BITCOIN2.0概況

2014.10.03 by SATO

AGENDA

- イントロダクション
- Webの進化（EtheriumとWeb3.0）
- スマートコントラクト＆スマートプロパティ（Codius/Counterparty）
- 組織・意思決定（DAC/DAO/Eris）
- ファンドレイジング（MaidSafe/Storj/Swarm）
- 金融プラットフォーム①：ゲートウェイ（Ripple/Stellar）
- 金融プラットフォーム②：交換所インフラ(NXT/Overstock/BitShares)
- クロージング

1. イントロダクション

1)Bitcoin2.0
2)Bitcoin2.0の方向性

1) Bitcoin2.0

- ◆ビットコイン
- ◆ビットコインの核心はブロックチェーン
- ◆ビットコイン技術の応用

2) Bitcoin2.0の方向性

- ◆応用方向性
- ◆サービスインしているBitcoin2.0のプロジェクト
- ◆Bitcoin2.0の立ち上げ方法

ビットコイン

- 2014年、一般人もビットコインを知ることになったが・・
- ビットコインのキラーアプリは何か？
- 決済？
- 圧倒的に早い決済スピードと、安価な手数料。
- 国際送金や企業間送金には有利だが、一般消費者の普段づかいには遠い。
- 普段づかいの小額決済であれば、ApplePayやお財布ケータイで十分。
- ビットコインのキラーアプリは、通貨決済とは別の側面で利点をもたらすもの。

ビットコインの核心はブロックチェーン

- ビットコインの本質は、ブロックチェーン（合意形成システム）。
  - ブロックチェーンは、誰が誰にいくらのビットコインを送金したかの取引履歴をすべて記録した台帳のようなもの。（裏書手形が連鎖したようなもの）
- ブロックチェーンを使うことで、中央機関のオーソリティなしに、ある状態の遷移や、ある値の移動について、参加者すべてが疑いなしに、それを正しいと合意できる。
  - ビットコインは、中央機関のオーソリティなしに、すなわち分散型の合意形成の仕組みを用いて、ある値の遷移を、お金の残高とみなすことによって、通貨としてのビットコインが成立っている。
- こうした、中央集権ではない分散型で合意形成・取引記録ができるシステムに、大きな可能性があるのではないか・・・。

ビットコイン技術の応用

- ビットコインを支える技術であるブロックチェーン、あるいはPoW（プルーフオブワーク）を、おカネ以外のものに応用しようというのが、「ビットコイン２．０」と呼ばれる動き。

- ビットコインの新バージョンではなく、新たな応用にむけた動きのこと。

- ビットコインという通貨だけではなく、多様な価値をブロックチェーン上で流通させようというのが・・・
「ビットコイン２．０」。

応用方向性 (1/2)

- 多種多様な応用が想定できる
  - 各種の契約や証明
  - ブロックチェーン上で自分の暗号通貨をつくる
  - 金融デリバティブ、ギャンブルシステム
  - 自分のディスクを貸し出す
  - 投票システム、クルマの所有権移動
  - 音楽配信などデジタル権利マネジメント
  - デジタル資産のオークション
  - 株式事務、株主総会
  - パーソナルID証明
  - P2P保険、クラウドファンディング
  - 製品・サービスのシェア、アイデア・メディアのシェア

応用方向性 (2/2)

- 「ビットコイン２．０」的なプレイヤー続々と増えつつある。
- インターネットの進化に例えると、20年前の1990年代。
- まだ大衆的な人気を得ておらず、
  キラーアプリを目指した混沌状態。
- ビットコインに乗り遅れるな、と言われるが、
  乗るなら、ビットコインの技術をその他の領域に応用する
  「ビットコイン２．０」。

サービスインしているBITCOIN2.0のプロジェクト

- 「ビットコイン2．0」には、多くのプロジェクトが存在。
- その中には、既にサービスインしているものも。
  - Namecoin
  - Colored Coins
  - MaidSafe
  - Storj
  - Counterparty
  - Stellar
  - Swarm
  - BitShares　など。

BITCOIN2.0の立ち上げ方法

	概略	メリット	デメリット
オプション1	独自のP2P ブロックチェーン サーバーネットワークを立ち上げる。 （例：Namecoin）	ブロックチェーンをアプリケーションに適合したものにモディファイできるので、自由に実現したいことができる。	賛同してP2Pサーバーを立ち上げる人を巻き込まねばならない。 (少人数であれば51%アタックに弱くなる)、 P2Pサーバーネットワークソフトウェアの検証が大変
オプション2	ビットコイン上にメタプロトコルを作る方法。 （例：ColoredCoins）	P2P認証サーバーネットワークは既に立ち上がっているビットコインの物を使用するので、立ち上げの労力は軽くなる。	SPV(Simplified Payment Verification)が使用できない等、できることの自由度が減る。
オプション3	ビットコインのスクリプトを利用する方法。	3つの方法の中でもっとも簡単。	スクリプトでできることには制限がある。

2. Webの進化（EtheriumとWeb3.0）

1) Etherium
2) Web3.0

1) Etherium

- ◆Etheriumとは
- ◆Etheriumで出来ること
- ◆Etheriumの仕組み
- ◆Ether売り出し

2) Web3.0

- ◆Web3.0とは
- ◆Web3.0の仕組み

ETHERIUMとは

- 以上をもう一段汎用化して、「個別にいろんな仕組みを作らずに、何でもできるような仕組みをを一個つくって、それに載せたらいいんじゃないのか？」という考えた人がいた。
- ブロックチェーンを使って通貨以外にどんな応用が可能かを考えているプロジェクトが、Etherium。

- 開発者がブロックチェーンに基づいた分散アプリケーションを構築できて、消費者がこれらの分散アプリケーションを安全・容易にできるようなプラットフォームを構築することを目指している。
- 具体的には、ブロックチェーン技術をつかって、世界中の資源で動くネットワーク上の仮想コンピュータ、或いは　分散処理ネットワークを統括する仮想OSのようなもの。

ETHERIUMとは

- 開発者は専用スクリプト言語（Java・Pythonなどの一般的な言語）でコードを書くことで、アプリケーション毎にP2Pサーバー網を立ち上げることなくEthereumのP2Pサーバー網を使用して、分散アプリケーションや複雑な契約を表現したりできる。

- 今年の冬に稼働される予定なので、リリースはまだ先のことだが、各種の契約や証明、ソフトウエアなどに活用が広がる可能性があることから、非常に能力の高い人たちが参加して、沸き立っている。

ETHERIUMで出来ること

- 金融デリバティブ
- Namecoinのような名前登録システム
- 自分のディスクを貸し出すデータストレージサービス
- 複数署名エスクロー
- 投票システム
- ギャンブルアプリ
- 分散・分権型組織
- 貯金ウォレット

ETHERIUMの仕組み

- Etheriumは「Ether」と呼ばれる独自通貨をもつ。
  - Etherは、Etheriumを利用するための基本的単位で、Etheriumを利用するにはEtherを支払わなければならない。
  - アプリケーションをEtheriumの分散・分権型ネットワーク上で実行する際にこの「Ether」を共通の燃料として参照する。

- あらゆるアクションの実行にはフィーが発生し、コードの各ラインの実行に際して「Ether」(燃料ガス)を消費する。
  - Etherは、Ethereum上で計算を行うときに必要な燃料
  - 実行を通じて「Ether」ガスが切れると、実行もストップする仕掛け。

ETHER売り出し

- 7月23日から42日間、「Ether」が売り出された。
  - 「Ether」の売り出しは今回が最初で最後。
  - 今後は「Ether」の売り出しはなく、マイニングで手に入れるか、市場価格で手に入れるのみ。
- Etherをビットコインと引き換えに販売することで、初期の開発費を獲得しようとしている。
  - Etherは、Etheriumを利用するための通貨・燃料のようなもの。
- 今回の「Ether」売り出しは、資金調達と、「Ether」の配布を兼ねたもの。
  - 従来の株式会社でいうとIPOに近い
- 発行の「Ether」に上限はなく、資金が集まった分だけ「Ether」が発行される仕組み。
  - 発行された「Ether」は合計で、60,102,216 Ethに及んだ。
  - 全世界から集めた総額は、31,529BTC。
- 調達時1BTC＝480$と換算して、約16億円弱の調達。
  - ネット上でビットコインを用いて資金調達したケースとしては、過去最大。

WEB3.0とは

- インターネットの構造を変えることを目的に、Etherium.orgのCTO Dr.Gavin Woodが発表したコンセプト
  - 詳細は未発表。
  - Etheriumのブロックチェーンを利用するという意味で、従来の中央集権的なクライアントサーバ型と異なる非集中型のウェブ。

- Etheriumの上で、Decenterlizedなアプリが構築できる。
  - Decentralized Application（分散アプリケーション）とは、誰でも参加したい人が参加して、システムの一部になるようなアプリケーション。
  - Bitcoinのように、会社や国のような権威が存在せず、ユーザでありながら、システムの一部になるもの

WEB3.0の仕組み

- Ethereumと、「Swarm」というモジュールと、「Whisper」というP2Pメッセージングモジュールを使って、インターネットの構造を変えることを目指している。

- 言語はEthereum Contract。
- 動かすのに、Etherが必要。
- 処理は全世界のマイナーが分散処理。
- 計算過程・結果はブロックチェーンに記録され、偽造不可。

3. スマートコントラクト＆スマートプロパティ

1) スマートコントラクト
2) Codius
3) スマートプロパティ
4) Counterparty

1) スマートコントラクト

- ◆スマートコントラクトとは
- ◆スマートコントラクトの適用例
- ◆スマートコントラクトのインパクト
- ◆Internet of Thingsとの関連
- ◆意思決定・契約・約款

2) Codius

- ◆Ripple Labsが始めたスマートコントラクトのプロジェクト
- ◆Ripple LabsがCodiusの上に描くアプリケーション

3) スマートプロパティ

- ◆スマートプロパティとは
- ◆資産への適用

4) Counterparty

- ◆P2Pの分散・分権型交換所
- ◆スマートプロパティによる株式事務
- ◆スマートプロパティにくるまれたドルの所有権：RealCoin

スマートコントラクトとは (1/3)

- Pull Paymentが可能
  - ‘I give you money’といった同意に基づく現金や小切手での支払い(＝Push payment)は仮想通貨によって解決できたが、‘you take the money’といった何らかの契約に基づく同意によって行われる口座自動引落・カード払いのような支払(＝Pull Payment)は解決できていなかった。
  - このPull Paymentを可能にするのが、スマートコントラクト。
- スマートコントラクトは、契約書の条項を自己実行するコンピュータコードであり、中央機関なしに、契約や同意を自動執行できる。
  - 同意内容を実行に移すことをで他者に依存するのでなく、コードの実行を通じて、自動的・自律的に遂行される

スマートコントラクトとは （2/3）

- スマートコントラクトがPull Paymentを実行するステップ
  - 1. 契約条項をコードへ翻訳
    - 契約履行によってもたらされる成果、契約不履行時のペナルティ
  - 2. 実行コードについて同意
    - 同意されると実際に実行されて終わることを保証
  - 3. 不正が行われる事なく実行する
    - 第三者または独立グループによって実行

スマートコントラクトとは （3/3）

- 仮想通貨が既存のお金の概念を変えているように、
スマートコントラクトは、紙の契約書を時代遅れの産物に追いやるだけではなく、法務の在り方を変えていく。

- 例えば、現状では、契約で何かトラブルがあれば、裁判の時間やコストが発生。企業は毎年法律関連のことに何千万円のコストを費やしている。

- スマートコントラクトを利用することの効用は、「スピード加速や効率性」の他、契約が同意されたとおり忠実に履行されるだろうという「信用」といった意義も。

スマートコントラクトの適用例

- クルマを売り買いするときのトランザクションの場合。
  - 代金(仮想通貨)と所有権がソフトウェア上で同時に入れ替わることで、購入が完了し、そのクルマを運転できるようになる。
- レンタル車両にリンクしたビットコインを発行するレンタカー会社の場合。
  - 各車両は、対応するビットコインを使うことによって、解錠され起動できる。
  - クルマの予約はオンライン上で完了し、スマホアプリ上に暗号化されたトークンを使って正しい所有者と認識され、クルマを解錠し、エンジン起動できる。
- クルマの所有権をブロックチェーン上で主張したが、元所有者がなかなか渡そうとしないといった場合。
  - ブロックチェーンの所有権をもとに、クルマをリモートコントロールで操作し、自分のガレージまで移動させることができる。

スマートコントラクトのインパクト

- 代金と所有権の入れ替わりが自動執行される点。
  - クルマの売り買いするときであれば、代金（仮想通貨）と所有権がソフトウェア上で同時に入れ替わる。
  - 代金と所有権の入れ替わりが自動執行される。

- 信用度の低い相手（あまり親しくない相手）とも契約が行える。
  - たとえば、日本にいながら、サンフランシスコのクルマを購入して、ロスのヒトに販売できる。

INTERNET OF THINGSとの関連

- パーキングメーターや家のサーモスタット、家電、クルマなど、多くのモノがつながって、コンピュータやインターネットにつながったモバイル機器の数に迫る、モノのインターネット(IoT)を形成。
- IoTを通じて自動的・自律的にコントロールできるだけでなく、スマートコントラクトを通じて、オーナーシップやコントロールを自動的に違うパーティへ移転させることが可能になる。
- 個々のマシンが、通信上のIDを得るだけでなく、スマートコントラクトを通じて、経済的なIDを得ることができ、ヒトや会社との間で新たな関係を構築できる可能性。
- 例えば、家やクルマ等の資産を証券化して貸しつけるようなことも可能で、AirbnbやUberのようなシェアリングエコノミーのサービスにおいて応用が可能かも。

意思決定・契約・約款

- ヒトとヒトの契約のみならず、会社のミッションといった取決めも、エンコードすることによって、会社が自身を自分で管理するような新たな生態系が生まれる可能性も。（＝DACとして後述）

RIPPLE LABSが始めたスマートコントラクトのプロジェクト

- Ripple Labsは、将来的に全ての産業が、スマートコントラクトを通じてデジタルアセットのやりとりを行うようになる、というビジョンを持っている。
  - そのRipple Labsが、包括的なスマートコントラクトシステム「Codius」の構築計画を発表した。
- 仮想通貨を用いて支払いを行うにあたり、決済や契約といったビジネスロジックを実行するもの。
  - Codiusの“ius”は、法律を意味する
- スマートコントラクトが、適切なインプットがあるときに実行されるのと同じように、Codiusは、条件を満たしたときに暗号カギのペア署名を行うことができる「smart oracles」を用いている。
  - 「smart oracles」が署名を行うことによって、分散ネットワークにおけるアクションが実行されるという仕組み。
- Codiusは、今後デジタルアセットをやり取りする上でのフレームワークとなる可能性。

RIPPLE LABSがCODIUSの上に描くアプリケーション

- クレジットカードやデビットカードのように、売り手が買い手に代わって支払いを実行できる仕組みや、日々の引出限度・取引の承認／無効化などの機能を備えた暗号通貨ウォレットをコントロールできる。
- オークションルールの自動実行に基づいて、デジタルアセットの所有権に関するオークションを実行できる。
- アセットのパフォーマンスをモニタリングする契約を通じて、先物・オプション・スワップ等のデリバティブ商品を実装できる。
- 事前に定めたルールに基づいて支払や権利の発動を行えるような証券を記述できる。

スマートプロパティとは

- 実態のある資産やデバイスの所有権を、ブロックチェーン技術を用いてコントロールするコンセプト。（スマートコントラクトの一種）
  - ブロックチェーンを用いて「誰が何の資産を所有するのか」をトラッキングすることによって、ブロックチェーンを通じて、所有権をコントロール。

- ビットコインは貨幣におけるイノベーションだが、これを拡張してあらゆる資産に関して適用し、ビットコイン同様の方法で、「所有権と取引の合意」をなそうとするもの。
  - 「誰が何を所有するのか」について、中央権力の介在を必要としない。
  - デバイスのような物理的な財産所有権に限らず、独自の通貨や、企業の株式や債権、リモートコンピュータのアクセス権といった「非」物理的な財産所有権も含む。

- 財産所有権をスマートにすることによって、信用が少ない中でも財産所有権のトレードが可能になるため、
  - 取引上の不正リスクや、仲介手数料を削減することができる。

P2Pの分散・分権型交換所

- 2014年1月に立ち上げられた、ブロックチェーン上でフリーP2Pマーケットや金融機関のP2Pトレーディングを可能にするオープンソースソフト。
  - 第三者の仲介を必要とせずに、オープンで安全な金融システムを提供。

- ビットコインが通貨それ自身に対して行っているように、仲介を介さずに資産をトレードできるようにすることを目指す。
  - インターネットが情報に対して、ビットコインがマネーに対しておこなったように、金融を民主化・分散化することがゴール。

スマートプロパティによる株式事務

- 面倒な手続きなく、発行数を入力するだけで株式コインを発行できる。
  - 株式コインを相手に送付すれば、世界中だれにでも株式コインを譲渡できる。
  - 相手は証券口座を持っている必要はないため、匿名で株主を管理できる。
- 株式コイン保有者に対して、比例配分にて、他の暗号通貨を送付することで配当を実現できる。
  - ブロックチェーン上のコイン残高に対して配当を送りつけるだけなので、株主の名前・住所・口座などを把握する必要がない。
- 配当と同様に、投票用コインを配当することで、株式コインの保有割合に応じた投票コインが配布される。
  - この投票コインを、投票選択肢に対応したビットコインアドレスに送付することで、株主総会の投票を実現できる。

スマートプロパティにくるまれたドルの所有権：REALCOIN

- スマートプロパティにくるまれたドルの所有権
  - ドルと1：1に対応したコインで、ドルとの交換を保証。
- RealCoinは、ドルのみでなく、ユーロや円についても同様のコインを発行予定。
- 日本円のスマートプロパティを発行して、円との交換を保証するような仕組みは、銀行のための新しい領域を開拓できる可能性あり。
  - 銀行がやらなければRealCoinや、他のスタートアップが銀行を作る気概で取り組む可能性

4. 組織・意思決定(DAC/DAO/Eris)

1) DAC/DAO
2) Eris

1) DAC/DAO

- ◆DAOとは
- ◆DACとは
- ◆これからのIPO（資金調達・起業形態）

2) Eris

- ◆Project Douglasによって立ち上げられた分散型意思決定システム
- ◆分散型コンセンサス形成

DAOとは

- Decentralized Autonomous Organization
- Contractによって人々がつながっている仮想的なエンティティ
- 67%以上のメンバー　または　シェアホルダがファンドを使ったりContract Codeを書き換える権利を持つもの

DACとは

- DAOのうち、参加者が株主のように異なる権利割合を持つ営利組織の場合に、DAC（Decentralized Autonomous Company）と呼ばれる。

- 伝統的な会社と同じように株主のためにカネを稼ぐ、ソフトウェアエンティティ。
  - 例えば、ネット上のContractで結ばれたDAOで、有料の分散アプリケーションを開発して、得られた利益をContractに沿って分配。
  - 「株式」を購入することによって持ち分保有者になり、その持ち分に応じて、どのように経営していくかについて発言権を与える。

- 「信用」を必要とせず、ビジネスルールがソフトウェア上に書込まれているビジネスルールに基づくコントロールのもと、人間の介在なしに動く。
  - 一種のロボットとして、人間の頭脳を代替する。
  - ブルーカラーの代替でなく、経営者をも代替してしまう点がインパクト。

DACとは

- 悪意ある個人やグループが、DACの意図する運営方針を破壊してしまうことのないようになっているという意味で、Decentralized。

- 特定の者に依存することなくサービスをマーケットに対して提供し続ける。
  取締役会なしに運用できるという意味で、Autonomous。

- 株主のためにカネを稼ぐという意味で、Company。

- ビットコインは、DACとして記述された最も知られた一例だが、厳密にこの定義に照らすと、コイン保有者がビットコイン法人のエクイティ持ち分保有者になるという意味で、DecentralizedでAutonomousだが、株主のための収入を生成しないので、DACではない。

これからのIPO（資金調達・起業形態）

- ビットコインと、ビットコイン2．0は、さまざまな意味において、起業を容易にする。
  - 例えば、ビットコインで予算を集めて資金調達し、DACでサービスを開発。
  - サービス開始前に、サービスで利用する独自コインを発行し配布することで資金調達した上で、サービスを開始して人気が出ると、発行した通貨の価格が上昇。

- VCから資金を集めて、株式を発行して円を調達すべく株式市場へ上場する、といった現在のIPOモデルと比べて、ハードルが低くなる。
  - スタートアップやIPO市場の在り方を大きく変える可能性。
  - 今後、多くのインフラ的なネットサービスが、DACで独自コインをつかって資金調達するように。

PROJECT DOUGLASが立ち上げた分散型意思決定システム

- Etheruimブロックチェーンテクノロジーを使うDAOのための意思決定支援プラットフォーム。
- Project Douglasの開発チーム（Dennis McKinnon, Casey Kuhlman, and Preston Byrne）によって立ち上げられた。
- Erisのソフトウェアは、オープンソースであり、以下に公開。
  - Erisのウェブサイトは、eris.projectdouglas.org
  - Erisのコードは、https://github.com/project-douglas/eris

分散型コンセンサス形成

- コミュニティの運営コストを削減し、意思決定やガバナンスプロセスを効率化。

- 各種のDAC/DAOが、Erisフレームワークを用いて実装されることによって、分散型のコンセンサス形成を通じた組織ガバナンスを、容易に可能にすることを目指す。

5. ファンドレイジング

1) 新たな資金調達方法
2) Maidsafe
3) Storj
4) Swarm

1) 新たな資金調達方法

- ◆直近のクラウドセール動向
- ◆従来の資金調達との違い
- ◆これからの資金調達スキーム

2) Maidsafe

- ◆Maidsafeの分散クラウドストレージサービス
- ◆MaidSafeの経済圏
- ◆独自通貨による資金調達

3) Storj

- ◆Storjが分散クラウドストレージサービス
- ◆Storjの経済圏
- ◆独自通貨による資金調達

4) Swarm

- ◆仮想通貨によるファンディングプラットフォーム
- ◆議決権や配当
- ◆発行コインを用いた意思決定投票

直近のクラウドセール動向

- ビットコインが新しい資金調達の可能性を広げている。
- 将来のリワードや利用券を約束して資金調達するクラウドファンディングに近く、「(暗号通貨の)クラウドセール」と呼ばれる。
- 株式発行・VCなどを通じた生態系による調達ではなく、暗号通貨による、暗号通貨の生態系の中だけで資金調達として、大規模調達が続く。
  - MaidSafeのクラウドセールスは、7億円を調達。
  - Storjのクラウドセールスでも、5000万の調達。
  - 最も金額が大きいのは、Etheriumで、16億円を調達。

従来の資金調達との違い

- 「株式会社」という形態ではなく、ネット上のプロジェクトやサービス。
  - 株式会社が株式を発行したりVCが投資してIPOするのではなく、独自のコインを発行し、世界中の一般投資家から資金を調達。
  - コインは仮想通貨の交換所で現金還元可能。
- この資金調達は、IPOといっためんどうな手続きを踏むことなく、全世界からお金を集めることができる。
  - 必要なコストも極めて低く、クラウドファンディングサイトのようにカード手数料もプラットフォームフィーも不要。
- これからのスタートアップは、VCやIPOではなく、DACでビットコインを調達し、独自コインを割り当てて資金調達する。
  - VCやIPOといった概念がなくなり、株式市場の形も大きく変わるなど、ビットコインが経済の根本を大きく変えてしまう可能性。

MAIDSAFEの分散クラウドストレージサービス

- スコットランドの分散クラウドストレージサービスプラットフォーム。
  - プロセッシングやメモリパワーを分散ネットワーク上でシェアすることによって、完全に分散・分権型のインターネットを創設することに使おうと試みている。
  - コミュニケーションをしたい二者の間に、インターネットのように中間者（サーバやデータセンターの層）を介在させず、完全にピアツーピアなネットワークを構築。
- その上で、各ユーザが自分が常用しているハードウェアをネットワークのインフラとしても提供。
  - リソース寄贈行為のことをfarming（農場拡大）と呼ぶ。
- これによって、ネットワーク上のすべてのコンピュータが繋がって、一つの巨大なデータセンターを構成。
  - 2014年度末のβ版立上げを目指してテスト中。

MAIDSAFEの経済圏

- 各ユーザが自分が常用しているハードウェアをネットワークのインフラとしても提供するにあたり、リソース提供による寄与貢献のインセンティブとして、独自コイン「SafeCoin」によって報いる仕組みをとっている。
- SafeCoinの現在価値はUSドル換算で約2セントだが、ネットワークの拡大とともに価値が上がることが期待されている。
- 2014年4月、5時間で7億円近くの資金調達に成功し話題になった。

STORJの分散クラウドストレージサービス

- Maidsafeにインスパイヤされて開発された、分散クラウドストレージサービスプラットフォーム。
  - 分散型かつ信用不要である、データ保管クラウドシステム
- 中央集権オペレーションはなされず、ブロックチェーンなどを利用した暗号化によってセキュリティを高めるとともに、より効率的で高速で民主的なストレージネットワークを保証。
  - 中央集権型ストレージサービスだと、盗聴や閉鎖のリスク有。
- ユーザは、イメージ、オーディオ、ビデオ画像などのファイルをStorjのP2P分散ネットワーク上のクラウドストレージへアップロード・貯蔵できる。
- ビットコインのブロックチェーンを利用して、利用可能なストレージスペースを購入できる他、空いたストレージスペースを売却することもできる。

STORJの経済圏

- Storjコイン（SJCX）という名前のサービストークンを発行。
- ストレージスペースを使いたい場合には、ユーザはこのSJCXを支払う。
- 空きストレージスペースを提供したい人は、Storjのクラウドにリソースを提供すると、スペースの提供代金としてSJCXが得られる。
- こうして、Storj内で、SJCXを通貨とした、一種の経済圏が出来上がる。

独自通貨による資金調達

- SJCXを、前売りというかたちで発行し、販売。
  - SJCXが欲しい人は、指定されたアドレスにビットコインを送るだけでよく、
  - その後、SJCXが送り返されてくる。

- ビットコインを提供した、クラウドセールスの参加者は、Storjの製品をいち早く使用する権利を得られる。
  - 調達したビットコインは、従業員の給与などに使用予定。
  - 公正を期すためにStorjは財布のアドレスを公開。
  - 調達したビットコインがどう使用されたかをGithub上に公開。

独自通貨による資金調達

- クラウドセールスは2014年7月18日に始まり、8月18日に終了。
  - 910BTC（日本円にして5000万程度）の調達がおこわれれた。
  - 全体発行量500,000,000 SJCXのうち、約35,000,000　SJCXを総額910BTCで売って、資金調達。
  - SJCXの15%は開発者へ、15%はコミュニティへ、残る70%がクラウドセールへ拠出。

- SJCXは、すでに、いわゆる仮想通貨の交換所でとりあつかわれていて、SJCX/BTCという通貨ペアがたっており、少量だが取引がある。
  - コインを発行して資金調達した瞬間にIPO/上場されて、Exitできる。
  - Storjに投資した人は、すぐさまそれを市場で売り払うことができる。

仮想通貨によるファンディングプラットフォーム

- 出資を募る事業者・プロジェクトが「自分のコイン」を発行し、それを購入してもらうことによってファンドレイジングを可能に。
  - 従来のクラウドファンディングは、寄付に留まるものが多く、出資者へのリターンは「御礼のTシャツ」レベルに留まりがち。
  - Swarmは、自社コインをどの程度発行したいか決めて、ブロックチェーン上のDACとして資金を調達。
- Bitcoin2.0テクノロジーによるクラウドファンディングプラットフォーム。
  - クラウドファンディング機能を、ビットコイン2．0技術で実現。
- Swarm自身も“Swarm Coin”を発行して、自身の資金集め。
  - そこで発行した“Swarm Coin”は今後のクラウドファンディングに充てることも可能。
- 仮想通貨の利便性を体現する上で、「仮想通貨によるエクイティ」がキラーアプリの1つに。

議決権や配当

- Swarmは、プロダクトのユーザでもあり同時に投資家にもなることができるようになる。
  - その意味で、「真のエクイティクラウドファンディング」を標榜。
- 仮想通貨を用いて出資を集めるとともに、出資者は議決権や配当を受け取ることができるプラットフォーム。
  - スマートコントラクトをブロックチェーン上に登録することを通じて、エクイティの取り分を得る。
- 出資者は、リアル通貨を以って上記「コイン」に換金することで出資。
  - 個々の「コイン」は、その会社・プロジェクトのエクイティの取り分に。
- 「コイン」のオーナーに等量のエクイティ比率が与えられる。
  - 当該企業・プロジェクトのエクイティのシェアとなって利益を得たり、配当・議決権を得ることができる。（＝仮想通貨によるIPO）

発行コインを用いた意思決定投票

- Swarmはユーザコミュニティによって所有されるDAOでもある。
- 資金調達のために発行した自社コインの用途について、コイン保有者の投票を募った。
  - 自社コイン保有者をSwarmの株主とみれば、会社の重要事項について株主総会を開いて株主の意向を問うているようなもの。

- 今回の議題は、発行予定24Kのコインについて、売れた10Kを引いた残りの14Kをどうするかという点。
  - 「比例配分」「破棄」「創業者が保有」の3つの選択肢について投票。
  - Swarm保有者に同数の投票用コイン（Swarm Vote 2）が配られ、3つの選択肢に対応するビットコインアドレスに送ると投票完了。
  - 投票結果はリアルタイムでブロックチェーンをのぞけば参照できる。

6. 金融プラットフォーム①:ゲートウェイ

1) Ripple
2) Stellar

1) Ripple
- ◆仮想通貨(XRP)
- ◆通貨間ゲートウェイ

2) Stellar
- ◆他通貨間との送受金むけ分散プロトコル
- ◆運営形態
- ◆法定通貨とデジタル通貨のブリッジを担うゲートウェイ

仮想通貨(XRP)

- Ripple Labsが運営・提供するサービス。
  - https://www.ripplelabs.com/
- Rippleと言えば
  - 「仮想通貨(XRP)」のことを指す場合
  - 「Rippleのシステム」のことを指す場合
  - 「Rippleの運営会社」を指す場合、がある。
- Rippleサービスの特徴
  - 1)XRPという仮想通貨を発行
  - 2)Rippleネットワークを通じた送金・受金
  - 3)IOUというXRP以外の仮想通貨(電子ポイント)
  - 4)仮想通貨どうしの取引ができるトレードシステム
- 「XRP」は、サービスシステム内で使用可能なリップルラボ発行の仮想通貨。

通貨間ゲートウェイ

- gatewayを介して、ドルやユーロ、BTC等とのクロスカレンシー取引が誰でもRippleシステム内で行う事ができる。

- ビットコインなどの通貨という枠を超えて、金やマイルポイント等の価値とも含めた、支払及び外貨両替システムでもある。

- Ripple財布（https://ripple.com/client/）で無償アカウントを取得して、上記gatewayを登録。
  受取側のrippleアドレスを指定すると、受取側の登録gateway次第で、
  - 送り手　JPY　→　受け手　Euro
  - 送り手　JPY　→　受け手　USD
  - 送り手　XRP　→　受け手　BTC
  - 送り手　BTC　→　受け手　USD
  - 送り手　BTC　→　受け手　JPY　　、、等を実行できる。

他通貨間との送受金むけ分散プロトコル

- おカネを送受信するための分散型プロトコルによる、通貨のP2P交換システム
  - いかなるペアの通貨同士であっても送受金を可能に
  - 任意通貨間のトランザクションをサポートするゲートウェイ
  - 例えば、送り手が円で送金を行って、受け手がユーロで受け取ることができる。
  - 円やユーロ、ドルだけに留まらず、ビットコインのような仮想通貨も送受金が可能。
- 「法定通貨とデジタル通貨との橋渡し」をするプロジェクト。
  - 送金側も受金側も、自分の都合の良い通貨や価値のある物で取引が行える、未来の財貨のあり方を目指す。
- 「stellar」と呼ばれる自身のデジタル通貨を保有する。
  - 1000億stellarsが初期総量。年間1%増やす予定
  - アカウント作成にFacebookアカウントを要求。アカウント数が20万突破

法定通貨とデジタル通貨のブリッジを担うゲートウェイ

- ゲートウェイに預けるとStellarネットワークを通じてクレジットを発行してもらえる。
- ゲートウェイに1万円預けると、ゲートウェイは入金を確認後、Stellarウォレットに対して、クレジット(10,000JPY)を発行。
- 発行されたクレジットに対して、ゲートウェイ自身は関与する事なく、Stellarの分散型為替システムを介して、様々な通貨・財貨と取引できる。
- ゲートウェイを通じて得たクレジットを使って、ゲートウェイ自身は関与する事なく、分散型為替システム上で売買が行える。
- 誰もがオファー(発注)でき、誰もがオファーを受け入れる事ができる。

7. 金融プラットフォーム②：交換所インフラ

1) NXT
2) Overstock
3) BitShares

1) NXT
- ◆ユーザ定義資産を取引できる分散型為替インフラ
- ◆NXTアプリケーションのエコシステム

2) Overstock
- ◆オンラインショッピングOverstockとビットコインの関わり
- ◆暗号証券による株式市場の再構築構想

3) BitShares
- ◆DACエコシステムの創出を目指すBitShares
- ◆分散型交換所や個人金庫を通じ銀行ビジネスを模すDAC：BitShares X
- ◆合意形成アルゴリズム：DPOS
- ◆予測市場に基づきリアル資産価値をトラックするトークン：bitAssets
- ◆Bitshares X事業における株式：btsx と 米ドルとの紐づけ：bitUSD

ユーザ定義資産を取引できる分散型為替インフラ

- 2014年5月12日に立ち上がった、初の分散為替インフラ。
- 中央の第三者を必要せず、ユーザが定義したアセットを、作ってトレードできる。
- 資産所有権などのデータをブロックチェーンへ書き込むことを、セキュアで容易なものに。
- NXTのアセット交換所は、200以上のユーザ定義アセットが作成済。

NXTアプリケーションのエコシステム

- 分散型為替システムへのアクセス
- myNXTといったウェブウォレット
- NxtBlocks and NXT Reportingといった、ブロックエキスプローラー
- Coinist.co and TrustYourAssetsといったアセットランキングサービス
- Nxt Legalといった、リーガルサポート

オンラインショッピングOVERSTOCKとビットコインの関わり

- CEOのPatrick Byrneは、仮想通貨よって巨大な銀行や政府に依存しない経済を築けると考えている。
- 2014年初めには、大手ネット小売業者として最初にビットコインでの支払いを受け入れ。
- ボーナスもビットコインにする。
- 自社株をスマートプロパティとして発行することを検討。

暗号証券による株式市場の再構築構想

- Overstockは、ビットコイン2．0技術の利用可能性を探索。
- ビットコインがおカネの貯め方・交換の仕方を一新したように、株式市場を一新することを目ざす。
  - 企業が“cryptosecurity：暗号証券”cryptosecurity（＝cryptocurrencyベース）の証券を発行するアイデアを発表。
  - Cryptosecuritiesを発行して、分散・分権型の交換プラットフォームを創設する。
- これにより、全ての株式取引はNASDAQやNYSEのような伝統的な証券取引所ではなく、もっと一般の業界で管理され、売買はオンライン上の帳簿で数学的に検証され、記録され、誰もがいつでもチョックすることができるようになる。
  - 証券取引所のような中央集権の中間人なしに、個人間で証券を取り引きできる。

DACエコシステムの創出を目指すBITSHARES

- BitSharesは、それを使ってDACを立ち上げることができるオープンソースソフト。
- 誰でもBitSharesのソフトを使ってDACを構築できる。
- 分散型のcrypto-equityとして、bitsharesを保有する株主とのコミュニティを通じて、銀行・証券取引所のような機能を実現することを目指す野心的な取組み。

3) BitShares

分散型交換所や個人金庫を通じて銀行ビジネスを模したDAC：BitShares X

- 香港をベースとする企業、DACSunlimitedによって、7月14日にリリース。
  - ソフトウェアは、バージニア州をベースとするInvictus Innovationsによって開発。
- 分散型「交換取引所」あるいは、クリプト資産を貯蔵・交換できる「個人金庫」として機能する。
  - BitShares Xを使って、bitAssetsと呼ばれるクリプトアセットを貯蔵・トレードできる。
  - 価値貯蔵のための「bank」として活動することを目指している。
- bitAssets と Exchange、この2つのコンポーネントを通じて機能。
  - 交換取引所としては、金・銀・さらには企業株式など、どんな種類の仮想アセットとも、購入・売却・交換取引できる。
  - 個人金庫としては、ユーザ自身だけがカギを持つ、仮想金庫を提供。

合意形成アルゴリズム:DPOS

- ファウンダーのDaniel LarimerはBitcoinによって使われるproof of workを“broken”と称し、proof of stakeこそ未来であると信じている。
- BitsharesXは、altcoinsで用いられることの多い「proof of stake」の別バージョンである、「Delegated Proof of Stake (DPOS)」を利用。
- 所有権によって重みづけられた101の代表者のためのBitsharesX 投票を所有するもの。
- 10秒というブロック確定タイムであり、取引の確定を極めて高速化できる。

予測市場に基づきリアル資産価値をトラックするトークン：BITASSETS

- BitAssetは、ドルや金銀など、リアル世界のアセットの価値をトラッキングするトークン。
- 予測市場の仕組みを用いて、価格の狂いを補正し、1BitUSDが、1米ドルと同じ価値であろう、等を紐づけ。
- BitShares Xのユーザは、自分のbitAssetsを、分散分権型の交換所でトレードできる。

BITSHARES X事業における株式：BTSX と米ドルとの紐づけ：BITUSD

- 「btsx」は、通貨単位というよりも、Bitshares X事業の株式。
  - 「btsx」を保有することは、証券取引において株式を保有することと同じようなもの。
  - 全てのトランザクション取引手数料は、「btsx」を通じて、BitSharesXの株式の所有者に対して還元される。
- 一方「bitUSD」は、現在の金融システムでダイレクトなアナロジーが無いコンセプトなので、少し難しい。
  - どれだけ多くのbtsxを1米ドルと同量と表現するかを示すアセット。
  - 例えば、現在のbtsxの市場価格が1btsxあたり0.028米ドルであれば、 1/0.028で1米ドルは35.71 btsxと表せる。
  - bitUSDは、定義次第で、法定通貨の米ドルと同じ購買力を持つため、利便性が高い。
- Bitshares Xを用いて、bitUSDを生成できるだけでなく、同様にbitEUR, bitJPYや、bitGoldなども生成できる可能性。

8. クロージング：新たな経済圏の構築

COLLABORATIVE ECONOMY

- ビットコイン2．0は、まだ途上の技術なので、今後の発展・改善に期待。
  - 大きくて中央集権的で官僚的なヒエラルキーから、テクノロジードリブンな個人・コミュニティによる分権ネットワークへとパワーシフト。
  - Airbnb, Uber, Lyftといったシェアリングエコノミーの新興サービスの先に、モノのインターネットとビットコイン2．0が融合して、所有権の移転・シェアが進展。

- 価値交換の手段であった「おカネ」の役割・機能が変わる。
  - 生活し、働き、遊び、旅行し、創造し、学び、貯え、消費する上において、巨大なパラダイムシフト。
  - 「会社」の役目も、急速に変わってきている。
  - 地域通貨とビットコイン2．0的なアーキテクチャが融合して、各種サービスを提供していくようになると地域社会の在り方も変わる。
  - 地域経済・都市経済の課題解決の動きとも歩調を合わせ、その基盤技術としてアプリ・サービス開発が進むと地域や国家にインパクトすらもたらしうる。

- ビットコイン2．0の技術・アーキテクチャ・サービスは、シェアリングエコノミーやコラボレーションエコノミー等、新しい経済の形・社会の形を提案できると面白い。