ブロックチェーンとTCG技術の関連性

11/20/2017

（社）日本デジタルマネー協会
（株）ユナイテッド・ビットコイナーズ
本間

自己紹介

・半導体メモリの営業・マーケティング、2006～2009年Trusted Computingの事業企画
・開発を経て、複数のベンチャービジネスに参画

・2013年　ビットコインを知り、その技術的革新性と組織のあり方に強い衝撃を受ける。ビットコインはオープンソースプロジェクトかつ要素技術がTCGと似通っていたため、疑問と怪しさを一つずつ払拭して、技術的プロジェクトとして、コミット開始

・2014年（社）日本デジタルマネー協会設立

・2017年（株）ユナイテッド・ビットコイナーズ設立

・エンジェル投資を4社

初めの注意・警告

・仮想・暗号通貨業界は詐欺師が多数いるので御注意ください

・情報商材屋、ネットワークマルチ販売屋が100%詐欺師です

・投資セミナーも危険です、詐欺師は帰れない雰囲気を作ります

・儲かる話に御注意ください

・無から有は生まれません

・ブロックチェーン、DLTはB2Bなので、比較的安全です

・仮想・暗号通貨周辺は詐欺師多数でDLTより危険です

本日のトピックス

・ビットコイン

・Ethereum

・プライベート・コンソーシアムチェーン aka DLT

・ICO

・TCG卒の活躍

・インターブロックチェーン

Comments by Steven Sprague

Bitcoin’s killer app is TCG.

TCG’s killer app is Bitcoin.

@Miami, Austin, NYC, Las Vegas, 2014

ビットコイン、ブロックチェーン、ICO、トークンエコノミー等はTCGの市場となる可能性高い

TCG vs ビットコイン

・TCG用語として、Root of Trust, Trust Chain

・ビットコイン用語として、Trustless, Untrusted

・Trustlessとは、Trusted Third Partyを必要としないシステム　Lightning Network等

・Untrustedとは、取引が中央サーバーを経由するが、サーバーがアリスとボブをチート出来ないシステム　TumbleBit等

Breadwallet

・Bitcoin側のTCG利用例

・ビットコイン財布として人気あります

・秘密鍵をiPhone Secure Enclave, Android Trusty Teeに保存

https://source.android.com/security/trusty/

インターネット 2.0

・インターネット 1.0　はテキスト、静止画、音声、動画等を扱っている

・インターネット 2.0　はコピー＆ペースト出来ない価値を扱う

・web1.0はユーザ側の読み、web2.0は読み書き、web3.0はGavin Woodが提案中

・ビットコインが先陣を切った

・ICO, P2P lending等が続くか？

・法定通貨、証券、債権もインターネット上を流動すると予測される

・今年、ICOのブーム以降、トークンエコノミーが加速中

・Polkadot, Cosmos, Interledger, TumbleBit, Atomic Swap等のインターブロックチェーン

本日のトピックス

・ビットコイン

・Ethereum

・プライベート・コンソーシアムチェーン aka DLT

・ICO

・TCG卒の活躍

・インターブロックチェーン

Bitcoinとは？

・bitcoindというオープンソースソフトウェアが5大陸で走るグローバルネットワーク

・採掘者は参加、撤退が自由

・開発者、事業者も参加、撤退が自由

・Linuxの金融版

・世界中から多様な才能が開発・事業に参加

Bitcoinとは？

・PKI, hash, P2P, 電子署名とPoWによるグローバル金融システム

・Trusted Third Partyをなくした（攻撃点をなくした）のが最大の特徴

・約20年間、100社が失敗した（PayPalが最初の成功例）反省が、TTPに頼らないシステム設計としてのビットコイン

・P2P electric cash system

・Internet of Money

・リーマンショック後の2009年にサトシナカモトがbitcoindを稼働開始（現在の金融システムに対する批判から生まれたと言われている）

Bitcoinの特徴

・分散型合意システム

・システムを構成する計算機パワーは、誰でも自由に参加出来て、自由に撤退出来る

・各ノードは悪意があっても構わない。悪意を持ってシステムを改竄するよりもPoWに参加して、ビットコインを採掘する方が儲かるという設計

・グローバル金融システムが、24/7/365で、ダウンタイムゼロを数年継続で、世界記録を更新中

・改竄に世界一お金が掛かるシステムがビットコインのブロックチェーン

Bitcoinとは？

・ビットコインスクリプト言語

・全ての命令が線形に1度だけ実行される・ループがない

・チューリング完全ではない・任意の関数を計算する能力を持たない

・命令は1Byteで表現されている = 256種類まで定義可能

なぜビットコインが通貨的振る舞いをするのか？

・世界の通貨の歴史を学びましょう

・野口悠紀雄先生
https://www.amazon.co.jp/dp/B00M7J9SKA/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1

・通貨、貨幣などは日本法で定義されてるため、法律家が詳しいです

・仮想通貨は改正資金決済法で定義されてます

本日のトピックス

・ビットコイン

・Ethereum

・プライベート・コンソーシアムチェーン aka DLT

・ICO

・TCG卒の活躍

・インターブロックチェーン

Ethereumとは？

・読み書き出来るビットコイン　＝　ワールドコンピュータ

・チューリング完全

・分散型ではあるが、立上げ時にICOをやってしまった（米SECから問題視？）

・Proof of Vitalik　な　Proof of Work　で　PoS　に移行予定

・2016年6月、TheDao事件を解決するため、巻き戻しを実行済

・現在、多数のICOが実行されていて、ビットコインに肩を並べる2017年の主役

・分散型ワールドコンピュータが、ペイするのか、スケールするのか？

Ethereumとは？

・目的はスマートコントラクトのプラットフォームだが、

・現実はICOを連発するバブル発生装置

・多数の才能あるプログラマを惹きつけてます

・2017年はBitcoin, Ethereum, Altコイン, ICOバブルで、計4つのバブルが重なった飛躍の年でした

Enterprise Ethereum Alliance

Enterprise Ethereum Alliance

・Ethereumは分散型のパブリックチェーンだが、

・EEAは、そこから派生したプライベートチェーン

・信頼の基盤はパブリックチェーン（トラストレス）ではなくて、企業

本日のトピックス

・ビットコイン

・Ethereum

・プライベート・コンソーシアムチェーン aka DLT

・ICO

・TCG卒の活躍

・インターブロックチェーン

ブロックチェーン aka DLT

・ビットコイン、イーサリウム、ICO等の分散型合意システムに対するreactiveな活動が、ブロックチェーン（DLT）

・金融機関がインターネット、スマホ、AIをフル活用するのは必然

・電子メールが普及後も郵便局が存在している様に、フィンテックが普及しても金融機関は存在し続けると予想される

・金融機関のリストラが始まったが、金融機関にしかやれない機能はある

・金融機関が生き残るにはGSのコピー、つまりプログラマを優遇して、インターネットをフル活用して、グローバル市場を開拓するのが適切

Blockchain（aka DLT）とは？

・ビットコインからProof of Workを引くと、ブロックチェーン

・ビットコインを支える計算機パワーはビットコインの発行益がインセンティブで、採掘者は参入・撤退共に自由

・プライベートブロックチェーンはビットコインと異なり、インセンティブとしての通貨発行機能・利益を持たない

・ブロックチェーンはDistributed Ledger Technologyとも呼ばれている

・RDB（実績十分） --- DLT（DB2.0） ---------- Bitcoin

・DB2.0, Shared DB, P2P DB

プライベートチェーン

・ビットコインのパブリックチェーンに対して、プライベート・コンソーシアムチェーンと呼ばれている

・Ripple（Interledger）はビットコイン以前の会社・技術

・ブロックチェーンをバズらせたのがDigital Asset Holdings

・GS, モルスタ等の大手金融が立上げたR3CEV（今年、初期の主要金融機関は離脱）のCordaで、日本のメガバンク3行と野村がジョイン

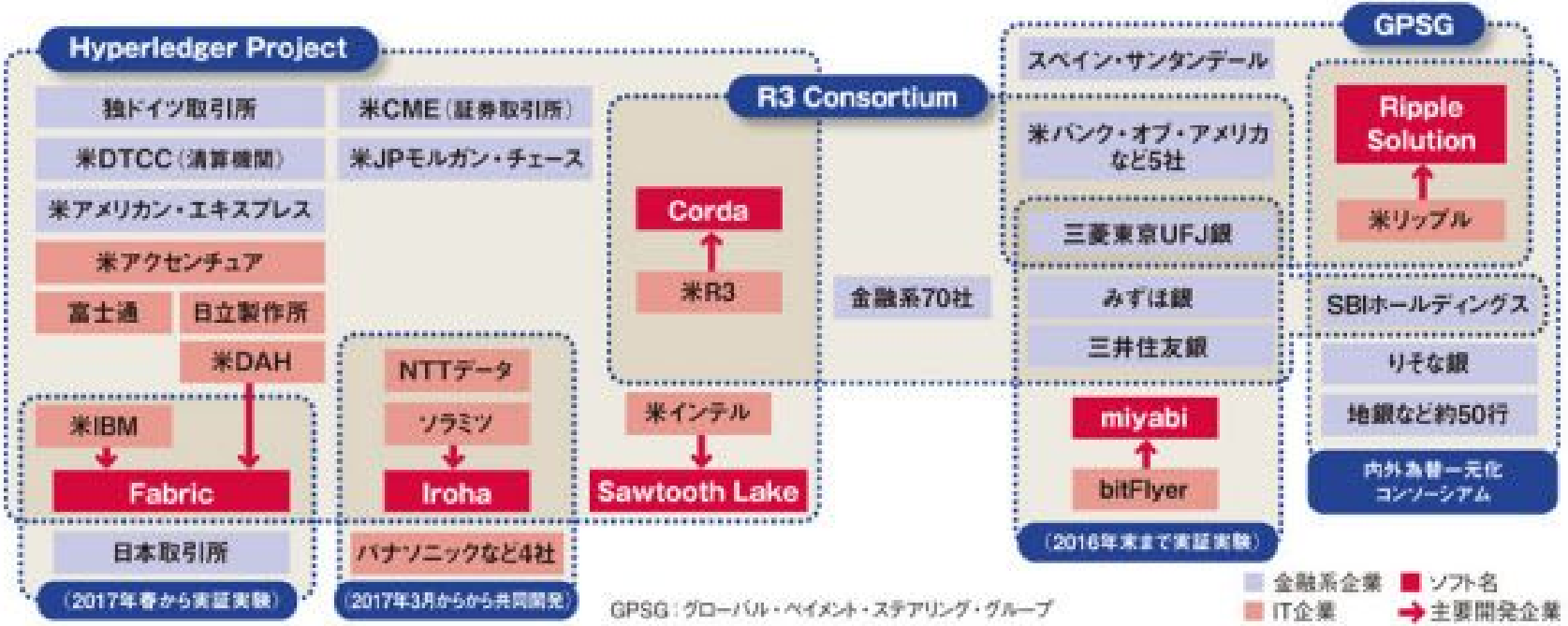
・その後、世界の大手企業がLinux Foundationの下で、Hyperledgerを立ち上げた

・Orb, Mijin, Miyabi, Irohaは日本のヴェンチャーが開発中

TCGに身近なプロジェクトは？

- **Hyperledger** Fablic by IBM, 日立, 富士通, NEC
- Hyperledger Sawtooth Lake by Intel
- Hyperledger Iroha by ソラミツ, パナソニック, NTTデータ
- Ripple by Ripple & SBI
- Orb, Mijin, Miyabi @ Japan
- **Enterprise Ethereum Alliance**

5/22 日経ITproより



伊藤穰一氏@MIT media labの予測

・インターネット以前は各国内で電信電話会社が全てを提供していた

・ミニテルが終了した様に、R3CEVも終了するだろう

・AOLが生き残った様に、Hyperledgerも生き残るだろう

・ベストな技術よりもベストなコミュニティが影響力を持つ（垂直水平各レイヤーとグローバルに相互作用必須のため）

・オンラインでの合意は困難で、F2Fでの合意が効率的

・以下、2017年11月ScalingBitcoin@スタンフォードのキーノートより

https://www.youtube.com/watch?v=3pd6xHjLbhs#t=25m

本日のトピックス

・ビットコイン

・Ethereum

・プライベート・コンソーシアムチェーン aka DLT

・ICO

・TCG卒の活躍

・インターブロックチェーン

Initial Coin Offering

・IPOは発行者側に有利なので、消費者保護のために規制されている

・ICOはIPOよりも更に発行者に有利で、現在は投機商品

・改正資金決済法で仮想通貨は規制されたが、ICOはグレー領域

・これまで、ICOの99%が詐欺的だったが、優良案件増えて90%が詐欺的

・米SECに有価証券とみなされると違法

・中国、韓国はICOを禁止

様々なICO

・2013年　XRP　ICO以前にサービスあり

・2014年　Ethereum　ホワイトペーパーのみ　ICO後、サービス開発

・2014～2015年　Mastercoin, Counterparty　一部で流行

・2016～2017年　Ethereumの場合、TheDaoは失敗するが、ERC20は大成功

・無数の詐欺コインも存在します（約90%）

本日のトピックス

・ビットコイン

・Ethereum

・プライベート・コンソーシアムチェーン aka DLT

・ICO

・TCG卒の活躍

・インターブロックチェーン

TCG卒の活躍

・Rivez by Steven Sprague https://twitter.com/skswave

・Stevenのプレゼン https://www.youtube.com/watch?v=uPotM2ItHPM

https://www.youtube.com/watch?v=BKDDY0iN-wI

・TCGのキラーアプリはBitcoin、Bitcoinのキラーアプリは TCG　と2014年、言ってました
@Miami, Austin, NYC, Las Vegas

Ari Singer, Advisor, rivetz

Ari Singer is an energetic and experienced strategist, high-tech product manager, entrepreneur and security specialist. He is co-founder and CTO of TrustiPhi, LLC, where he leads technical strategy and solution delivery for enabling hardware-based security in next-generation devices. He is a former VP of Trusted Computing at Digital Management, Inc. and at NTRU Cryptosystems, where he was integral to helping to define the US Department of Defense's Trusted Computing technical strategy and enabling industry leaders to deploy Trusted Computing technologies. Ari has frequently served in leadership roles in standards organization including as chair of the Trusted Computing Group (TCG) Trusted Platform Module (TPM) and TPM Software Stack (TSS) working groups, as chair of the IEEE P1363 working group for public key cryptography and as security editor for IEEE 802.15.3, IEEE 802.15.4 and Efficient Embedded Security Standard (EESS) #1. Ari received a BS in Mathematics and a BA in Music from

Greg Kazmierczak, Advisor, rivetz

Greg participated heavily in standards organizations for over 20 years. He was a member of the Board of Directors and the technical oversight committee (TC) in the Trusted Computing Group (TCG) and directly participated as an author, editor or contributor to over 60 Publications and Specifications by TCG, IETF, OASIS, IEEE, and NIST. His primary contributions have been on standards relating to platform trust services, attestation, and key management with a special focus on hardware-enforced isolated execution environments such as Trusted Platform Modules, Trusted Execution Environments, and Self-Encrypting Drives. In addition, Greg has contributed to numerous government-industry initiatives and committees, has been a spokesman for the Trusted Computing industry and a frequent speaker and expert panel member at conferences and industry events such as RSA, Cybersecurity Information Forum, and Trusted Computing Conference.

Steven Sprague

・2014年2月　@Austin, Texas

TCGを情熱的に説明

https://www.youtube.com/watch?v=XCLxf0z3_s0

Steven Sprague, CEO at Rivetz - The North American Bitcoin Conference 2/16/2017

・trezorの場合、trusted display, trusted input, trusted executionまであるが、attestation verificationに欠けるとの指摘

https://www.youtube.com/watch?v=JCCVryYq428

Steven at Texas, 10/29/2017

・2014年以降のStevenの技術の進化と洗練が解るプレゼン

・TCG技術をビットコイン・ブロックチェーンに応用

・しかし、too much感あり

・TCG技術は依然として高価

・TCGの応用として最新かつ最高のプレゼン？

・ICOを含む

https://www.youtube.com/watch?v=GCIwvVz1xws

TEE を活用するセキュリティ by rivetz

・Secure Display

・Protected Keys

・Secure PIN

https://www.youtube.com/watch?v=MJ8OBXCV760

https://www.youtube.com/watch?v=zD-2Q_YTiGs

秘密鍵の取り扱い

・rivetzはTEEを利用する高度なセキュリティを提供中だが、

・多くの消費者は公開鍵暗号の理解が浅く、秘密鍵の存在自体を知らない

・秘密鍵を取引所に預けたり（危険）

・Android, iPhoneを利用（取引所よりは安全か？）

・trezor, ledger nano等の専門HWを利用（$50～150）

・一般ユーザーにはtrezorで十分だが、rivetzはその先のセキュリティを提供中

rivetzのICO

・ID/passwordによる認証をトークンでリプレース？

・米国の2FAは、SMSが多かったが、電話番号を悪用されて、IDを乗っ取られる事例が多発。これをリプレースしたい

・テレグラムにグループあって、日々試行錯誤中

rivetzのICO　cyber security token

・Stevenによる説明
https://www.youtube.com/watch?v=cEpAa0eNsc4
https://www.youtube.com/watch?v=XI1mgrxgyo4

・肯定派
https://www.youtube.com/watch?v=Ejh8g1_lecs
https://www.youtube.com/watch?v=xkn0YFdTBuc

・否定派
Everything Wrong with the Rivetz $200 million ICO
https://www.youtube.com/watch?v=H4rIeRaT4QE

トークンエコノミー

・有価証券型のICOは違法

・Appトークン、Utilityトークンならば OK

・機能提供以外にソーシャルな面を持つ

・ビットコインの場合、トークンホルダーがインフラ＆アプリ層の開発者でもある

・サードパーティがトークン価値向上のために働くとトークンエコノミーは成功（ビットコイン、イーサリウム、モナコイン）

・モナコインはライトコインのパクりで、ライトコインはビットコインのパクリだが、モナコインは国産コインなので言語の壁はない

本日のトピックス

・ビットコイン

・Ethereum

・プライベート・コンソーシアムチェーン aka DLT

・ICO

・TCG卒の活躍

・インターブロックチェーン

今後、ブロックチェーン・金融システムはどうなるか？

・ビットコインがレイヤー2以上でスケールを続けて、ザ・金融インフラになる可能性　＝　各国の法定通貨、証券をIOUあるいはアセットとして流動させる

・ビットコイン以外のイーサリアムやICOが持続的に発展して、インターブロックチェーンが花開く可能性　＝　Polkadot, Cosmos, Interledger, TumbleBit, Atomic Swap等が機能する。そしてプライベート・コンソーシアムチェーンと接続する

・web3.0　クライアント・サーバーではなく、P2P接続されるweb

Parity Technologies, Advisor, rivetz

Founded by Gavin Wood, founder and former CTO of Ethereum, Parity Technologies is a VC funded enterprise dedicated to trust-free technology. Its flagship product, Parity Ethereum, is the world's fastest Ethereum client that integrates directly into your browser. "We are pleased to be and advisor to the Rivetz project to help bring advanced cybersecurity controls to protect the private keys and instructions for decentralized services and help customers achieve the provable controls required for Blockchain applications, cloud access, and secure IoT," said Dr. Gavin Wood.

消費者向け　回復パスフレーズ

・iPhone, Androidのビットコイン財布の中には、秘密鍵をサーバーに預けるタイプと階層的決定性鍵ペアを持つタイプがある

・階層的決定性財布の場合、仮にスマホを紛失しても、回復パスフレーズの入力で、一意に鍵ペアが復活する

・パスフレーズ　→　マスターシード　→　一意な鍵ペア

結論

・TCG技術はビットコイン、イーサリウム、ブロックチェーン、ICO、インターブロックチェーン周辺のビジネスに役立つ可能性が高い

・TCG技術者（特に暗号に強い人）にとって新たな成長市場である

・UI, UXは常に課題である（セキュリティ、プライバシー、UI, UX）

・消費者向けは、使いやすさ・解りやすさが要求されるのでTCGはtoo muchで、ビジネス・政府・軍事向けが適当