ブロックチェーンの６つの通説を覆す

2017.09.25

（株）ユニバーサルエネルギー研究所

ここで話題にあがるブロックチェーン技術は、Bitcoin に使用されているバージョンを取り上げるものとする。

ブロックチェーン技術を用いて Bitcoin の仕組みが完成したのは 2009 年だ。それ以来 9 年間、Bitcoin に見つかった深刻な脆弱性はただ 1 つ、ある悪質な犯罪者が 920 億 BTC の不正入手に成功したときだった。この問題を解決するのは非常に困難であったが、それでも、9 年間で脆弱性がたった 1 つというのは、優秀である。

ブロックチェーンは素晴らしい用途をいくつも示してきた有用な技術であり、短所はありながらも、他にはない優れた長所を持ち合わせている。ただ、話題性と革新性を追い求めるあまり、多くの人が利点だけに注目し、全体像を冷静に見ることを忘れ、不都合な点に目をつむっているのではないか。

ブロックチェーン技術に心酔して短所が見えなくなっている人もいれば、技術の仕組みを理解していない人もいるだろうし、また全てを理解していながら自分にとっては有利なシステムだと考える人もいるだろう。

今回はブロックチェーンの話題性と革新性を追い求めるあまり、全体像を冷静に見ることを忘れ不都合な点に目をつむることがないよう、ブロックチェーン技術の短所を取り上げる。

問題提起されるブロックチェーンの通説は以下の６つ

- ブロックチェーンは巨大な分散型コンピューターである
- ブロックチェーンは永続的なもの。ブロックチェーンに記録された内容は永遠にそこに残る
- ブロックチェーンは極めて有効で拡張性にも優れている。従来型の通貨はやがて消えてなくなるだろう
- マイナーの存在がネットワークセキュリティを担保する
- ブロックチェーンは中央管理システムがないため破壊できない
- ブロックチェーンの匿名性とオープン性は良いことである

1. ブロックチェーンは巨大な分散型コンピューターである

ブロックチェーンの仕組みを詳しく調べたことのない人は、ブロックチェーンとはある種の分散型コンピューターであるという印象を持っているかもしれないがそれは誤りである。膨大な数のコンピューターが行っているのは、次のような処理だ。

・同じルールに従って同じ取引を検証し、同じ演算を実行する。
・同じものを 1 つのブロックチェーンに記録する。
・全履歴を保存する（この履歴はどのノードでも常に同じ内容）。

このように並行処理、共同作業、相互支援などというものは一切なく、瞬時に数百万の複製が行われるだけである。効率とは正反対だが、ブロックチェーンの基本原則の 1 つ「誰も信用しない」ことを達成するには、このように P2P 方式で成り立つようにしなければならないのだ。

2. ブロックチェーンは永続的なもの。ブロックチェーンに記録された内容は永遠に残る

先ほど述べたようにブロックチェーンのデータはネットワーク上すべてのノードで同じになるようにしなければならないため、データが大きくなりすぎると毎回のダウンロードと検証に莫大な時間がかかってしまう。実際、Bitcoin ネットワークの全取引履歴を保管している高い計算能力を持つノードは、すでに 130 GB もの大きさに達している(2017/09

現在)。

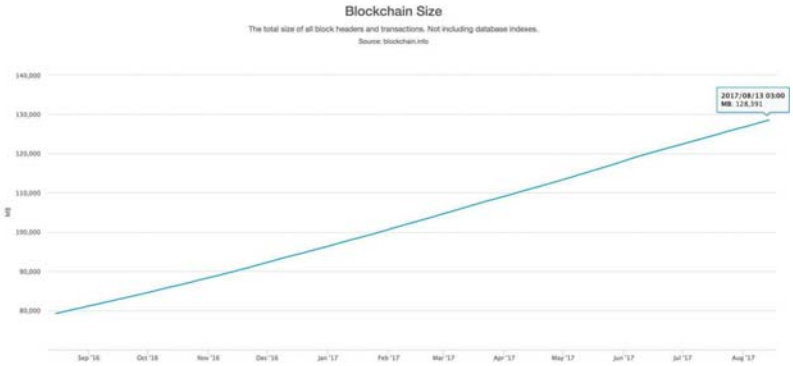

図 1. ブロックチェーンのサイズの推移。
出典:blockchain.info

Bitcoin ネットワークで処理される取引の数が増えるほど、ブロックチェーンのサイズが拡大するスピードも速くなるため、現状では、ブロックチェーンの寿命は 10 年に制限されている(ハードディスク容量の拡大スピードの方が、間違いなく遅いため)。

「データがまったく同じなら、すべてのネットワークノードに保管するのをやめればいいのでは?」と考える人はいるかと思う。しかしそれでは、ピアツーピア方式のブロックチェーンではなく、従来型のクライアント/サーバー型アーキテクチャになってしまい、クライアントがサーバーを信用する必要が出てきてしまうのだ。

3. ブロックチェーンは極めて有効で拡張性にも優れている。従来型の通貨はやがて消えてなくなるだろう

ブロックチェーンの場合、各ネットワークノードが同じ処理をするので、ネットワーク全体のデータ処理能力は 1 つのネットワークノードのデータ処理能力と同様になり、Bitcoin ネットワークは、1 秒あたり最大 7 件の取引を処理可能となっている(最大ブロックサイズ 1MB/(平均メッセージ容量 250B*ブロック承認時間 600 秒))。しかし世界各地の膨大な数の利用者に対して、この程度しかならないのだ。

加えて、Bitcoin ブロックチェーンの取引は 10 分に 1 回しか記録されない試用になっている。さらに、決済の安全性を高めるため、新しい取引が記録されてから 50 分以上待つのが一般的である。従来型の通貨の代わりとなったときスナック菓子1つ買うのに 1 時間並んで待つことができるだろうか?

現時点で世界中の 1,000 人に 1 人しか Bitcoin を利用していないことを考えると、今後アクティブユーザーの数を大幅に増やすことは、どう考えても不可能である。

比較のために例に挙げると、Visa は 1 秒間に数千件の取引を処理しており、必要に応じて簡単に処理量を増やすことができる。結局のところ、従来型のバンキング技術は拡張性に優れているのだ。

4. マイナーの存在がネットワークセキュリティを担保する

マイナーとは大量の電力を使いブロックを「美しく」、ブロックチェーンに追加できる形になるまで「計算」する役割を持っている。しかしそのために消費される電力は、人口 10 万人の都市で消費される電力量に相当し、さらに、Bitcoin のマイニング専用の、高額なマイニング機器の費用もかかる。

ここで問題になるのが、今後何らかの事情(電力の値上がり等)でマイナーが減った時に、マイニングに使用されている計算能力の過半数を特定の人が管理することによる「51%攻撃」のリスクが生じるということである。

仮にマイナーの数が現在の 1,000 分の 1 で、消費電力も 1,000 分の 1 であっても、

Bitcoin の効率は現在と変わらないだろう。その場合でも 10 分に 1 個の頻度でブロックが生成され、同じ数の取引が処理され、同じスピードで運営されるはずだ。

今のところマイニングからは利益が生まれ、ネットワークの安定性は保たれているため多くのマイナーが存在しているが、マイニングから利益が産めなくなった時に、マイナーの人口が減りネットワークの安全性が確保されているかというと、それは怪しいものである。

5. ブロックチェーンは中央管理システムがないため破壊できない

Bitcoin には、サーバーやそれに類するものがない以上、閉鎖しようにも相手がいない。と見る人もいるかもしれないが、その考えは幻想にすぎない。

実は、「個人」のマイナーは、少額でも確実に収入を得たいという前提の下、カルテルに参加するしかない状況になっているのだ。

ここで生じうる問題は、その内の大規模カルテルが 1 つに集約されてしまうことである。

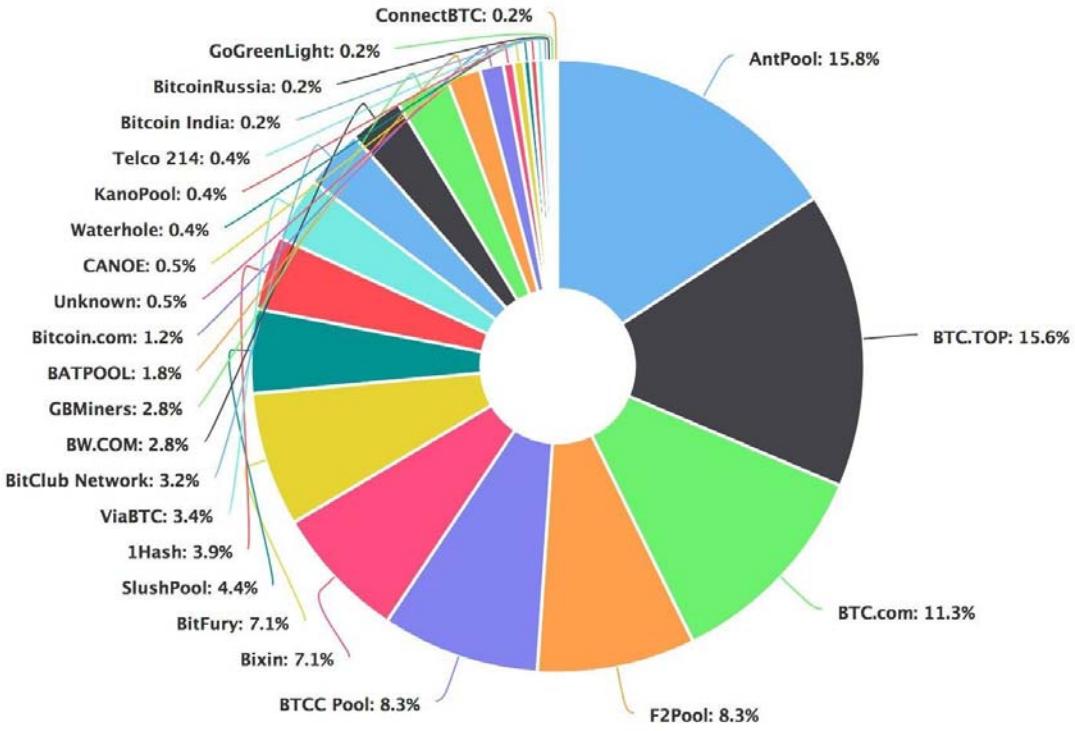

図 2. 大規模マイニングプール間の計算能力の推定分布。
出典:blockchain.info/pools

上の円グラフは、大規模マイニングプール（スパコン）の上位約 20 グループを示しているが、全計算能力の 50%以上が上位 4 グループに集中している。これだけの計算能力を我が物にした人は、Bitcoin を二重支払いできることになるのだ。そうなれば、Bitcoin の価値は下落するだろう。

しかし、事態はこれよりも深刻になっている。現在マイニングプールと計算能力の大半が、中国に集中しているのだ。一国の中に位置していれば、計算能力を掌握して Bitcoin を乗っ取ることは格段にやりやすくなる。

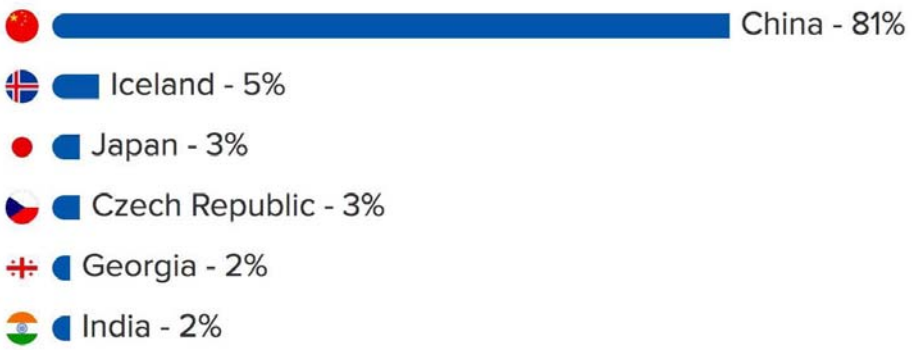

図 3. 国別の保有するマイニングプールの計算能力
出典: https://www.buybitcoinworldwide.com/mining/pools/

6. ブロックチェーンの匿名性とオープン性は良いことである

ブロックチェーンはオープンな仕組みで、誰もがすべてを見ることができる。したがって、ブロックチェーンには本当の意味での匿名性はなく、そこにあるのは「偽名性」になる。悪意ある人が偽名を使うことによって生じる深刻な問題はさておき、ここでは悪意のない人にとってなぜ偽名性が良くないのか、単純な例を挙げて説明する。

私は数 BTC を自分の母親に送金しようとしている。このとき母は次の内容を知ることができるのだ。

「任意の時点で私がいくらお金を持っているか。私がどれくらいお金を使っているか、さらには、何にお金を使っているか。また、何を買ったか、どんな賭けごとをしたか、どの政治家を「匿名で」支持しているか。」

ある程度知られても個人間では許容されるかもしれないが、企業間ではそうはいかない。会社の取引先、売上、顧客、契約金額、その他のごく瑣末な事柄まで、すべてが公になるのだ。取引履歴が丸見えになることは、おそらく Bitcoin を使用する上で最も不利益な点の 1 つになるだろう。

★参考文献

・ブロックチェーンと Bitcoin にまつわる 6 つの通説を覆す
https://blog.kaspersky.co.jp/bitcoin-blockchain-issues/17658/
・Bitcoin におけるブロックチェーンサイズ
https://blockchain.info/charts/blocks-size?timespan=all
・国別の保有するマイニングプールの計算能力
https://www.buybitcoinworldwide.com/mining/pools/
・秒間 3000～4000 取引の処理性能に到達したプライベートブロックチェーン_さくらのナレッジ
http://knowledge.sakura.ad.jp/knowledge/7332/

以上