Bitcoin/Blockchainの技術的動向と今後

Digital Garage

自己紹介

DG LAB
OPEN INNOVATION PLATFORM

渡辺 太郎 / Taro Watanabe

☆ DG Lab CTO（Blockchain）開発チーム率いる

☆ Bitcoin Core をサポート

☆ チームは全員 Bitcoin Core Contributor

☆ 地域通貨 / Value Exchange / Smart Contract等

☆ Blockchainデベロッパーの教育プログラム

Blockchain Core Camp [BC²] を不定期開催

https://bc-2.jp/

DG LAB
OPEN INNOVATION PLATFORM

Bitcoinの技術にフォーカスしています

DG LAB
OPEN INNOVATION PLATFORM

一番の理由は現存するBlockchainの中で

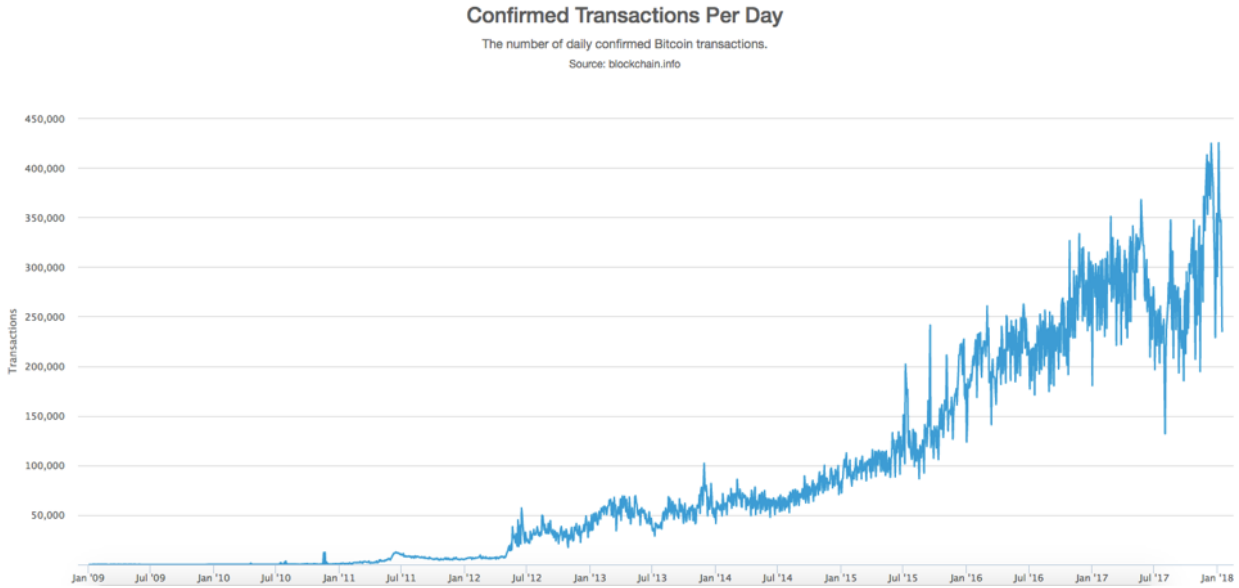
最もセキュリティに長けていると評価しているため

技術的な動向について

Scaling問題

Bitcoinの技術を採用しようとした時に必ずついて回る課題は、“Scaling問題”
現在は投機目的のトランザクションが増大し、手数料の高騰や承認速度の遅延など
様々な問題が起こっている。当然、決済に応用しようとしてもVISAネットワークの
ような処理性能を求めると同じ課題に突き当たる。

これを一般に”**Scaling問題**”※と言っている。 ※ その他プライバシーの課題なども含まれる

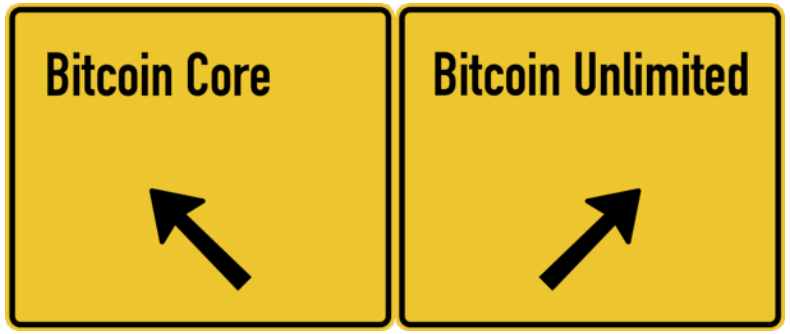


引用: https://blockchain.info/ja/charts/n-transactions?timespan=all
http://www.capturecommerce.com/blog/general/caution-heavy-traffic-ahead-how-to-prepare-your-site-for-a-visitor-spike/

2つの派閥

Scaling問題を解決する方法の一つとして、**ブロックサイズを大きくして**1ブロックに格納できるトランザクション量を増やし、処理性能を上げようというアプローチがある。

去年巷を騒がせたようにBitcoinには度々分裂問題が勃発するが、基本的にこの分裂論争はこのブロックサイズを大きくしようとする**”ビッグブロック”派**と、安易にサイズを大きくしたくない**”慎重”派**の意見の相違から発生する事象。



引用: http://p2plendingexpert.com/the-bitcoin-scaling-debate-for-beginners-part-1/

単純に考えれば、ブロックサイズを大きくすることでこの課題が解決するのであれば、そうすれば良いという結論になるが、この判断にはもう一つ重要な視点が必要となっており、これが**慎重派の重要な論点**となっている。それは**セキュリティとのトレードオフの発生**、それから**非中央集権ネットワークというBlockchainの本質的価値棄損**の可能性という2点

慎重派のメンタリティ

引用: https://www.crypto-news.net/mining-pools/1
https://danielmiessler.com/study/vulnerability-assessment-penetration-test/

ブロックサイズを大きくするには、

Blockchain自体にシステム上の大きな改変を施さなければならない

その過程でセキュリティを損なってしまうリスク

ブロックサイズを大きくすることで一部の大きな設備を持つ参加者にマイニングが集中してしまう

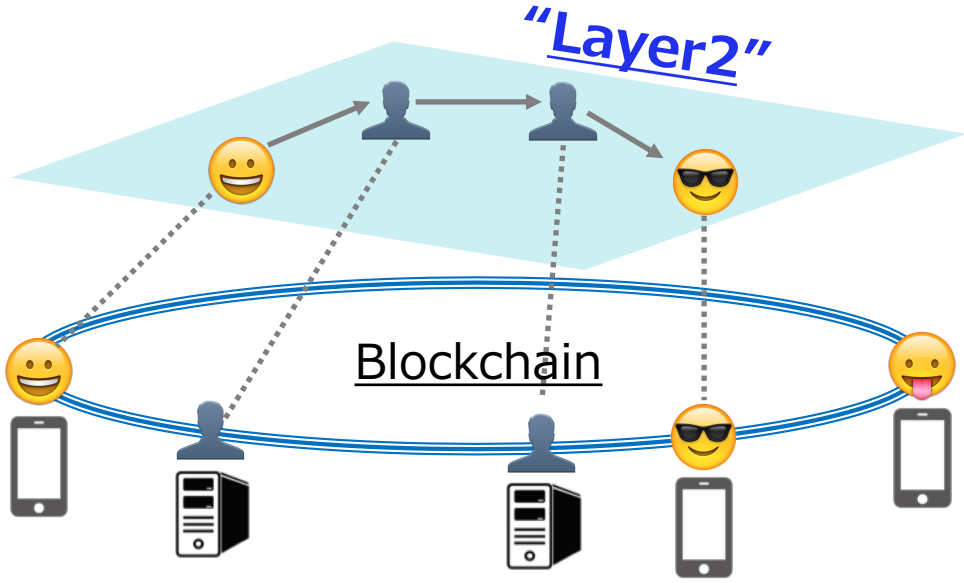
非中央集権でなくなってしまうリスク

つまり、社会インフラとしての未来を考えれば考えるほど「システム改変や開発には慎重にならなければならない」というのが慎重派の行動原理となっている。分裂問題が議論される際、この主張が取り上げられることは少ない。

慎重派の解決方法と今後の技術動向

では、その慎重派はどのような方法でScaling問題を解決しようとしているのか？

そこで出てくるのが**”Layer2”**と呼ばれる技術、
これは基本的にBlockchainの外で処理性能を
上げようという技術的試み（Off-Chainとも）
つまり、セキュリティを重視し、Blockchain
そのものには手を入れず、Blockchainの上に
上位階層を作り、そこで処理性能向上させよう
というアプローチ



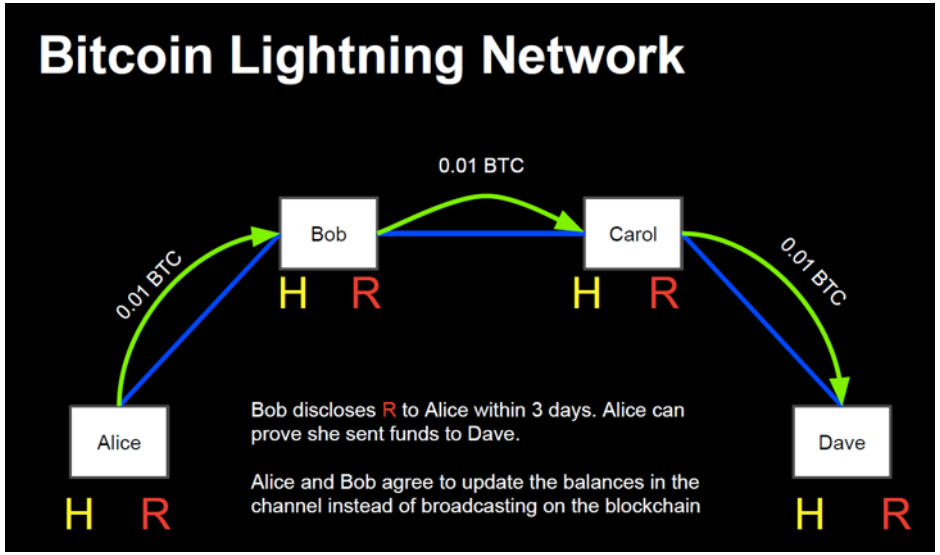
代表的なもので**Lightning Network**という仕組みがよく知られているが、近年、多様なLayer2技術（Discreet Log Contracts、Lightning上でのAtomic Swap等）が注目を集めている。今後はセキュリティを損なわずにScalingさせる”Layer2”の応用例が盛んに議論され、実例が出てくるのではと考える。

ちなみに、マイナーを中心に構成される”ビッグブロック”派がこの解決策に賛同しないのはLightning Networkが導入されてしまうことで、手数料収入が大幅に減ってしまうという背景があると言われる

＜参考＞Lightning Networkの仕組み

例えば、AさんとBさんの間で仮想通貨をBlockchain上で複数回やり取りしようとした場合、送金の都度ブロックに書き込まなくてはならない、つまりAさんとBさんで10回取引したら10回分のトランザクションをブロックに書き込む必要がある、当然その都度手数料と承認時間が発生することになる。

これに対しLightning NetworkはこれをBlockchainの外での取引成立を実現する仕組み。Lightning Network上ではペイメントチャネルという独自ネットワークが利用されており、このペイメントチャネルを経由して送金が行われる。ペイメントチャネルを利用して送金している間は手数料は（ほぼ）かからず、ブロックにも書き込まないので、承認時間は不要。つまり非常に安価で高速な送金が実現できる。

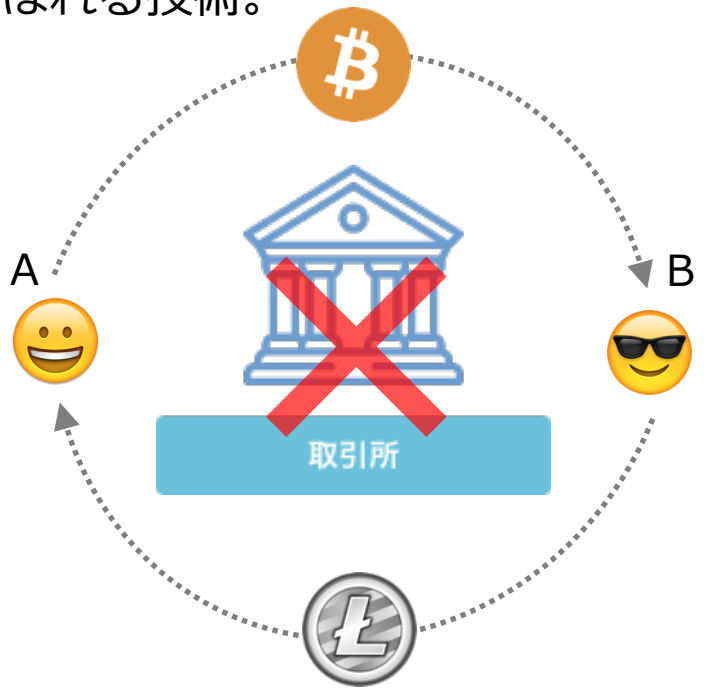


引用: http://blockchainstuff.eu/the-bitcoin-lightning-network/

ブロックへはAさんとBさんの間でペイメントチャネルを開設する時と閉じる時のみ書込みが発生するので、10回の取引でも2回分の書込みで済む仕組み。このようにBlockchain自体に処理速度の向上を求めるのではなく、Blockchainの外で処理速度の問題を解決しようとしたのがこの “**Lightning Network**”

＜参考＞Atomic Swapの仕組み

異なる仮想通貨（例えばビットコインとライトコイン）を1トランザクションで交換させてしまう仕組み。
通常、通貨の交換を行おうとすると、AさんからまずBさんへビットコインを送金、その後、BさんからAさんへライトコインを送金という流れになるが、この場合、Bさんがビットコインを受け取った時点で逃げてしまうことができてしまう。これを解決するのがAtomic Swapと呼ばれる技術。

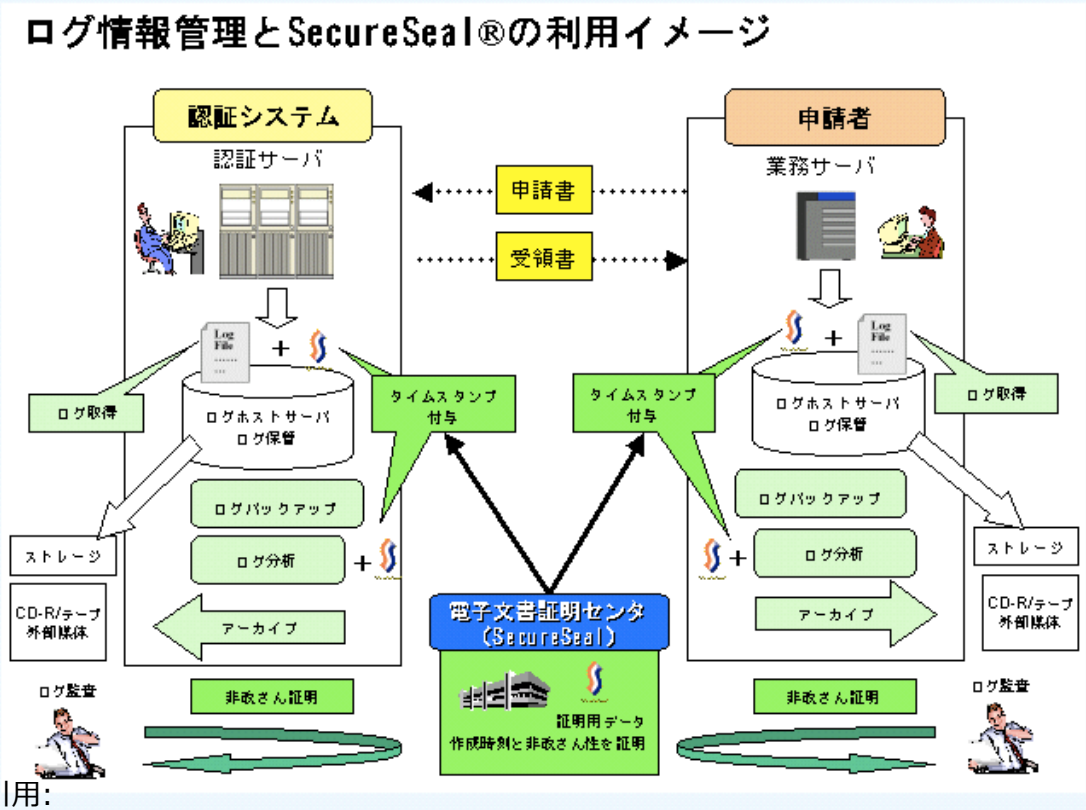


通貨の交換というのは仮想通貨取引所を利用する際にも発生している（現金と仮想通貨の交換）。この場合は、取引所という免許を持った事業者が約定及び、当事者の持逃げなどができないような仲介（管理）者の役割を果たしている。（その代わり彼らに手数料を支払う仕組み）
これはある意味、取引所が中央集権的な立ち位置になってしまっており、本来のBlockchainの性質からすると望ましい状況ではないと言える。

将来、現金が電子化し仮想通貨として流通するようになった場合、この**”Atomic Swap”**は取引所というものを介さずにユーザー同士が直接通貨の売買ができる世界をもたらすことなどに期待されている。

実証実験ラッシュを超えて

Private Blockchainに対する評価



引用:
http://www.nttdata.com/jp/ja/news/release/2003/img/022400-01.gif

- ここ1-2年はまさに実証実験が多かった印象 -

そろそろその評価についての結論が出はじめる？

国内で実証実験と言われているもはほぼ、

プライベートまたはコンソーシアム型

（パブリックでの実証実験は数少ない印象）

つまり、評価が下されるのは

「プライベート(コンソーシアム)型Blockchainの価値とは…」ということになるのではないか？

（あくまで私見だが）プライベートBlockchainは、管理者が存在することで当該ノードが他者に乗っ取られた場合、ネットワークが汚染されてしまうこと、またそれを防ぐ為に従来のクライアントサーバシステム、RDBシステムと同様のセキュリティ設備を必要とすること、などから従来のクライアントサーバシステム、RDBシステム比較しても格段に大きなメリットが得られる可能性は低いのではと考えており、実証実験の従事者は当初Blockchainに期待していたイメージがやや縮小するケースが出てくるのではないか？（もちろんメリットを全否定するものではない）

今後どうなっていくのか / どうするべきか

Public Blockchainへ

プライベートBlockchainへの評価を経て、パブリックBlockchainの本質的な価値へ目を向ける傾向が表れるのではないか？本来Blockchain最大のメリットを享受しようとすると、パブリック型Blockchain（もしくはパブリック志向のコンソーシアム型など）が最も適していると言える。
確かに、中央コントロールしづらいネットワークになっていくことで現在の商慣習上、相容れない業態もあると思われる。

ただ、Blockchainは本来、**誰もコントロールできず、参加者に悪意を持つものがいたとしても、その悪意を挟む余地がないネットワークである**ということが本質的な価値。

その原理に相容れないのであれば、そもそもBlockchainという技術そのものがその業態には適していないということ
（かもしれない。。）

引用:http://startupmanagement.org/2016/11/06/understanding-semi-private-blockchain-applications/

セキュリティを損なわずにScalingを

パブリックBlockchainにとって最も重要なのは**セキュリティ**

前述の通り**”Layer2”**を代表とする、セキュリティを毀損せずにBlockchainをScalingさせる技術の研究、開発が今後重要になっていくと考える。

ここで言えるのは、まだBlockchainは研究開発段階にある。ということ。

そのため、技術者の育成とサポートが重要になってくる。社会インフラとしての将来を熱望されながら、パブリックBlockchainを扱える技術者は現在のところほんの一握り。

技術者の育成と既存技術者のモチベート（インセンティブ）が必要

DG LAB
OPEN INNOVATION PLATFORM

コアデベロッパーたちの献身

Bitcoin Core Developer




















まとめると

整理…

- ✓ 実証実験の結果からプライベートBlockchainに対する一定の評価がなされる
- ✓ それを受けてのパブリックBlockchainの本質的見直し
- ✓ セキュリティを維持しながらScalingを実現するLayer2技術の研究開発
- ✓ 技術者やその育成をバックアップする仕組みが必要

DG LAB
OPEN INNOVATION PLATFORM

ありがとうございました。