2019/5/29

3班（柳　藤井　近藤　川村）

これでわかったビットコイン

著者：斎藤賢爾（2014）　出版：太郎次郎社エディダス

匿名？　追跡可能？ 担当：柳（p.42~45）

●追跡することで何がわかるか

・ネットに保管されている取引履歴から情報を引き出してみた所、オンラインのギャンブルなどで使われていたりしていた。

　→このことからある程度の追跡は可能

・取引を隠すための「ミキシングサービス」がある。

　ミキシングサービスとは？

ＢＴＣの送金を無関係なアドレスから転送することで、追跡を混乱させるシステム。
信用取引なので持ち逃げされる可能性もある。
巨額の取引は分けて取引するため手間がかかる。

・どのみちＢＴＣを現金化しようとすれば足がつくので盗むにはリスクが大きい。

●捜査当局は何をするべきか

・ＢＴＣが資産として認められないといけない。
・ＢＴＣの取り扱いをするのに個人情報を登録させることで取引所を常に監視できる。
・非正規な取引は麻薬捜査と同じ要領で捜査される。
・プライベートキーを無くしてしまうとＢＴＣが自分のものと証明できない。

感想

　ＢＴＣと現金の違いは社会的に認められているかの違いが大きいと感じました。社会的な基盤やバックアップが無ければ貨幣として扱いにくいなと思いました。通帳やカードをなくしても何とかなる円と違ってＢＴＣはプライベートキーをなくしてしまうと財産を失ってしまうので非常に使い勝手が悪いと思いました。

ビットコインが盗まれたら？　担当：藤井（p.45~48）

●　匿名性は幻想

・「ビットコインの取引は匿名性が高い」というのは、幻想。
・ビットコインの場合は、取引の履歴をネットワークの中に保存して、維持している。どの《アドレス》からどの《アドレス》へと BTC の送金があったかがわかる。違法な売買に使われた BTC がその先どこに行ったのかを、どこまでも追っていくことが可能。

・このことを気持ちが悪いと思う人が多いため、ビットコイン・コミュニティでは、現在、ユーザーが取引ごとに《アドレス》を変えることを勧めている。
・このことには、利点よりも難点が多い。
・BTC をなくしたり、盗まれたりすることが問題となるのはシステムに匿名性を持たせているから。仮に、《プライベートキー》が実名の人物と結びつく設計になっていれば《プライベートキー》をなくしたときの再発行や、本人以外による使用を妨げることが可能にでき、紛失や盗難に対する対策ができる。

● 詐欺、誤操作のあったときは？
・ビットコインでは、一度起きた取引は取り消せない。
・誤操作の場合には送金し返してもらうしかない。
・詐欺にあった場合には、《アドレス》をたどることにより、盗まれた BTC を追跡していくことができる。ただ、《アドレス》から個人を特定することは一般の人には難しい。

● なくしたり盗まれたりしたら？
・《プライベートキー》をなくすと、対応する BTC は、誰も使えなくなる。
・《プライベートキー》が盗まれ、BTC が送金されてしまうと、その不正な取引は取り消せない。ただ、送金先の《アドレス》は明白だから、今後の法整備と捜査当局の対応によっては、取り返せる可能性は残っている。
・よく確認せずに、《ウォレット》のアプリをアップデートして動かしたら、手持ちの BTC がすべて知らない相手に送金されてしまった、という事例もある。
→ダウンロードしたものが不正に改竄されたものでないか確認する必要がある。

取引に消費税や印紙税はかからない？ 担当：藤井（p.48~49）
● 国の決まりに従う
・シンガポールやドイツでは課税する方向。
・ユーロ圏における税制上の BTC の扱いは統一されていく。
・デンマークでは課税しない。
● 日本ではどうするのか
・日本ではまだ決まりができていない。
・2014 年 3 月 7 日、政府はビットコインをどう扱うかを示した「回答書」を閣議決定。
・BTC は通貨ではなく、それ自体が何かの権利を表すものでもないため、銀行や証券会社が BTC を通過や証券として扱って、預かる口座を開設したり円との交換を行うことはできないとしている。
・一方で、BTC を対価とすることを禁止する法律はないともしている。

2019/5/29
3 班（柳　藤井　近藤　川村）

コメント
　ビットコインの場合、たとえ盗まれたとしてもどの《アドレス》からどの《アドレス》に送金があったかが明白であるため、どこまでででも追跡できるということは理解できた。しかし、《アドレス》から個人を特定することは一般人にはできないようなので、著者の言う実名での取引なら盗まれた時の対処はできると思った。

ビットコインで商取引のかたちが変わる？　担当：近藤(p.49～52)

● オンライン決済の導入は容易に

・インターネット上で商売を始めオンライン決済を導入したいのであれば、BTC での支払いの受付は導入コストはがほぼゼロ
・簡単に、手数料も安く、システムを導入し、実際に決済できる

● 日常の買い物は変わらないかも

・ビットコインは支払いの手続きをしてからその支払いがネットワークの最初に認証されるまで平均で約 10～15 分のタイムラグがあり、その取引が確定するまで約 1 時間強かかる
・BTC で払う場合、現金と同じように、BTC が送金元から送金先に確実に移動したと確認できるまで顧客にそばにいてもらわなければならず、日常生活の中でビットコインが使われていくことへの大きな障壁となる
・タイムラグの緩和のために、店での小口決済には、BTC の額面をチャージしたプリペイドカードを使うという方法が使われていくだろう

● 送金が、より簡単になる

・ビットコインでは送金がとても簡単なのでなんにでも手軽に支払いできる
・現金に似せているビットコインもチップのような習慣が生まれるのに役立つかもしれないが、BTC が希少であり続けるならそんなふうには使われない
・ビットコインが人々のあいだを十分に回っていくためには、希少性が強くなっていくことは大きな障壁となる

● グローバル化は進行する

・ビットコインやそれに類するものが普及していけばこれまで以上に国と国の間の垣根がなくなるということは起きてくるだろうが、よいことばかりではなく、より激烈な競争にさらされることになる
・グローバル化が進むにつれてそうした傾向は強まっている

コメント
メキシコのセブンイレブンではビットコインが利用できるということに驚いた。

ビットコインが普及していき、グローバル化が進んでいくことはよいことだけが起こるわけではないので、それにどう対応していくかが課題になっていくのではないかと思った。

これから大きくバージョンが変わったりしないの？担当　川村（p.53~56）

- バージョンの変わり方
  →使用されている限り改善されていく。
  ビットコインはオープンソースのソフトウェア
  ただしユーザー全ての意見が尊重されるわけではない
- どう変わるのか、どう変えるのが良いのか
  →ビットコインはインフラとして心もとない
  匿名性の追求よりも個人の識別に重点を置くべき
  プライバシーやセキュリティ面を重視…
- ビットコインの亜種の存在
  →ビットコインのソースコードを参考に別種のデジタル通貨を造る
  参考元と同じ性質や問題を抱えている。
  ex)ライトコイン　ドゲコイン

コメント

様々なデジタル通貨が発行されている現在、もっと競争が行われてもいいのではないかとも思う。それらの通貨はお互いに不干渉だというイメージが私の中にある。通貨を選べるレベルまで人々に認知させること。そして使用される中でその通貨たちを取捨選択し、競争させ淘汰することによって、より、洗礼された通貨が生まれるのではないかと感じた。