【BMA2018 秋季大会講演スライド】

ブロックチェーン最前線

福島良典｜株式会社 LayerX 代表取締役社長、株式会社 Gunosy 取締役ファウンダー

略歴

東京大学大学院工学系研究科修了。大学院在学中に「Gunosy（グノシー)」のサービスを開発し、2012 年 11 月に株式会社 Gunosy を創業、代表取締役に就任後、2013 年 11 月代表取締役最高経営責任者に就任。2012 年度 IPA 未踏スーパークリエータ。2018 年 8 月より AnyPay と Gunosy の合弁会社「 株式会社 LayerX 」の代表取締役に就任。

Agenda

１：LayerXについて

２：ブロックチェーンビジネス最前線

３：LayerXでの活用事例

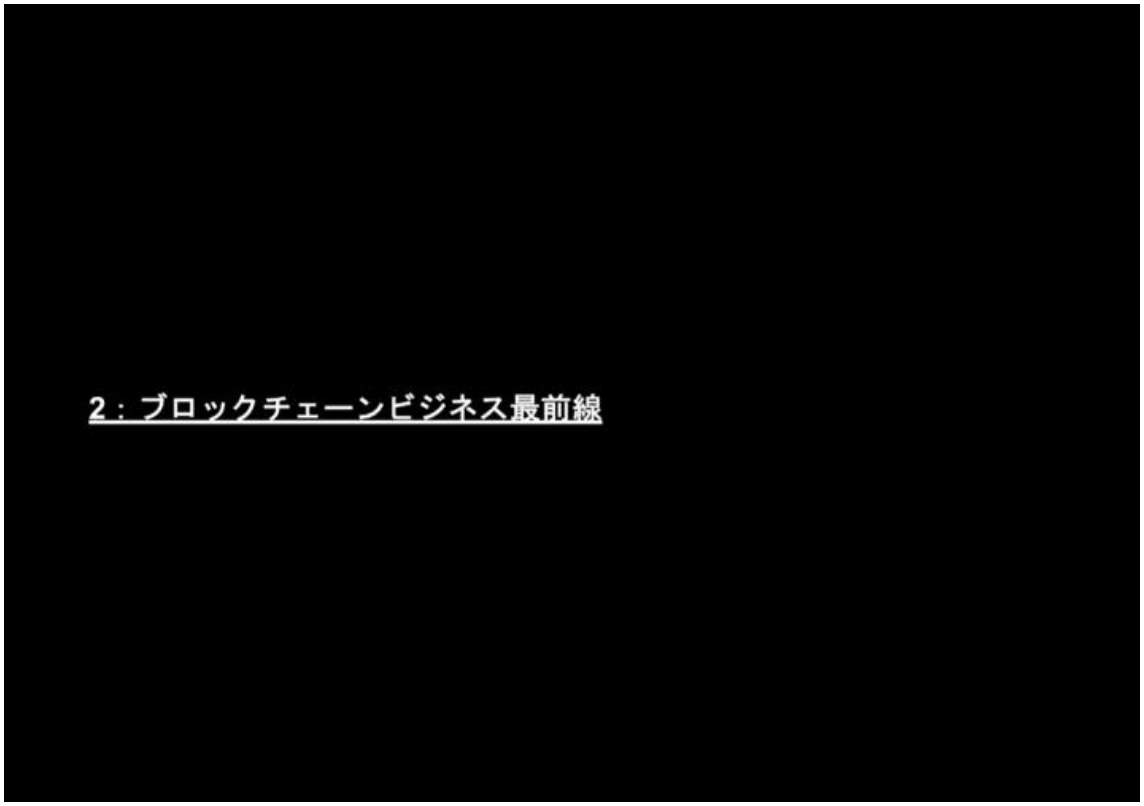
１：LayerXについて

事業概要

LayerX

フィジビリティスタディやコード監査、開発サポート、コンサルティングと、形態にこだわらずお客様に最適なソリューションをご提供。一方で、ブロックチェーン技術はまだ発展途上であるため、実世界への浸透のために、ビジネスのための事業のみならず、R&Dやコミュニティ育成を行い、業界全体への貢献も重視している。

技術とビジネスの両方が弊社の強み。
ご要望に応じてカスタムメイドなサービスを提供させていただきます。



トレンドの変化

LayerX

2017-2018年	現在
独自トークンを発行し、ICOを行い、トークン設計を複雑に考える	ICOのためのトークンは無駄。equityで調達し、トークンはシンプルに。経済圏をどうやってコントラクトで置き換えるか、その規格(スタンダード、プロトコル)をつくるか
ICOで集めたお金は、非中央集権なプロトコルやアプリケーションの実現に使っていく	プロトコルの非中央集権性は重要だが、アプリケーションは中央集権で良いよね。またプロトコルにも中央集権性をみとめて現実的に実現していこう
仮想通貨の価格高騰やICOバブル、取引所ビジネスの急成長により、投機や取引所ビジネスに注目が集まる	仮想通貨やICOバブルの崩壊により、本質的にブロックチェーンがコスト構造を変えるところはどこか、技術的な課題をどう解決するかに投資が集中

CryptoFundの動向

LayerX

Placeholder Capital

「中央集権なアプリを分散化したプロトコル上に作るのが良い組み合わせ」

Pantera Capital

「① exchange領域 ② Custodian領域 ③ Scalability領域 ④ アセットマネジメントや機関投資家向けTradingの領域 ⑤ Enterprise Blockchain領域 ⑥ マーケットプレイスを作る領域」

Union Square Ventures

「インフラ整ってからキラーアプリが生まれるのではなく、キラーアプリが生まれてからそれをマスが使うためのインフラが整備される」

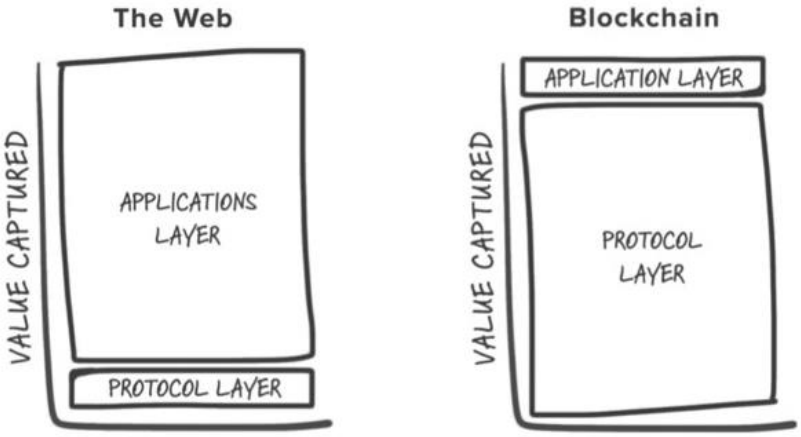
1Confirmation

「アプリケーション層が世の中に広まる前に、必ずプロトコルレイヤー・ミドルウェアレイヤーの発展が必要なので、そこに継続して投資していく。」

世界で最も情報が集まるcrypto fundも、現実的な応用例を作る。そしてその下にできるスタンダードやプロトコル、ゲートウェイに注目し、集中的に投資する傾向がある

Fat Protocol 「富むプロトコル、貧するアプリケーション」

LayerX

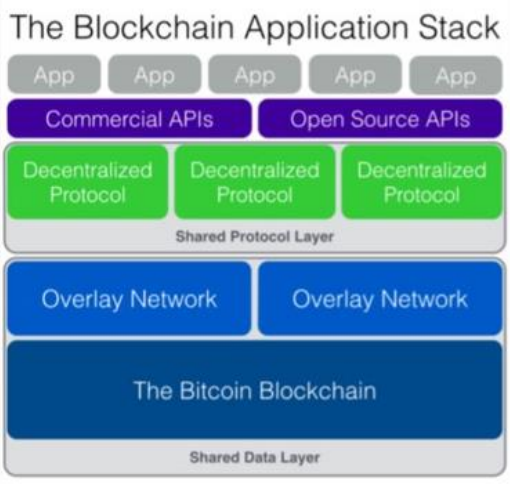


出所: http://www.usv.com/blog/fat-protocols

USVにより提唱された概念。ブロックチェーンビジネスを理解する上で重要な概念となる「fat protocol」。
Webではアプリケーションレイヤーへの投資が高いリターンをもたらした。ブロックチェーンではプロトコルレイヤーへの投資が高いリターンを生むという概念。

The Blockchain Application Stack

LayerX

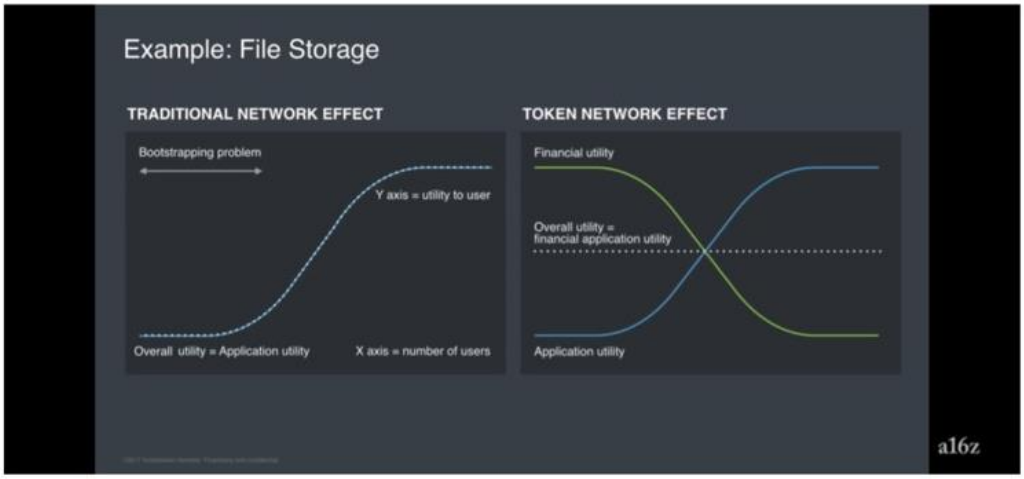


出所: https://www.coindesk.com/blockchain-application-stack/

プロトコルにも大きく、Shared Data Layer層とShared Protocol Layer層がある。
どのPJがどの層の話をしているかを意識することがとても大事

Bootstrapping problem「はやく賭ける」

LayerX

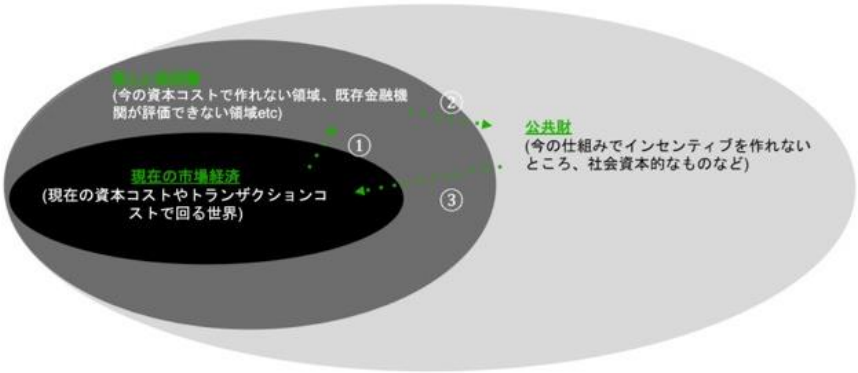


出所:https://www.youtube.com/watch?v=yiRCdMgkkFY

プロトコルのマネタイズが可能になった、というのが大きな流れ。多くのプロトコルは「Bootstrapping problem」を抱えるが、トークン化し、流動性を得ることで価値の配分が「はやく」来る。また最近ではstakingして収益を得る、ガバナンストークンとユーティリティトークンを分離するモデルが増えてきている。

Why Blockchain? 「ブロックチェーンでしかできないこと」

LayerX



① 今の市場経済で**アクセスが難しい、新しい経済圏**の調達手段

② 今の市場経済では**インセンティブをつくるのが難しい、公共財**のエコシステム

③ 今の市場経済で**中央集権的で非効率な部分**の非中央化

Fat protocol? Fat Dapp? Fat wallet?

LayerX

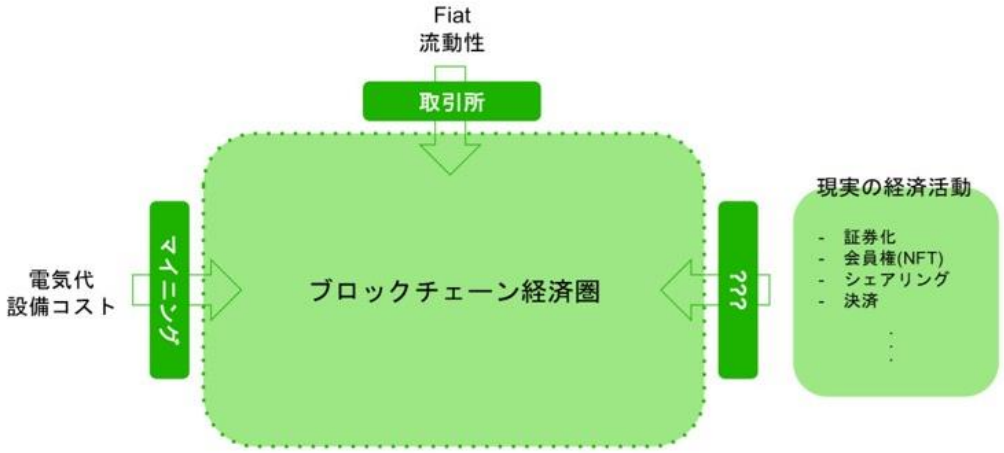
出所:https://twitter.com/ricburton/status/987706443896967169

ユーザー向けに様々なDappやその入口としてのウォレットが提供されているが
まずブロックチェーンが普及するのは金融系とそのプロトコル領域である

LayerXが考える重要領域

LayerX

現実の経済活動 -> ブロックチェーンが次の大波



黎明期は、PoWマイニングによるコストの投入により、ブロックチェーン資産が作られた。取引所の誕生によって流動性ができ
価値がついた。その流れの勝者が「取引所」と「マイニング」である。Ethereum誕生以降、より現実経済に即したものが
ブロックチェーンにのってくる。ここが次の大波

LayerXが考える最新トレンド

LayerX

① ICO用に無駄なトークンを作らない

ICOのユーティリティトークン -> 失敗に終わる, PJや経済合理性をゆがめる
資金調達はSTO, トークン設計は本質的なガバナンストークンに
経済圏の理解と、スマトートコントラクトをどう設計するかが大事

② スタンダード(規格)をつくる

ERC20, ERC721だけでなく、様々なトークンスタンダードが提案されて、規格をつくりエコシステムを構築していくことが重要
(ex)
ERC725(Identity Standard) <- origin protocol
ERC1068(Loan Standard),
ERC1155(crypto item standard),
ERC1337(Subscription Standard),
ERC1400(Security Token Standard) <- polymath, habor, Securitize, Openfinance etc

③ decentralizedなプロトコル, centralizedなアプリケーション

IOU型のstablecoin, asset backed tokenの競争が今最も激しい。
発想としてはdecentralizedなプロトコルが提供するコスト削減に乗りながら、難しいところは中央集権的に実用的にしていくというもの

事例A: セキュリティトークンスタンダード(①, ②の事例)

LayerX

- EIPでは1400で提案(Polymathの提案)
- R-token, DS protocol, ST-20, S3(Smart Securities Standard)などが規格競争
- 基本的な発想はトランスファーの制限(KYC/AMLやSecurity Lawの強制執行)と自由なメタデータの表現(優先株、配当条件、劣後条件etc), ガバナンスのコントラクト化(議決権投票など)

主要PJ

POLYMATH THE SECURITIES TOKEN PLATFORM　HARBOR　OpenFinance NETWORK　Securitize

特徴・要件

- transferが成功するor失敗するならその理由を返すということをチェック出来るようなインターフェースが必要
- 法的措置(legal action)やリカバリ(fund recovery)のためのforce transferが必要
- トークンの発行(issuance, mintのこと)と買い戻し(redemption, burnのこと)する時のeventが必要
- ある株主(shareholder)固有の権利やtransferを制限するためのメタデータが必要
- transfer時に渡すパラメータ・on-chainのデータ・off-chainのデータに基づいて、transfer時にメタデータを書き換えられることが必要
- バリデーションのためにtransfer時にsigned dataを送ることがおそらく必要
- アセットのクラスを特定のものに制限すべきではない
- ERC20, ERC777と互換性を持つほうが良い

事例B: stable coin, asset backed token(③の事例)

LayerX

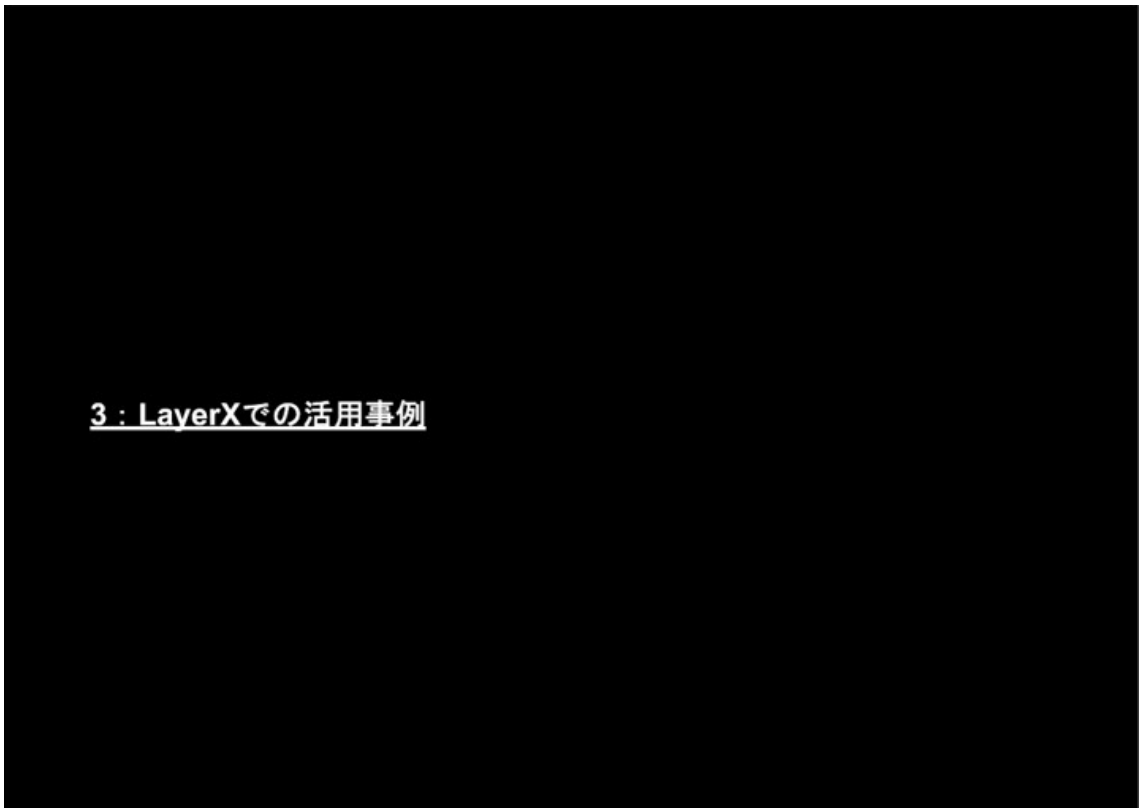
- IOU型, crypto担保型, シニョリッジシェア型の3種類がある
- 特に直近はSTOの文脈とも絡めたIOU型が注目
- ブロックチェーン上に資産を発行する際、オラクルの問題が発生する(Tetherの残高問題)。ここの問題をうまく既存の仕組みを使うことで解決している

主要PJ

TrustToken (TrueUSD)　WBTC (Wrapped Tokens)　GEMINI (Gemini Dollar)　DIGIX

特徴・要件

- DEXやDappsでの利用が簡単なようにERC20互換で実装されている
- 中央集権的な仕組みを利用することで、バックにあるアセットの担保を保証している
- 中央集権的な仕組みをコンソーシアム型にし、互いに牽制が効くようなガバナンスを持ち込むPJもある
- Tokenのmint/burnや、信託などで手数料収入を得る



LayerXでのブロックチェーン活用事例

LayerX

① プロトコルレイヤーでの活用

スマートコントラクトの形式的検証 * ゼロ知識証明でトラストレスにスマートコントラクトの安全性を証明できるプロトコルの開発

② エンタープライズ領域での活用

不動産のトークン化のスタンダードの共同開発
(その他、複数領域でエンタープライズへの活用を検討中)

事例①: プロトコルレイヤーでの活用

LayerX

スマートコントラクトの形式的検証 * ゼロ知識証明でトラストレスにスマートコントラクトの安全性を証明できるプロトコルの開発

Why?

LayerXではコード監査事業を行っている。現状コード監査事業はマニュアルで行われることが多く、監査結果に関してもレポートを出すことがアウトプットとなっており、定量的にスマートコントラクトの安全性を評価できるものにはなっていない。

また今後の様々なスタンダード(規格)競争が行われていく。スタンダードな実装に対してきちんとバグや規制の観点で問題なく実装できているかを定量的、かつ自動的でトラストレスに評価できるプロトコルは非常に重要と考えている。(我々これをtoken版"https"と呼んでいる)

What?

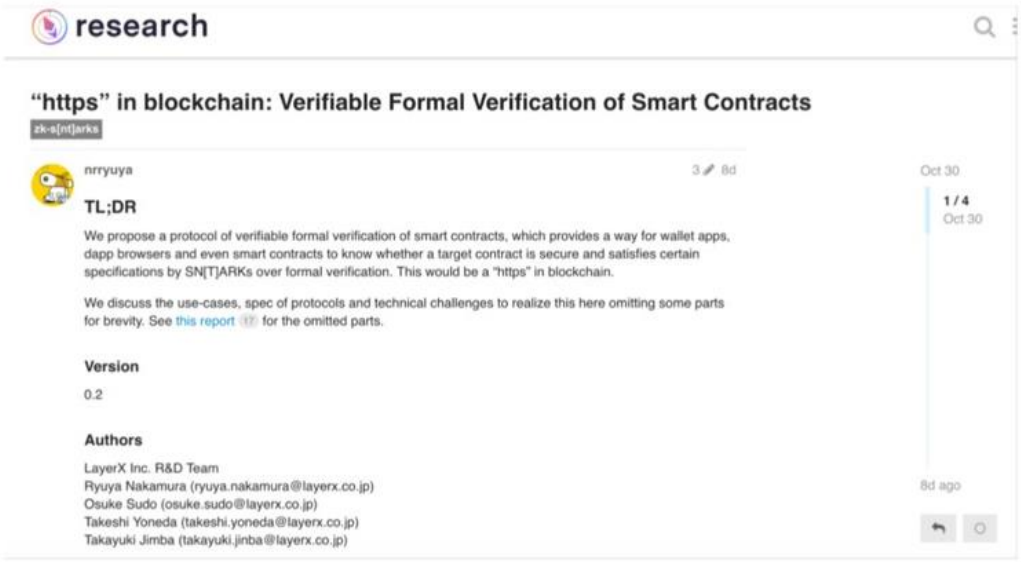
形式的検証: バイトコードレベルで、仕様に沿った実装が行われるかを数理的に検証する手法。今後ERCxxxのような規格が増えていくと正しい仕様の定義もしやすくなるのでスマートコントラクトの検証のメインストリームになる可能性がある

ゼロ知識証明: 中身を明かすことなく, その中身の検証を行うことができる。またその検証結果(proof)は圧縮されたサイズになるという特徴がある

この2つを組み合わせ, スマートコントラクトの検証が数理的に検証されかつそのproofをパブリックチェーンに乗せることで、コントラクトの安全性をトラストレスに担保する

事例①: プロトコルレイヤーでの活用

LayerX



詳細はethresearch:
https://ethresear.ch/t/https-in-blockchain-verifiable-formal-verification-of-smart-contracts/3999

事例②: エンタープライズ領域での活用

LayerX

- 複数の利害関係者を調整する必要がある
- ミドルマンの存在や再利用性が低いためにコストが高止まりしている
- 嘘つきがいることで経済圏が破壊され、そこを担保するコストが掛かっている
- 市場規模が大きい

(ex)
不動産, 電力, 教育, 金融, 貿易, 商社, 権利証明 etc

これらの経済圏をスマートコントラクトで置き換えるとこを置き換え、コスト効率を良くすることができるかに焦点

End