能性。
  - Bitcoin Cashのクライアントは複数存在。Bitcoin ABCがシェアの過半数を占め、次いでBitcoin Unlimitedが40%弱、それ以外は現状どれも僅かなシェア。
  - マイニング大手BitmainはABCアップグレードに賛成。CoinGeekはSVを支持。

Bitcoin ABC	nChainによるBitcoin SV（Satoshi Vision）
● 11月15日のハードフォークは、長らくロードマップにあったもの。 ● Bitcoin Cashクライアントの中で最も利用者の多いBitcoinABCが提案したアップグレード。 ● OP_CHECKDATASIGの追加 • ブロックチェーン外からの任意のデータ・メッセージに対する署名をスクリプト内で検証可能に • オラクルから取得したデータを検証できる他、クロスチェーンアトミックスワップへの応用が可能 ● Canonical transaction orderingの導入 • ブロックにトランザクションを格納する際の順序にルールを設けるもの • スケーリングソリューションGrapheneの将来的導入のベースになるもの	● Bitcoin ABCが発表した変更内容にnChainが反対表明。 • nChainのCraig Wright氏の不満は、Bitmain Wormhole Partnershipに起因。 ● 「OP_DATASIGVERIFY」「Canonical transaction ordering」を実装するクライアントを使用したマイニングせず。 • 両機能の実装も無し ● オリジナルのBitcoinプロトコルを復元。 • オリジナルのSatoshi OPコードを復活させる（OP_MUL, OP_LSHIFT, OP_RSHIFT, OP_INVERT） • スクリプトごとのOPコード数の上限を撤廃（現状はスクリプト毎に201個まで） ● スケーリング：最大ブロックサイズを128MBに。

→ 出典: https://bravenewcoin.com/insights/bitcoin-cash-hard-fork-looking-likely-for-november
→ 出典: https://bchnews.jp/bitcoincashnews-e/2051
→ 出典: http://www.bitcoinabc.org/2018-08-20-announcing-bitcoin-abc-0-18-0/
→ 出典: https://nchain.com/en/blog/bitcoin-sv-launch/

2. Ethereumエコシステムの動向

- Ethereum2.0
- Ethereumハードフォーク延期

ETHEREUM2.0

- CasperFFGの廃止
- Ethereum2.0のアーキテクチャ（BeaconChain・ShardChain・CrossLink）
- Validator・Active Validator Set・ProposerおよびAttester
- RANDAOおよびVDF
- EVMとWASM
- ロードマップ

CasperFFGの廃止

- CasperFFG廃止の経緯
  - CasperFFGを単一コントラクトとして実装することで開発が進み2017年末にはテストネットリリースに至ったものの、一方でEVMからEWASMへの切り替え、シングルチェーンCasperからShardingされたCasperへの切り替えが難しくなった。
  - 活動が分断した為、不必要な重複作業がCasperチームとShardingチームに発生。そこで2018年6月、「コントラクトとしてのハイブリッドCasperFFG」をスクラップし、代わりにSharding統合をより容易なものとする設計「フルCasper（フルPoS）」追求のシフトを決定。
  - ShardingとPoS（双方むけにバリデータが必要、など）インフラのオーバーラップを考慮すると、アプローチをマージすることによって、冗長性であったり、マージ／同期問題を軽減できるメリット。
- 廃止されたCasperFFGの仕組み
  - CasperFFGはPoSベースコンセンサスシステムにむけたEthereumの最初のアプローチであり、EIP1011に仕様が示されたもの。
  - PoWチェーン上に存在するスマコンとして設計された（ハイブリッドなPoW・PoS）。
  - バリデータになるための最低ステーク1500ETHという高額設定。
- 廃止されたCasperFFGの問題点（全投票をCasperスマコン内で収集・検証）
  - ノーマルPoWチェーンへ依存するため、ブロックサイズあたりのブロック生成時間は、毎秒15TXという制約が、1500ETHという非常に高いミニマムデポジットサイズに繋がり、分散化を阻害。
  - １エポックの投票に必要な見込時間も膨大となり、現実的でないという署名検証ボトルネック。

→ 出典：https://threadreaderapp.com/thread/1029900695925706753.html
→ 出典：https://medium.com/ethereums-transition-from-casper-ffg-to-beacon/from-casper-ffg-to-full-casper-chain-cbd522751a7e

ETHEREUM2.0のアーキテクチャ（BEACONCHAIN・SHARDCHAIN・CROSSLINK）

- Ethereum2.0は、Casper＋Shardingを組み合わせたもので、 Shasperとも。
  - ビーコンチェーン（Ethereum2.0のコア）とシャードチェーンによるPoSシステムとなる。

メインチェーン	• ステーキングを提供する位置づけのPoWチェーン。

ビーコンチェーン	• シャーディングシステムのベースとなる中央のPoSチェーン。
	• 乱数を提供する位置づけ。
	  • ビーコンチェーンは、バリデータセットの再シャッフルやアロケートのためのシードとして、乱数を提供する存在でもある。
	• アクティブなPoSバリデータのセットを格納＆管理する。
	• 各シャードの証拠（Attestation）のトラックを保持する。
	  • それゆえ、独立したシャードチェーンむけビーコンを管理する。
	• ビーコンチェーンをメインネットから分離することによって、より多くのバリデータを可能に。
	  • 個々のバリデータステイクも、1500ETHから32ETHに減じることができる。

シャードチェーン	• ユーザTXが発生し、アカウントデータが格納するチェーンのひとつ。 • データを提供する位置づけ。 • 各シャードは、それ自身がPoSチェーンであり、TXやアカウントが格納される。
クロスリンク	• シャード内ブロックを証明するコミッティからの署名セットであり、ビーコンチェーンへ含める。 • ビーコンチェーンがシャードチェーンの更新後ステートを学習するための主たる手段となる。 • 十分な数の認証が同一シャードブロックにたまると、クロスリンクを生成し、シャードセグメントをビーコンチェーン内のシャードブロックへ承認する。 • クロスリンクは同期クロスシャードコミュニケーションむけインフラとしても機能する。
VM	• ステート実行結果を提供する位置づけ。

→ 出典：https://github.com/ethereum/eth2.0-specs/blob/master/specs/beacon-chain.md
→ 出典：https://medium.com/ethereums-transition-from-casper-ffg-to-beacon/from-casper-ffg-to-full-casper-chain-cbd522751a7e
→ 出典：https://docs.google.com/presentation/d/1VY997VlsbLdjePiLh4fAF0t-JKlcMJk4A1oJJ_oNqns/mobilepresent?slide=id.g3d4e599995_0_223

VALIDATOR・ACTIVE VALIDATOR SET・PROPOSERおよびATTESTER

バリデータ	• Casper/Shardingコンセンサスシステムの参加者。
	• 32ETHをCasperメカニズムへデポジットすることによってバリデータになることができる。
	  • 64スロットの所与のビーコンノードサイクル内でシャッフルされ、ブロックをアテスタによる投票されるノードへ提案できる。
	  • ブロックや証明を交換するために、ビーコンノードとコミュニケートする必要がある。

アクティブ
バリデータセット
	• ブロックやクロスリンクやコンセンサスオブジェクトを生成・証明するバリデータ。
	  • 参加者がいったんバリデータプールに入ると、あるシャードへ割り当てられる。
	  • ５秒のタイムスロットで当該タイムスロットのブロックを生成するようバリデータを割当。
	  • 割り当ては完全にランダム。VDFを用いてバイアス無しのランダムを実現。
	• バリデータセットは64スロット毎（1スロット＝８秒）にランダムシャッフルされ、N個の同サイズのスライスに分割。

コミッティ	• アクティブバリデータセットから擬似ランダムにサンプルされたサブセット。
	  • コミッティ内のバリデータがそれぞれブロックへ署名することで証明。
	  • 署名はBLS署名集約で蓄積され、証明人数によるブロックサイズ爆発を回避。

プロポーザ	• 各タイムスロットにて当該タイムスロットにブロック生成するように割当てられるバリデータ。 • 以前のブロックの証明を集約して、プロポーズドブロックとし、プロポーザルブロックをビーコンノードへ送る。

アテスタ	• 所与のスロットにおけるブロックに関する投票やサインオフの権利を付与されたバリデータ
	  • ビーコンノードはプロポーズドブロックをとって、それを証明されるべきブロックのためにアテスタに送る。
	  • アテスタは自身の証明をビーコンノードへ送り返す。

→ 出典：https://github.com/ethereum/eth2.0-specs/blob/master/specs/beacon-chain.md
→ 出典：https://medium.com/ethereums-transition-from-casper-ffg-to-beacon/from-casper-ffg-to-full-casper-chain-cbd522751a7e
→ 出典：https://medium.com/nearprotocol/detailed-overview-of-ethereum-2-0-shard-chains-committees-proposers-and-attesters-a9992d2fd103

RANDAO

- CasperFFGの古いバージョンは、フルPoS機能ではない。
  - 分散でありながら決定論的なシステムにおいて、過失に耐えるランダムネスを得ることは難しいと考えられたため。
  - そのためブロックを生成・提案するバリデータをランダムに選択するかわりに、バリデータはPoWチェーンによって提案されるエポック毎に投票されるものとした。
- 不正利用不能なランダムネスを生成するため、RANDAOを用いる。
  - RANDAO（ランダム＆DAO）は、オンチェーン（スマートコントラクト）の乱数サービス。
  - シードを生成する中央ソースを持つかわりに、ランダムネスがコミュニティによって３フェーズで生成。

フェーズ１	• 生成プロセスに参加することを望む全参加者が、ランダムに選択された数値 s のハッシュを一定額のETHをステイクとして添えた上で、一定タイムフレーム内に、RANDAOコントラクトへ送付する。
フェーズ２	• 参加者が選択した数字 s を、他のタイムウインドウ以内にそれを送付することによって、コントラクトに対して明かす。 • コントラクトが s がフェーズ１で提出されたハッシュとマッチするかを検証し、s を乱数生成関数のシードへ保存する。
フェーズ３	• 参加者による全ての乱数 s を収集した後、最終乱数に関数 f （ｓ１、ｓ２、、、、）を適用し、その結果をランダムシーケンスを必要とする全コントラクトへ送る。

- ラストアクター問題を避けるためにVDF（検証可能な遅延関数）が必要。

→ 出典：https://docs.google.com/presentation/d/1VY997VIsbLdjePiLh4fAF0t-JKlcMJk4A1oJJ_oNqns/mobilepresent?slide=id.g3d4e599995_0_223
→ 出典：https://medium.com/ethereums-transition-from-casper-ffg-to-beacon/from-casper-ffg-to-full-casper-chain-cbd522751a7e

VDF（検証可能な遅延関数）

- Ethereum2.0チェーンにおけるバリデータの一人が、新しいブロックを提案しようとしており、それゆえ乱数シードを最初に知っていると、結果に影響を与えることが可能。
  - ①ブロックを生成し、乱数を明かし、ブロック報酬をうけとる。
  - ②ブロックを生成せず、乱数を再びシャッフルするが、ブロック報酬を緩める。
- プロポーザが前もって、いくつのスロットが選択されるかを知っていれば、システムを不正利用する余地がうまれるため、可能なアウトカムを事前に計算することができないようなシステムが必要。
- VDFは、計算の並行不可能でありながら、高速に検証可能な関数。
  - 一方向で計算に長い時間がかかり、アウトカムが予測不能で、それでいて検証が容易。
  - 換言すれば、VDFは時刻非同期の特性を持つ。
- プロポーザが、VDF計算のためのソースデータを決定するデータを提出しようとしていると仮定する。
  - 他のソースデータとともに、それは時刻Tにおいて明かされる。
  - その提出は時刻T+D以前になされなくてはならない。
  - 一方で、ソースデータに対してVDFを実行するには、保守的な環境のもとでW（W>>D）の時間が必要となり、ロポーザがリリース前に異なるコミットをすることを禁ずることになる。
- VDFをEthereum2.0でランダムビーコンとして用いることが有望視されている。

→ 出典：https://medium.com/ethereums-transition-from-casper-ffg-to-beacon/from-casper-ffg-to-full-casper-chain-cbd522751a7e

EVMの制約とWebAssemblyとの相違

- バイトコードを実行するEVM（256ビット）はプレコンパイルにコストを要する。
  - ステートルートが全ブロックに記録される。
  - 256ビットアーキテクチャでほとんどのハードウェアむけフィットに貧相。
  - 限定的なコンパイラサポート。

- これに対して、W3Cグループにより開発されWebAssembly(WASM)は軽量な命令セットかつ広範な言語のコンパイル可能でプラットフォーム独立ゆえDappsに向いており、DfinityやEOSの実行レイヤーなどで既に標準として、将来的なWebパフォーマンスやスマートコントラクト実行レイヤー双方で有用な可能性。
  - 標準化され・最適化されている。
  - 広い範囲におよぶ実装。
  - 強力なコンパイラサポート。
  - プロトコルからのプレコンパイルを除去。

→ 出典：https://docs.google.com/presentation/d/1VY997VIsbLdjePiLh4fAF0t-JKlcMJk4A1oJJ_oNqns/mobilepresent?slide=id.g3d4e599995_0_223
→ 出典：https://medium.com/zkcapital/webassembly-the-future-of-blockchain-computing-1a0ae28f7e40

ロードマップ

- メインチェーン（ステーキングを提供）：PoW ←2018
- ビーコンチェーン（乱数を提供）：PoS、CasperFFG ←2019
- シャードチェーン（データを提供） ←2020
- VM（ステート実行結果を提供） ←2021

フェーズ0	PoSビーコンチェーン（2019？）	• サイドチェーンとしてPoSビーコンチェーンを実装 • 乱数生成シード：RANDAOを用いたVDF • BLS12-381楕円曲線を用いるBLS集約署名 • 5秒ブロックタイム、定期的ファイナリティ • 32ETHのステークでバリデータに。Slashingメカニズム導入 • PoWマイニング報酬を80%削減（3 ETH→0.6ETH）
フェーズ1	シャードによるトランザクションハンドリング（2020？）	• TXむけシャーディングインフラ追加 • それぞれのシャードが、追記のみ可能なTXデータログを維持 • プロポーザ、アテスタ、バリデータのメカニズムを実装 • ビーコンチェーンへクロスリンクを実装 • メカニズムデザインのテスト
フェーズ2	シャードによるステートハンドリング（2021？）	• シャードへステート実行を追加 • eWASMエンジンがEVMをリプレイス？ • 同期または非同期シャード内・間コントラクトコール • 軽量クライアントやステートレスクライアント

→ 出典：https://docs.google.com/presentation/d/1VY997VlsbLdjePiLh4fAF0t-JKlcMJk4A1oJJ_oNqns/mobilepresent?slide=id.g3d4e599995_0_223

ETHEREUMのハードフォーク、2019年に延期へ

- コンスタンティノープル（Constantinople）」と呼ばれる今回のソフトウェア・アップグレードのテスト中のコードにバグを発見
  - これを受け、2018年11月に実施する見込みだったハードフォークは、2019年に持ち越し。

- コンセンサスアルゴリズムの1つである「difficulty bomb」に関連している。
  - 新たなブロックを採掘する難易度は着実に高くなると見られる
  - difficulty bombの当初案
    - PoWからPoSへの移行を進めるための計画の一部であった
    - ネットワークが切り替わると、マイナーは古いブロックチェーンの採掘を続けられなくなる
  - プルーフ・オブ・ステークのシステム開発には予想以上に時間がかかっている
    - ディフィカルティ・ボムの導入を延期必要に

- ブロック報酬
  - コア開発者らは1ブロックあたりの報酬を3イーサ（ETH）から2イーサに変更することで決着していた
  - しかし、アップグレードは早くとも2019年1月にまで延期

→ 出典：https://www.technologyreview.jp/nl/ethereums-difficulty-bomb-will-change-the-currency-forever-when-it-finally-drops/

3. プラットフォーム全般の動向

- プライバシーとアイデンティティ
- 識者の視点
- 分散金融エコシステム動向
- 証券トークン
- クリプトエコノミクス
- ブロックチェーンガバナンス
- プレイヤーエコシステムマップ

プライバシーとアイデンティティ

- プライバシー確保が求められる背景
- プライバシー関連技術
- 暗号通貨プライバシー概観
- 分散アイデンティティ

プライバシー確保が求められる背景

- ブロックチェーンは参加者間における透明さやトラストをひきだす力があるとされる。
  - プライベート或いはセンシティブなデータを扱うことができれば、ブロックチェーンのポテンシャルをいかすことができる。
- 分散金融プラットフォーム（送金のフンジビリティや証券トークン等）として、データセキュリティおよびプライバシーは、最も機微な側面をもつテーマ。
  - アセットベーストークン化されたプロダクトは、トレードに関わる機微な情報の保護を確かにすべく、FINRAプライバシールールが定められている、など。
- 自身のデータをデジタルアセットとして所有・貸出・売却可能にすることを通じて、マネーがデータ化したようにデータをマネー化するという文脈でもプライバシーは重要。
  - 例えばトークンとして医療レコードを絵画同様のユニークなアセットとして、ある時点においめ単一エンティティのみが所有できるように。
  - トークンとしてトラッキングし、暗号通貨によるマイクロトランザクションによるファイナンスを通じて、既存の利益モデルを守ったりコストダウンではなく個人に力を取り戻しデータファームが豊かになる可能性。
- 分散的な方法でプライベートデータを計算するためのスケーラブルなソリューションが必要。

→ 出典: https://hackernoon.com/the-elephant-in-the-room-security-and-privacy-protocols-in-security-tokens-a6687af8d1d6
→ 出典: https://qz.com/1381355/the-currency-of-the-future-is-personal-data/
→ 出典: https://blog.coinmarketcap.com/2018/10/09/privacy-for-blockchains-an-introduction/

プライバシー関連技術 （1/2）

CryptoNote およびリング署名	• トレーサブルなリング署名を用いてグループ間でメッセージを難読化するもの。 • CryptoNoteはMoneroの背後で使われている。

sMPC
- Secure Multi Party Computation
(単にMPCとも)
	• トラストされない参加者を組み合わせることによって、データをおくって我々のかわりに計算してくれることをトラストできるが、プライベートデータを漏えいすることのない、トラストされた第三者をエミュレートするもの。
	  • 計算過程でデータが漏えいすることのない、分散ネットワークを設計できる。
	  • インプットをプライベートに保ちながら、インプットの集合への計算実行を可能とするため、ネットワーク上のそれぞれのコンピュータは暗号化されたデータを見ることができるが、意味あるものとしては見えない。
	  • ネットワーク上の全参加者が結託してデータを漏えいさせようとすることによってのみ、平文を復元できる。

完全準同型暗号	• 完全にソフトウェアベースのプライバシーソリューション。
	  • AとBという値があるとき、暗号化されたEAとEBを得る。
	  • EA+EBを計算すると、E(A+B）と等しい。
	  • ECが復号されると、A+Bの合計が得られる。

ゼロ知識証明
（ZKP）
	• ある種のセキュア計算で、他のデータを明かすことなく、証明人に証明させるもの。
	  • 証明人は、秘密データそのものを明かすことなく、秘密データの知識を有することを示さなくてはいけない。
	  • 認証の場合、パスフレーズの知識を持つことを示すことによって、秘密をダイレクトに提供することなく、自分のアイデンティティを証明する。

→ 出典：https://hackernoon.com/the-elephant-in-the-room-security-and-privacy-protocols-in-security-tokens-a6687af8d1d6
→ 出典：https://blog.coinmarketcap.com/2018/10/09/privacy-for-blockchains-an-introduction/

プライバシー関連技術　(2/2)

ZK-SNARKs	• ZKPの特別な形態。 　• Non Interactive＝証明人・検証人が同時にオンラインである必要なし。 　• Succinct＝証明が小さなサイズであり検証が高速。 　• 欠点は、「証明生成が遅いことと（シンプルなステートメントの証明でも数分）」および「用いられる暗号学的仮定がかなり新しく、十分アカデミアや産業界で確立できてないこと」など。
ZK-STARKs	• ZK-SNARKsは、証明の複雑さがDBサイズに対して線形でスケールするため適用が難しいのに対して、ZK-STARKsでは、かわりにリーンな対称暗号、衝突耐性あるハッシュ関数を必要とする。 　• そのため、トラストされたセットアップの必要をなくす点が特徴で、量子コンピュータ耐性もある。
TEE	• ハードウェアベースのプライバシー技術であり、ブロックチェーンにおける機密計算をオフロードする位置づけ。 　• 安全なハードウェアを用いて、ハードウェア自身の外部へ漏えいすることからデータを保護する。アプリ実行は安全に保護され、第三者からのアクセス不可能。 　• SGXの場合、孤立コード実行・リモート保持・セキュアプロビジョニング・セキュアデータストレージ・コード実行むけトラステッドパスなどを備える。 　• トレードオフは、ハードウェアが侵入されていないことをトラストしなくてはいけない反面、パフォーマンスは純粋なソフトウェアベースの安全計算より高速。

→ 出典：https://hackernoon.com/the-elephant-in-the-room-security-and-privacy-protocols-in-security-tokens-a6687af8d1d6
→ 出典：https://blog.coinmarketcap.com/2018/10/09/privacy-for-blockchains-an-introduction/

暗号通貨プライバシー概観

- プライバシーコインとしてはZcash、Monero、Mimblewimble/Grinの他にMobileCoinやBEAMの名。
- プライバシーインフラとしてはOrchid、BOLT、NuCypher、Starkwareの名。
  - スケーリングからDandelionやSchnorr署名・Taprootといったフンジビリティ・プライバシーへ。
- スマートコントラクトプライバシーとしてはZether、Keep、Enigma、Origo、Cavalent、Oasis LabsのEkiden。
  - スマートコントラクトのプライバシーについてはオフチェーン化のほか、Simplicity言語もちいた形式証明つきコントラクトについて言及。
- プライバシー研究トピックとしては、ゼロ知識（zkSNARKs、zkSTARKs、Bulletproof）、MPC（マルチパーティ計算）、完全準同型暗号。
  - Confidential Transaction適用にむけたトランザクションサイズのトレードオフ。
  - Bulletproofはサイズ縮小するがインフレ課題残る。
- Enigmaの秘匿投票コントラクトのプロトコルも、 TCRむけ投票などに有効。

→ 出典：https://twitter.com/kanzure/status/1043484879210668032?s=21
→ 出典：https://blog.enigma.co/secret-voting-smart-contracts-with-enigma-a-walkthrough-5bb976164753
→ 出典：https://thecontrol.co/an-overview-of-privacy-in-cryptocurrencies-893dc078d0d7

分散アイデンティティ – ネームスペース関連

- パスワードなどの機微情報が漏洩・盗難被害に遭う時代にあって、個人データのオーナーシップを企業や政府から個人に取り戻し、自ら望む場合にデータを共有できるようにする動きが、デジタルアイデンティティへのブロックチェーン応用。
  - 改竄困難な状態遷移ログとして、アイデンティティを継続的にトラッキングするもの。
  - 分散アイデンティティは、中央レジストリ無しに、ヒトやデバイスなどのエンティティを特定するもので、主なフォーカスはネームスペース（アドレス）と認証証明の２つ。
- ネームスペース

Namecoin	• ビットコインフォークによる分散ネーミングシステムだったが、UX悪く普及せず。
Onename	• ビットコインブロックチェーン上にユーザー名とプロフィールデータを格納する。 • dappプラットフォームBlockstackのネームスペースレジスタとして、各種dapp横断でパーソナルデータのオーナシップを保持できるようにしている。
ENS	• Ethereum向けDNS。レジスタとしてのスマートコントラクトがネーミングの更新・管理。
Handshake	• 分散DNSルートゾーン。 • 新たなUTXOブロックチェーン上に構築され、全P2Pフルノードがルートゾーンファイルをホストするルートサーバーとして、ルートゾーンを検閲不能でパーミッションレスする。 • 既存CAを代替すべきものとしての、非中央集権型のDNS互換ネーミングプロトコル。 • 全ノードがバリデータとしてルートゾーンの管理に責任もつ。 • 非中央集権的なやり方でインフラ全体のルートサーバー（サイト名やIPアドレス記したルートゾーンファイルを門番として管理・配布するICANN）のリプレイスを目指す。

→ 出典：https://medium.com/zkcapital/handshake-ens-and-decentralized-naming-services-explained-2e69a1ca1313
→ 出典：https://thecontrol.co/understanding-decentralized-identity-433abb343279

分散アイデンティティ – 認証・証明関連

- 認証証明
  - トランザクションやコントラクト実行に先立ち、オンライン上の人物が確かに本人であることを第三者無しに認証証明するもの。運転免許証など無しに、スタンドアロンで現実のアイデンティティと紐付けるのが、セルフソブリンアイデンティティ。
  - Dapp間でポータブルなアイデンティティとして、マイナンバー情報などの属性データの認証を、当該データコピー生成無しに行うもの。
  - セルフソブリンアイデンティティに取り組んでいるものとして、ERC725やuPortが代表例。

ERC725	• オンチェーンアイデンティティをEthereum上で管理するための標準として提案された。 • アイデンティティコントラクトがコントラクトオーナーの署名を含むものとして、メアドなどのアイデンティティ情報をコントロールする。
Originプロトコル	• ERC725を用いてアイデンティティの検証を行うもので、シェアリング経済向けスマートコントラクト実行に利用している。
uPort	• セルフソブリンアイデンティティのウォレットとして、アイデンティティやパーソナルデータのコントロールを可能とするもの。 • パスワード無しにdappにログインしたり、パーソナル情報の管理・検証や、トランザクション承認や、ファイルへのデジタル署名を行うことができる。 • 更に3Boxと呼ばれる分散データストレージを開発しており、これはdapp横断でデータのアップロードや共有を可能とする。

→ 出典：https://thecontrol.co/understanding-decentralized-identity-433abb343279

識者の視点

- 競争的地位確立へむけた政策選択
- デジタルアセットのルール形成とテクノロジー活用
- デジタルアセットを巡るルール形成にむけたテクノロジー視点・金融業界視点の融合
- ブロックチェーンプラットフォーム確立へむけたソフトウェアスタック整備
- 非中央集権性とトラストレス性

競争的地位確立へむけた政策選択 ～ Coin Centerの米上院公聴会むけ資料（1/2）

- ブロックチェーン技術が社会的・経済的・組織的・サイバーセキュリティ問題の解決策と喧伝されることを否定し、パブリックコンセンサスメカニズムが電子的現金・アイデンティティ・IoTに係る特定の問題を解決するに過ぎないと主張している。
- 電子的現金
  - 電子的現金が解決するのは既存の電子的なマネー送信が実現できない効率性（口座開設しないと送受金不可など）。パブリックコンセンサスメカニズムを通じた所与のルールと経済インセンティブによって、台帳の生成・維持を自動化することで、現金同様の電子トランザクションを実現する、と。
- アイデンティティ
  - インターネットに欠けているのがネイティブなアイデンティティ層。インターネットユーザーは脆弱なパスワードや秘密の質問に頼らないとアイデンティティ検証ができない。ここにアイデンティティデータを記録するための共有かつ誰かに所有されるものでないプラットフォームを作ることで解決を図る。
- IoT
  - IoTデバイスアイデンティティやユーザーアクセス認証のための分散データ構造を作ることによって、製造者によるサポート終了の判断によりプロダクトへアクセス不可となるなどを防止できる。
  - また、デバイス通信やデータストレージや計算をP2Pネットワーク上で共有できるた、デバイス間の相互運用性や互換性が向上できる。加えて、電子的現金システムを通じて、ネットワークインフラを維持するためのデバイスペイメントが効率的に可能となる。

→ 出典：https://www.banking.senate.gov/imo/media/doc/Van%20Valkenburg%20Testimony%2010-11-18.pdf

競争的地位確立へむけた政策選択 ～ Coin Centerの米上院公聴会むけ資料（2/2）

- ブロックチェーン技術のインパクトについて
  - 電子的現金、アイデンティティ、IoTといった意味での便益は現実であり、例えば電子的現金により効率的なマイクロトランザクションや金融包摂が可能となる他、頑健なアイデンティティはオンラインセキュリティ問題を解決し、ブロックチェーンベースのIoTシステムはよりセキュアで競争力あるものになる。
  - 「とはいえ、これら3点は氷山の一角であり、1995年にFacebookやUberの登場を予見できなかったように、自由でパブリックな実験プラットフォームが提供されたときに、クリエイティブで多様なマインドがどのように発揮されるかは知る由もない」と結んでいる。
  - パブリックコンセンサスメカニズムはトラストを非中央集権化し、参加者横断でネットワーク上のパワーを拡散することによって、ユーザーの主権・相互運用性・忠実性・可用性・プライバシー・政治的中立性を確かなものにすることに寄与するもの。
- 結び
  - 米国がグローバルなテクノロジーマーケットで競争的地位を維持するような政策選択をするためには、より詳細で生産的議論が必要であり、どのようにコンセンサスがとられるかの基本的理解などが必要。

→ 出典：https://www.banking.senate.gov/imo/media/doc/Van%20Valkenburg%20Testimony%2010-11-18.pdf

デジタルアセットのルール形成とテクノロジー活用 ～ コア開発者によるSECへのオープンレター（1/2）

- デジタルアセット分野におけるルール形成の課題
  - デジタルアセットは強み・能力の面でユニークなアセットクラスだと考えているが、その強みを反映しないやり方によるルール適用には警鐘を鳴らしたい、とする。
  - このアセットクラスにおいて、従来には可能ではなかった方法を通じて投資家保護をはかるべきで、そのソリューションは政策ではなくテクノロジーに拠るものであるべき。

- テクノロジー観点からみた従来型アセットとデジタルアセットの比較
  - デジタルアセットの強みは、個人レベルでコントロールできる点であり、透明性や頑健性の面でも従来型アセットと比較してレベルアップを提供する。
  - 従来型アセット向けにデザインされた今日のルールにのみ依拠するのでなく、利用可能な技術の利点を見極めてルールに組み込むべき。

- テクノロジー活用を通じたデジタルアセットの安全・柔軟な管理
  - デジタルアセットの安全・柔軟な管理に適用できるテクノロジーを用いることによって、利便性やイノベーションを犠牲にすることなく、投資家や金融機関の支払い能力を保護する、そうしたデジタルアセットの安全管理モデルを構築することが可能。
  - テクノロジーの力を活かして、透明性・監査可能性・支払能力証明などを組み込むことによって、デジタルアセットのカストディに関するベストプラクティスを形成できる。

→ 出典：https://www.sec.gov/divisions/investment/allen-bishop-crespigny-fearey-long.pdf

デジタルアセットのルール形成とテクノロジー活用 ～ コア開発者によるSECへのオープンレター（2/2）

- デジタルアセット管理へのテクノロジー活用へむけた例
  - Locktimeトランザクションを通じ暗号鍵紛失時にクリアリングハウスがアセットのリカバリ可能に。
  - マルチシグトランザクションを通じて、特定条件を満たすまで資金をロック。
  - デジタルアセットの保有を、アセット残高を明かさずに証明。
  - 規制をアセットレベルでコーディングし準拠を担保。

- 結び＝テクノロジーに通じたメンバを巻き込んだルール形成の必要性
  - こうしたテクノロジーの力を活かしたルール形成するためにも、SECはテクノロジーに通じたエンジニア、開発者、交換業者、スマートコントラクト設計者などを巻き込んで、ベストプラクティスを実装していくべき。

→ 出典：https://www.sec.gov/divisions/investment/allen-bishop-crespigny-fearey-long.pdf

デジタルアセットを巡るルール形成にむけたテクノロジー視点・金融業界視点の融合

- @34roは、論考の中で、「仮想通貨について、定性的価値として捉えるインターネット業界、定量的価値として捉える金融業界と、それぞれ違う見方をしているのではないか」と主張している。

- Coinbase CEOは、「テック企業と金融企業のブレンドだが、一つを選ぶとすればテック企業であり、それはこの20年で世界を変えたのが金融機関でなく、テクノロジーこそが革新や成長をもたらすから」と主張している。
- その上で、ただし「ただし究極には二者択一ではないクリプト企業。テクノロジーにも金融にも制約があり、両業界や他業界から才能を集め、ルールメイクしていきたい」とも述べている。

→ 出典：https://blog.coinbase.com/is-coinbase-a-finance-or-tech-company-f474b852272d
→ 出典：https://medium.com/@34ro/インターネット業界と金融業界では仮想通貨を全く違う視点で見ている-86283cb2d148

2) 識者の視点

ブロックチェーンプラットフォーム確立へむけたソフトウェアスタック整備

- a16zは、インターネットとブロックチェーンの違いについて、「インセンティブデザインを、ハードウェア依拠でなくソフトウエアで実現しているため、クリプトネットワークとしての可能性を広げている」との見方を示している。

- USVは、プラットフォームライフサイクルに関する論考の中で、「まずアプリケーションが登場し、その課題解決すべくインフラが整備され、それをベースにアプリが出来、そのニーズを踏まえインフラがさらに整備され、、のサイクルを踏む」というイメージを示している。

- こうしたブロックチェーンプラットフォームを巡る全体像を俯瞰する中で、スタック構造としての整理と、カテゴリー別集計が示されるようになってきている。
  - レイヤー4（アプリケーション）
  - レイヤー3（計算、セキュリティ・アイデンティティ、ガバナンス、エクスチェンジ、tablecoin）
  - レイヤー2（スケーリング・プライバシー・相互運用性）
  - レイヤー1（暗号通貨と台帳）

→ 出典：https://a16z.com/2018/07/31/cryptonetworks-decentralization-web-scale-building-blocks/
→ 出典：https://www.usv.com/blog/the-myth-of-the-infrastructure-phase?ref=tokendaily
→ 出典：ブロックチェーンのレイヤー構造と、レイヤーカテゴリー別集計

非中央集権性とトラストレス性

- コア開発者のMattは、「Decentralizationという曖昧な表現より、Trustlessnessという表現が好ましいのではないか」と主張している。
  - ビットコインを使うのは第三者をトラストしたくないから。ビットコイン以前の電子マネーが上手くいかなかったのは誰かをトラストする必要があったから。
  - 自ノードをトラストして検証するだけで済むのが、安全なセツルメント手段としてのデジタルゴールドの側面。
  - コンセンサスグループの分散や検閲耐性を諦めて、誰もが自分でノードを立てて検証できるのではなく、少数のエンティティによるトランザクション検証とするアプローチもあるが、トレードオフであり、それはビットコインではない、とのこと。
- 非中央集権システム構築には「当初は集権性がある程度は残る」という見方も。
  - その要因は、スケーラビリティ・手数料・規制・アダプション・ガバナンス可能性・エコノミクス・ノベルティの七つ。
- PlaceholderのBurniskeは、「非中央集権と集権のバランスが重要」と主張。
  - 全てを非中央集権化するのでなく、分散プロトコル上の集中型アプリケーション（例えばCoinbase）というあり方。
  - その場合、グローバル規模の立ち上げ、オンデマンドによる低コスト、オープンソース活用による竣敏さ、といったメリットを享受することができる。

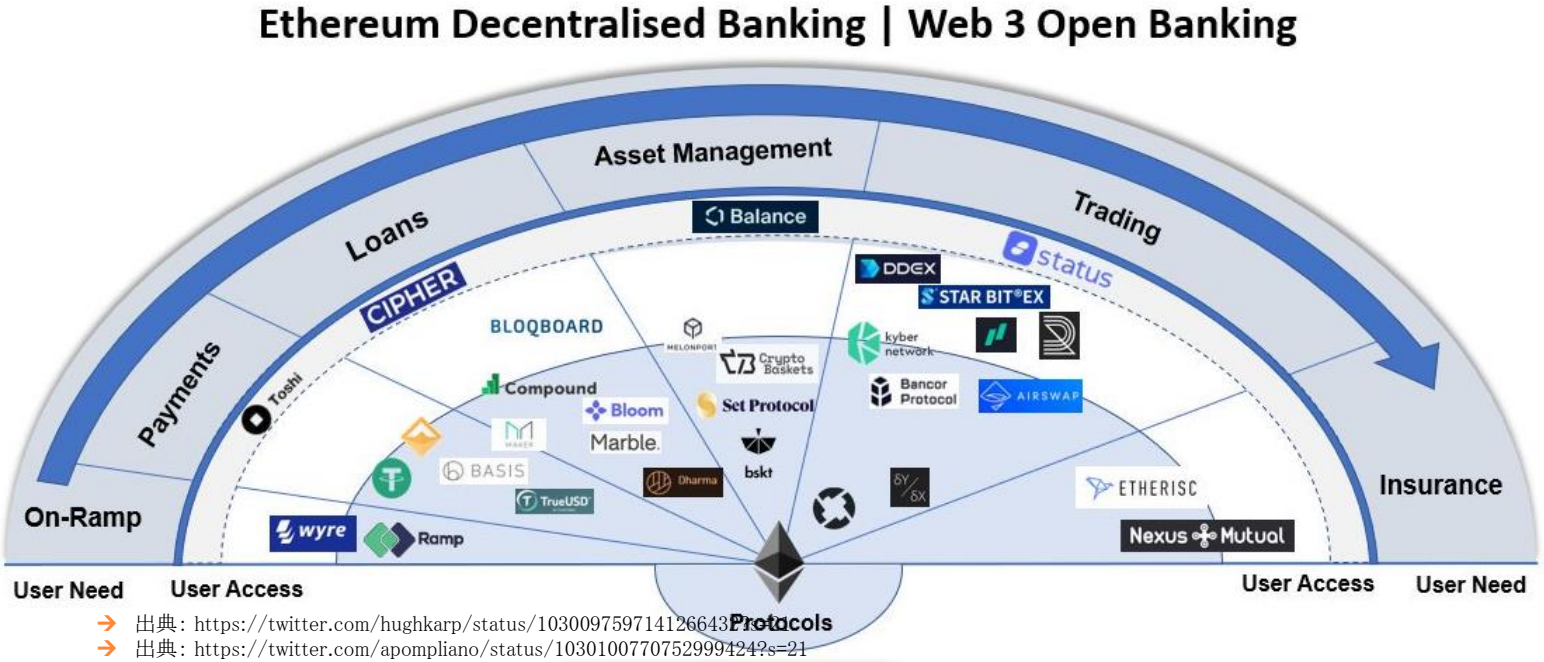
→ 出典：https://twitter.com/lopp/status/1043394297603739648?s=21
→ 出典：https://medium.com/2gether/the-seven-obstacles-we-have-encountered-building-a-decentralized-bank-27c13fca72d0
→ 出典：https://twitter.com/cburniske/status/1055476651914600449?s=21

分散金融エコシステム動向

- ユーザー視点からみた分散金融マップ
- 動向の俯瞰
- Stablecoin

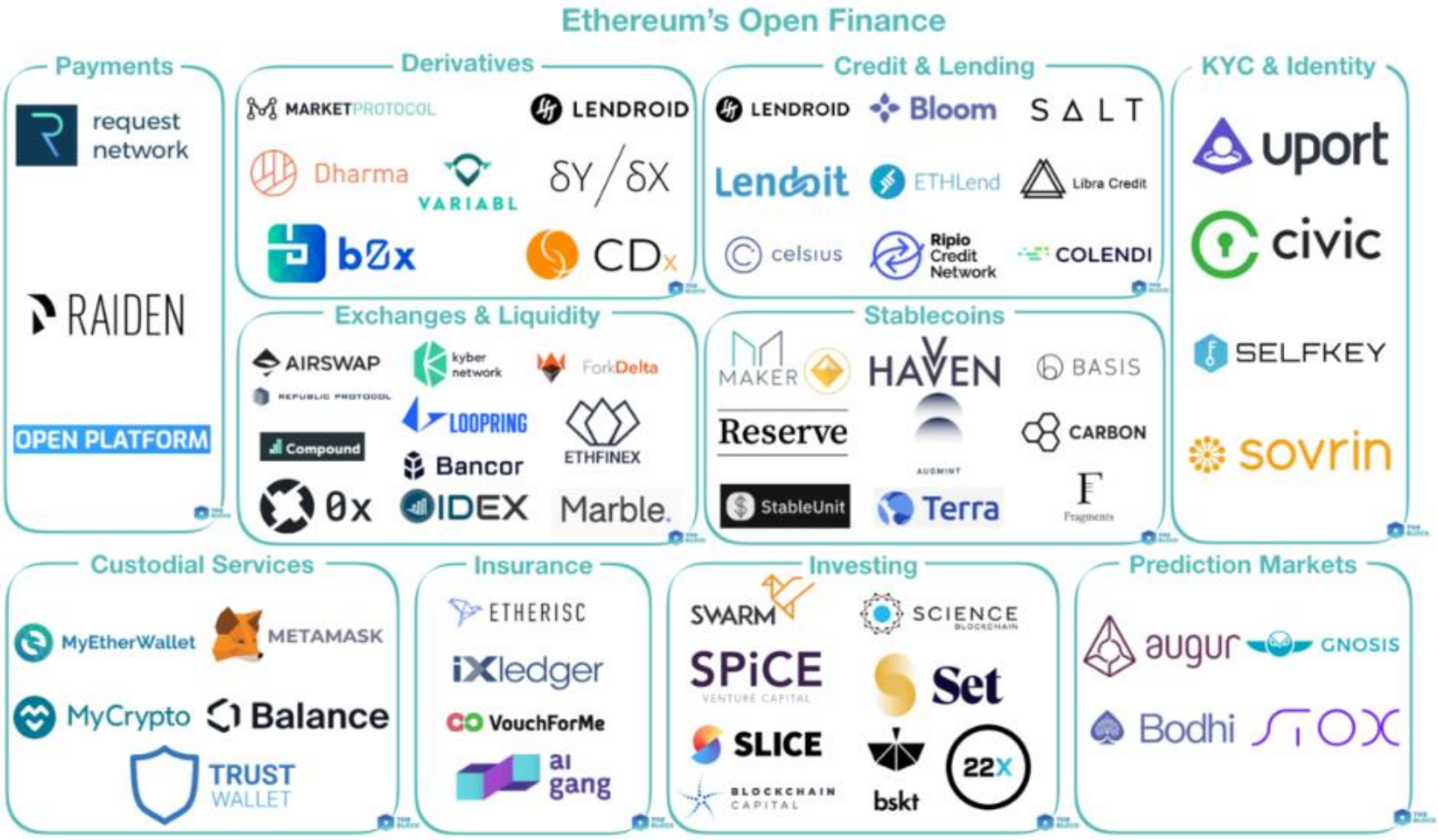
ユーザー視点からみた分散金融マップ

- コアになるベースプロトコルから、ペイメント・ローン・アセット管理・トレード・保険といった領域別プロトコル、そしてユーザーアクセスとなるブラウザ・ウォレットという全体構図。
  - 1) トレードへの偏重
  - 2) シンプルなユーザーアクセスポイントにおける大きな乖離
  - 3) 容易な入口から始まるマスアダプション
  - 4) 金融プロトコルにアクセスするブラウザが将来の金融機関になる可能性
    - 関連して、ウォレットが、銀行・証券仲介・デジタルアイデンティティ・データ金庫・監査人の役目を果たしていくという見方も。



→ 出典：https://twitter.com/hughkarp/status/1030097597141266432?s=21
→ 出典：https://twitter.com/apompliano/status/1030100770752999424?s=21

ETHEREUM上のオープン金融エコシステムマップ

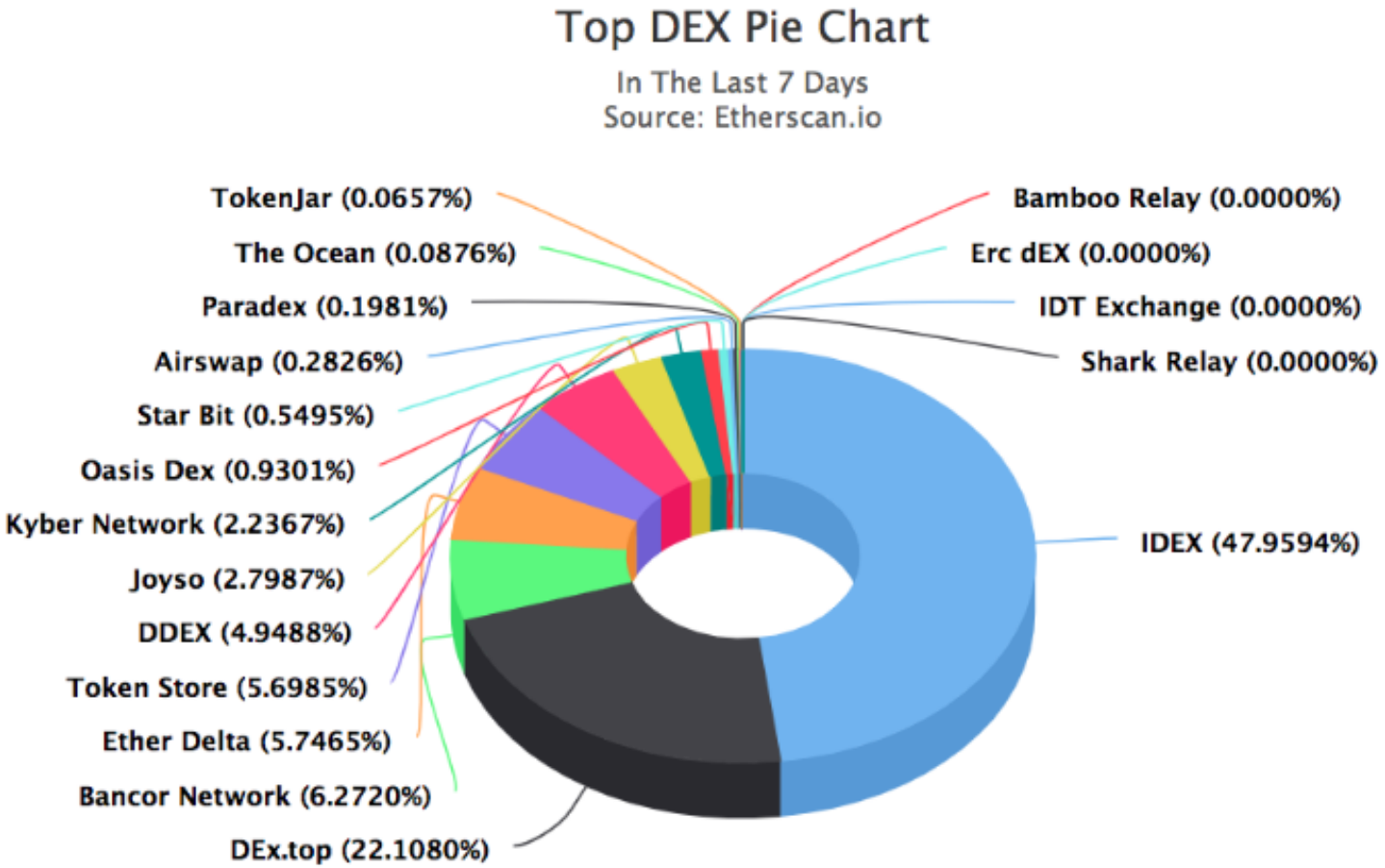


→ 出典: https://www.theblockcrypto.com/2018/10/12/mapping-out-ethereums-open-finance/

動向の俯瞰

分野	動向	URL
流動性	0xプロトコルがv2をメインネットデプロイ	https://blog.0xproject.com/0x-protocol-v2-0-is-live-183aac180149
	Ethereum-EOSクロスチェーンによる流動性ネットワークBancorX	https://medium.com/@taiki.tring/bancor-ethereumとeosをつなぐ初のクロスチェーン分散型流動性ネットワークbancorxを発表-f2dbee201c53
証券	Polymath、ST-20規格の証券トークンによる資金調達5社を発表。90日間にわたるSTO実施へ	https://twitter.com/polymathnetwork/status/1030145160393318400?s=21
デリバティブ	dYdX、ETHショートをメインネットローンチ	https://medium.com/dydxderivatives/dydx-is-live-on-mainnet-margin-trade-now-on-expo-d35d2a8b646
信用取引	信用取引プロトコルbZxがメインネットローンチ	https://medium.com/@b0xNet/bzx-announces-mainnet-launch-releases-zk-labs-security-audit-and-unveils-upcoming-relay-a690cc6c7bf1
貸付	ETHLendの新しいトークン経済モデルとしての「マイクロステーキング」	https://blog.ethlend.io/introducing-a-new-economy-model-decentralized-microstaking-cf8b2e41fa6?gi=f9aef0f830aa
マネーマーケット	マネーマーケットプロトコルCompoundがローンチ	https://medium.com/compound-finance/compound-launches-money-markets-for-ethereum-assets-f50920f04488 https://lab.stir.network/2018/10/13/compound-protocol-basic/

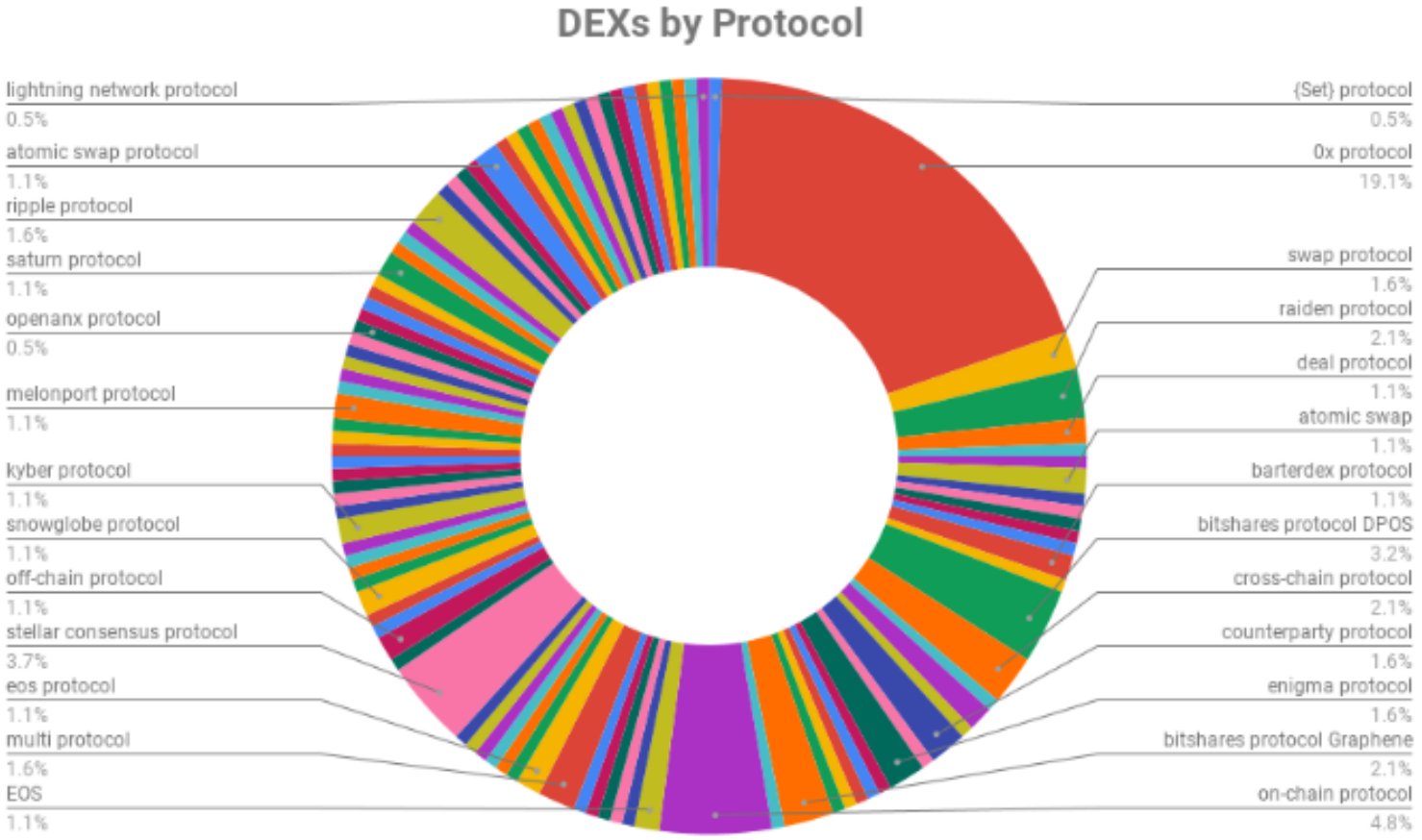
DEXの現状俯瞰



The ultra-competitive race for the DEX market (by % of trade volume among DEXs).

→ 出典：https://hackernoon.com/who-will-run-the-decentralized-exchange-of-the-future-59e9cd29b1ba

DEXの現状俯瞰



DEXs by protocol (Source: https://github.com/distribuyed/index)

→ 出典：https://hackernoon.com/who-will-run-the-decentralized-exchange-of-the-future-59e9cd29b1ba

STABLECOIN（①法定通貨担保型）

主要プレイヤー	• TrueUSD： 　• 発行にあたり、ユーザーは信託パートナーへファンドを送り、マネーを銀行口座へデポジット後に、それら機関がEthereumスマコンをつかってトークンを当該ユーザのEthereumウォレットへ発行する。週次・月次でレコード開示。 　• トークンを償還するには、ユーザはスマコンをつかってバーンする。 • 9月にはいって３つの新規参入。GUSD・USDC・PAX 　• 「法定通貨→暗号通貨スワップ」「暗号通貨→法定通貨償還」を、自身の流動性ポータルを用いて速やかに可能。 　• GeminiUSD（GUSD）：GeminiのインハウスStablecoin。Ethereum上 　　• Gemini＝NYのBitLicense 　• USD Coin（USDC）：Circle/PoloniexのインハウスStablecoin 　　• Circle＝FINCEN規制。50州から送金ライセンス 　• Paxos Standard（PAX）：NYDFS規制 • 欧州では、マルタ拠点のSTATISがSTATIS EUR（EURS）を7月ローンチ。 　• ファイナンスはAAA格付けの欧州機関によって管理。 　• 欧州初のEURペグStablecoinとして魅力。
留意点	• 3つのカテゴリーの中でもっともシンプルで理解しやすく、投資が集まっている。 • 規制保護や透明度あるものは、投資家に受けがよい。 • トークン償還のコントロールにおいてトラストが必要。カウンターパーティリスク、低い透明性。 • 究極には、ファイナンスの仲介人の再生産をしているかたち。PAXやGUSDであれば同じカストディアンが直接資金にアクセスしたりトランザクションを巻き戻す力をもつ。

→ 出典：https://bitcoinmagazine.com/articles/search-stability-overview-budding-stablecoin-ecosystem/

STABLECOIN（②暗号通貨担保型）

主要プレイヤー	• Dai
	  • CDPプラットフォームを通じて1$とペグを維持し、CDPは新規Dai発行にも責任もつ。
	  • Dai発行には、ユーザは、ボラティリティにヘッジするための担保をCDPにロックアップ
	  • CDPは少なくとも生成するDaiの1.5倍の価値で担保必要。
	  • 担保を開放するには、CDPのオーナーはポジションのDebt（当初生成したDaiの金額）とポジションから生じる利子をDaiでペイバック。
	  • Daiの価格が$1を下回ると、ターゲットレートを高め、Dai生成にコストかかるようにして、流通コイン数を減らすように働く。
	  • Dai保有へと動機付け、発行されるDaiも小さくなると、価格が上昇・安定化。
	  • Daiの価格が$1を上回ると、ターゲットレートを低め、Daiが鋳造しやすくする。
	  • 価格が低下し、Dai保有動機が薄れ、価格安定化。
	  • 現時点、EthのみがDaiの担保。
	  • PooledETH（PETH）で額面表記され、担保ETHをMakerのスマコンへ提示すると、ユーザのデポジットがPETHとして償還されCDP内で使用可能に。
	• Havven
	  • EthereumとEOSの双方に対応。
	  • Havven Coin（HVN）による裏付担保債権を通じてnomin(nUSD)を生成。

留意点	• 需要・発行・流通は、HavvenおよびMakerのコミュニティメンバーによって全てドライブされる。 • 運営責任機関が無く、ガバナンス・リスク管理がMakerの場合はMKR保有者の負担に。 • 法定通貨担保型よりも分散度が高い。中央コントロールがなく、法定通貨から分断。 • ボラティリティの大きな暗号通貨というアセットゆえ、安定度におけるメリットを感じにくい。 • 主流派の投資家やユーザが距離を置きがち（Stablecoinむけ投資のうち９％に留まる）。

→ 出典：https://bitcoinmagazine.com/articles/search-stability-overview-budding-stablecoin-ecosystem/

STABLECOIN（③アルゴリズムによる裏づけ型）

主要プレイヤー	• Basis：Robert Samsにより開発されたシニョレッジシェアモデル。
	  • スマコンと債券を用いて安定化を達成
	  • このモデルは複雑だが、伝統的経済理論で予測され、ペグを維持する動機づける。
	  • 市場膨張時（コインが$1を上回る）は、スマコンがコインを鋳造して流通をインフレさせて価格を下げる。
	  • $1を下回ると債券を発行して、Basisコインへ売却して、それゆえ余剰通貨をエコシステムから回収して価格を上げてもどす。
	• Carbon（CUSD）：法定通貨担保とアルゴリズムのハイブリッド
	  • CUSD価格がペグ閾値を下回ったときには、債券のかわりに、リバースダッチオークションを用いて、Carbon Creditというトークンを発行。
	  • Basis同様に、望まない値上がりから価格を下げるために、新規コインを発行せねばならないときに、このクレジットトークンは償還される。
	  • ネットワークをスタートする時点においては、法定通貨バックモデルで立上げ。
	• Kowala（kUSD）：2018年9月にメインネットα版ローンチ。
	  • Ledgerによりインテグレートされた。

留意点	• StablecoinむけVCファンディングの50%を占めるダークホース。（トライや試行の途上にあるモデルであり、最終的に勝つと言う保障は無いもの、期待は集まっている） • メインネットβへ最も近いKowalaすら、α版であり、マーケットでトライアルに至ってない。 • 担保アセットから分離され、アルゴリズムにのみ存立するため、理論上は最も分散度が高い。 • 価格が急落した際に自由落下し回復不能になる「デススパイラル」の可能性。 • BasisやCarbonのbond/debtコントラクトはこのリスクを軽減するためのものだが、そのモデルも、コミュニティがコインの経済モデルに十分確信しているという仮定。

→ 出典：https://bitcoinmagazine.com/articles/search-stability-overview-budding-stablecoin-ecosystem/

STABLECOINローンチがブーム化

- Gemini、ブロックチェーン上のUSDとしてGemini Dollarをローンチ。規制対応Stablecoinとして
  - オープンAPIで監査可能。パブリックチェーン上で許可制スマートコントラクトを動かすハイブリッドとすることで、コインのインセンティブ無しに安全性・監査性を備えるアプローチとのこと。
  - アルゴリズムによるものと違いClearmaticのUtility Settlement Coinのようなインターバンクソリューションに近いとも。

    → 出典：https://medium.com/gemini/gemini-launches-the-gemini-dollar-62787f963fb4
    → 出典：https://www.marketwatch.com/story/winklevoss-twins-gemini-trust-launches-worlds-first-regulated-stablecoin-2018-09-10
    → 出典：https://prestonbyrne.com/2018/09/10/thoughts-on-geminicoin/

- Paxosも米ドルベースStablecoinとしてPaxos Standard検討

  → 出典：https://www.bloomberg.com/news/articles/2018-09-10/controversial-crypto-coin-tether-to-get-regulated-competitors
  → 出典：https://www.dfs.ny.gov/about/press/pr1809101.htm

- リヒテンシュタインユニオン銀行、規制準拠の証券トークンおよびStablecoin発行

  → 出典：https://bitcoinexchangeguide.com/liechtensteins-union-bank-to-launch-regulated-security-token-and-stablecoin/

- 英London Block Exchange、ポンドベースのStablecoin「LBXPeg」発表

  → 出典：https://lbx.com/blog/lbx-peg/

- 杭州市政府支援のブロックチェーンファンド、日本円ペグStablecoinを計画

  → 出典：https://www.coindesk.com/1-billion-blockchain-fund-founders-plan-japanese-yen-stablecoin/

GEMINI DOLLARとPAXOS STANDARD含めたSTABLECOINプレイヤーマップ

→ 出典：https://theblockcrypto.com/2018/09/14/block-by-block-stablecoins/

STABLECOINリスト（既に80種を超える）

Corion Foundation Stablecoin market research 2018 Q3.

Nr.	Project name	Name of stablecoin	Website	Pegged to	Backed by	Project stage	Technical
1	AAA Reserve	AAA reserve currency	https://www.arcgy.org/	usd	Asset	launched	ETH token
2	Alchemint	SD-eur, SD-usd, SD....	https://alchemint.io/#/home	usd	Hybrid	before launch	NEO
3	Augmint	A-Euro	https://www.augmint.cc/	euro	Crypto	before launch	ETH token
4	Aurora	Boreal	https://auroradao.com/platform/boreal/	usd	Hybrid	before launch	ETH token ?
5	Basis	Basis (Basecoin)	https://basis.io/	usd	Comm/algorith	before launch	ETH Token
6	Bitcar	CAR	https://bitcar.io/	usd	Asset	before launch	N/A
7	Bitshares	BitUSD	https://bitshares.org/technology/price-stable-	usd	Crypto	launched	own blockchain
8	Carbon	CarbonUSD (CUSD)	https://www.carbon.money/	usd	Comm/algorith	before launch	Hedera Hashgraph
9	Celo	Celo	https://celo.org/technology	usd	Crypto	before launch	N/A (Proprietary?)
10	Centre	Centre	https://www.centre.io/	usd	FIAT	before launch	N/A
11	Circle	Circle USDC	https://www.circle.com/en/usdc-faq	usd	FIAT	before launch	ETH token
12	Corion Coin	Corion (COR)	https://corion.zendesk.com/hc/en-us	usd	Comm/algorith	launched	ETC token
13	CryptoDT	TWDT-ETH token	https://www.cryptodt.io/	TaiwanUSD	FIAT	launched	ETH token / own
14	CryptoPeg	bUSD	http://www.cryptopeg.org/	usd	Crypto	before launch	Bitcoin
15	Digix Global	DigiX (DGX)	https://digix.global/	gold	Asset	launched	ETH token
16	Egold	Egold (EGD)	https://egold.trade/	asset	Hybrid	before launch	ETH token / own
17	Fiatpeg	FiatPeg (PEGUSD)	http://fiatpeg.com/en/	usd	Asset	launched	NEO blockchain
18	Fragments	USD Fragment	https://www.fragments.org/	usd	Comm/algorith	before launch	ETH token
19	Gemini Dollar	GeminiDollar	https://gemini.com/dollar/	usd	FIAT	launched	ETH Token
20	Globcoin	Globcoin (GLX)	https://globcoin.io/	fiat avarge 15	FIAT	before launch	ETH token
21	Goldmint	GoldMint	https://www.goldmint.io/	gold	Asset	launched	ETH / own with PoS
22	Havven	Nomin (nUSD)	https://havven.io/	usd	Crypto	launched	ETH token
23	Kowala	kUSD	https://www.kowala.tech/	usd	Comm/algorith	before launch	own blockchain, Tendermint prot
24	Librebank	LibreCash	https://librebank.com/	usd	Crypto	before launch	ETH token
25	Maker DAI	DAI	https://makerdao.com/	usd	Crypto	launched	ETH token
26	MoneyToken	MTC (MoneyTokenCoin)	https://moneytoken.com/	usd	Hybrid	before launch	ETH Token
27	NuBits	NuBits	https://nubits.com/	usd	FIAT	launched	own blockchain
28	OneGram	OneGram coin/token (OGC)	https://onegram.org/	asset	Asset	before launch	own blockchain
29	Paxos	PAX	https://www.paxos.com/standard/	usd	FIAT	launched	ETH Token
30	Saga	SGN	https://www.saga.org/	IMF's SDR	Asset	before launch	ETH token
31	Stableunit	Stableunit	https://stableunit.org/	usd	Hybrid	before launch	own blockchain ?
32	Stably	Stably (StableUSD token)	https://www.stably.io/	usd	FIAT	before launch	ETH & Stellar
33	Stasis	EURS token	https://stasis.net/	euro	FIAT	launched	ETH token
34	SteemDollar	Steem Dollar (SD, SBD)	http://www.steemdollar.com/	usd	Crypto	launched	own blockchain
35	Stronghold, IBM	Stronghold USD	https://stronghold.co/stronghold-usd/	usd	FIAT	before launch	Stellar
36	Sweetbridge	BRC	https://sweetbridge.com/platform/	asset	Asset	before launch	ETH token
37	Terra money	Terra	https://terra.money/	IMF's SDR	Crypto	before launch	?
38	Tether	Tether (USDT)	https://tether.to	usd	FIAT	launched	OMNI Protocol
39	The White Company	WS dollar (WSD)	https://thewhitecompanyus.com/	usd	FIAT	launched	Stellar network
40	TrueUSD	trueUSD (TUSD)	https://www.trusttoken.com/trueusd/	usd	FIAT	launched	ETH token
41	Ubpay	UUSD	https://ubpay.io/stable-coin/	usd	Crypto	before launch	own blockchain
42	Unum	Unum	https://unum.one/#/learn	usd	Comm/algorith	launched	ETH Token
43	Vault	UsdVault (UsdV)	http://vault.ch/	usd	Asset	before launch	ETH Token
44	X8	X8Currency (X8C)	https://x8currency.com/	fiat basket of 8	FIAT	before launch	ETH token

→ 出典：https://twitter.com/corionplatform/status/1049649629283921920?s=21

STABLECOINリスト（既に80種を超える）

CONCEPT / UNDER REVIEW							
45	Alfa-enzo	under review	https://www.alfaenzo.io/home	-	-	under review	-
46	Anchor USD	UsdX	https://www.anchorusd.com/	usd	FIAT	concept	Stellar
47	CorionPay	CorPay	https://www.corion.io	usd	Hybrid	concept	ETH Token
48	CP processor	under review	https://coinpaymentprocessor.org/	-	-	under review	-
49	Cryptopeg	under review	http://www.cryptopeg.org/	-	-	under review	-
50	Feron	under review	http://www.feron.io/	-	-	under review	-
51	Freedium	under review	https://freedium.io/	-	-	under review	-
52	goldscape	under review	http://www.goldscape.net/gold-blog/gold-bac	-	-	under review	-
53	Jibrel Network	under review	https://jibrel.network/	-	-	under review	-
54	MoneyOnChain	Dollar on Chain (DoC)	https://www.moneyonchain.com	usd	Crypto	concept	RSK Bitcoin sidechain
55	Ndau	under review	https://ndau.io/	-	-	under review	-
56	Onramp	under review	https://onramp.tech/	AUD	-	under review	ETH token
57	orcs	under review	https://orcs.fund/static/docs/whitepaper.pdf	-	-	under review	-
58	Peblik	under review	https://peblik.com/	-	-	under review	-
59	PHI on Difinity	PHI	https://dfinity.org/pdf-viewer/pdfs/viewer?file	-	Comm/algorith	concept	Dfinity
60	Pier	under review	https://github.com/pierprotocol/pier-smartco	-	-	under review	-
61	QUANTMRE	under review	http://launch.quantmre.com/	-	-	under review	-
62	Reserve	Reserve	https://www.reserve.org	-	N/A	concept	N/A
63	Rockzplatform	under review	alprockz.io	-	-	under review	-
64	Ryō	Ryō	https://ryo-coin.io/	-	N/A	concept	N/A
65	Sendgold	under review	https://www.sendgold.com/	-	-	under review	-
66	Soy-coin	under review	https://cryptocoinpravda.com/soycoin-the-fu	-	-	under review	-
67	Spankbank	under review	https://github.com/spankchain/spankbank	-	-	under review	-
68	Staticoin	StatiCoin	http://staticoin.com/	-	Crypto	concept	ETH Token
69	SwissRealCoin	under review	https://www.swissrealcoin.io/	-	-	under review	-
70	The Relay System	Relay Dollar (XRD)	https://www.relaystablecoin.com/	usd	Crypto	concept	N/A
71	Topl protocol	Topl	https://topl.co/	usd	-	concept	N/A
72	universalusd	under review	https://www.universalusd.com	-	-	under review	-
73	Xank	Xank	https://xank.io/	IMF's SDR	Crypto	concept	ETH Token
74	Xaurum	under review	https://www.xaurum.org/en/home	-	-	under review	-
75	XDR - Mile unity	under review	https://mile.global	-	-	under review	-
76	XOV	under review	https://www.xov.io/	-	-	under review	-
77	zabercoin	under review	https://zabercoin.io	-	-	under review	-
78	Monerium	under review	-	-	-	under review	-
79	Kinesis Money	under review	-	-	asset	under review	-
80	Cryptopound (LBKPeg)	under review	https://lbx.com/blog/lbx-peg/	-	-	under review	-
81	Mongolian 'Candy'	under review		-	-	under review	-
82	Tiberius coin	under review	https://www.tiberiuscoin.com/	-	-	under review	-

Corion Foundation / Stablecoin　　www.corion.io

→ 出典：https://twitter.com/corionplatform/status/1049649629283921920?s=21

証券トークン

- 証券トークンの特徴
- テクノロジースタックイメージ
- 関連エコシステムのイメージ
- コンセンサスモデルのイメージ
- ERC1400 - Security Token Standard

証券トークンの特徴

- 証券トークンは、リアルワールドアセットのオーナシップ。
  - 例えば商業不動産やプライベート企業や投資ファンドや債権、美術など。

- ブロックチェーンがトランザクションを決済するために効率的な方法であるばかりでなく、本質的にマーケット構造を変更でき、さらにはインターネット自身のアーキテクチャをも取り込むことが可能になる。
  - 発行者にとって：安価な資本コスト＆コンプラ
  - 投資家にとって：アクセスしやすさ、流動性
  - 規制当局にとって：可視性や執行可能性

- ステークホルダーのニーズをみたす上で、新技術スタックおよびエコシステムが必要。
  - オンチェーンスマートコントラクトおよびオンチェーンのネットワークが、一体として包括的ソリューションを、証券の発行・トレードおよび監査に対して提供する。

→ 出典：https://medium.com/harborhq/securitytokenstack-e6a273c1104e

テクノロジースタックイメージ

- Exchange層の下に、コンプラプラットフォーム層があり、発行人デューデリや発行人要件などをオフチェーンで確認した上で、結果をオンチェーンホワイトリストに渡す。
  - その下で、オンチェーンの証券トークン層が、ホワイトリストチェック実行や、発行人や当局の求める形式で遵法トランザクションをブロックチェーン層へ渡すことによって、全トランザクションが所定ガイドラインを充たすことを担保する、という流れ。

交換機能層	• Ocean、Sharespost、Airswapなど。
交換プロトコル層	• 0xなど。
コンプライアンスプラットフォーム層（Harborなど）	• トレードのコントロール、保険、ポリシー＆プロシージャ適用、監査など。 • 投資家の参加要件確認や、発行人デューデリといったオフチェーンプロセスを含む。 • オフチェーンプロセス結果をオンチェーンホワイトリストへ渡すことによってオフチェーンとオンチェーンの橋渡しを行う。
証券トークン層（Harborの場合、「R-Token」が該当）	• 下記機能を提供するオンチェーン技術層。 • コンプラプラットフォームと組み合わせることによって、発行人や当局に求められる遵法トランザクションを執行する。 • コンプラプラットフォームより提供されたホワイトリストを使ってチェックを行うことによって全TXが必要なガイドラインを充たすことを確保する。
ブロックチェーン層（Ethereum等）	• トラストレスなトランザクション、高速なセツルメント時間、セキュリティを提供する。 • 発行者や規制当局に対しては、可視性を提供する。 • 投資家に対しては、接続容易性や流動性を提供する。

→ 出典：https://medium.com/harborhq/securitytokenstack-e6a273c1104e

関連エコシステムのイメージ （1/2）

流動性向上	• クリプト分野の証券において、重要なチャレンジ。
ガバナンス	• シンプルなコンプラや有効検証から、洗練された配当配分ダイナミクスに至るまで、投票およびガバナンスモデルが組み込まれることが必要。
プライバシー	• 現在のトランザクションは基本的にプライバシーが無いも同様なレベル。 • 今後、業種間で一体となった証券トークンを可能とするうえでは、プライバシーポリシーモデルを可能にすることが重要。
ディスクロージャー	• アセットについて何も知らなければ、価格を正しく予期できない。 • 証券に関するデータセットへアクセスを可能にすることは、流動性やコンプラを実現する上でも不可欠。
サイドチェーン	• Ethereumの制約に左右されず、Ethereumの能力を拡張する新たな環境を用意する上で、サイドチェーンは一つの選択肢。
Debt	• 証券のユースケース・利便性を高める上で重要。
デリバティブ	• 現在、ロングトレードにフォーカスした新しいアセットクラスを開発することがほとんど不可能。 • トークン証券を洗練する上で、ショートやヘッジむけメカニズムの実装が重要に。

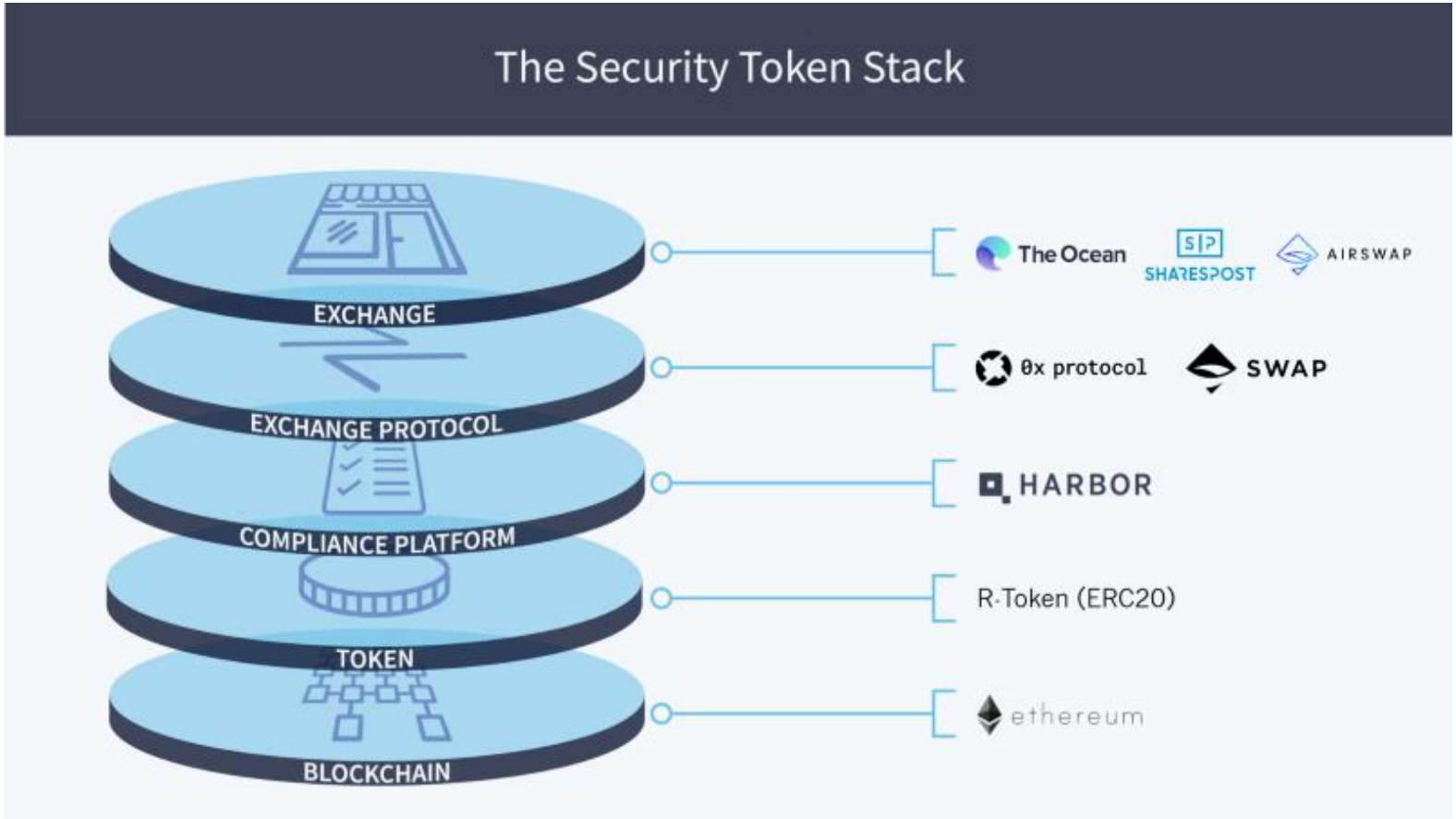
→ 出典：https://hackernoon.com/some-cool-protocols-to-consider-for-the-next-generation-of-security-token-platforms-98697f0c55e6

関連エコシステムのイメージ （2/2）

流動性	Bancor	• スマコン内に他トークンのバランスを保持する「スマートトークン」に基づいて、流動性を提供するプロトコル。 • 証券トークンを作成するにあたり、スマートトークンとの互換性を通じて、流動性を向上させる。
ガバナンス	PoA	• アイデンティティベースのコンセンサスモデルの１つであり、証券トークンにおけるガバナンスモデルを可能とする材料。 • POA Networkは、異なる証券トークンPFにも適用可能なEthereum互換のサイドチェーンを用いてPoAを実装。
プライバシー	Bulletproofs	• 秘匿トランザクション向けに高いパフォーマンスのプロトコルを提供する。
	ZK-SNARKs	• Ethereumにおいて、様々な場面で実装されている。
ディスクロージャー	IPFS	• コンテンツやデータストレージむけのプロトコル。
サイドチェーン	Loom	• DChainAppsの実装を可能にするプロジェクト。 • Ethereumメインネットと相互互換を維持しながら、DApps自身のサイドチェーンにおいて実行できる。
Debt	Dharma	• 分散型Debtむけに頑健なプロトコル。
デリバティブ	dYdX	• トークン化されたデリバティブ。 • 信用取引や先物・オプションなどの金融機能を提供するプロトコルの集合体。
バスケット	Set Protocol	• トークンバスケット生成むけプロトコル。

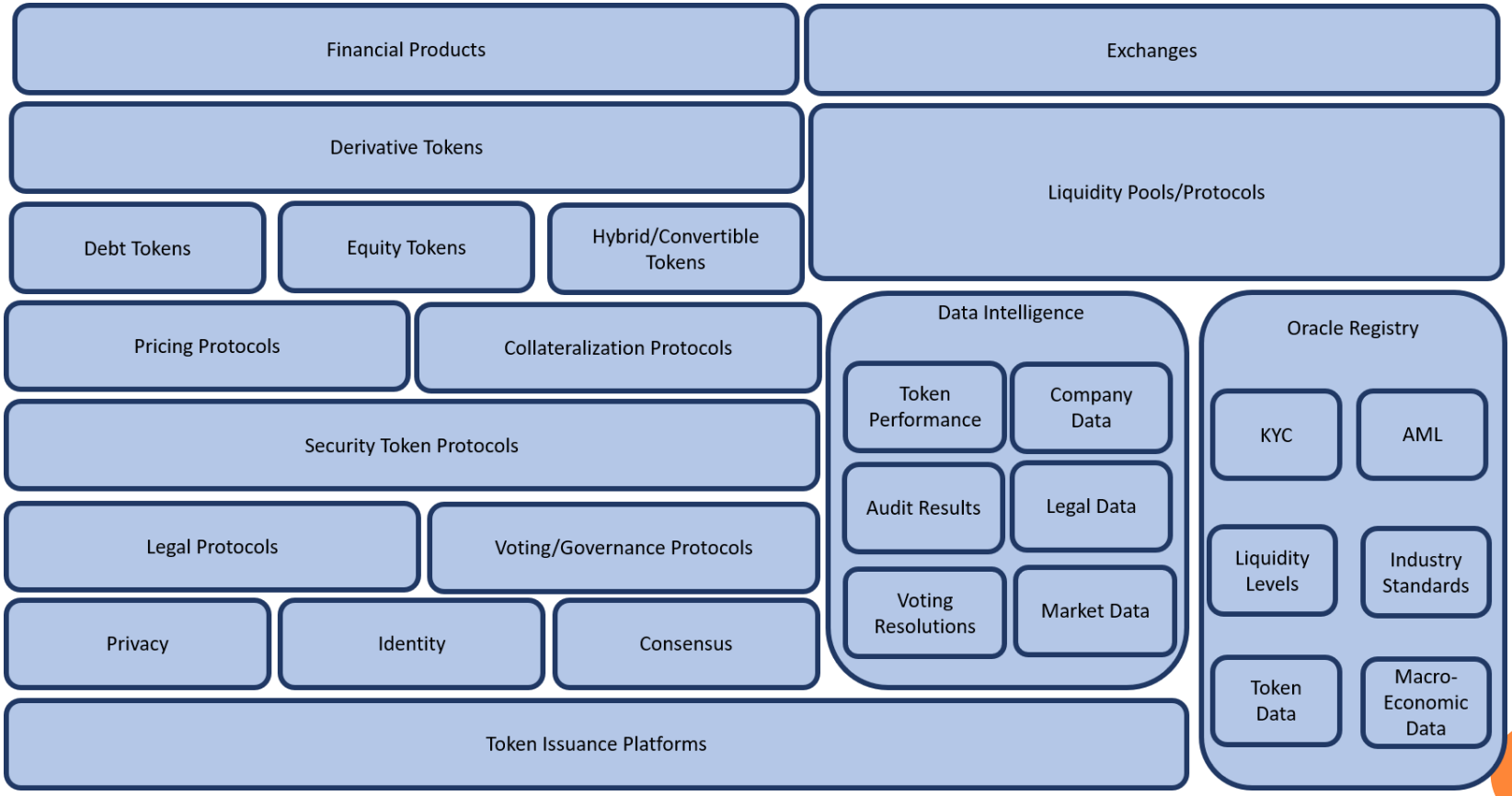
→ 出典：https://hackernoon.com/some-cool-protocols-to-consider-for-the-next-generation-of-security-token-platforms-98697f0c55e6

証券トークンの技術スタックイメージ



→ 出典：https://medium.com/harborhq/securitytokenstack-e6a273c1104e

証券トークンの技術スタックイメージ



→ 出典：https://twitter.com/jrdothoughts/status/1029357758020284416?s=21

コンセンサスモデルのイメージ （1/2）

- 証券トークントランザクションは、「トークン化されたトランザクション」であり且つ「証券法規制に準拠する必要がある」と整理できるため、証券トークン検証プロセスは２段階に分けられる。
  - ①トランザクションのコンプラ要件検証（KYC/AML、アセット所有権、資本要件など）
    - たとえば「特定の国の国民のみが所有できる」「トークン保有者は1Mドルの流動性を持つ必要がある」「投資家は金融ディスクロージャにアクセスする必要がある」など。
  - ②ブロックチェーンへのコミットに先立ち、トランザクションの金銭的正当性を検証（二重消費）

- 現在のプラットフォームは、 KYC/AMLコンプラ検証を事前定義したホワイトリストにてらして集中サービスで行っているが、こうした集中型モデルは以下の問題を抱える。
  - ①大量の無効トランザクションを検証人に送りつけるなどのスパム攻撃
  - ②トランザクションライフサイクルへ過剰な影響を検証人が持つようになる問題
  - ③検証人が悪事を回避するためのインセンティブ欠如

- 次世代の証券トークンではアイデンティティ管理プロセスの整流化・分散がテーマに。
  - KYC/AMLメカニズムをスマートコントラクト通じて自動化する。
  - 各国毎のKYC/AMLルールをコード化することでクロスボーダー取引をより効率的にしていく期待。

→ 出典：https://www.securitytokenacademy.com/info/three-waves-of-a-new-financial-internet-1745/
→ 出典：https://hackernoon.com/some-ideas-about-a-consensus-protocol-for-security-tokens-part-i-bda1f0fac54f

コンセンサスモデルのイメージ　(2/2)

- 整流化・分散化されたコンセンサスベースのトランザクション検証プロセスとしては、たとえば、次のような「２フェーズコンセンサスモデル」が考えられる。
  - ①トランザクションのコンプラに係るコンセンサス
  - ②トランザクションの金銭的有効性に関するコンセンサス
- このとき、ネットワーク内のノードを下記２種類に区分する。
  - ①コンプラ検証人＝KYC/AMLや資本要件などコンプラに特化して検証する。
    - ネットワーク内で既知のアイデンティティである必要があり、ある程度の匿名性を保つ。
  - ②バリデータ＝従来型の二重消費などをチェック
- 下記のような２フェーズコンセンサスモデルが考えられるが、攻撃の可能性に対処する上では、ゲーム理論的な観点からも対策を講じることが有効。

フェーズ１	• たとえば「特定の国の国民のみが所有できる」「トークン保有者は1Mドルの流動性を持つ必要がある」「投資家は金融ディスクロージャにアクセスする必要がある」といった要件を想定。 • コンプラバリデータのランダムグループを選択し、トランザクションの有効性について投票によるコンセンサスを得る。 • コンプラバリデータ間のコンセンサスモデルを実装する上では、アイデンティティや評判がメインのステーキングメカニズムとして、PoAによるインセンティブが考えられる。
フェーズ２	• 取引の金銭的有効性別につき、既存のコンセンサスプロトコルに基づき、コンセンサス。

→ 出典：https://www.securitytokenacademy.com/info/three-waves-of-a-new-financial-internet-1745/
→ 出典：https://hackernoon.com/some-ideas-about-a-consensus-protocol-for-security-tokens-part-i-bda1f0fac54f

ERC1400 – Security Token Standard

- 下記７点をスタンダードの要件として提案している。
  - 所有権の移転が成功裏に完了したかを問い合わせ、失敗理由を提供する標準インターフェイスを持つこと。
  - 法的アクションや資金のリカバリプロセスを通じて移転の強制執行を可能とすること。
  - 発行や償還のためのリリース標準イベントを保持すること。
  - 特定ステークホルダーの権利や、移転制限に関するデータなど、ユーザー残高のサブセットに対してメタデータの添付を認めること。
  - 移転時にはオンチェーン・オフチェーンデータに従うほか、移転パラメータに基づく形で、メタデータ変更を可能とすること。
  - データをトランザクションへ渡す前に、ユーザーにオンチェーンにて検証すべくデータへの署名を求めることが望ましい。
  - ERC20およびERC777互換とすること。

→ 出典：https://github.com/ethereum/EIPs/issues/1400
→ 出典：https://cryptovest.com/news/security-tokens-might-have-new-standard-on-ethereum--erc-1400/

クリプトエコノミクス

- インセンティブ設計の重要性
- アセットバックトークンに関する財産権からの示唆
- ハードフォークにおける協調ゲーム
- 協調ゲームの均衡に関する設計要素
- ブロックチェーン格納情報に係る見えない検証コスト

インセンティブ設計の重要性

- 行動に影響もたらすシステム設計に着目したとき、インセンティブデザインとして「契約理論」・「マーケットデザイン」・「情報の経済学」という3領域を活用して、ブロックチェーンプラットフォームを設計することが有用。
- プロトコル、アプリケーション、エコシステムそれぞれの設計において、テクノロジー・リーガル・そしてエコノミクスの三つの視点から設計することが必要。
  - ブロックチェーンデザインとガバナンス・エコノミクスの接点としては、「社会選択」「契約理論」「メカニズムデザイン」の３領域がある。

社会選択	契約理論
• ユーザーとコインホルダーとではインセンティブも異なるため、コインホルダーがユーザーにとっての最善な選択をするとは限らない。 • ブロックチェーンのガバナンスを設計する上では、参加者の持つ情報やインセンティブを踏まえることが必要。 • ステークホルダー間の異なるインセンティブをどう扱うか。	• 契約は本来的に不完全なものであるという前提に立つこと。 • 契約は第三者によってイベントやアクションが検証される場合にのみ執行できる。 • もし関連する情報がすべて検証可能であっても、契約があらゆるコンティンジェンシーを含む契約を記述することはできない。 • 対処①＝契約が本来的に完全なものではないため、ガバナンスシステムが必要になる。 • 対処②＝より多くの条項をコントラクトに記述できるよう、情報品質改善にフォーカス。

→ 出典：https://medium.com/prysmeconomics/blockchain-incentives-101-what-they-are-and-why-they-matter-5127afb56aeb
→ 出典：https://medium.com/prysmeconomics/incomplete-contracts-and-blockchain-ac9f348a2e6f
→ 出典：https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca
→ 出典：https://cesc.io/

アセットバックトークンに関する財産権からの示唆

- 財産権のトークン化では、コントロール権の保有者および権利行使方法が重要。
  - 「誰がビルのコントロール権を持っていて、どのようにコントロール権を行使するのか」の特定。
  - 請求権とコントロール権の分離はインセンティブ齟齬きたすため、両者は揃えるべき。
- 契約の不完全性に備えるためアルゴリズムで自動化するだけでは不十分。
  - 契約の予期しない事態に意思決定するのがコントロール権持つオーナー。
  - オーナーによる合同でのガバナンスが機能しない場合にアセットの価値をも毀損することになる。

オーナーシップ	• 財産権の経済学において、オーナーシップは特別な権利。オーナーシップはアセットに対するコントロール権であり、オーナーはあらゆる意思決定を行うことができる。 • トークン発行時にアセットコントロール権の割当が、ホルダーまたは発行者へ行われる。 • コントロール権をホルダーに付与できない場合は、他の形でインセンティブをそろえるメカニズムが必要。
ガバナンス	• どのようにコントロール権が行使されるか。 • どのグループ例えば一連のジョイントアセットオーナーが統合された意思決定を行うか。
アセット価値へのインパクト	• いくらで賃貸にだすのかといった意思決定コントロール権を「誰が持つ」かというのは、アセットによって生み出される収益に対して、直接的に重要なインパクトをもたらす。
契約の不完備性	• アルゴリズムに組み込んだとしても、予期されない意思決定が行われる必要がある。 • 契約が完全でないからこそ、少なくともコントロール権を持つオーナーを特定要。

→ 出典：https://medium.com/prysmeconomics/asset-backed-security-tokens-what-you-can-learn-from-the-economics-of-property-rights-391dd20becd4

ハードフォークにおける協調ゲーム

- 国のガバナンスとブロックチェーンガバナンスの相違点
  - 通常の行政選挙の場合、負けた方は、グループを去って自ら立ち上げることは容易ではない。
  - これに対して、ハードフォークはほぼコスト無くかつ結果的に自律的に可能。
  - そのため、ハードフォークがコミュニティにとってのオプションである場合に、ブロックチェーンのガバナンスシステムが重要。

- ブロックチェーンにおけるネットワーク効果の役目
  - ネットワーク効果は、ユーザ・消費者にとっての価値が、ユーザベース増加とともに、増加すること。
  - ブロックチェーンを維持したり、プラットフォーム上でやりとりしたり、セカンダリマーケットでトークン売買しようとするユーザが増えるほど、プラットフォームのUXも改善する。

- 社会的行動であるハードフォークがもたらす協調ゲーム
  - ネットワーク効果は、ハードフォークが個人的かつ社会的行動であるかを決める上で重要。
  - ユーザがハードフォークに参加したいかどうかの問いは、「自身が新規チェーン上の政策をどれくらい好むか」ということだけでなく、「どれだけ多くの他ユーザが新規フォークに参加するか」にする。
  - 適切なデザインの無い場合、ハードフォークや不均衡な結果のような望まない結果をもたらす可能性があるため、ブロックチェーン開発者にとっても協調ゲームの理解が重要。

→ 出典：https://prysmgroup.io/blockchain-upgrade-as-a-coordination-game/

協調ゲームの均衡に関する設計要素（1/2）

- 協調ゲームは、複数のナッシュ均衡を伴う戦略的ゲーム。
  - ナッシュ均衡は、参加者の誰もがアクション選択の変更を望まない、戦略ゲームの結果。
  - 均衡になるためのプラットフォームにとって望ましい結果にとって、重要。
  - 複数の均衡がある場合、全てのゲームプレイヤーが同じナッシュ均衡上で協調することが、実現されるべき均衡便益のためには必要。

- プレイヤーが、他の参加者の選択を知ることなく、同時にアクション選択せねばならない場合、プレイヤーにとって協調することが大変難しい。
  - ブロックチェーンエコシステムのマイナーやユーザは、中央オーソリティによるコントロールされず、他の参加者の行動を考慮にいれながら、自身のアウトカムの最大化にむけて行動。
  - 分散プロトコルのコントロールは美人投票のようなもので、他のステークホルダーが賭けるであろう選択肢への投票が解となる。

- ブロックチェーンアップグレードにおいて、ガバナンスシステムは、皆が受け入れる均衡についてコミュニティの協調を促す上で重要な設計要素となる。
  - 例えば、マジョリティルールガバナンスシステムは、コミュニティが他ユーザが結果に従うと信じる場合、このガバナンスシステムはFocal Point（全プレイヤーが理解することを示すパブリックシグナル）として機能するため、オンチェーンでコミュニティ協調を促すことになる。
    - → 出典：https://medium.com/prysmeconomics/nash-equilibrium-and-blockchain-d6a6f47a7a37
    - → 出典：https://medium.com/prysmeconomics/blockchain-and-coordination-games-failures-and-focal-points-e166cc244973

協調ゲームの均衡に関する設計要素（2/2）

- 設計上の選択は容易に意図しない結果をもたらすため、プラットフォームの設計において、戦略ゲームの均衡についても考慮に含める必要がある。

局面	検討項目
設計	• 均衡について決定する前に、「どんなとりうるアクションがそれぞれの参加者にあって、それぞれの選択からのペイオフがどれだけか」を明らかにする。 • 「参加者がプレイする戦略ゲームの均衡がどこで起こることを望むか」をプラットフォームの設計に落しこむ。
検証	• とりうる参加者のアクションやペイオフを明らかにしたのち、「望まれる行動がゲームの均衡点かどうか」をチェックする。 • 複数の均衡がありえる中において、「望む均衡が選択されるかどうか」をチェックする。 • 「望まないゲームの均衡点は無いかどうか」をチェックする。

→ 出典：https://medium.com/prysmeconomics/nash-equilibrium-and-blockchain-d6a6f47a7a37
→ 出典：https://medium.com/prysmeconomics/blockchain-and-coordination-games-failures-and-focal-points-e166cc244973

ブロックチェーン格納情報に係る見えない検証コスト

- 全員が同意するには重要な情報に皆がアクセス可能な必要があるが、情報によっては簡単に公開できない場合があり。
  - 公園の天気は誰もが検証可能だが、建物の構造の健全性は専門知識が必要。
- ブロックチェーンの活用を広げる上では、検証コストを検討することが必要。
  - これらが満たされない場合、ブロックチェーンの情報は既存仲介人を介した検証よりも高くつく可能性があるということ。

見えない検証コスト	検討内容
トランザクションにおいてどんな情報を検証必要か	• 誰が情報提供するか • そこにバイアスや利益相反は起きないか
検証において必要となる情報へアクセス可能とするためにどんな仕組みが必要となるか	• 共有ルール守らない場合のペナルティなど

→ 出典：https://medium.com/mit-cryptoeconomics-lab/hidden-costs-of-verification-4925cac38a47

ブロックチェーンガバナンス

- ブロックチェーンガバナンスにおける示唆
- オフチェーンガバナンスとオンチェーンガバナンス
- 証券トークンプラットフォームの場合のオンチェーンガバナンスイメージ

ブロックチェーンガバナンスにおける示唆（1/2）

- クリプトネットワークのガバナンスは、ガバナンスの無いフェーズから、必要性認知・投票など既存の転用のフェーズを経て、個々のアプリケーションに応じたカスタムメイドのガバナンスを目指すフェーズへ。

- クリプトネットワーク評価の見方を、技術第一（スケーリング優先）、マネー第一（セキュリティやトラスト優先）、ガバナンス第一（ガバナンスやコミュニティで差別化）に大別できる中、何に力点をおいて設計するかの見極めが重要。

- ガバナンスフレームとして、オンチェーンガバナンス（アルゴリズム内で意思決定）、公式・オフチェーンガバナンス等があるが、あらゆるガバナンスメカニズムは汚職や利潤追求行動のインセンティブをもたらす可能性がある。（例：Block Producerによる票の買収やカルテル形成）

- ガバナンスは投票だけでなくコミュニケーションや教育や提案プロセスを含むものであるため、アプリケーションに見合った仕立てのガバナンスが必要。

→ 出典：https://medium.com/crypto-oracle/the-10-most-insightful-comments-on-our-crypto-governance-consensus-conf-call-9eeda0a89abc

ブロックチェーンガバナンスにおける示唆（2/2）

- オンチェーンガバナンス・オフチェーンガバナンスともにトレードオフがある。
  - オフチェーンガバナンスは、集中化が残るものの、技術的情報ある開発者が意義ある開発をもたらすことにつながるというトレードオフ。
  - 一方、投票通じて直接民主制を実装するオンチェーンガバナンスは、開発者やマイナー達からユーザーへとパワーシフトをもたらす（チェーンのリライトなどを可能とする）反面、プラットフォームにとってベストな選択をできるだけの技術知識もたないというネックがあると。

- ガバナンスにおいて民主制だけが解とは限らない。
  - 技術的に未解決課題を多く抱えた実験的なソフトウエアであり、バランスとれる有能なテクノロジスト達の周辺にテクノロジーガバナンスを構築すべき、との見方も。
  - IETFやLinux Foundationは民主制ではないほか、国と違いexitして他へ移ることも容易でもある点も、ブロックチェーンに民主制が向かない理由。
  - 直接民主制は衆愚政治につながるほか、投票委譲を認めると賄賂・プロバガンダなど余計なエネルギーが必要になる。

→ 出典：https://blockonomi.com/blockchain-governance/
→ 出典：https://hackernoon.com/blockchains-should-not-be-democracies-14379e0e23ad

オフチェーンガバナンスとオンチェーンガバナンス

- 特定アセットホルダーの投票というインプットを通じて、特定トランザクションに関するアセットホルダの希望を表現する。
- 特定アセット保有者の投票にインパクトをもたらすことがインセンティブとなる。
- 協調アクションに係る投票において、全参加者の決定を組み合わせる誘因に。

オフチェーンガバナンス	オンチェーンガバナンス

• ブロックチェーン外の規制・コンプラをベースとしたメカニズム。
• オフチェーンガバナンスの結果をオンチェーンアクションに組み込む。
• スケールしにくいデメリット有。
	• 投票やガバナンス決定をプログラム可能なブロックチェーンインタフェースとする。
	• 証券トークンにかかる規制コンプラメカニズムは相対的にスマコン用いてモデル化しやすい。
	• 例えば、バリデータノードのグループによる投票を用いて、オンチェーンガバナンスは、資本要件などの検証を自動化できる。
	• オンチェーンガバナンスモデルにおけるゲーム理論的な攻撃リスク
	  • バリデータグループが一緒に投票プロセスを操作する共謀攻撃
	  • 投票バリデータを削除することで投票結果を予測可能なものにする攻撃
	  • インサイダーな価格操作攻撃

→ 出典：https://hackernoon.com/security-tokens-2-0-about-on-chain-governance-part-ii-ca9378cea172
→ 出典：https://medium.com/@jrodthoughts/security-token-2-0-some-thoughts-off-chain-vs-on-chain-governance-2cba087389ab

証券トークンプラットフォームの場合のオンチェーンガバナンスイメージ

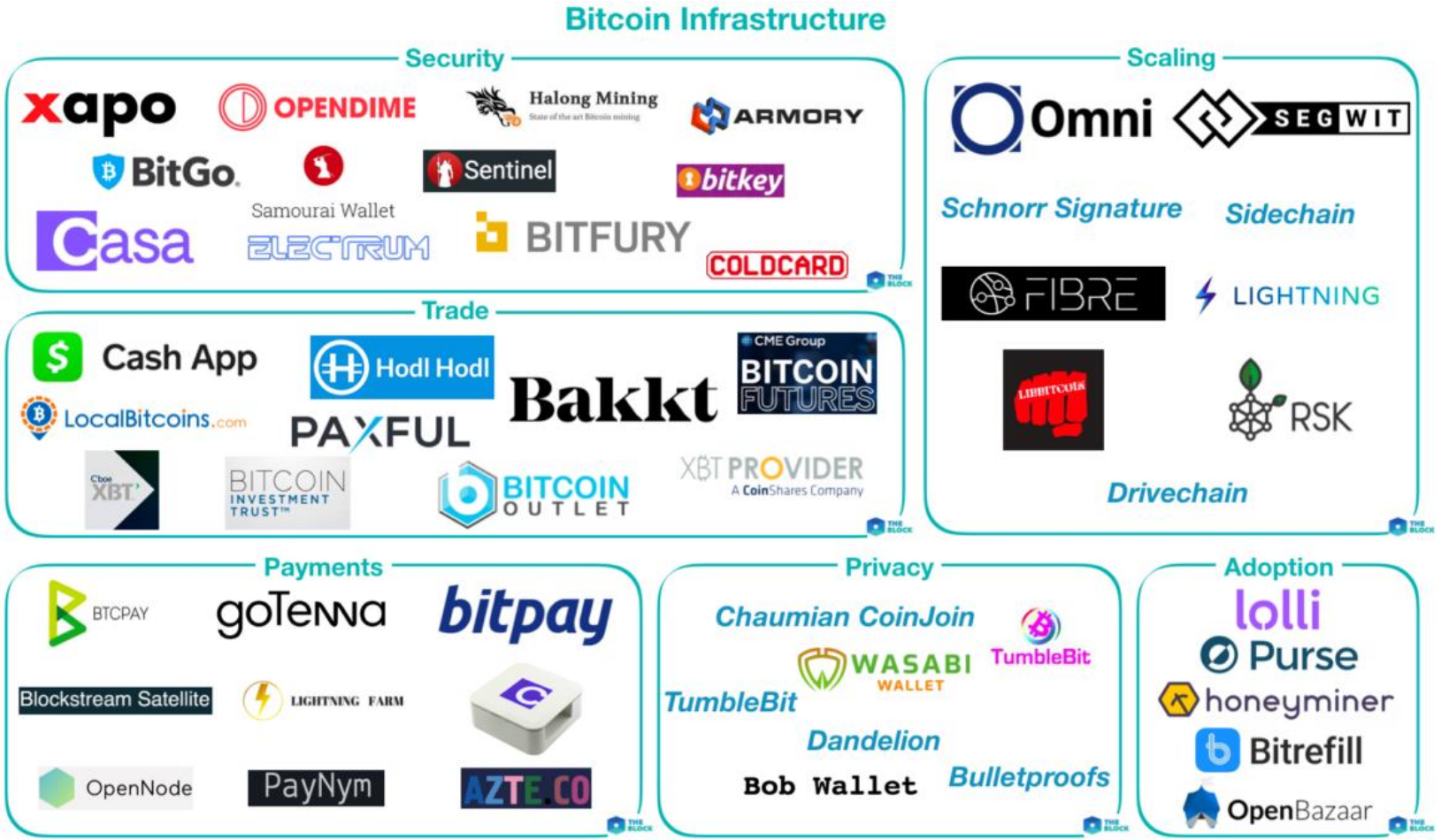
ブロックチェーンベースガバナンス	• バリデータの追加・削除 • フォークの決定 • プロトコル修正やロードマップ投票
プロトコルベースガバナンス	• 証券トークン移転における特定の情報に係るプライバシー • プロトコル修正への投票 • 売り手と買い手の双方にかかるコンプラルール • クロスチェーンの証券トークン移転
トークンベースガバナンス	• アイデンティティ検証 • トークン配布やライフサイクル管理 • フィナンシャルポリシー
Exchangeベースガバナンス	• デジタルアセットの追加・削除 • 監査や公示 • カストディルール • 取引の停止やモニタリング

→ 出典：https://hackernoon.com/security-tokens-2-0-about-on-chain-governance-part-ii-ca9378cea172

プレイヤーエコシステムマップ

- ビットコインインフラのエコシステムマップ
- カストディ関連のエコシステムマップ
- マイニング分野のエコシステムマップ
- PoSアルゴリズム主要プレイヤーリスト
- EOSのエコシステムマップ
- イスラエルのブロックチェーン
  スタートアップマップ（2018Q3版）
- スイスクリプトバレーのプレイヤーマップ
- 中華系プレイヤーマップ
- ゲームセクターのエコシステムマップ
- 不動産関連プレイヤーのエコシステムマップ
- Gartnerのハイプサイクル

ビットコインインフラのエコシステムマップ

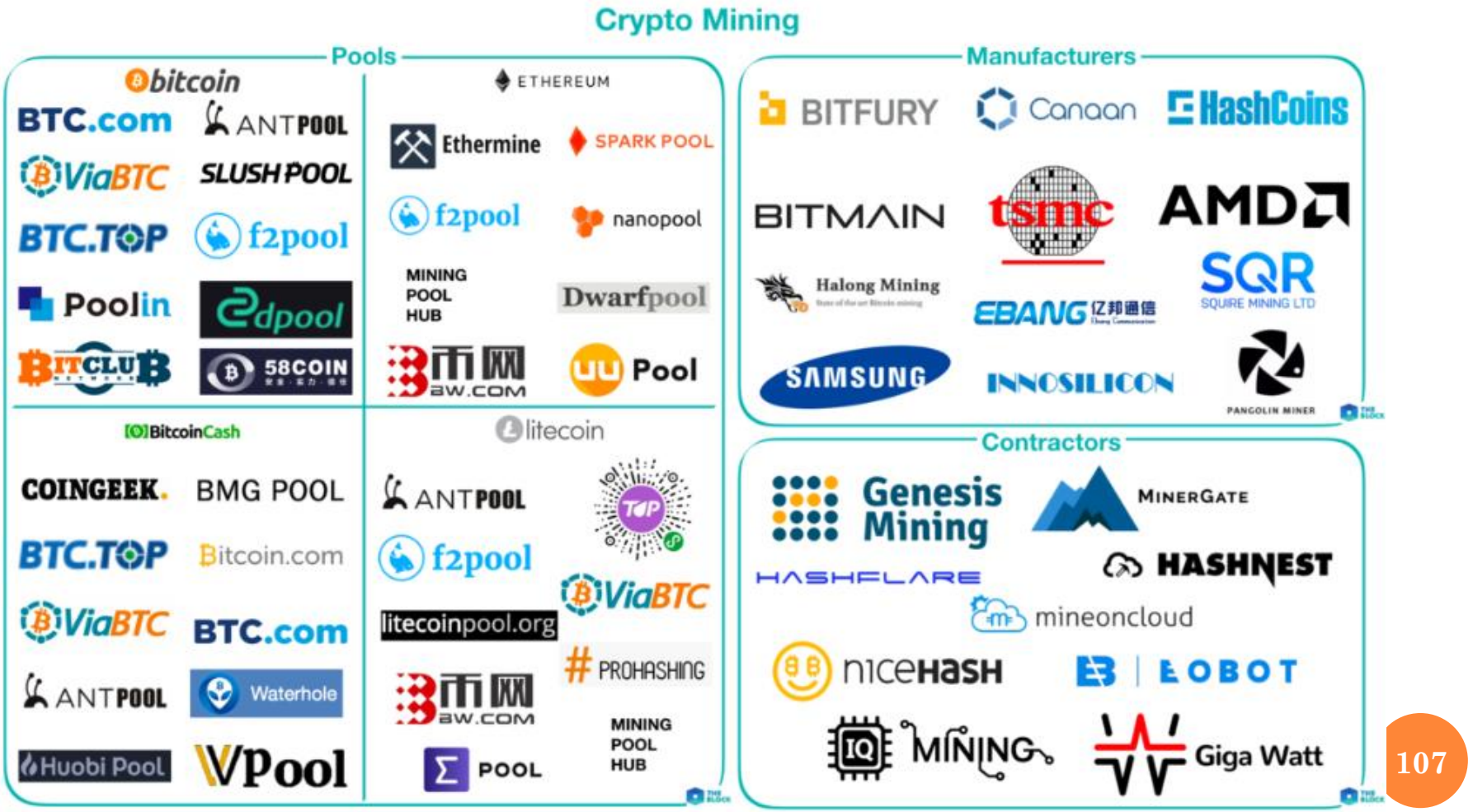


→ 出典：https://twitter.com/eos_io/status/1054306704702222336?s=21

カストディ関連のエコシステムマップ

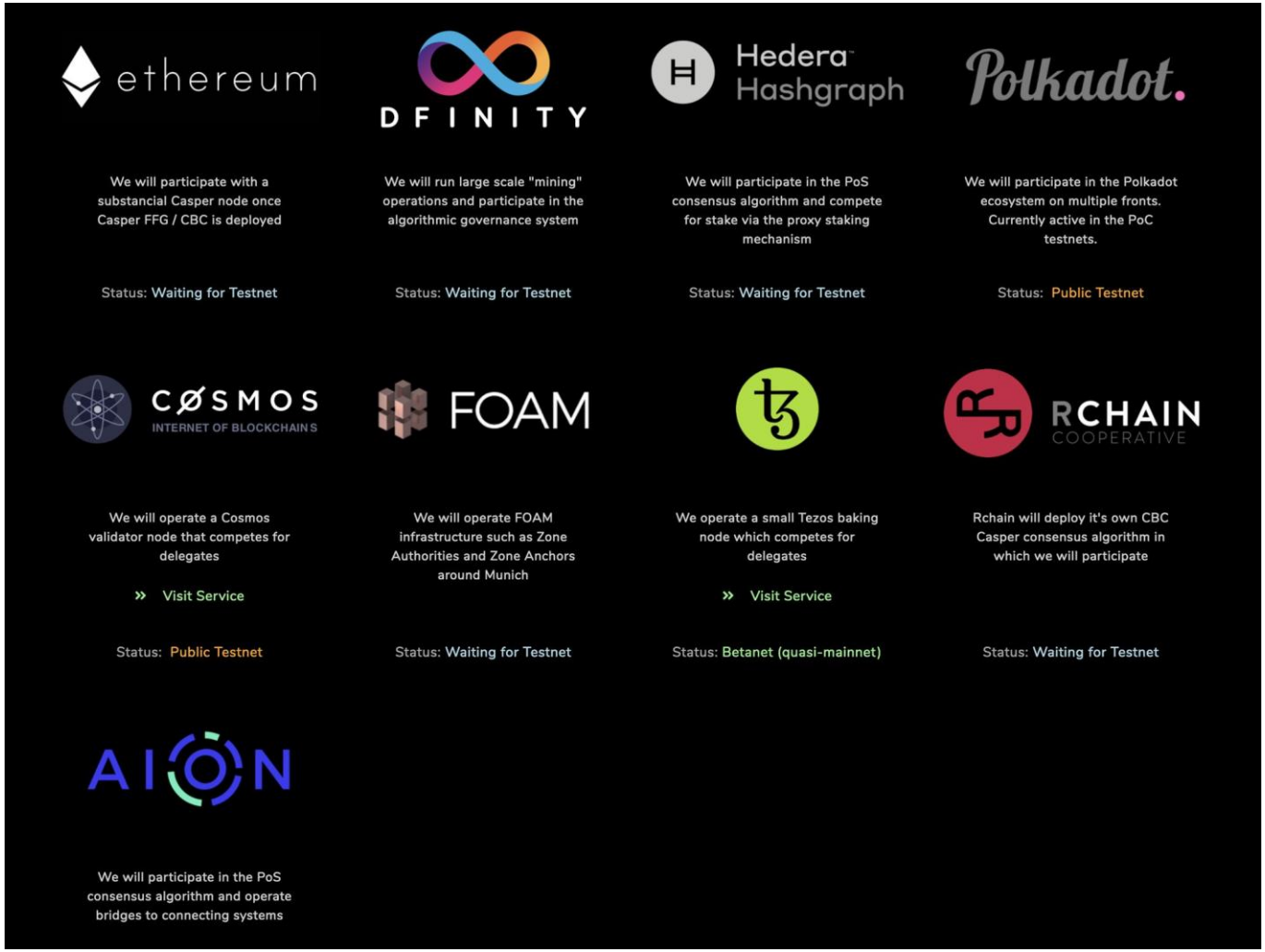
→ 出典：https://twitter.com/eos_io/status/1054306704702222336?s=21

マイニング分野のエコシステムマップ



→ 出典：https://twitter.com/eos_io/status/1054306704702222336?s=21

PoSアルゴリズム主要プレイヤーリスト

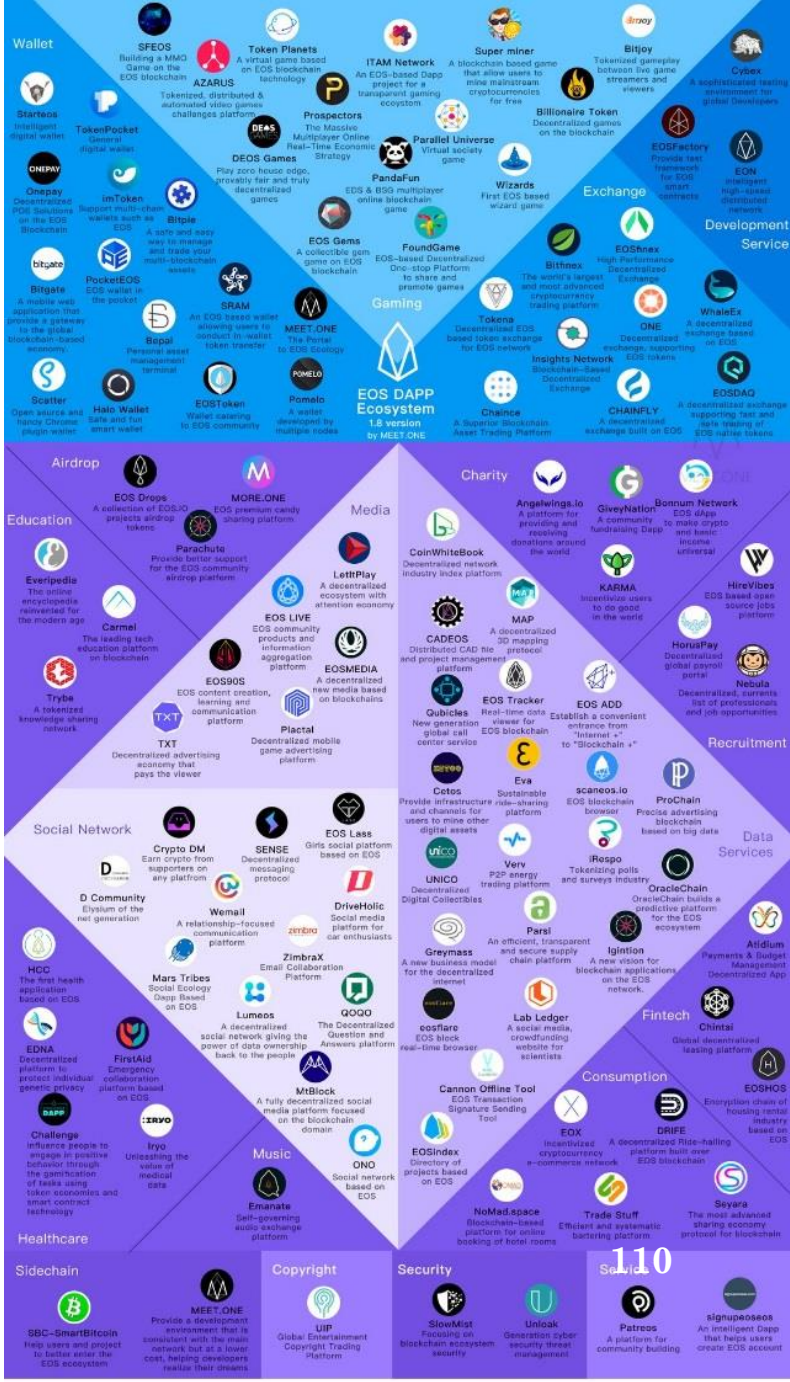


→ 出典：https://twitter.com/stakingfac/status/1031526405652275201?s=21

EOSのエコシステムマップ

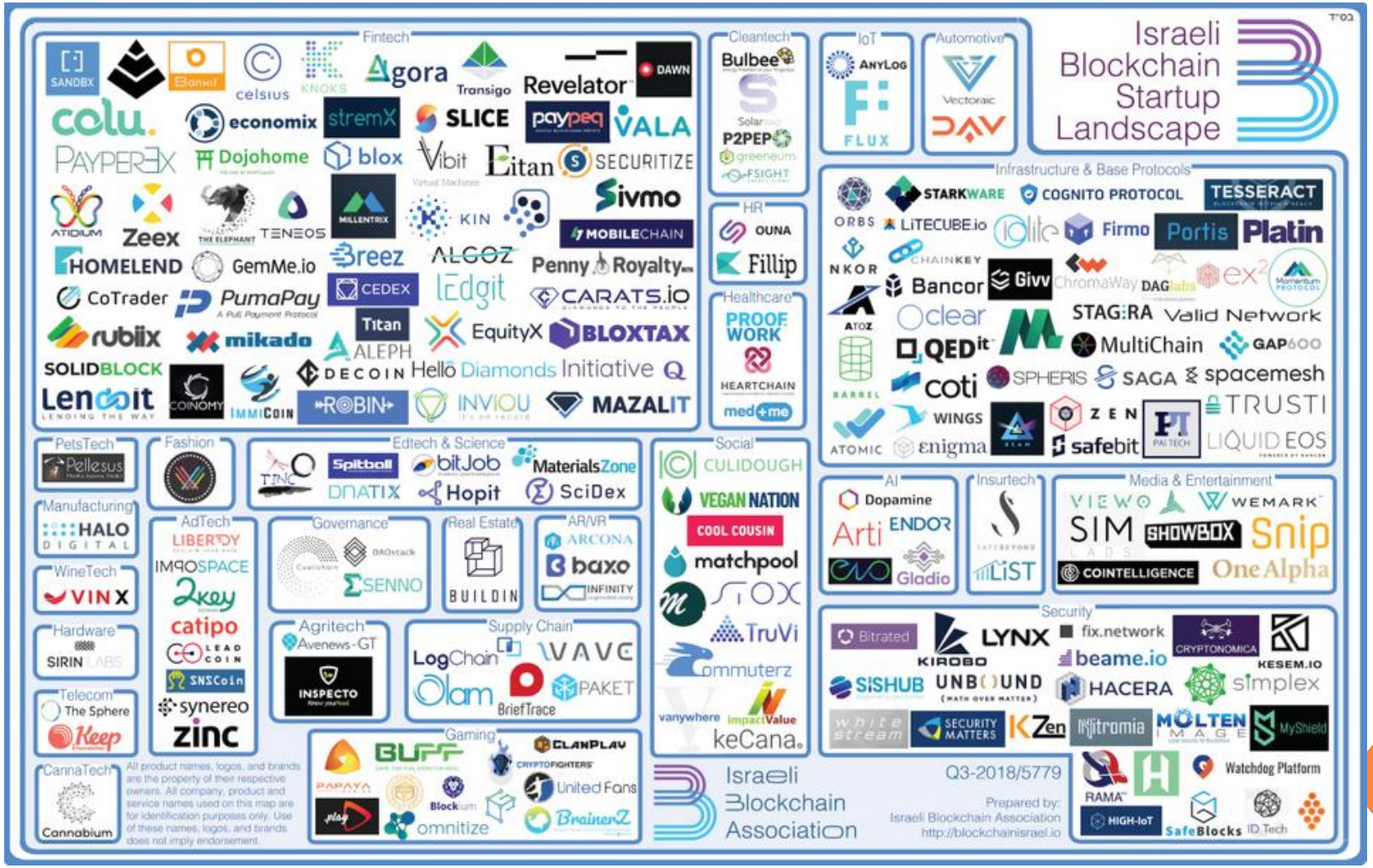
→ 出典：https://twitter.com/eos_io/status/1054306704702222336?s=21

EOSのエコシステムマップ



→ 出典：https://twitter.com/meetdotone/status/1028850642507378688?s=21

イスラエルのブロックチェーン スタートアップマップ（2018Q3版）

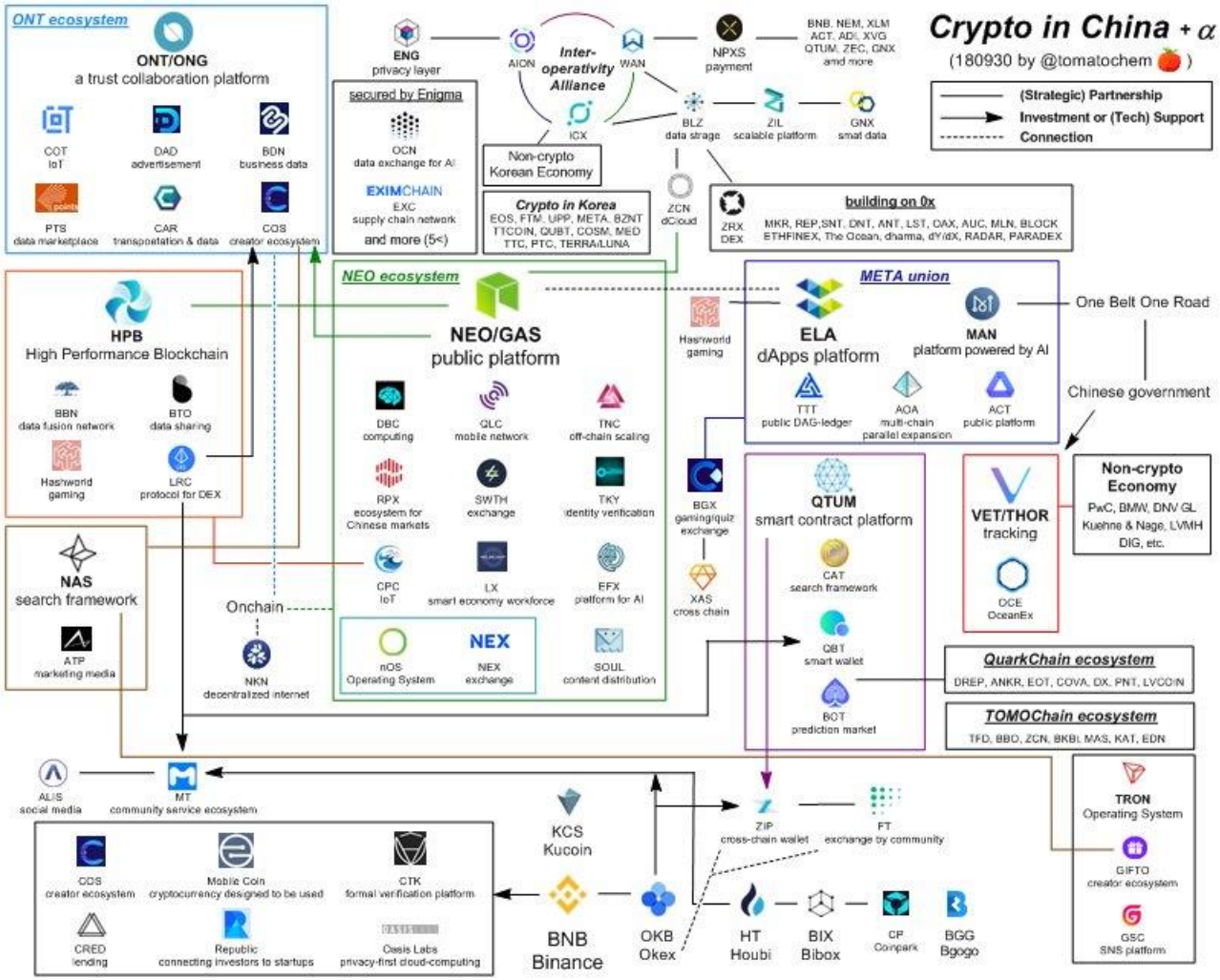


→ 出典：https://www.forbes.com/sites/rachelwolfson/2018/10/23/blockchain-startups-in-israel-have-tripled-why-israel-can-become-a-leading-blockchain-nation/

スイスクリプトバレーのプレイヤーマップ

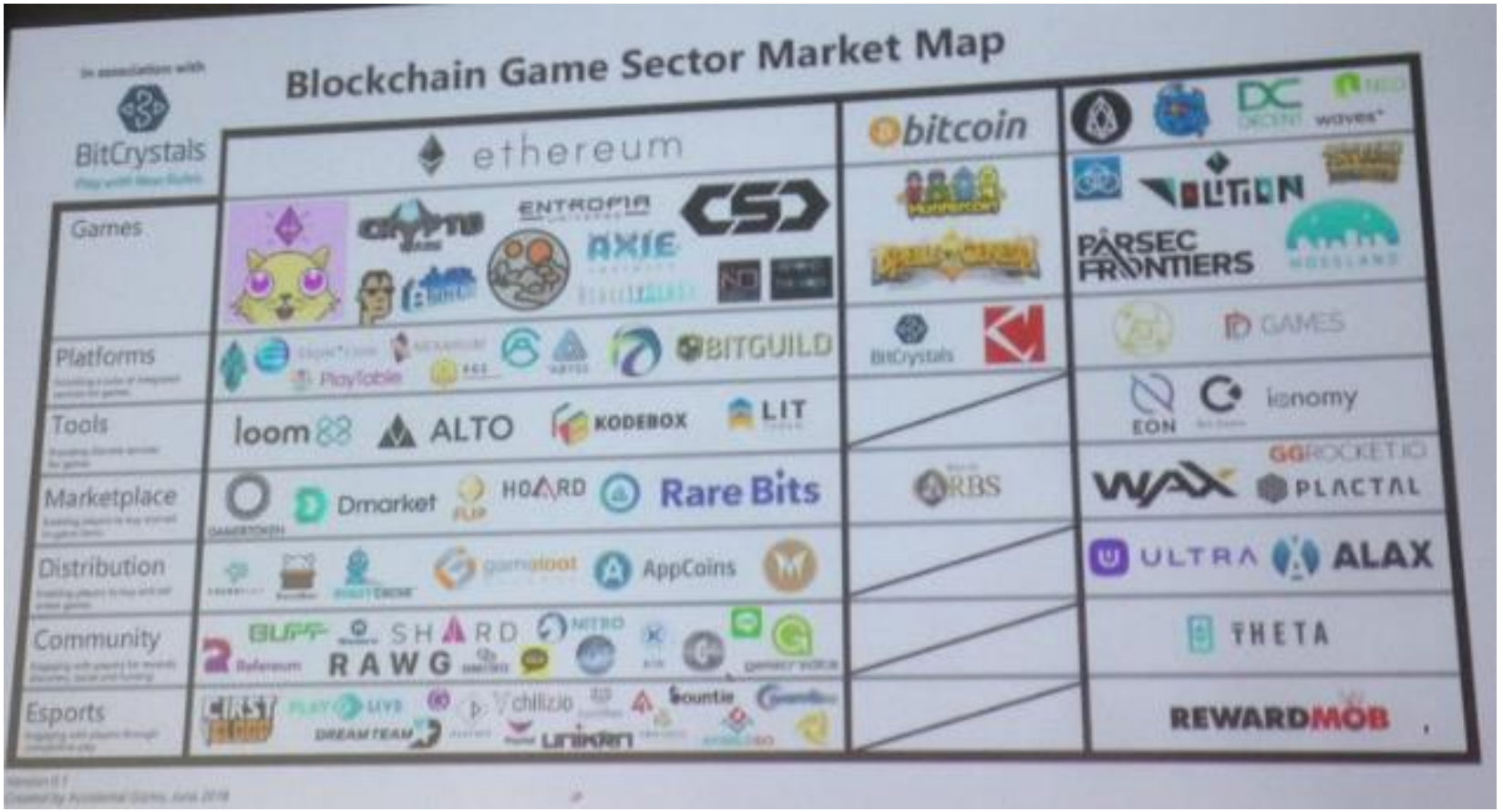
→ 出典：https://cvvc.com/index.php/about-us/mediacorner/report-top-50-companies-blockchain-crypto

中華系プレイヤーマップ



→ 出典：https://twitter.com/tomatochem/status/1046290734662344704?s=21

ゲームセクターのエコシステムマップ

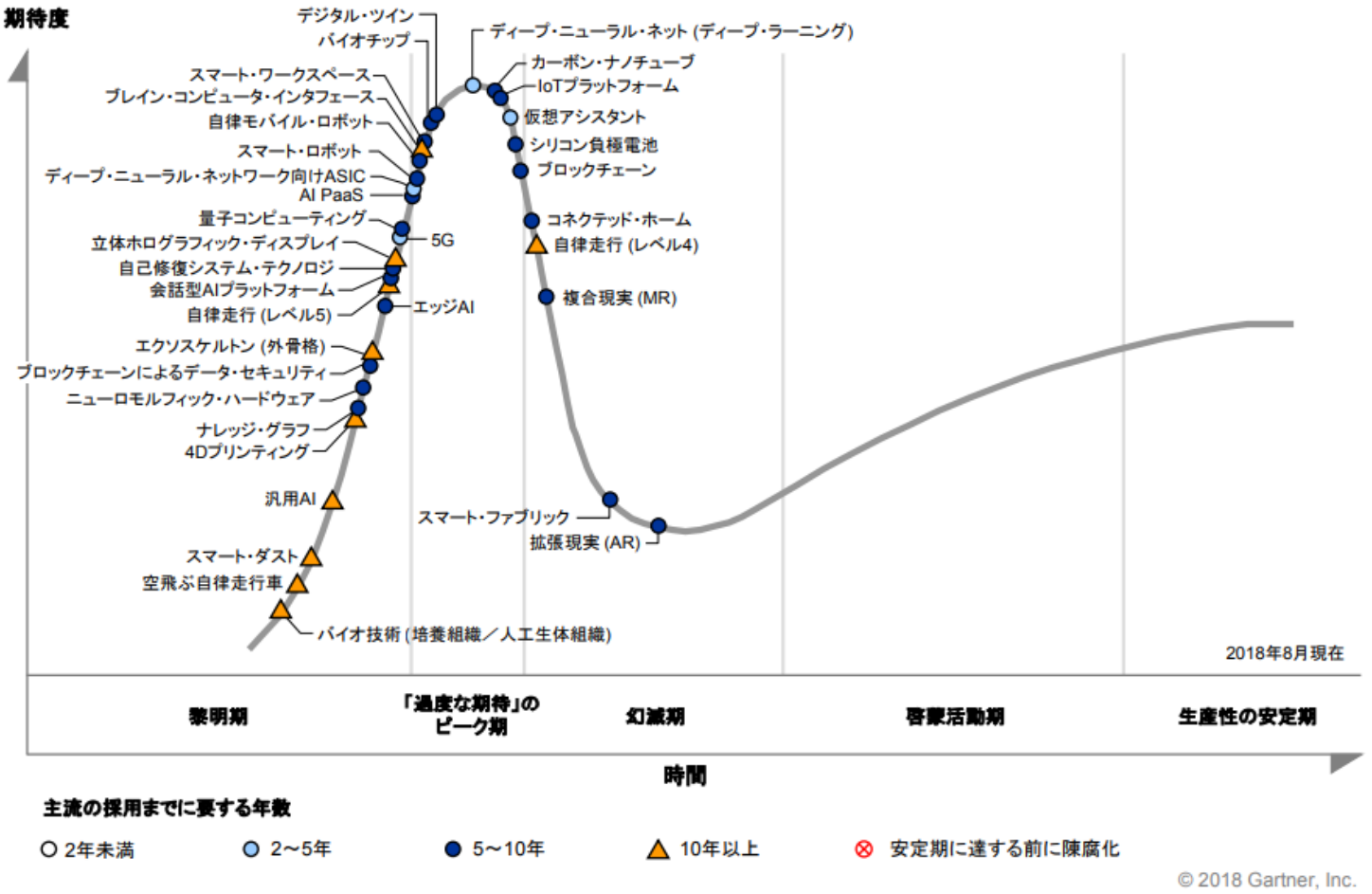


→ 出典：https://twitter.com/btc_wires/status/1044574652272726016/photo/1

不動産関連プレイヤーのエコシステムマップ

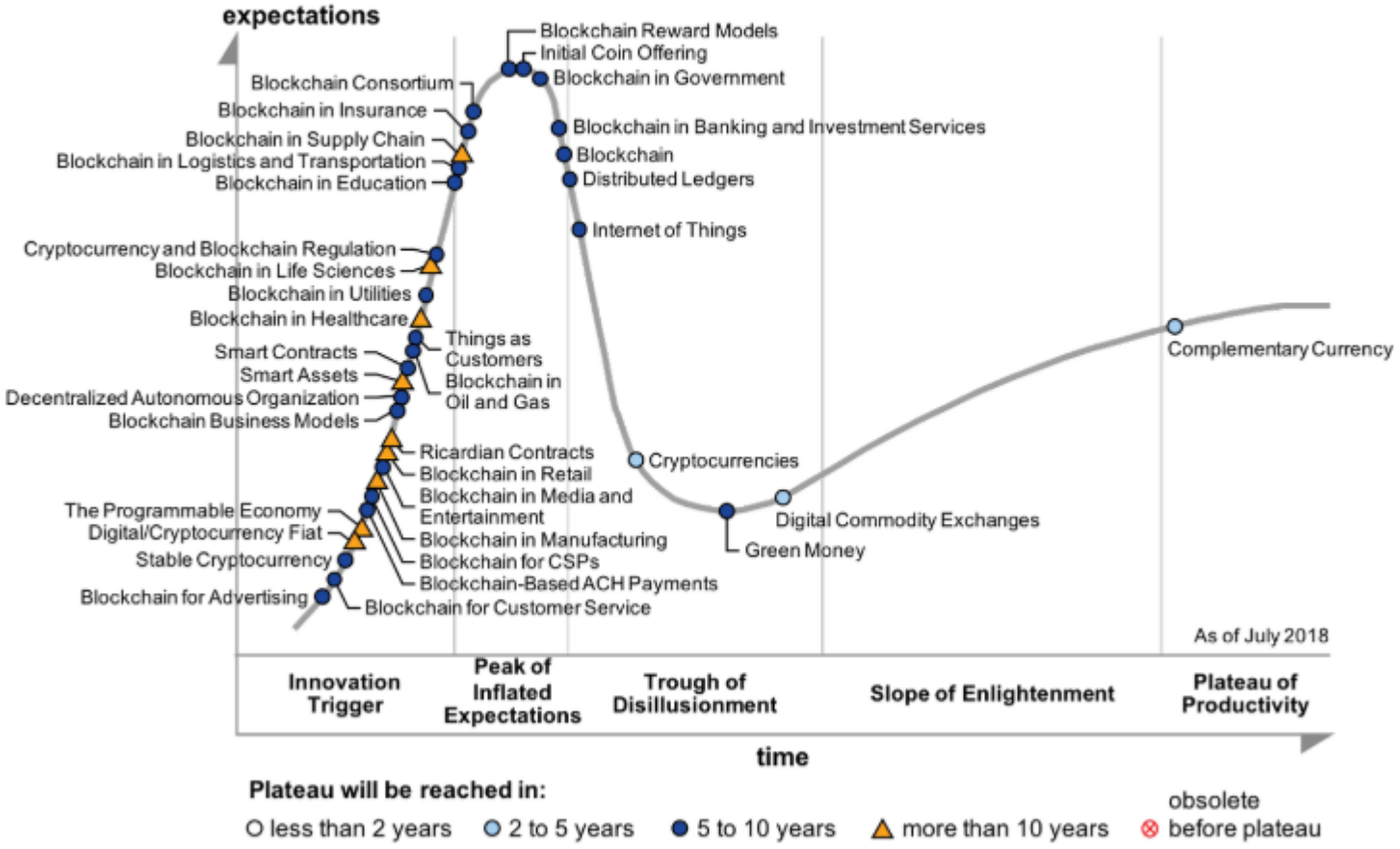
→ 出典：https://twitter.com/ryugunsun/status/1042207052460810240?s=21

GARTNERのハイプサイクル



→ 出典：https://www.gartner.co.jp/press/pdf/pr20180822-01.pdf

GARTNERのハイプサイクル



→ 出典：https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/

4. Startup/Dapps系

4-1. プラットフォーム分野
4-2. ライフスタイル分野
4-3. シビックテック分野
4-4. 金融分野

4-1) プラットフォーム分野①

名称	サービス概略	URL
3box	uPortによる分散データストレージ。ウォレット使うdapp横断で情報のアップロードおよび共有を可能に	→ https://medium.com/uport/announcing-3box-and-ethereum-profiles-dba9841e0952
LOKI	Moneroベースのプライバシープロジェクト	→ https://loki.network/
KOVRI	Moneroにより開発された分散匿名技術	→ https://getkovri.org/
Celer Network	オフチェーンスケーリングソリューション	→ https://www.celer.network/
DEXON	Dapps開発むけブロックチェーンプラットフォーム	→ https://dexon.org/
CrypticLabs	セキュリティやプライバシーおよびトラストに着目したリサーチ機関	→ http://crypticlabs.org/
Spark	c-lightning向けLightningウォレット	→ https://medium.com/@notgrubles/spark-a-new-gui-for-c-lightning-2cf2f024500c
Casa Lightning Node	Lightning ノード立ち上げを容易に	→ https://medium.com/casa/announcing-the-casa-lightning-node-596df7a7427

4-1) プラットフォーム分野②

名称	サービス概略	URL
CertiK	スマートコントラクト向け形式検証プラットフォーム	→ https://certik.org/
LN Monitor	Bitfuryの LightningPeachチームによるLightningモニタリングツール	→ https://medium.com/meetbitfury/announcing-the-ln-monitor-69480719356a
Braiins OS	暗号通貨デバイス向けオープンソースOS	→ https://medium.com/@braiins_systems/braiins-os-introduction-45c545d13d51
Skale Labs	Dapp向けにPlasma上でEVMを稼働	→ https://www.skalelabs.com/
Helena	ConsenSysによる分散型リサーチ機関	→ https://helena.consensys.net/ → https://media.consensys.net/title-84ca4003f2d2
OpenCourt	ブロックチェーンベースの法的仲裁	→ https://media.consensys.net/opencourt-legally-enforceable-blockchain-based-arbitration-3d7147dbb56f
Kyokan	BOLT#1および#2をサポートし、Ethereum上でlndと相互運用可能なLightningのプロトタイプを実装	→ https://github.com/kyokan/drawbridge

4-2) ライフスタイル分野

名称	サービス概略	URL
Twicash	Twitterのリツイート数にトークンをbetして報酬を得る	→ https://alis.to/mozk/articles/3D4OBElg8nyd
Ethernaut	スマートコントラクトのハックを通じて進むことができるゲーム	→ https://ethernaut.zeppelin.solutions/
Dmunity	ソーシャルキュレーションマーケット	→ https://dmunity.com/curated
LCNEM	転売防止チケットシステム公開	→ https://prtimes.jp/main/html/rd/amp/p/000000003.000034101.html#click=https://t.co/rs0DSqRaN3 → https://yu-kimura.jp/2018/09/20/ticket-p2p/
Laoru	Lightning Network用いたビデオストリーミングプラットフォーム	→ https://www.bitcoinlightning.com/laolu-lightning-network-powered-video-platform/
Destream	Lightning Network用いたビデオストリーミングプラットフォーム	→ https://destream.io/ → https://www.bitcoinlightning.com/destream-implements-lightning-network/
Origin	シェアリングエコノミー向けマーケットプレイスとしてメインネットローンチ	→ https://techcrunch.com/2018/10/10/origin-protocol/ → https://www.originprotocol.com/en
Lightning Playground	LNベースのアプリ・ゲーム向けマーケットプレイス	→ https://www.lightningplayground.co/

4-3) サプライチェーン分野

名称	サービス概略	URL
Eximchain	サプライチェーンむけエンタープライズパブリックチェーン	→ https://eximchain.com/

4-4) シビックテック分野

名称	サービス概略	URL
Building Blocks	ヨルダン難民キャンプで試行されたWFPによる送金アイデンティティ	→ https://innovation.wfp.org/project/building-blocks
Clan	コラボレーションインセンティブプログラム	→ http://www.amatus.com/clan/
BlockEstate	米国ベースの不動産トークン	→ https://blockestate.com/
Energy Web Chain	EWFによるエネルギー送信ブロックチェーン	→ https://energyweb.org/papers/the-energy-web-chain/
reLease	ワークスペース不動産のリースサービス	→ https://leasing.meridio.co/

4-5) 金融分野

名称	サービス概略	URL
Wyre	オンチェーンによるKYCプロバイダ	→ https://www.sendwyre.com/
Etherisc	ハリケーン向け自動保険がプエルトリコへ	→ https://www.forbes.com/sites/michaeldelcastillo/2018/09/11/hurricane-victims-edge-closer-to-automated-insurance-payouts-with-ethereum/
SILO	GuardtimeとMetacoによる金融機関むけ暗号通貨カストディプラットフォーム	→ https://silo.metaco.com/#/
expo	dYdXプロトコル上の信用取引サービス	→ https://www.expotrading.com/ → https://medium.com/dydxderivatives/introducing-expo-ffe74a328f85
Tokenizeu	欧州圏のトークンプラットフォーム	→ http://tokenizeu.com/
Hibana Wallet	LNのスマホ向けウォレット	→ https://youtu.be/GzLRY_NiPpw

5. 規制関連の動向

① 規制・制度
② 暗号通貨アダプション

①規制・制度 – 国際協調

名称	概略	URL
国際協調	FATF、仮想通貨のAMLむけグローバルスタンダードを合意へ	→ https://www.ft.com/content/1a67f6b2-bbf7-11e8-94b2-17176fbf93f5
国際協調	FATF、規制スタンダードを改定。レコメンデーションとして、仮想通貨含むあらゆるアクティビティに適用するマネロン・テロリスト対応むけ包括要件を打ち出すもの	→ http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html

①規制・制度 – 米国(SEC)

名称	概略	URL
米国	米SEC、個人IRA年金へのクリプトアセット運用についてアラート発表	→ https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-self-directed-iras-risk-fraud
米国	米SEC、ProshareおよびDirexionなど９つのETFについて「取引所による詐欺や相場操縦への対策不十分」を理由として否決。否決発表後、レビュー実施となり否決は一旦保留に	→ https://www.sec.gov/rules/sro/nysearca/2018/34-83912.pdf → https://www.sec.gov/rules/sro/nysearca/2018/34-83912-letter-from-secretary.pdf
米国	米SEC、SolidX ETF判断延期	→ https://www.sec.gov/rules/sro/cboebzx/2018/34-84231.pdf
米国	コア開発者のBryan Bishop等によるSEC宛open letter	→ https://www.sec.gov/divisions/investment/allen-bishop-crespigny-fearey-long.pdf
米国	米SEC、法規制につき直接対話できるようにすべくFinTech向けハブの立ち上げ発表	→ https://www.sec.gov/news/press-release/2018-240

①規制・制度 – 米国（議会）

名称	概略	URL
米国	米上院、マイニングおよび公共分野でのブロックチェーン利用について公聴会開催	→ https://www.coindesk.com/us-senators-raise-crypto-mining-concerns-propose-government-blockchains/ → https://www.energy.senate.gov/public/index.cfm/hearings-and-business-meetings?ID=61CD5B55-EA3E-41F2-BB4B-3EEB7879131F
米国	米上院、仮想通貨およびブロックチェーンについて公聴会。NYUのNouriel Roubini、Coin CenterのPeter Van Valkenberghのコメント文書	→ https://www.banking.senate.gov/hearings/exploring-the-cryptocurrency-and-blockchain-ecosystem → https://twitter.com/jchervinsky/status/1050574956042604544?s=21
米国	米国議会によるブロックチェーンプロジェクトCaucus	→ https://emmer.house.gov/media-center/press-releases/emmer-spearheads-groundbreaking-legislation- → support-blockchain → https://emmer.house.gov/media-center/press-releases/reps-emmer-foster-announced-co-chairs- → congressional-blockchain-caucus
米国	Brave、米上院に対して米国もGDPR的なデータ保護を進めるべきとレター発出	→ https://brave.com/us-gdpr-senate/

①規制・制度 – 米国(その他)

名称	概略	URL
米国	米CFTC委員長、仮想通貨は機能不全に陥った法定通貨の代替となる可能性ありと言及	→ https://www.ccn.com/cryptocurrency-is-here-to-stay-cftc-chairman-giancarlo/
米国	米CFTC、開発者によるコードへの責任に言及し、コンプラコストへのインパクト懸念	→ https://cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16
米国	米FINRA、ICOに関して投資家むけアラート発表	→ http://www.finra.org/investors/alerts/initial-coin-offerings-what-to-know
米国	北米証券監督協会NASAA、200以上のICOや暗号通貨関連商品についてCryptosweep実施	→ http://www.nasaa.org/45901/nasaa-updates-coordinated-crypto-crackdown/ → http://www.nasaa.org/regulatory-activity/enforcement-legal-activity/operation-cryptosweep/
米国	米連邦裁、ICO不正には証券法適用へ	→ https://www.bloomberg.com/news/articles/2018-09-11/u-s-judge-says-initial-coin-offering-covered-by-securities-law
米国	カリフォルニア州、暗号通貨とブロックチェーンを定義する法案通過	→ https://news.bitcoin.com/california-passes-bill-defining-blockchain-and-crypto-terms/
米国	米NSAのCodebreaker Challenge、Ethereumを題材	→ https://codebreaker.ltsnet.net/challenge

①規制・制度 – 欧州(1/3)

名称	概略	URL
欧州	欧州議会、ICO規制を新たなクラウドファンディングルール中へ包含の意向	→ http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-626.662&format=PDF&language=EN&secondRef=02
欧州	ユーロポール、暗号通貨関連犯罪としてハッキング・脅迫・マイニングマルウェアに言及	→ https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018
欧州	欧州規制当局ESMA、ICOはケースバイケースで証券に該当との見方	→ https://uk.reuters.com/article/us-eu-crypto-regulations/eu-regulators-studying-crypto-assets-case-by-case-idUKKCN1MI1VD
イギリス	英FCA、暗号通貨投資スキャムへのアラート発表	→ https://www.fca.org.uk/scamsmart/cryptocurrency-investment-scams
イギリス	英国財務省特別委、暗号アセットへ規制求める	→ https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/news-parliament-2017/digital-currencies-report-pubished-17-19/ → https://www.bbc.com/news/business-45558593
ドイツ	独Neufund、連邦議会へオープンレター発出	→ https://blog.neufund.org/open-letter-to-the-bundestag-on-blockchain-regulation-in-germany-754dd48d68d8

①規制・制度 – 欧州(2/3)

名称	概略	URL
フランス	仏AMF、ICO向けガイドライン制定へ	→ https://news.bitcoin.com/new-french-law-sets-out-guidelines-for-icos/ → https://www.trustnodes.com/2018/09/16/france-passes-the-most-progressive-legislation-on-icos-bank-accounts-to-be-guaranteed
フランス	クリプトアセット仲介業者むけガイドライン導入へ	→ https://www.kramerlevin.com/en/perspectives-search/france-set-to-enact-the-first-regulatory-framework-for-crypto-asset-intermediaries.html
スイス	スイス銀行協会SBA、クリプト企業とのコワークへガイドライン	→ https://www.reuters.com/article/us-crypto-currencies-switzerland/switzerland-tries-to-stem-blockchain-exodus-by-improving-access-to-banks-idUSKCN1M11H3 → https://www.jetro.go.jp/biznews/2018/10/9500b1783f08316f.html
ベルギー	FSMA、暗号通貨関連詐欺に関する警告を発表	→ https://www.fsma.be/en/warnings/warning-against-new-cryptocurrency-trading-platforms

①規制・制度 – 欧州(3/3)

名称	概略	URL
マルタ	暗号通貨・ブロックチェーン・ICOむけガイダンスを示す法律を11/1より施行	→ https://dcebrief.com/maltas-new-crypto-laws-to-go-into-effect-nov-1st/
マルタ	マルタのクリプト規制についての解説	→ https://flagtheory.com/malta-crypto-regulations-ico-exchanges/

①規制・制度 – 中国(1/2)

名称	概略	URL
中国	ブロックチェーンや暗号通貨関連ニュース提供WeChatアカウント停止	→ http://www.scmp.com/tech/article/2160805/china-cracks-down-wechat-accounts-offering-blockchain-and-cryptocurrency-news
中国	124のトレードプラットフォームへのアクセスが禁止に	→ https://www.ethnews.com/chinese-regulators-to-block-access-to-124-different-crypto-trading-platforms → http://news.cnstock.com/news,yw-201808-4262742.htm
中国	PBoC、違法な資金調達に警告	→ https://jp.reuters.com/article/china-pboc-blockchain-idJPKCN1L90RR
中国	Baidu、AlibabaやTencentに続き暗号通貨対応厳格化	→ https://www.scmp.com/tech/article/2161451/chinese-internet-giants-move-shut-cryptocurrency-forums-and-transactions-amid
中国	香港SFC、暗号通貨トレーディング禁止はインターネット世界において機能しないことからトレーディング向け規制検討	→ https://www.newsbtc.com/2018/10/15/hong-kong-to-propose-regulation-for-cryptocurrency-trading/

①規制・制度 – 中国(2/2)

名称	概略	URL
中国	中国共産党、ブロックチェーン技術のガイドブック発行	→ http://theory.people.com.cn/n1/2018/0813/c40531-30225582.html
中国	中国最高裁、ブロックチェーン記録を法的拘束力あるエビデンスと認定	→ http://www.court.gov.cn/zixun-xiangqing-116981.html
中国	PBoC、デジタル通貨研究ラボを拡張し南京に新設	→ https://www.coindesk.com/pbocs-digital-currency-lab-launches-new-research-center-outside-of-beijing/ → http://news.cnstock.com/news,yw-201809-4268560.htm
中国	中国サイバースペース監督局（CAC）、ブロックチェーン情報サービスにおける本人確認規制強化へむけた草案発表	→ https://www.coindesk.com/chinas-internet-censor-releases-draft-regulation-for-blockchain-startups/ → http://www.cac.gov.cn/2018-10/19/c_1123585598.htm
中国	香港証取、ブロックチェーン関連金融は既存規制を適用すべきとの見方	→ https://www.hkex.com.hk/-/media/HKEX-Market/News/Research-Reports/HKEx-Research-Papers/2018/CCEO_Fintech_201810_e.pdf
中国	深セン国際仲裁院、ビットコインを法的に保護されるべき財産として認定	→ https://www.coindesk.com/chinese-arbitration-court-says-bitcoin-should-be-legally-protected-as-property/ → https://mp.weixin.qq.com/s/U_qDgQN9hceLBbpQ13eEdQ

①規制・制度 – アジア太平洋域

名称	概略	URL
シンガポール	MAS、トークンは証券でないとの見方表明	→ https://news.bitcoin.com/regulations-round-up-mas-tokens-securities-sec-bookkeeping/
シンガポール	MAS、暗号通貨関連企業の銀行口座開設を支援へ	→ https://www.ccn.com/singapore-central-bank-will-aid-crypto-startups-in-opening-bank-accounts/
オーストラリア	ASIC、暗号通貨およびICOへのモニタリングを厳格化	→ https://download.asic.gov.au/media/4855947/asic-corporate-plan-2018-22-focus-2018-19-published-31-august-2018.pdf
オーストラリア	ASIC、ICO巡る誤解について警鐘	→ https://asic.gov.au/about-asic/media-centre/find-a-media-release/2018-releases/18-274mr-asic-acts-against-misleading-initial-coin-offerings-and-crypto-asset-funds-targeted-at-retail-investors/
タイ	7つの事業者を国内での暗号通貨関連業務運営で認可	→ https://news.bitcoin.com/thai-crypto-firms-legally-operate-thailand/
フィリピン	暗号通貨取引やICOへの規制強化	→ https://www.manilatimes.net/cryptocurrency-trading-rules-eyed/437546/
インド	銀、仮想通貨はインド通貨に当たらずとの声明を最高裁へ提出	→ https://coinpost.jp/?p=46061

①規制・制度 – 中東

名称	概略	URL
UAE	UAE当局、2019年にもICO受け入れへ	→ https://www.reuters.com/article/emirates-ico/uae-plans-initial-coin-offerings-to-boost-capital-markets-regulator-idUSL8N1WO2QI
サウジアラビア	トレーダーへのリスク理由に仮想通貨を違法と取扱	→ http://www.sama.gov.sa/en-US/News/Pages/news12082018.aspx

①規制・制度 – 日本(2/2)

名称	概略	URL
日本	金融庁新長官、暗号通貨業界について過度に抑制する意向は無く、適切な規制のもとでの成長を見守りたい旨をコメント	→ https://www.reuters.com/article/us-japan-regulator/japan-regulatory-head-scolds-weak-regional-banks-dont-blame-boj-idUSKCN1L70RX
日本	金融庁、仮想通貨交換業登録の審査を厳格化。質問項目400点へ4倍にするとともに取締役会議事録提出など	→ https://headlines.yahoo.co.jp/hl?a=20180901-00000064-jij-bus_all
日本	匿名仮想通貨禁止・ICO関連ガイドライン・反社対策強化など業界団体が自主規制の概要を金融庁にて説明	→ https://crypto.watch.impress.co.jp/docs/event/1143119.html
日本	金融庁、平成30事務年度 金融行政方針発表	→ https://www.fsa.go.jp/news/30/20180926.html
日本	警察庁、仮想通貨解析ソフトを全国の警察に導入へ	→ https://www3.nhk.or.jp/shutoken-news/20180830/0017640.html

①規制・制度 – 日本(2/2)

名称	概略	URL
日本	金融庁、日本仮想通貨交換業協会を資金決済法に基づく自主規制団体として認定	→ https://www.fsa.go.jp/news/30/virtual_currency/20181024-1.html
日本	日本仮想通貨交換業協会、規則・ガイドラインを公開	→ https://jvcea.or.jp/about/rule/
日本	金融庁、仮想通貨交換業者の登録審査プロセスなどについて発表	→ https://www.fsa.go.jp/news/30/virtual_currency/20181024-2.html

②暗号通貨アダプション – 北米（COINBASE 1/3）

名称	概略	URL
米国	Coinbase、Distributed Systems社を買収	→ https://github.com/dsys → https://medium.com/dsys/distributed-systems-acquired-by-coinbase-1d17ed4f0340
米国	Coinbase、Toshiの名称をCoinbase Walletへリブランディング	→ https://blog.coinbase.com/goodbye-toshi-hello-coinbase-wallet-the-easiest-and-most-secure-crypto-wallet-and-browser-4ba6e52e4913
米国	Coinbase、ビットコインペイメントシステムで特許	→ http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=10,050,779.PN.&OS=pn/10,050,779&RS=PN/10,050,779 → https://coinpost.jp/?p=41648
米国	Coinbase、資産運用BlackRockとETF検討	→ https://www.businessinsider.com/coinbase-is-exploring-a-bitcoin-etf-2018-9
米国	CoinbaseやCircle、ロビイング団体Blockchain Association立ち上げ。Protocol LabsやDCG、Polychain Capitalなどもメンバーに	→ https://www.washingtonpost.com/technology/2018/09/11/get-ready-big-bitcoin-cryptocurrency-industry-opens-dc-lobbying-arm/

②暗号通貨アダプション – 北米（COINBASE 2/3）

名称	概略	URL
米国	Coinbase、NYCオフィスに100名増員計画	→ https://www.coindesk.com/coinbase-crypto-jobs-hiring/
米国	Coinbase、新たにアセット上場ポリシー発表	→ https://blog.coinbase.com/new-asset-listing-process-a83ef296a0f3 → https://coinpost.jp/amp/?p=48102#click=https://t.co/dTscmm8UGO
米国	Coinbaseの第三四半期振り返り	→ https://blog.coinbase.com/what-we-accomplished-at-coinbase-in-q3-2018-e68deddb1e16
米国	Coinbase、800億ドルのバリュエーション到達	→ https://www.recode.net/2018/10/2/17928274/coinbase-tiger-global-8-billion-funding-deal
米国	Coinbaseで機関投資家向けGDAXを築いたAdam White氏、Bakktへ移籍	→ https://theblockcrypto.com/2018/10/11/coinbases-adam-white-is-joining-bakkt-as-its-coo/
米国	Coinbase ProでZRX取引可能に	→ https://blog.coinbase.com/zrx-is-launching-on-coinbase-pro-29ae77eadc42

②暗号通貨アダプション – 北米（COINBASE 3/3）

名称	概略	URL
米国	Coinbase、IPOを計画。80億ドルの評価額	→ https://youtu.be/NDhGs9DGvGU
米国	Coinbase Custody、NY州の認定カストディアンとしてのライセンス取得	→ https://blog.coinbase.com/coinbase-custody-receives-trust-charter-from-the-new-york-department-of-financial-services-532c92797215
米国	Coinbase、CircleをCENTREコンソーシアムの共同設立者とした米ドル担保型Stablecoin USD Coinを発表	→ https://blog.coinbase.com/coinbase-and-circle-announce-the-launch-of-usdc-a-digital-dollar-2cd6548d237 → https://www.centre.io/pdfs/centre-whitepaper.pdf → https://www.centre.io/usdc

②暗号通貨アダプション – 北米（スタートアップ）

名称	概略	URL
米国	Square、暗号通貨ペイメントで特許	→ https://www.ccn.com/bitcoin-accepted-everywhere-square-wins-patent-for-cryptocurrency-payment-network/
米国	OpenFinance、証券トークンむけATSをローンチ	→ https://www.coindesk.com/openfinance-launches-regulated-trading-platform-for-security-tokens/
米国	Bittrex、マルタの証券トークン取引所Palladium社の株式10%購入	→ https://www.financemagnates.com/cryptocurrency/news/bittrex-buys-10-percent-of-maltese-ico-securities-exchange/
米国	AirSwap、大口投資家向けにOTC取引プラットフォームをクローズドベータ版ローンチ	→ https://www.ccn.com/decentralized-crypto-exchange-airswap-launches-otc-market-to-unlock-new-world-of-liquidity/
米国	Swarm、Robinhood社のエクイティトークン取扱い	→ https://invest.swarm.fund/explore/details/12
米国	Indiegogo、ホテル不動産を裏付けとした証券トークン発行へ	→ https://www.theverge.com/2018/8/23/17766128/indiegogo-real-estate-shares-blockchain
米国	BitGo、South Dakotaでデジタルアセットの適格カストディアンとして認定	→ https://www.coindesk.com/bitgo-receives-regulatory-approval-to-custody-crypto-assets/

②暗号通貨アダプション – 北米（スタートアップ）

名称	概略	URL
米国	Gemini、ブロックチェーン上のUSDとしてGemini Dollarをローンチ。規制対応Stablecoinとして	→ https://medium.com/gemini/gemini-launches-the-gemini-dollar-62787f963fb4 → https://www.marketwatch.com/story/winklevoss-twins-gemini-trust-launches-worlds-first-regulated-stablecoin-2018-09-10 → https://prestonbyrne.com/2018/09/10/thoughts-on-geminicoin/
米国	Paxos、米ドルベースStablecoinとしてPaxos Standard検討	→ https://www.bloomberg.com/news/articles/2018-09-10/controversial-crypto-coin-tether-to-get-regulated-competitors → https://www.dfs.ny.gov/about/press/pr1809101.htm
米国	Gemini、オンラインホットウォレット上のデジタルアセットについて保険締結	→ https://medium.com/gemini/digital-assets-insurance-adbfb0c44e74
米国	Circle、クラウドファンディングSeedinvestを買収へ	→ https://blog.circle.com/2018/10/05/circle-announces-acquisition-of-seedinvest/
米国	tZERO、法令遵守型の優先証券トークン発行	→ https://bitcoinexchangeguide.com/overstocks-tzero-mint-security-tokens-are-locked-for-90-days-trading-platform-in-development/

②暗号通貨アダプション – 米国（証券会社）

名称	概略	URL
米国	Morgan Stanley、ビットコインスワップ商品を開発へ	→ https://www.ccn.com/morgan-stanley-is-building-a-bitcoin-swap-trading-product-report/
米国	CitiGroup、機関投資家むけカストディサービス提供へ	→ https://www.ccn.com/citigroup-to-offer-low-risk-crypto-product-for-institutional-investors-report/ → https://www.ccn.com/citigroup-is-the-latest-bank-to-offer-crypto-custody-heres-how-it-will-affect-the-market/
米国	CBOE、年内のETH先物ローンチ向けて検討中	→ http://uk.businessinsider.com/ether-futures-on-the-way-at-cboe-2018-8
米国	Barclays、長引く弱気市場の中で暗号通貨トレードプロジェクトを凍結	→ https://www.ccn.com/uk-banking-giant-barclays-cryptocurrency-project-put-on-ice-report/
米国	Fidelity、機関投資家むけにカストディおよびブローカレッジ業務を提供するデジタルアセットプラットフォーム開設	→ https://www.fidelitydigitalassets.com/overview
米国	Goldman Sachs、BitGo出資	→ https://www.bloomberg.co.jp/news/articles/2018-10-18/PGSO8G6KLVR401
米国	Bakkt、先物取引を12/12ローンチ予定	→ https://bitcoinmagazine.com/articles/bakkts-futures-platform-slated-begin-trading-december/

②暗号通貨アダプション – 北米

名称	概略	URL
米国	カリフォルニア州、暗号通貨による政治献金を禁止	→ https://www.apnews.com/e17fb80a62f24552bf4340f6e5d9cf8b
米国	Google、暗号通貨関連広告禁止を撤廃。日米で規制適応済み交換業者による広告枠購入認める	→ https://www.cnbc.com/2018/09/25/google-reverses-ban-on-cryptocurrency-exchange-advertising-in-us-japan.html
米国	米大統領選へのロシア介入において捜査で起訴。運営に際してビットコイン使用も	→ https://www.justice.gov/file/1080281/download

②暗号通貨アダプション – 欧州(1/2)

名称	概略	URL
スイス	プライベートバンクFalcon Private Bankに続いてMaerki Baumannが暗号通貨関連企業への金融サービス提供へ	→ https://www.financemagnates.com/cryptocurrency/news/second-swiss-private-bank-opens-doors-to-cryptocurrency-deposits/
スイス	SIX、仮想通貨デリバティブの要件示す	→ https://www.six-exchange-regulation.com/dam/downloads/regulation/admission-manual/circulars/07_03-CIR3_en.pdf
スイス	クリプトバレーVC、100億円規模を投資へ	→ https://cvvc.com/ → https://www.swissinfo.ch/eng/lofty-targets_swiss-investors-launch--100m-blockchain-start-up-factory/44414812
マルタ共和国	マルタ証取、Binanceと証券トークン取引プラットフォーム立ち上げへMOU締結	→ https://www.ccn.com/binance-partners-malta-stock-exchange-to-launch-new-digital-exchange/
マルタ共和国	マルタ首相、国連総会でブロックチェーンは暗号通貨を不可欠なマネーの未来像ならしめるものとの声明	→ https://www.ccn.com/malta-pm-at-un-general-assembly-crypto-is-the-inevitable-future-of-money/
リヒテンシュタイン	リヒテンシュタインユニオン銀行、規制準拠ベースの証券トークンおよびStablecoin発行へ	→ https://bitcoinexchangeguide.com/liechtensteins-union-bank-to-launch-regulated-security-token-and-stablecoin/

②暗号通貨アダプション – 欧州(2/2)

名称	概略	URL
英国	英London Block Exchange、ポンドベースのStablecoin「LBXPeg」発表	→ https://lbx.com/blog/lbx-peg/
英国	ロイズ、暗号通貨カストディに保険適用	→ https://jp.cointelegraph.com/news/lloyds-of-london-to-insure-custody-platform-for-digital-currency
フランス	ユニセフフランス、暗号通貨による寄付受け入れ	→ https://www.unicef.fr/article/l-unicef-france-collecte-maintenant-des-dons-en-crypto-monnaie
スウェーデン	スウェーデンNasdaq、ビットコイン上場投資証券(ETN)を上場	→ https://www.bloomberg.com/news/articles/2018-08-15/lovelorn-u-s-bitcoin-etf-fans-may-find-satisfaction-in-sweden?srnd=cryptocurriences
アイスランド	アイスランドFSA、初めて暗号通貨交換業者を登録	→ http://icelandreview.com/news/2018/09/07/first-cryptocurrency-exchange-registers-financial-supervisory-authority
ロシア	ロシア中銀、ICOパイロット実施の成功を発表	→ https://www.ccn.com/russias-central-bank-ico-pilot-a-success-legal-hurdles-remain/

②暗号通貨アダプション – 中国

名称	概略	URL
中国	杭州市政府支援のブロックチェーンファンド、日本円ペグStablecoinを計画	→ https://www.coindesk.com/1-billion-blockchain-fund-founders-plan-japanese-yen-stablecoin/
中国	PBoCのCN Finance、中国元ペグStablecoinの研究必要性を主張	→ http://www.cnfinance.cn/magzi/2018-10/09-29008.html → https://coinpost.jp/amp/?p=50533

②暗号通貨アダプション – 中国(BINANCE)

名称	概略	URL
中国	Binance、リヒテンシュタインでユーロ・スイスフラン取引	→ https://www.ccn.com/binance-lcx-collaborate-to-launch-fiat-to-cryptocurrency-exchange-in-liechtenstein/
中国	Binance、教育サイトBinance Academyがベータ版ローンチ	→ https://www.binance.vision/
中国	Binance、アフリカ進出を計画	→ https://www.ccn.com/crypto-exchange-giant-binance-outlines-plans-to-expand-in-africa/
中国	Binance、シンガポールで法定通貨との交換立ち上げ検討	→ https://www.financemagnates.com/cryptocurrency/news/binance-to-open-fiat-exchange-in-singapore/
中国	Binance、各大陸への交換業立ち上げを検討	→ https://www.coindesk.com/binance-reveals-plan-to-launch-crypto-exchanges-on-almost-every-continent/
中国	Binance、年末までにDEXベータ版をローンチ予定	→ https://twitter.com/cz_binance/status/1045928683586772992?s=21 → https://www.ccn.com/how-binance-decentralized-crypto-exchange-beta-launch-in-2019-will-impact-the-market/

②暗号通貨アダプション – 中国（BINANCE）

名称	概略	URL
中国	Binance、豪州ペイメントプロバイダTravelbyBitへ出資	→ https://www.businessinsider.com.au/queensland-blockchain-startup-cryptocurrency-exchange-binance-2018-10
中国	Binance、上場手数料を全額寄付へ	→ https://support.binance.com/hc/en-us/articles/360017664751-Binance-Listing-Fee-Update
中国	Binance、シンガポールへの拡大へ向けてVertex Venturesからの投資	→ https://www.businesstimes.com.sg/banking-finance/temaseks-vertex-invests-in-cryptocurrency-exchange-binance-to-expand-in-Singapore
中国	Binance、西日本豪雨被災地支援寄付内容を公開	→ https://medium.com/binanceexchange/2018-west-japan-flood-donation-report-67c858edda9f

②暗号通貨アダプション – 中国（スタートアップ）

名称	概略	URL
中国	Huobi、証券トークンプラットフォームOpenFinance Networkへ出資	→ https://medium.com/@openfinance/press-release-huobi-one-of-worlds-largest-crypto-exchanges-invests-in-openfinance-network-44649b62de2
中国	Ant Financial、Alipayモバイルアプリ上における暗号通貨のOTC取引について当局と調査	→ https://www.coindesk.com/alibaba-affiliate-to-step-up-scrutiny-over-crypto-otc-trading-using-alipay/ → http://www.bjnews.com.cn/finance/2018/08/24/501012.html
中国	Huobi、日本の登録仮想通貨交換業者BitTradeの株式過半数取得	→ https://prtimes.jp/main/html/rd/p/000000001.000037562.html
中国	Huobi、StablecoinとしてHUSDをローンチ	→ https://huobiglobal.zendesk.com/hc/en-us/articles/360000170601-Announcement-on-the-Launch-of-HUSD-solution-on-Huobi-Global

②暗号通貨アダプション – 日本

名称	概略	URL
日本	GINKAN、株式にトークン転換権を導入し販売する「Token Equity Convertible（TEC）」で資金調達	→ https://jp.cointelegraph.com/news/ceres-and-synchrolife-talk-about-new-financing-scheme-tec
日本	楽天、みなし仮想通貨交換業者「みんなのビットコイン」株式取得を発表	→ https://corp.rakuten.co.jp/news/press/2018/0831_02.html
日本	LINE、ブロックチェーンと独自コインによるLINKエコシステムを発表。日本では独自通貨LINKポイント、海外では仮想通貨LINKを発行	→ https://japan.cnet.com/article/35124921/ → https://link.network/whitepaper/link_whitepaper_en.pdf → https://www.release.tdnet.info/inbs/140120180831402666.pdf
日本	GMOインターネット、アジア圏で日本円と連動したStablecoinを2019年度に発行へ。グループ内の銀行への信託を利用	→ https://www.gmo.jp/news/article/6177/ → https://coinpost.jp/amp/?p=50261&p=50261

②暗号通貨アダプション – その他

名称	概略	URL
英国	警備サービス大手G4S、暗号通貨ストレージサービスを開発	→ http://www.g4s.com/en/media-centre/news/2018/10/16/cryptocurrencies---secure-vault-storage-in-the-wild-west
韓国	Bithumb、年内にDEX立ち上げへ	→ http://www.businesskorea.co.kr/news/articleView.html?idxno=25420
韓国	Bithumb、株式の約4割を353百万ドルでシンガポールBK Globalに売却	→ https://thenews.asia/en/2018/10/12/bithumb-sold-for-353-million-to-bk-global-consortium/
ベネズエラ	ベネズエラ、仮想通貨のための中央銀行設立を検討	→ https://btcnews.jp/5ygek78518193/
ベネズエラ	ベネズエラ、年金および給与システムをPetroと連動へ	→ https://www.coindesk.com/venezuela-to-peg-pension-salary-systems-to-petro-cryptocurrency/
ベネズエラ	ベネズエラ、ハイパーインフレの中でDash受け入れ進む	→ https://www.businessinsider.com/dash-cryptocurrency-surges-in-venezuela-as-hyperinflation-explodes-2018-8
ベネズエラ	ベネズエラPetro、Dashのコピーかとの指摘	→ http://petro.gob.ve/descargas/Petro_whitepaper.pdf → https://dash-docs.github.io/img/dev/en-tx-overview-spending.svg
ドバイ	自国開発のブロックチェーンベース	→ https://www.ccn.com/dubai-to-launch-

6. Enterprise/Government系

6-1. プラットフォーム分野
6-2. ライフスタイル分野
6-3. サプライチェーン分野
6-4. シビックテック分野
6-5. 金融分野

6-1) プラットフォーム分野

名称	サービス概略	URL
豪州CSIRO（連邦科学産業研究機構）	企業のコラボレーション促進へスマートコントラクトによるクロスインダストリープラットフォームをIBMと開発へコンソーシアム組成	→ https://www.csiro.au/en/News/News-releases/2018/New-blockchain-based-smart-legal-contracts
IBM	ブロックチェーン用いたセキュリティイベントモニタリングで特許	→ http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=10,091,228.PN.&OS=pn/10,091,228&RS=PN/10,091,228
ソニーコンピューターサイエンス研究所	非接触ICカード型ハードウェアウォレット技術開発	→ https://www.sonycsl.co.jp/press/prs201810-2/ → http://www.itmedia.co.jp/news/spv/1810/23/news095_0.html

6-2) ライフスタイル分野

名称	サービス概略	URL
欧州サッカー UEFA	モバイルチケットへのトライアルを完了	→ https://www.uefa.com/insideuefa/about-uefa/news/newsid=2566998.html
LINE	Dapps発表しLINEトークンエコノミー始動へ	→ https://coinpost.jp/amp/?p=48153 → https://dappsmarket.net/other/linkchain-line/
BMW	レンディングサービス拡充へBloomと提携	→ https://www.press.bmwgroup.com/usa/article/detail/T0284774EN_US/bmw-group-financial-services-announces-six-startups-selected-to-join-first-u-s-collaboration-lab?language=en_US → https://blog.hellobloom.io/inside-the-bmw-and-bloom-partnership-streamlining-the-lending-experience-f93ff1b9c065
ソフトバンク	モバイルペイメントのPoC実施	→ https://www.softbank.jp/corp/group/sbm/news/press/2018/20180912_01/
近鉄グループ	三菱総合研究所およびchaintopeと近鉄ハルカスコインの実証実験	→ http://www.kintetsu-g-hd.co.jp/common-hd/data/pdf/sai180907hd20180907140715362968405.pdf

6-2) ライフスタイル分野

名称	サービス概略	URL
AT&T	IBM・Microsoftと協業で製造・小売・ヘルスケア企業向けブロックチェーンソリューション展開を発表	→ http://about.att.com/story/2018/att_blockchain.html → https://www.business.att.com/learn/att-solutions-for-blockchain.html
ソニー	音楽・映像の生成者・日時証明をブロックチェーンで管理。ソニーグローバルエデュケーションの教育むけシステムもとに開発	→ https://www.sony.co.jp/SonyInfo/News/Press/201810/18-1015/index.html → https://www.nikkei.com/article/DGXMZO36487870V11C18A0X20000/
トヨタ	デジタル広告の透明化・効率化を目指してLucidityと提携	→ https://lucidity.tech/toyota-campaign/ → https://www.prnewswire.com/news-releases/luciditys-blockchain-pilot-with-toyota-results-in-21-lift-in-campaign-performance-300731983.html → https://coinpost.jp/amp/?p=51530
ルーデン	不動産売買を仮想通貨で即時決済。スマートコントラクトの実証実験結果を発表	→ https://crypto.watch.impress.co.jp/docs/news/1140165.html
エアカナダ	分散トラベルプラットフォームWindingTree参加	→ https://www.newswire.ca/news-releases/air-canada-partners-with-winding-tree-on-a-blockchain-based-travel-distribution-platform-698409851.html

6-3) サプライチェーン分野
A) 貿易

名称	サービス概略	URL
Maersk	IBMとの協働によるTradeLens、94社が参加	→ https://www.cnet.com/news/ibm-maersk-tradelens-blockchain-alliance-cuts-shipping-times-40-percent/
NTTデータ	貿易情報共有システム構築	→ https://it.impressbm.co.jp/articles/-/16592
米税関・国境取締局CBP	輸入証明書の検証・貨物追跡システムのライブテスト	→ https://www.coindesk.com/cbp-our-live-fire-blockchain-test-is-entering-the-proof-of-concept-phase/
英国港湾協会	港湾へのブロックチェーン導入パイロットへMarine Transport International (MTI)と覚書	→ http://www.abports.co.uk/newsarticle/698/
穀物大手Cargill等4社	グローバルトレードのデジタル化へブロックチェーンやAI活用発表	→ https://www.adm.com/news/news-releases/agribusinesses-seek-to-modernize-global-agricultural-commodity-trade-operations

6-3) サプライチェーン分野
B) 配送

名称	サービス概略	URL
UPS	ロジスティック合理化へむけたブロックチェーン活用で特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%220180232693%22.PGNR.&OS=DN/20180232693&RS=DN/20180232693
UPS	自律サービス選択システムで特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%220180232693%22.PGNR.&OS=DN/20180232693&RS=DN/20180232693
Walmart	ドローンなどによる配達識別情報管理への活用で特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%220180248685%22.PGNR.&OS=DN/20180248685&RS=DN/20180248685
Walmart	自動配達ドローンのブロックチェーンによる接続で特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=10&p=1&f=G&l=50&d=PG01&S1=blockchain&OS=blockchain&RS=blockchain

6-3) サプライチェーン分野
C) トラッキング

名称	サービス概略	URL
米海軍航空システムコマンド	航空部品トラッキングへの応用検討	→ https://www.prnewswire.com/news-releases/naval-aviation-enterprise-exploring-blockchain-with-indiana-based-company-itamco-300716633.html
Walmart	大腸菌などの食中毒防止へブロックチェーン用いてトラッキングした葉物野菜の販売を計画。2019年9月までにIBM製トラッキングシステムIBM Food Trust導入をサプライヤーに要請	→ http://news.walmart.com/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens → https://corporate.walmart.com/media-library/document/blockchain-supplier-letter-september-2018/_proxyDocument?id=00000166-088d-dc77-a7ff-4dff689f0001

6-4) シビックテック分野
A) エネルギー

名称	サービス概略	URL
九州電力	電力・環境価値の取引プラットフォームに出資	→ https://crypto.watch.impress.co.jp/docs/news/1140648.html
仏エネルギー大手Engie	アジアおよび南欧のクライアント向けスピンオフBlockchain Studio設立	→ https://www.engie.com/en/journalists/press-releases/engie-maltem-come-together-to-found-blockchain-studio/
関西電力	消費者・プロシューマー同士が太陽光発電による余剰電力の売買価格の決定および直接取引ができる新システムの実証研究を三菱UFJ銀行と開始	→ https://www.kepco.co.jp/corporate/pr/2018/1015_1j.html → https://www.kepco.co.jp/corporate/pr/2018/pdf/1015_1j_01.pdf

6-4) シビックテック分野
B) ヘルスケア

名称	サービス概略	URL
Ant Financial	航天信息と提携して医療電子請求書を発行	→ https://technode.com/2018/08/17/ant-financial-blockchain-e-bills/ → https://tech.sina.cn/i/gn/2018-08-17/detail-ihhvciiw6914206.d.html?from=wap
IBM	ウェアラブルデバイスからブロックチェーン上に医療データを格納する特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&s1=%20180167200%22.PGNR.&OS=DN/20180167200&RS=DN/20180167200

6-4) シビックテック分野
C) 不動産

名称	サービス概略	URL
AirSwap	Propellrと提携してNYの不動産トークン化へ	→ https://medium.com/fluidity/airswap-technology-and-a-new-model-for-tokenized-securities-7f347818b574
GA technologies	ブロックチェーンを活用した「不動産デジタルプラットフォーム」発表	→ https://crypto.watch.impress.co.jp/docs/event/1144891.html

6-4) シビックテック分野
D) アイデンティティ

名称	サービス概略	URL
国連UNHCR	シリア難民むけに虹彩認証とブロックチェーン用いた食糧支援システム	→ https://www.nikkei.com/article/DGXMZO34372330Q8A820C1000000/
国連UNDCFおよびUNDP	シエラレオネとブロックチェーンベースのIDシステム構築へ	→ https://www.ccn.com/sierra-leone-united-nations-to-develop-blockchain-digital-id-system/

6-4) シビックテック分野
E) 投票記録・証拠保管

名称	サービス概略	URL
つくば市	日本初のブロックチェーン投票	→ https://jp.cointelegraph.com/news/japanese-first-blockchain-voting-started-in-tsukuba-city
ケニア	投票結果の記録へブロックチェーン利用検討	→ https://www.ccn.com/kenyas-electoral-commission-to-adopt-blockchain-for-enhanced-vote-integrity/
英司法省	デジタル形態の証拠に関する安全保管へブロックチェーン活用可能性を検討	→ https://www.coindesk.com/uk-government-pilots-blockchain-in-bid-to-secure-digital-evidence/

6-5) 金融分野
金融機関 – 米国

名称	サービス概略	URL
Capital One	認証システムへの活用で特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180234241.PGNR.&OS=dn/20180234241&RS=DN/20180234241
BoA	暗号タグシステムで特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220180240112%22.PGNR.&OS=DN/20180240112&RS=DN/20180240112
IBM	Stellarベースのペイメントシステム Blockchain World Wire開発	→ https://www.coindesk.com/ibm-debuts-stellar-powered-blockchain-world-wire-payments-system/ → https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=00018400USEN
VISA	Hyperledger Fabric用いたデジタルIDシステムB2B Connectを2019Q1にローンチへ	→ https://www.ccn.com/visa-integrates-open-source-hyperledger-tech-for-b2b-blockchain-payments/
Nasdaq	スマートコントラクトを監査証跡ワークフローに組み込む特許	→ http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=10,108,812.PN.&OS=pn/10,108,812&RS=PN/10,108,812

6-5) 金融分野
金融機関 – 米国

名称	サービス概略	URL
MasterCard	P2Pトランザクション処理の記録システムで特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%220180260879%22.PGNR.&OS=DN/20180260879&RS=DN/20180260879
MasterCard	許可制ブロックチェーン上で複数暗号通貨をサポートしてブロック生成する特許	→ https://www.ethnews.com/mastercard-may-develop-blockchain-platform-capable-of-handling-multiple-currencies
MasterCard	暗号通貨の部分準備銀行に関する特許	→ http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%220180308092%22.PGNR.&OS=DN/20180308092&RS=DN/20180308092
MetLife	シンガポールのイノベーションセンターLumenLabで妊娠性糖尿病を対象とした自動保険ソリューションの試行	→ https://www.businesswire.com/news/home/20180820005644/en/MetLife%E2%80%99s-New-Blockchain-Health-Insurance-Product-Eliminates
国民保険AAIS	Hyperledger Fabric用いて保険レポートシステム	→ https://www.coindesk.com/insurance-ratings-bureau-pilots-ibm-blockchain-for-automatic-reporting/

6-5) 金融分野
金融機関 – 中国

名称	サービス概略	URL
BoC	銀聯と提携して決済システム構築へ	→ https://jp.cointelegraph.com/news/bank-of-china-partners-with-china-unionpay-to-explore-blockchain-for-payment-systems
中国浙商銀行	ブロックチェーン上で6600万ドルの証券発行	→ https://www.coindesk.com/china-zheshang-bank-issues-securities-worth-66-million-on-blockchain/ → https://www.shclearing.com/xxpl/fxpl/abn/201808/t20180813_412231.html
PBoC	トレードファイナンスシステムがテストフェーズに	→ https://www.coindesk.com/pboc-backed-blockchain-trade-finance-platform-enters-test-phase/ → https://m.21jingji.com/article/20180904/herald/2d66ef9b438cab86aef580dcf177bdea.html

6-5) 金融分野
金融機関 – 欧州

名称	サービス概略	URL
オーストリア	パブリックEthereumベースの公証サービス用いて11.5億ユーロ相当の国債発行へ	→ https://www.kleinezeitung.at/wirtschaft/5502515/115-Milliarden-Euro_BundesanleihenAuktion_Oesterreich-setzt-auf
イタリア	銀行14行、Corda用いて銀行間取引のトライアル実施	→ https://www.ccn.com/14-italian-banks-complete-interbank-transactions-on-r3-blockchain-corda/
Zurich	契約保証書の管理システムをロールアウトへ	→ https://newsroom.accenture.com/news/accenture-and-zurich-benelux-apply-blockchain-technology-to-help-streamline-customer-experience-and-improve-transparency.htm
ロシアNSD	ポストトレードへのブロックチェーン活用でソラミツと会社設立	→ https://www.nikkei.com/article/DGXMZO36762470S8A021C1EE9000/

6-5) 金融分野
金融機関 – アジア太平洋域

名称	サービス概略	URL
シンガポールMAS	デジタルアセットのDvP決済にむけてSGX・NasdaqやDeloitteと協働	→ https://cointelegraph.com/news/singapore-central-bank-partners-with-deloitte-nasdaq-on-blockchain-asset-settlement → http://www.sgx.com/wps/wcm/connect/sgx_en/home/higlights/news_releases/MAS_and_SGX_partner_Anquan_Deloitte_and_Nasdaq_to_harness_blockchain_technology_for_settlement_of_tokenised_assets
タイ中銀	ホールセール向けデジタル法廷通貨のプロトタイプをCordaで開発へ	→ https://www.bot.or.th/Thai/PressandSpeeches/Press/News2561/n5461e.pdf
インド中銀	法定デジタル通貨のフィージビリティスタディ実施	→ https://economictimes.indiatimes.com/news/economy/policy/rbi-panel-to-study-feasibility-of-digital-currency/articleshow/65601646.cms

6-5) 金融分野
金融機関 – アジア太平洋域

名称	サービス概略	URL
豪州 Commonwealth Bank	世界銀行の債券発行単独主幹事としてブロックチェーン債券で1.1億豪州ドルを起債完了	→ https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million
豪州 Commonwealth Bank	農業資産の管理プラットフォーム開発	→ https://www.finextra.com/newsarticle/32568/cba-applies-blockchain-and-iot-to-agribusiness
豪州 Commonwealth Bank	CSIRO（連邦科学産業研究機構）と保険支払いへの活用を試行	→ https://www.csiro.au/en/News/News-releases/2018/Smart-Money-trial-explores-potential-for-blockchain
豪州ASX	CHESSシステムのリプレイスを半年延期へ	→ https://www.reuters.com/article/asx-blockchain/australias-asx-delays-blockchain-transition-by-6-months-idUSL3N1VQ1KI

6-5) 金融分野
金融機関 – 中東

名称	サービス概略	URL
ドバイ財務省	ペイメントのリコンサイル・セツルメントシステムをローンチ	→ https://www.zawya.com/mena/en/story/Smart_Dubai_Launches_BlockchainPowered_Payment_Reconciliation_and_Settlement_System-ZAWYA20180923101214/
イスラエル証券規制当局ISA	サイバーセキュリティ対策でブロックチェーン利用へ	→ https://www.timesofisrael.com/israel-securities-authority-starts-using-blockchain-for-cybersecurity/

6-5) 金融分野
金融機関 – 日本

名称	サービス概略	URL
大和証券	25社共同による証券ポストトレード業務へのDLT適用協議を発表	→ http://www.daiwa-grp.jp/data/attach/2589_121_20180912a.pdf
SBIグループ	Sコイン実証実験結果を発表	→ http://www.sbigroup.co.jp/news/2018/0925_11269.html → https://imagine-orb.com/【プレスリリース】「sコイン」の実証実験に関す/
SBI RippleAsia	「内外為替一本化コンソーシアム」からxCurrent用いた銀行間セツルメントアプリMoneyTap発表	→ https://moneytap.jp/
楽天証券	KYC共通化への応用を発表	→ https://www.rakuten-sec.co.jp/web/company/newsrelease/pdf/press20180925.pdf

6-5) 金融分野
金融機関 – 業界コンソーシアム

名称	サービス概略	URL
komgo	シェル・MUFG・Societe Generaleなど、コモディティ向けトレードファイナンスkomgo開発を発表	→ https://komgo.io/wp-content/uploads/2018/09/130918-komgo-launch-press-release.pdf
Interbank Information Network	JP MorganによるQuorumベースの銀行間決済システムInterbank Information Network、75銀行参加して実証実験へ	→ https://www.jpmorgan.com/pages/detail/1320570135560 → https://www.jpmorgan.com/pages/detail/1320562088910 → https://www.coindesk.com/over-75-new-banks-jpmorgan-expands-blockchain-payments-trial/

7.参考資料リンク集

① イベント
② 教材
③ 統計情報
④ レポート
⑤ 論文リスト

イベント（1/6）

開催日・開催地	名称	URL
6/15@Tokyo	「仮想通貨交換業等に関する研究会」（第４回）議事録	→ https://www.fsa.go.jp/news/30/singi/20180615-2.html
7/3-7/4@Lisbon	Building on Bitcoin	→ https://building-on-bitcoin.com/ → https://www.youtube.com/channel/UCCP7NPTxVrt01-FlSiWYSzQ → https://twitter.com/build_on_btc/status/1047852453721460736?s=21
8/10-8/12 @Bangalore	ETHIndia	→ https://ethindia.co/ → https://ethindia.co/livestream/ → https://forum.livepeer.org/t/transcoder-campaign-livepeer-emerging-markets-0x8909/295 → https://youtu.be/NWRE5H50pQ4 → https://blog.lendroid.com/eth-india-pleasant-with-a-forecast-of-crypto-47aac9925928 → https://m.youtube.com/watch?v=wDFq6wiACwk
8/17-8/19 @Santa Barbara	CRYPTO 2018	→ https://crypto.iacr.org/2018/affevents/cryptocurrencies/page.html

イベント（2/6）

開催日・開催地	名称	URL
9/1@Berlin	Lightning Hackday #3	→ https://lightninghackday.fulmo.org/ → https://www.youtube.com/watch?v=QrX1SpD6l9g → https://the-lightning-times.ongoodbits.com/2018/09/04/issue-3
9/5@Berlin	Zero Knowledge Summit	→ https://www.reddit.com/r/ethdev/comments/9gjzu4/zero_knowledge_summit_zk0x02_recap/ → https://blockchainweek.berlin/events/zero-knowledge-summit/
9/7-9/9@Berlin	ETHBerlin	→ https://ethberlin.com/ → https://ethberlin.com/livestream/
9/12、Tokyo	金融庁 仮想通貨交換業等に関する研究会（第5回）	→ htthttps://www.fsa.go.jp/news/30/singi/20180912-2.html
9/19-9/20 @Singapore	Consensus Singapore	→ https://youtu.be/z98Sh3ldRNk
9/21-23 @Tbilisi, Georgia	World Digital Mining Summit	→ http://miningconf.org/ → https://www.youtube.com/watch?v=t3Vp7gIxqHk → https://youtu.be/8llaf3k2Bt4 → https://youtu.be/5M7kctekfB4

イベント（3/6）

開催日・開催地	名称	URL
9/22-23@Riga	Baltic Honeybadger 2018 / The Bitcoin conference of the year	→ https://bh2018.hodlhodl.com/ → http://diyhpl.us/wiki/transcripts/baltic-honeybadger/2018/ → https://youtu.be/66ZoGUAnY9s → https://youtu.be/D2WXxgZ8h-0 → https://youtu.be/PN88h-d09qs
10/3@Tokyo	「仮想通貨交換業等に関する研究会」（第６回）	→ https://www.fsa.go.jp/news/30/singi/20181003.html → https://www.fsa.go.jp/news/30/singi/20181003-2.html
10/4-10/5 @Tokyo	Bitcoin Edge Dev++ / BC2 TECHNICAL BOOTCAMP	→ https://keio-devplusplus-2018.bitcoinedge.org/#speakers → http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/edgedevplusplus/ → https://youtu.be/WcOIXsOLJ3w → https://youtu.be/EUUQbveGF5E → https://youtu.be/iPt2ekHoEy8
10/6-10/7 @Tokyo	ScalingBitcoin	→ https://scalingbitcoin.org/ja/ → https://tokyo2018.scalingbitcoin.org/#schedule → http://diyhpl.us/wiki/transcripts/scalingbitcoin/tokyo-2018/ → https://www.youtube.com/channel/UCmwaDulmQtX-H8FOSQTKqMg

イベント（4/6）

開催日・開催地	名称	URL
10/6@Berlin	ETHSecurity	→ https://github.com/ethsecurity/berlin-workshop/blob/master/README.md → https://blockchainweek.berlin/events/security-unconf-by-secureth/
10/5-10/7 @San Francisco	ETH San Francisco	→ https://ethsanfrancisco.com/ → https://youtu.be/BkMZdbzKZ9k → https://twitter.com/kylesamani/status/1050921181371613184?s=21
10/8-10/10 @Tokyo	Bitcoin Core Dev Tech	→ https://coredev.tech/ → https://diyhpl.us/wiki/transcripts/bitcoin-core-dev-tech/
10/10-10/11 @San Francisco	CryptoEconomics Security Conference	→ https://cesc.io/
10/16-10/18 @Gargnano Italy	Satoshi's Vision Conference	→ https://satoshisvisionconference.com/ → https://www.youtube.com/channel/UCJHGWgmZdkQlZA28fuGfNmA
10/19@Tokyo	「仮想通貨交換業等に関する研究会」（第７回）	→ https://www.fsa.go.jp/news/30/singi/20181019.html
10/22-10/25 @NYC	Lightning Residency	→ https://twitter.com/chaincodelabs/status/1042474160042201094?s=21
10/29@Prague	D1Conf	→ https://d1conf.com/

イベント（5/6）

開催日・開催地	名称	URL
10/22-10/24 @Berlin	Web3 Summit	→ http://web3summit.com/ → https://web3summit.com/tickets/ → https://medium.com/web3foundation/web3-summit-tickets-on-sale-a9a72a691990 → https://web3summit.com/program/main-space/ → https://medium.com/web3foundation/web3-summit-a-recap-3f53d14de87e → https://twitter.com/lrettig/status/1054499500058910720?s=21 → https://twitter.com/lrettig/status/1054650753309175809?s=21 → https://twitter.com/lrettig/status/1055011753938030593?s=21 → https://www.youtube.com/channel/UClnw_bcNg4CAzF772qEtq4g → https://twitter.com/i/moments/1056170029656535040
10/24 @Tokyo	第1回　納税環境整備に関する専門家会合	→ http://www.cao.go.jp/zei-cho/gijiroku/noukan/20181024/30noukan1kai.html
10/27-10/28 @NYC	Lightning Network Hackday New York City	→ https://lightninghackday.fulmo.org/ → https://youtu.be/FGxFd944jMg → https://youtu.be/bFQINN_mQpc

イベント（6/6）

開催日・開催地	名称	URL
10/30-11/2 @Prague	Devcon4	→ https://blog.ethereum.org/2018/05/11/devcon4-announcement/ → https://blog.ethereum.org/2018/07/03/devcon4-ticket-sales/ → https://blog.ethereum.org/2018/07/17/an-update-on-devcon4-ticket-allocations-and-sales/ → https://docs.google.com/spreadsheets/d/e/2PACX-1vTmQ1maZLMDSo3r7wVCzwMadNUCGctmE5byRgv1za6R52wTUgZw-XB9P9dNO7-QBRka1AAwKrXO4kTP/pubhtml#
11/7-11/11 @Krakow	SteemFest3	→ https://steemit.com/steemfest/@roelandp/save-the-date-steemfest-krakow-poland-7-8-9-10-11-november-hotel-packages-now-available
1/30-2/1 @Stanford	Stanford Blockchain Conference	→ https://cyber.stanford.edu/sbc19

教材

- Crypto Reading List（a16zのCrypto Canonをうけて）
  - https://thecontrol.co/crypto-reading-list-c54da8cab26a
- BUIDLにむけたConsenSysによる非技術者のためのスキルアップリスト
  - https://media.consensys.net/how-to-buidl-on-the-blockchain-if-youre-not-a-dev-29fba4139b1f
- Mastering Ethereumのコンテンツ
  - https://github.com/ethereumbook/ethereumbook/find/develop?q=
- Ethereum開発者向けツールリスト
  - https://qiita.com/sot528/items/6ff13ebfc846aa313307
- Ethereumにおけるセキュリティに関するリソースリスト
  - https://github.com/trailofbits/awesome-ethereum-security/blob/master/README.md

教材

- クリプトエコノミクス分野のリソースリスト
  - https://blockchain-society.science/2018/09/25/a-curated-list-of-awesome-resources-for-cryptoeconomics-research/
- Plasmaの学習サイト
  - https://www.learnplasma.org/
- Statechannelの学習サイト
  - https://www.learnchannels.org/
- LayerXのScrapbox
  - https://scrapbox.io/layerx/
- Cryptoeconomics LabのScrapbox
  - https://scrapbox.io/cryptoeconimicslab/
- 東工大の暗号通貨講義コースカリキュラム
  - http://www.ocw.titech.ac.jp/index.php?module=General&action=T0300&GakubuCD=4&GakkaCD=342222&KeiCD=22&course=22&KamokuCD=342222&KougiCD=201804021&Nendo=2018&vid=03

教材（過去分の再掲①）

- Crypto Canon / a16zによる暗号通貨関連リンク集
  - http://a16z.com/2018/02/10/crypto-readings-resources/
- Cryptoacademia / Comprehensive collection of papers and other resources compiled and managed by Blockchain at Berkeley
  - https://drive.google.com/drive/mobile/folders/0B7TsBdkClBm1c3lzaHBneEt1dU0
- BITCOIN RESOURCES
  - https://lopp.net/bitcoin.html
- Bitcoin Edge Workshops
  - https://bitcoinedge.org/tutorials
  - 2017年11月のScalingBitcoin前にStanfordで開催されていたワークショップの模様が動画公開
- Sixty free lectures from Princeton on bitcoin and cryptocurrencies
  - https://www.reddit.com/r/Bitcoin/comments/7m0gu3/sixty_free_lectures_from_princeton_on_bitcoin_and/

教材（過去分の再掲②）

- 暗号通貨ツールリンク
  - http://individua1.net/cryptocurrency-tools/
- Deep Dives - Blockchain at Berkeley Research and Development
  - https://docs.google.com/document/d/12w7rAEQUSFd6NbLr6dUxJcLbF70YHcnzhG6mHZQjYCA/edit
- おすすめの暗号通貨系YouTubeチャンネル、ポッドキャスト（英語）
  - http://individua1.net/recommendable-cryptocurrency-youtube-channel-podcast/
- Banking On Bitcoin - Full Documentary Film
  - https://youtu.be/7Jts0OMAhTw
- Learning Bitcoin From Command Line
  - https://github.com/ChristopherA/Learning-Bitcoin-from-the-Command-Line
- Mastering Ethereum、GitHubにコンテンツ
  - https://github.com/ethereumbook/ethereumbook/blob/develop/README.md

教材（過去分の再掲③）

- プリンストン大学のビットコイン講義のスライド&動画
  - https://piazza.com/princeton/spring2015/btctech/resources
- Courseraによる暗号通貨コース教材
  - https://www.coursera.org/learn/cryptocurrency
- Ethereumリーディングリスト
  - https://github.com/Scanate/EthList/blob/master/README.md

教材（過去分の再掲③）

- とりあえずド素人が読むべきブロックチェーン入門論文・書籍・サイト
  - https://qiita.com/onokatio/items/7db58947b05c17d1f44e
- カリフォルニア大学バークレー校のビットコインと仮想通貨無料オンライン講座
  - http://kaatcrypto.com/cryptclass
- ConsenSys Academyの開発者向けコース
  - https://github.com/ScottWorks/ConsenSys-Academy-Notes?files=1
- Stanford大学の暗号学講義テキスト
  - http://toc.cryptobook.us/
- Learn Blockchain
  - https://learnblockcha.in/

統計情報
①交換所

- トレードボリューム順の交換業者ランキング
  - https://coinmarketcap.com/rankings/exchanges/
- 交換所ランキング
  - https://www.blockchaintransparency.org/exchangerankings/
- 暗号通貨交換業者のグローバルファンダメンタルズランキング
  - https://twitter.com/bestofbritish96/status/1040336941546438657?s=21
- 交換業者の格付けサイト
  - https://platform.cryptoexchangeranks.com/#/mobile/rating
  - https://icorating.com/pdf/59/1//96s8XtOZ3Op87iYjRqwzXQPRXhC4CoTweFvyUCzN.pdf
- Coinbase、アクティブユーザー数の推移
  - 2017Q3と比べ30%増も、2018Q1比では70%減。取引高は2017Q3比で80%減
  - https://diar.co/volume-2-issue-40/

統計情報
②Bitcoin

- Bitcoin Cashのノード分布比率
  - https://cash.coin.dance/nodes

- Bitcoin Cash Wormholeのエクスプローラー
  - https://blockchair.com/bitcoin-cash/wormhole

統計情報
③Ethereum

- トランザクションからの関数コール
  - https://plot.ly/~johannespfeffer/37/#/

- スマートコントラクトからの関数コール
  - https://plot.ly/~johannespfeffer/35/#/

統計情報
④ICO

- 2018年のICO調達額の月次トレンド
  - https://www.icodata.io/stats/2018
- ICO（Elementus社）
  - https://elementus.io/blog/ico-market-august-2018/
- ICO統計
  - https://twitter.com/tokendata/status/1046744176593960960?s=21
- ICO統計
  - https://twitter.com/lawmaster/status/1046834490289664005?s=21
- ICO統計
  - https://next.autonomous.com/thoughts/crypto-september-icos-90-down-from-january-but-venture-funding-is-ray-of-hope
- 証券トークン
  - https://stocheck.com/stos

統計情報
⑤規制

- 各国の仮想通貨規制（米国議会図書館）
  - https://www.loc.gov/law/help/cryptocurrency/world-survey.php

- 米国・欧州間で進むクリプト関連規制の主導権について
  - https://www.trustnodes.com/2018/09/16/europe-rises-to-embrace-icos

統計情報
⑥VC投資

- ブロックチェーン領域へ投資するファンド・エンジェルリスト
  - https://twitter.com/lawmaster/status/1046834490289664005?s=21

- クリプトVC上位30社リスト（暗号通貨・ブロックチェーンプロジェクト数の順）
  - https://thenextweb.com/hardfork/2018/08/09/cryptocurrency-blockchain-investments/

- Blockchain Capitalが投資する仮想通貨・ブロックチェーン企業の一覧
  - https://ico-post.com/vc/blockchain-capital/

ZAIFのハッキング被害

日付	概要	URL
9/20	Zaif、入出金用ホットウォレットの一部がハッキング被害に遭ったことを発表。被害額は5966BTC（MONAおよびBCH含め総額約70億円相当）	https://prtimes.jp/main/html/rd/p/000000093.000012906.html http://d.hatena.ne.jp/Kango/20180920/1537414861 https://prtimes.jp/main/html/rd/p/000000094.000012906.html
9/20	フィスコ、テックビューロへシステム面・金融面でサポート実施へ	http://www.fisco.co.jp/uploads/20180920_fisco_pr.pdf https://www.caica.jp/wp-content/uploads/pdf/2018/20180920_1_oshirase.pdf
9/25	近畿財務局、テックビューロへ業務改善命令。テックビューロはこれを受けて改善計画書を提出	http://kinki.mof.go.jp/file/rizai/pagekinkihp025000049.html https://corp.zaif.jp/info/10225/ https://corp.zaif.jp/info/10252/
10/10	テックビューロ、Zaif事業をフィスコ仮想通貨取引所へ譲渡する事業譲渡契約を締結。事業譲渡日は11/22	https://prtimes.jp/main/html/rd/p/000000098.000012906.html http://www.fisco.co.jp/uploads/20181010_fisco_ir.pdf

レポート
①ビットコイン

名称	URL
ビットコインクライアントをめぐるBitcoin Coreとの競争について	https://blog.bitmex.com/bitcoin-cores-competition/
Tether発行によるビットコイン価格への影響は軽微との論文	https://www.sciencedirect.com/science/article/pii/S0165176518302556
マイニングマルウェアレポート	https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf
Bitcoin・Bitcoin Cash・Ethereum・Litecoin・MoneroといったPoWチェーンにおける電力消費量の定量化について	https://www.ofnumbers.com/2018/08/26/how-much-electricity-is-consumed-by-bitcoin-bitcoin-cash-ethereum-litecoin-and-monero/
仮想通貨交換所のセキュリティ対策についての考え方（パブリックドラフト）	https://t.co/5vQN7Ok62i

レポート
②デジタルアセット

名称	URL
Circleのアセットチェックフレームワーク	https://www.circle.com/marketing/pdfs/en/circle-asset-framework.pdf
金融安定理事会FSBのクリプトアセットマーケットレポート	http://www.fsb.org/2018/10/crypto-asset-markets-potential-channels-for-future-financial-stability-implications/
BlockchainによるStablecoinレポート	https://www.blockchain.com/ja/research
トークンエコシステムについて	https://outlierventures.io/wp-content/uploads/2018/03/Token-Ecosystem-Creation-Outlier-Ventures-1.pdf
クリプトアセット分類レポート	https://www.cryptocompare.com/media/34478555/cryptocompare-cryptoasset-taxonomy-report-2018.pdf https://twitter.com/thedailybitnews/status/1052612786675732481?s=21
Satis Groupによるクリプトアセットバリュエーション	https://research.bloomberg.com/pub/res/d37g1Q1hEhBkiRCu_ruMdMsbc0A

レポート
③ブロックチェーン全般

名称	URL
Gartnerのブロックチェーンレポート	https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/
IDCによるブロックチェーン関連市場予測レポート	https://www.idcjapan.co.jp/Press/Current/20180905Apr.html
Cambridge大によるDLTシステムフレームワークレポート	https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-08-20-conceptualising-dlt-systems.pdf

レポート
④特定分野 – 中央銀行

名称	URL
中央銀行デジタル通貨について	https://www.omfif.org/media/5415789/ibm-central-bank-digital-currencies.pdf
ペイメントシステムにおけるプライバシーの重要性について、セントルイス連邦準備銀行のレポート	https://research.stlouisfed.org/publications/review/2018/07/16/payment-systems-and-privacy

レポート
④特定分野 – AML

名称	URL
Ciphertraceによる暗号通貨AMLレポート	https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf
米シンクタンクCenter on Sanctions and Illicit Financeによるレポート	https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-yfanusie-20180907.pdf
暗号通貨に係るAML規制	http://www.allenovery.com/publications/en-gb/Documents/AML18_AllenOvery.pdf

レポート
④特定分野 – 規制

名称	URL
規制動向まとめレポート	https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations
BIS、仮想通貨規制に関するレポート	https://www.bis.org/publ/qtrpdf/r_qt1809f.htm https://www.bis.org/publ/qtrpdf/r_qt1809f.pdf
ニューヨーク州検事総長事務局による仮想通貨交換業者レポート	https://virtualmarkets.ag.ny.gov/

レポート
④特定分野 –特定業界への応用

名称	URL
Stanford大によるソーシャルインパクト向けブロックチェーン活用に関するレポート	https://www.gsb.stanford.edu/faculty-research/publications/blockchain-social-impact
Microsoftより、分散IDについてホワイトペーパー発表	https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY
BCGによるコモディティ取引とブロックチェーンに関するレポート	https://www.bcg.com/ja-jp/publications/2018/reality-check-blockchain-commodity-trading.aspx
PwCと世界経済フォーラムによる環境保護への応用レポート	https://www.pwc.com/gx/en/sustainability/assets/blockchain-for-a-better-planet.pdf
電力業界におけるブロックチェーン利用の方向性(P2P電力取引の事業機会と課題)	http://www.keieiken.co.jp/pub/infofuture/backnumbers/59/report03.html
サプライチェーンファイナンスに関する世界経済フォーラムのレポート（P8-P10）	http://www3.weforum.org/docs/White_Paper_Trade_Tech_report_2018.pdf

2018 3Qの関連論文リスト(1/8)

タイトル	URL
Distributed Ledger Technology Systems: A Conceptual Framework	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013
Tokenomics: Dynamic Adoption and Valuation	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3153860
Erays: Reverse Engineering Ethereum's Opaque Smart Contracts	→ https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-zhou.pdf
Economics of Blockchain	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751
米NSAによる匿名電子キャッシュに関する暗号の論文（1996年）	→ http://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm
SoK: A Consensus Taxonomy in the Blockchain Era	→ https://eprint.iacr.org/2018/754
Is Bitcoin Really Un-Tethered?	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066
A Discourse on Token Valuation	→ https://savantspecter.github.io/research/A_DISCOURSE_ON_TOKEN_VALUATION.pdf

2018 2Qの関連論文リスト(2/8)

タイトル	URL
RapidChain: Scaling Blockchain via Full Sharding	→ https://eprint.iacr.org/2018/460.pdf
Security of the Blockchain against Long Delay Attack	→ https://eprint.iacr.org/2018/800
Bitcoin Mining: A Game Theoretic Analysis	→ https://eprint.iacr.org/2018/780
Liberal Radicalism: Formal Rules for a Society Neutral Among Communities	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3243656 → https://medium.com/coinmonks/breaking-down-buterin-hitzig-and-weyls-liberal-radicalism-paper-ba5192248b2
Distributed Ledger Technology Systems: A Conceptual Framework	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013
Wasabi: A Framework for Dynamically Analyzing WebAssembly	→ https://arxiv.org/abs/1808.10652
An Efficient Framework for Concurrent Execution of Smart Contracts	→ https://arxiv.org/abs/1809.01326
Pitchforks in Cryptocurrencies: Enforcing rule changes through offensive forking- and consensus Techniques	→ https://eprint.iacr.org/2018/836
BITE: Bitcoin Lightweight Client Privacy using Trusted Execution	→ https://eprint.iacr.org/2018/803

2018 2Qの関連論文リスト(3/8)

タイトル	URL
Aurora: Transparent Succinct Arguments for R1CS （SNARKsからSTARKsそしてSNARGsへ）	→ https://eprint.iacr.org/2018/828
Coin-Operated Capitalism	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3215345
Towards a Smart Contract-based, Decentralized, Public-Key Infrastructure	→ https://eprint.iacr.org/2018/853
Decentralized P2P Energy Trading under Network Constraints in a Low-Voltage Network	→ https://arxiv.org/abs/1809.06976
A Game-Theoretic Analysis of Shard-Based Permissionless Blockchains	→ https://arxiv.org/abs/1809.07307
Block Chain based Intelligent Industrial Network (DSDIN)	→ https://arxiv.org/abs/1809.06551
An Overview of Blockchain and Consensus Protocols for IoT Networks	→ https://arxiv.org/abs/1809.05613
A blockchain framework for smart mobility	→ https://arxiv.org/abs/1809.05785
Formal Barriers to Longest-Chain Proof-of-Stake Protocols	→ https://arxiv.org/pdf/1809.06528.pdf
Fraud Proofs: Maximising Light Client Security and Scaling Blockchains with Dishonest Ma jorities	→ https://arxiv.org/pdf/1809.09044.pdf
Proving the correct execution of concurrent services in zero-knowledge	→ https://eprint.iacr.org/2018/907

2018 2Qの関連論文リスト(4/8)

タイトル	URL
Defining the Collective Intelligence Supply Chain	→ https://arxiv.org/abs/1809.09444
An Agile Software Engineering Method to Design Blockchain Applications	→ https://arxiv.org/abs/1809.09596
Chaos and Order in the Bitcoin Market	→ https://arxiv.org/abs/1809.08403
A privacy-preserving, decentralized and functional Bitcoin e-voting protocol	→ https://arxiv.org/abs/1809.08362
Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory	→ https://arxiv.org/abs/1809.08387
Trusted Multi-Party Computation and Verifiable Simulations: A Scalable Blockchain Approach	→ https://arxiv.org/abs/1809.08438
Split-Scale: Scaling Bitcoin by Partitioning the UTXO Space	→ https://arxiv.org/abs/1809.08473
On Using Blockchains for Safety-Critical Systems	→ https://arxiv.org/abs/1809.08877
Formal Barriers to Longest-Chain Proof-of-Stake Protocols	→ https://arxiv.org/abs/1809.06528
Privacy in Blockchain Systems	→ https://arxiv.org/abs/1809.10642
Bitcoin and Sentiment	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230572

2018 2Qの関連論文リスト(5/8)

タイトル	URL
Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains	→ https://arxiv.org/abs/1804.03903
Lightning Factories	→ https://ia.cr/2018/918
Compact Multi-Signatures for Smaller Blockchains	→ https://eprint.iacr.org/2018/483.pdf
Risks and Returns of Cryptocurrency	→ https://economics.yale.edu/sites/default/files/files/Faculty/Tsyvinski/cryptoreturns%208-7-2018.pdf
The Economic Limits of Bitcoin and the Blockchain	→ https://faculty.chicagobooth.edu/eric.budish/research/Economic-Limits-Bitcoin-Blockchain.pdf
Blockchain Upgrade as a Coordination Game	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192208
BitML: A Calculus for Bitcoin Smart Contracts	→ https://eprint.iacr.org/2018/122.pdf
Compact Sparse Merkle Trees	→ https://eprint.iacr.org/2018/955
Survey of Consensus Protocols	→ https://arxiv.org/abs/1810.03357
The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin	→ https://arxiv.org/pdf/1810.02466.pdf

2018 2Qの関連論文リスト(6/8)

タイトル	URL
The Use of Smart Contracts and Challenges	→ https://arxiv.org/abs/1810.04699
Constructing Trustworthy and Safe Communities on a Blockchain-Enabled Social Credits System	→ https://arxiv.org/abs/1809.01031
Blockchain access control Ecosystem for Big Data security	→ https://arxiv.org/abs/1810.04607
The Curses of Blockchain Decentralization	→ https://arxiv.org/abs/1810.02937
The Two Token Waterfall	→ https://tokenwaterfall.io/
Fast Multiparty Threshold ECDSA with Fast Trustless Setup	→ http://stevengoldfeder.com/papers/GG18.pdf
Initial Coin Offerings and the Value of Crypto Tokens	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137213
Antitrust and Costless Verification: An Optimistic and a Pessimistic View of the Implications of Blockchain Technology	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3199453
On the Instability of Bitcoin Without the Block Reward	→ http://randomwalker.info/publications/mining_CCS.pdf
Zexe: Enabling Decentralized Private Computation	→ https://eprint.iacr.org/2018/962

2018 2Qの関連論文リスト(7/8)

タイトル	URL
Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody	→ https://eprint.iacr.org/2018/987
PaLa: A Simple Partially Synchronous Blockchain	→ https://eprint.iacr.org/2018/981
PiLi: An Extremely Simple Synchronous Blockchain	→ https://eprint.iacr.org/2018/980
Algorithmic Blockchain Channel Design	→ https://arxiv.org/abs/1810.07603
On the Origins and Variations of Blockchain Technologies	→ https://arxiv.org/abs/1810.06130
Cryptocurrency Pump-and-Dump Schemes	→ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3267041
QuisQuis: A New Design for Anonymous Cryptocurrencies	→ https://eprint.iacr.org/2018/990
The Two Token Waterfall	→ https://tokenwaterfall.io/
Scalable, Efficient, and Consistent Consensus for Blockchains	→ https://arxiv.org/abs/1808.02252
Niji: Bitcoin Bridge Utilizing Payment Channels	→ https://arxiv.org/abs/1810.10194
Using Ethereum Registration Authorities to Establish Trust for Ethereum Private Sidechains	→ https://jbba.scholasticahq.com/jbba.scholasticahq.com

2018 2Qの関連論文リスト(8/8)

タイトル	URL
Blockchain-based Supply Chain Traceability: Token Recipes model Manufacturing Processes	→ https://arxiv.org/abs/1810.09843
Traceability Decentralization in Supply Chain Management Using Blockchain Technologies	→ https://arxiv.org/abs/1810.09203
Security Services Using Blockchains: A State of the Art Survey	→ https://arxiv.org/abs/1810.08735
What's Really Driving the Cryptocurrency Phenomenon?	→ https://iterative.capital/thesis/
Enter the Crypto Idea Maze	→ https://jonchoi.com/cryptoideamaze/

お役に立てば嬉しいです

- **BTCアドレス**

  1LGC2U2kbAoVCK2VUdLasUcv1kCzZxSBjK

→おしまい