仮想通貨とブロックチェーン技術の現状と課題

2017年9月15日

認定NPO日本システム監査人協会　近畿支部　定例研究会

荒牧 裕一
（京都聖母女学院短期大学）

1

仮想通貨の最近の動き（2016年）

- 2月20日　香港合意（4月よりSegwitのリリース）
- 5月25日　資金決済法改正（1年以内に施行）
- 6月17日　The DAO事件
- 7月 9日　ビットコイン半減期　25BTC→12.5BTCへ
- 7月20日　Ethereumがハードフォークを実施
  （Ethereum Classic（ETC）との並存）
- 8月 3日　Bitfinex（香港）事件　ハッキングにより
  119,756BTC（約70億円）が流出

2

改正資金決済法の概要

仮想通貨の定義（2条5項）
①電子的に記録・移転でき、法定通貨または法定通貨建ての資産ではない財産的価値
②次のいずれかの性質を有する
(1)不特定の者に対して、代金の支払等に使用でき、かつ、法定通貨と相互に交換できる
(2)不特定の者が(1)と相互に交換できる

仮想通貨交換業者の規制（63条の2～63条の22）
①登録制の導入（9月末まで猶予期間）
②利用者への適切な情報提供
③利用者財産の分別管理
④取引時の公的証明書の確認（マネーロンダリング対策）

3

The DAO事件（2016年）とは

新世代仮想通貨　Ethereum上のアプリでの問題
（スマートコントラクトを可能にするプラットフォーム）

The DAO（投資ファンド）が7,620,000ETH（当時の相場で約150億円）をクラウドファンディングで調達

The DAOのコードに脆弱性があり、3,641,694ETHが流出（ただし、仕様により27日間保留される）

関係者が検討の結果、流出分を返還させるハードフォーク（分岐）を実施

分岐反対派がEthereum Classic（ETC）を作る

4

仮想通貨の最近の動き（2017年）

- 4月 1日　改正資金決済法施行
- 5月23日　ニューヨーク合意（Segwit2xの導入）
- 6月22日　Ethereumがフラッシュクラッシュ（$317.81→$18）
- 7月23日　Segwit有効化（非賛同のブロックを拒否）
- 7月25日　BTC-e（ブルガリア）事件　経営者が逮捕
- 8月 1日　ハードフォークでBitcoin Cash（BCH）誕生
- 8月24日　Segwitアクティベーション
- 11月中　　Segwit2xのハードフォーク（予定）

5

スケーラビリティ問題

ビットコイン取引が活発化しブロック容量が問題となる（取引記録容量は1Mバイト／B、約60万件／日）
→手数料の高騰（500円程度）、送金遅延（2週間）

解決策①　**Segwit**（Segregated Witness、BIP141）
取引記録容量は変えず、認証データーを整理して、取引記録件数を2倍弱に引き上げ（ソフトフォーク）

解決策②　**Segwit2x**
取引記録容量を2Mにする（ハードフォーク）

解決策③　**Bitcoin Cash等**
取引記録容量を最大8Mにする（ハードフォーク）

6

Segwitの特徴

長所
①取引記録件数の増加（1件のデータ量の減少）
②トランザクション展性（トランザクションIDを後から変更できる性質）の解決
③ライトニングネットワークを導入可能にする修正

マイナーに不利な点
①ASIC Boost（採掘効率を20～30%向上させる裏技的な技術）が使えない
②短期的に送金手数料の収入が減少する
③ライトニングネットワークはマイナーに取って不利

7

ライトニングネットワークとは

ビットコインが苦手とする送金取引
①高速取引（1確認に10分もかかる）
②大量取引（Segwitでも約100万件／日）
③手数料未満の少額取引（マイクロペイメント）

高速・大量・少額取引向けの送金手段の付加
①ペイメントチャネル
　特定2者間での送金をオフチェーンで実行
②ライトニングネットワーク（LN）
　不特定多数間での送金を可能にするネットワークを、別途レイヤ2として構築する

8

Bitcoin Cash騒動（2017年）とは

ニューヨーク合意に納得しない中国マイナー勢力がハードフォークを実施して誕生（略称：BCH）

①取引記録容量を段階的に8Mまで拡大
②ハードウェアウォレットセキュリティの向上　等

・分岐以前のチェーンはBTCと共通（アドレスも共通）
→分岐時点のBTC保有者は、BCHも同量取得
・BTCのマイニング機器と互換性あり

・価格は、1BCH＝0.1～0.2BTC程度で推移
・参加マイナー数は、難易度により変動（逆転も）

9

Bitcoin Cash騒動の派生的問題

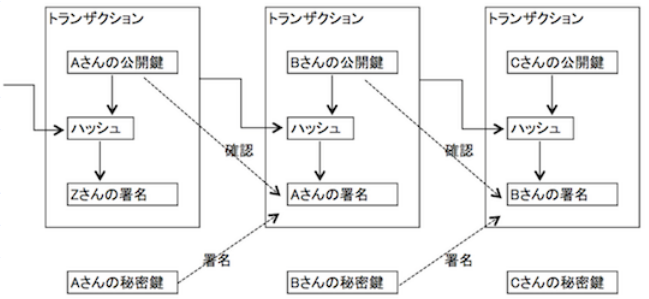
取引所等が、顧客に同量のBCHを配布するか
・日本の多くの取引所はBCHを配布（時期は様々）
・Bitstamp等は配布しない旨を事前に宣言
※BCHを配布しない、または配布が遅れた取引所等は、BTC現物を保有していない可能性有

分岐前にBTCを借りた者は、分岐後にBCHも合わせて返済しなければならないか
→Coincheckでは返済義務を課した（7月21日公告）
・レバレッジ取引でショートポジションを持つ者
・信用取引でビットコインを借りている者

10

ビットコインの仕組（概要）

ビットコインそのもののデータは存在せず、
ディジタル署名を使った取引データだけを管理



（出典：「ビットコインのしくみ」http://bitcoin.peryaudo.org/design.html）

11

二重譲渡の危険

ディジタル署名を使うことにより、正当な権利者からの譲渡であることは保証される

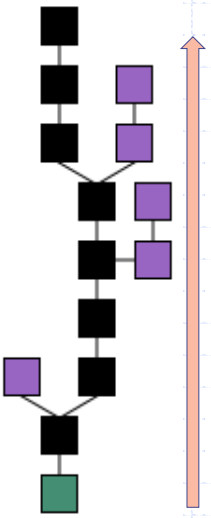
しかし、ディジタル署名やハッシュ値はコピー可能であるため、二重譲渡は防げない

通常の送信ソフトには二重譲渡検出機能があるが、それだけでは防止できない

登記簿のような登録台帳が必要となり、
ブロックチェーンと呼ばれる独自の登録台帳が用いられている

12

ブロックチェーンのイメージ



複数の取引をまとめて1ブロックを生成する（約10分に1ブロック）

新しいブロックを、これまでのブロックがつながったチェーンに追加する

ブロックチェーンに追加するには、一定の条件を満たしたキー（nonce）が必要

分岐した場合は、後続ブロックが長くなった方が正当なものと扱われる

13

ブロックチェーンの承認作業

ブロックチェーンに追加するために必要な「キー（nonce）」を計算で見つける作業

「直前のブロックのハッシュ値」
「新ブロックのハッシュ値」
「キー（nonce）」の3つを合わせて再度ハッシュ化した値が、一定値以下でなければならない。

一定値を変動させることで、難易度が調整される

平均10分でキーが見つかるように、難易度が定期的（約2週間）に見直される。

14

承認作業(コンセンサスアルゴリズム)の分類①

Proof of Work(PoW)

参加者が、特定の条件を満たす解を求める計算を繰り返し、最初に解を求めた者に承認の権利を与える方法
Bitcoinでは、単純なハッシュ関数による計算が採用されているため難易度が非常に高まり、資源の浪費が問題となっている。そのため、Litecoin等ではScrypt(S-Crypt)を採用して難易度の上昇を抑えている
Bitcoin、Litecoin等で採用

15

コンセンサスアルゴリズムの分類②

Proof of Stake(PoS)

仮想通貨の保有割合や保有期間等に応じて、承認の優先権を与える方法
大量の仮想通貨を持つノードが不正を働くと、自ら仮想通貨の信頼を低下させ、価値を下げることになるため、不正をしないインセンティブが働くとされる(本当か?)
「何も賭けていない問題(分岐した全てを承認すれば困らない)」等も指摘されている
Ethereum(予定)、Bitshares、NXT 等で採用

16

コンセンサスアルゴリズムの分類③

Proof of Importance（PoI）

ノードごとの取引額・残高を指標とした取引グラフ分析により、残高と取引状況をクラスタリングして、個別のノードの重要性を計算し、より重要なノードにハッシュ計算の優先権を与える（より難易度の低いハッシュ計算問題を割り当てる）方法

NEM で採用

17

参加者の範囲による分類

パブリック（Public）
不特定多数が参加可能

コンソーシアム（Consortium）
特定の団体や企業グループのメンバで参加する

プライベート（Private）
単一の組織や企業内で利用する

コンソーシアムやプライベートのメリット
- **不正をしようとするノードを事前に排除できる**
- **高速処理が可能**
- **バージョンアップを頻繁に出来る**

18

ブロックチェーンの活用

ビットコインのブロックチェーンを活用
・文書存在証明
・資産管理・交換（Colored Coins、Counterparty ）
・クラウド・ファンディング

パブリックのブロックチェーンを活用
・ドメイン（.bit）の管理（Namecoinで実現）
・スマートコントラクト（Ethereum等）

コンソーシアムやプライベートのブロックチェーンを活用

19

ブロックチェーンの活用

出典：野村総合研究所,「平成27年度　我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書」,P33

20

ブロックチェーンの一般的な定義

- P2Pベースの分散型ノード間でトランザクションデータを共有する。
- 複数のトランザクションデータが1ブロックにまとめられる。
- 参加ノードにより承認されたブロックがチェーン（台帳）に結合される。
- ブロックは前のブロックとハッシュ関数等で繋がれ、チェーン内の過去のデータを部分的に変更することを防止する。

21

ブロックチェーンの一般的な問題点

- フォーク（分岐）が可能である
- 複数のブロックチェーンの併合は難しい
- 取引の確定（ファイナライズ）に時間がかかる
- 全ての取引がブロックチェーンに記録される保証がない（網羅性に問題が生じる）
- 厳密な時刻管理が難しい（分散処理一般）
- CAP定理（分散処理一般）

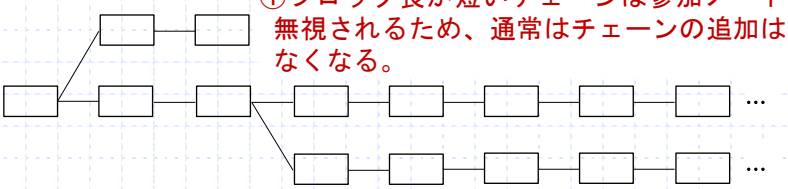
22

システム監査上の留意点①

分岐（フォーク）が可能である

＊正当でないチェーンも消えるわけではない
＊二重台帳となる危険性がある
＊POS、POIでは、長いチェーンも比較的容易

①ブロック長が短いチェーンは参加ノードから無視されるため、通常はチェーンの追加はされなくなる。



②意図的に分岐させ、それを一部のノードだけで維持し続けることも可能である。

23

システム監査への配慮

メインチェーンであることを客観的に確認できる仕組みが必要

・スーパー・ピアが、チェックポイント・ブロックを挿入して確定（Orbで採用）

→P2P分散型システムの利点を減殺

・独立した第三者が承認作業に参加
（システム監査人自身、それ以外の機関）

24

システム監査上の留意点②

複数のブロックチェーンの併合は難しい

＊既存のブロックチェーン同士の併合は難しい
＊新ブロックチェーンへ残高を移行する形か
＊ブロックチェーンには、取引データは記録されるが、アドレス別の残高一覧表はない

併合には慎重な検討が必要
・データの残高の確定
・移行すべきデータに漏れはないか
・不正なデータが追加されていないか
・移行期間はどの程度必要か

25

システム監査上の留意点③

取引の確定（ファイナライズ）に時間がかかる

＊理論的には分岐のリスクはゼロにならない
＊参加ノード、承認作業時間によってリスクが変化する
＊取引の順番に承認されるとは限らない

確定と見なす基準が適正か
・〇回ブロックが続けば確定
・独立した第三者が承認した時点で確定
・スーパー・ピアが、チェックポイント・ブロックを挿入して確定（Orbで採用）

26

システム監査上の留意点④

全ての取引がブロックチェーンに記録される保証がない（網羅性に問題が生じる）

＊ビットコインでは、タイムアウトで承認されないことがある
＊プライベート・チェーンなら、全ての取引を記録する仕組みも可能か

対策の内容を確認する
・取引時間が早いデータを優先的にブロックに入れる仕組み
・個別取引の帳簿データに記録を残す

27

システム監査上の留意点⑤

厳密な時刻管理が難しい（分散処理一般）

＊全てのノードの時刻を統一する必要がある
＊パブリックやプライベート・チェーンなら、ある程度の時刻管理が可能な場合もある
（NTP、独自プロトコル）

時刻管理に関する要件と対処法を確認
・時刻管理の方法と予想される誤差
・誤差が許される範囲か
・通信時間や取引確定との時間差にも留意
・日をまたいだ場合の処理のルール等

28

システム監査上の留意点⑥

CAP定理（分散処理一般）

次の3つのうち完全に満たせるものは2つのみ
＊ C（Consistency、一貫性）：全てのノードで最新のデータを同時に保持している
＊ A（Availability、可用性）：特定のノードの障害により、他のノードが影響を受けない
＊P（Partition-tolerance、分断耐性）：ネットワークに障害があっても継続して動作すること

・ビットコインでは、A，Pを満たす、Cが犠牲

29

参考文献・資料

1.中本哲史,「ビットコイン：P2P 電子マネーシステム」,2009年
2. 野村総合研究所,
「平成27年度　我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書」,2016年3月（2016年4月28日 経済産業省HPにて公表）
3. ビットバンク株式会社,『ブロックチェーンの衝撃』編集員会,『ブロックチェーンの衝撃』,2016年6月13日
4.金融庁,「資金決済法パンフレット」
http://www.fsa.go.jp/common/about/20170403.pdf
5.MUFJ,「ブロックチェーン」『INNOVATION HUB』
https://innovation.mufg.jp/category/blockchain/
6. 大石哲之,「ライトニングネットワークの衝撃～ビットコインによる本当のマイクロペイメントがもたらすもの」『ビットコイン研究所ブログ』
http://doublehash.me/what-is-lightning-network/
7.Coincheck HP,「2017年8月1日「Bitcoin Cash」に係る対応方針と一部機能の停止について」,https://coincheck.com/blog/4042

30