仮想通貨技術　三つの話題

2018年4月27日
(株)IT企画　才所敏明
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp/

 1

自己紹介

福岡出身:　香椎中学➔福岡高校➔東京大学

1970年　東芝入社

社内計算機利用環境企画・構築・活用指導・支援

情報セキュリティ研究開発企画・推進、事業支援

2007年　(株)IT企画設立

事業支援活動(顧問・相談役)

大学教育活動(情報セキュリティ講師)

研究開発活動(研究員)

研究対象分野:サイバーセキュリティ、IoT、FinTech、ビッグデータ

 2

仮想通貨技術　三つの話題

（１）Bitcoin is harmful!
　　元凶は、PoW（マイニング競争）

（２）法定仮想通貨の時代に？
　　国家による仮想通貨発行の動向

（３）仮想通貨技術の新潮流
　　ビッグデータ対応およびIoT対応

 3

（１）Bitcoin is harmful!

ビットコインの
コンセンサスアルゴリズム（PoW）
が引き起こす社会課題

 4

ビットコインのPoW（Proof of Work）

トランザクション（取引）の承認権を得るための競争
　承認者は、報酬（現在は12.5BTC）をGet！
　　（マイニング（採掘）競争）

ブロックを構成するトランザクションの集合に
　任意の数（nounce）を加え、
　SHA-256によるハッシュ値（hexadecimal）が
　先頭に0が一定数（現在は18個）並ぶようなnounceを
　最初に見出したら、承認権をGet！

作業のための計算量は、
　　一般に10分程度で決着がつくように設定

5

Bitcoin is harmful!

トランザクション1件処理に必要な電力消費量は、
　　VISAの4000倍以上が必要，　米国家庭9軒の1日分に相当
現在のビットコインネットワークの計算能力の総計は、
　　世界の高速スーパコン500番目までの合計の10万倍以上
現在、ビットコインネットワークの
　　電力消費量は31 terawatt-hours/year
　　1日当たり450 gigawatt-hours増加中
　　（ハイチ（1085万）の全国の電力消費量の1年分に相当！）
現在のペースで電力使用量が増加すると・・・
　2019年7月までに、ビットコインネットワークは
　　米国全体の現在の電力を上回る電力を必要となる見込み
　2020年2月までに、ビットコインネットワークは
　　世界全体の現在の電力と同程度の電力を使用する見込み

6

コンセンサス（合意形成）アルゴリズム

PoW：Proof of Work　　代表例：Bitcoin
　最初にマイニング（採掘）に成功した人に、
　　承認権と報酬
PoS：Proof of Stake　　代表例：Etherium
　保有している量に応じて、承認権と報酬
PoI：Proof of Importance　代表例：NEM
　保有している量に加えて、
　　取引を活発にしている人に、承認権と報酬

＜社会システムでは、PoWの利用はあり得ない＞

（2）法定仮想通貨の時代に？

国家による仮想通貨発行の動向

仮想通貨規制の動き

背景　現在の仮想通貨の問題

マネーロンダリング（資金洗浄）

テロリストへの資金流入

ICOまがいの詐欺の横行

価格変動による金融システムの不安材料

仮想通貨への規制の動き

中国：昨年、国内3大取引所での仮想通貨と人民元の取引禁止

今年、更に規制強化の動き

韓国：今年、国内仮想通貨取引所閉鎖の検討を発表

日本：昨年、改正資金決済法の施行

「仮想通貨交換業」としてのマネロン対策の義務化

仮想通貨のルール作りには国際的な協力が必要（ドイツ、フランス）

3月のG20財務省・中央銀行総裁会議で規制案が提案される模様

国家による仮想通貨発行
ベネズエラ・ボリバル共和国：Petro

背景：2017年当初今年初めに1ドル3000ボリバルであったのが、

2017年12月には103000ボリバルにまで通貨価値が下落

Petroは、自国の石油資源（世界一の埋蔵量）を担保にして発行。

イーサーリアムのブロックチェーン上で発行（2月頃？）され、

時価総額50億ドル相当のトークンとなる予定

ベネズエラでの税金の支払い、公共サービス支払い、オンライン取引などに使用可能。更に、石油資源に担保されているため、ペトロの価格は理論上市場の原油価格と連動して推移するため、ベネズエラ国外に住む人は投機商品として利用することもできる。

多くの場所や用途で利用されることが予想され、少なくとも3100万人のベネズエラ国民が使用。これは現在の世界における仮想通貨の利用人口よりはるかに多い。

10

国家による仮想通貨発行
エストニア共和国：Estcoin

背景：IT立国を目指すIT先進国。安定した経済成長、政府主導のデジタル戦略、スタートアップ環境の整備等により、優秀な起業家・エンジニアの誘致に成功、欧州圏のIT市場のオフショア開発拠点へ。

e-Government構想：エストニア国民はICチップ入りの国民カード1枚で、投票から医療、教育、納税、銀行、警察関連など全ての手続がオンライン上で完結。

e-Resident構想：外国人もエストニアのデジタル市民となり、オンラインで行政サービスを利用したり、起業したり等が可能。（現在、138か国の2万2千人以上が登録済み（日本人も400人以上）。エストニアの人口は130万人。）

Estcoinの詳細は未発表：

欧州中央銀行総裁は、ユーロ圏の通貨はユーロのみ、と反応。

エストニア政府は発行主体にならず、e-Residencyの一環として、

別組織による発行となるかも（国家の仮想通貨とはならない？）。

（イーサリアムの創業者Vitalik Buterinがアドバイザーになる可能性？）

国家による仮想通貨発行
各国の動向（噂も含め）

ウルグアイ：eペソ（2017年11に試験運用開始）

ロシア：クリプトルーブル（プーチン大統領が発行指示？）

カナダ：CADコイン（Bank of Canadaが研究中）

オランダ：DNBコイン（De Nederlandsche Bankが研究中）

米国：Fedcoin（噂）

「世界中から紙幣が廃止されるまでは、もはや時間の問題」

「全ての中央銀行は最終的には独自の暗号通貨を必要とするようになる」

日本では・・・　日本銀行は、仮想通貨、各国の動向を注視中

＜MUFGコイン（三菱東京UFJ）、Jコイン（みずほ、郵貯、地銀）＞

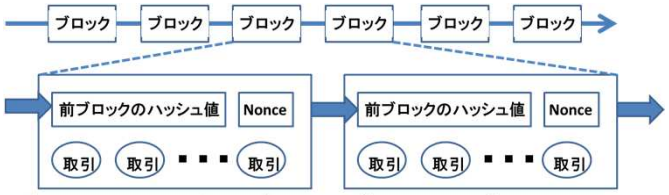
（3）仮想通貨技術（ブロックチェーン）の新潮流

ビッグデータ対応とIoT対応

仮想通貨技術（ブロックチェーン）特徴機能

（1）記録情報の改ざんが困難である

情報のハッシュ値を利用した情報の連鎖



ビットコインの例：ブロック高　51万ブロック

（2）記録情報が障害に強い

記録情報の分散管理（重複管理）

ビットコインの例

フルノードの数　7000程度

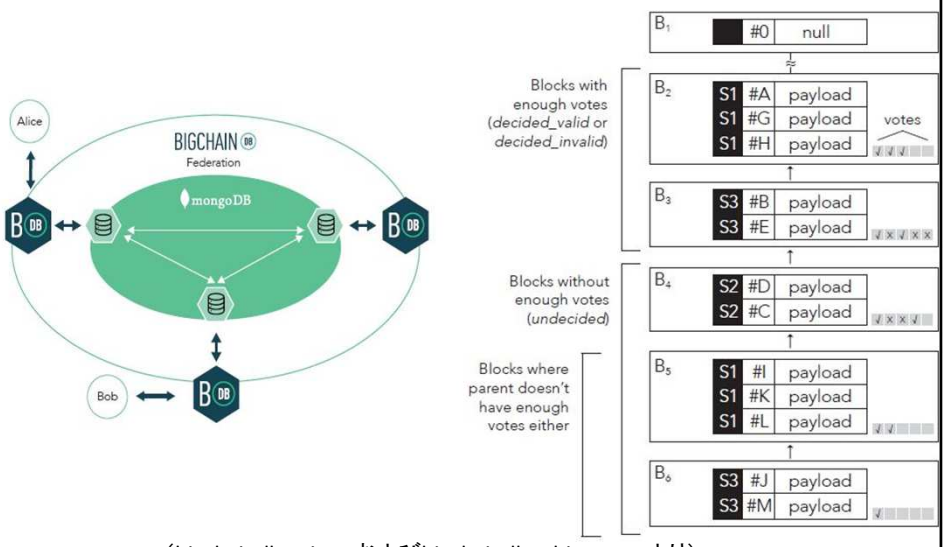
（フルノードのデータサイズ　180GB程度）

仮想通貨技術の新潮流？
ビッグデータ対応：BlockchainDB

概要：大企業が求める処理能力、大容量、
および多様な検索・アクセス制御を提供する
データ管理機能に加え、ブロックチェーンの特徴機能
（記録データの不変性、分散コントロール、
資産の登録・移転等）を提供

実現方式：ビッグデータ管理システム
（MongoDB：NoSQL DBMS）へ
ブロックチェーンの特徴機能を付加

BlockchainDB



（bigchaindb-primerおよびbigchaindb-whitepaperより）

BlockchainDB

開発元：BlockchainDB GmbH（ベルリン）　発表：2016年2月

現状：オープンソースとして公開（機能強化は継続中）

Apache License 2.0で再配布可能

世界で20社以上がパートナー企業となり、

応用PJが進行中（日本企業：リクルート、トヨタ）

トヨタは、MITのメディア・ラボと協力し、

ブロックチェーン技術企業と提携

具体的には、TRI（Toyota Research Institute）が主導

BigchainDBは、自動運転や自動運転テストの

データの安全な共有にための分散暗号化DBを担当

 17

仮想通貨技術の新潮流？ IoT対応：IOTA

概要：機械と機械が直接取引を行うことを想定した、

IoT向けの仮想通貨/決済プロトコル

特徴は、マイナーが不要で、

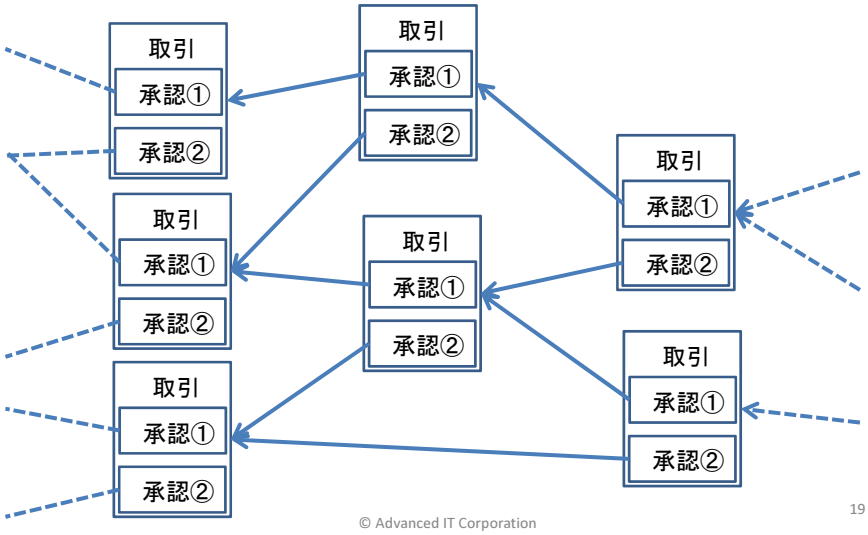
取引手数料がかからないこと

実現方式：ブロックチェーンでは無く、

Tangle（DAG：有向非巡回グラフ）を使用

 18

Tangle（イメージ）



IOTA

開発元：IOTA Foundation　2016年7月

現状：オープンソースとして公開（機能強化は継続中）
2017年11月、IOTA上で
分散型データ販売市場確立のため
20社以上とパートナーシップ契約
（マイクロソフト、富士通、シスコ、
フォルクスワーゲン、サムスン等）

終