HACK CHAIN 班 報告書

立命館コンピュータクラブ 2017 年度 前期グループ活動

HACK CHAIN 班

前川　彰 *
山口　流星 †
浜田　和幸 ‡
芹澤　拓也 §

2017 年 8 月 9 日

概要

この数年, 金融と IT を組み合わせた FinTech が注目を浴びており, 実際に多くの IT 企業が銀行等と連携して革新的なサービスを提供し始めている. その FinTech の潮流の 1 つであるブロックチェーン技術は, 次世代ネットワーク技術として様々な機関が研究をし, 実証段階に入っている機関もみられる.

そうした情勢を踏まえ, コンピュータクラブとしてブロックチェーン技術のリテラシーを高めるべく, 本プロジェクトを結成した. 本報告書では, ブロックチェーンとはどういったものか, またブロックチェーンを使用している代表的な暗号通貨である Bitcoin にも踏み込んで調査した. 調査を進める中で 2017 年 7,8 月は Bitcoin 分裂問題で社会的注目も浴びたため, 分裂問題に関しても深く考察を行った.

* 理工学部 電気電子工学科 三回生
† 理工学部 数理科学科 一回生
‡ 情報理工学部 一回生
§ 情報理工学部 一回生

目次

1　はじめに

文責：山口　流星

このプロジェクトでは, 次世代技術のブロックチェーンについて踏み込み, 研究及び調査を行った. 本稿では, ブロックチェーンとは何かから始め,Bitcoin について, またその派生である Altcoin についてまとめ, 考察を行う.

2　ブロックチェーン

2.1　暗号通貨

暗号通貨とはなにか. ネットワーク上で取引される現金や電子マネー, クレジットカードでもない通貨のことである. 暗号通貨の中には, 次世代ネットワークを担う技術, ブロックチェーン技術が使われており, あらゆる面で応用が利くことで注目を浴びている. ここでは, 暗号通貨の中で使われているブロックチェーン技術について見ていく.

2.2　ブロックチェーン

ブロックチェーンとは, 公開取引簿とも呼ばれ, 全てのユーザが見ることができるネットワーク取引の記録が載っている場所である. ブロックとブロックが鎖のようにつながっている様子からそう呼ばれるが, ただブロックが繋がっているだけではブロックチェーンとは呼ばず, 次項目からのブロックヘッダーのハッシュ値が大きく関係している. また, この技術が使われているとき, 正当なブロックチェーンはただ 1 つ存在し, もしこのチェーンが場合によって分岐した場合, 分岐後に最も長いチェーンが正当なブロックチェーンとし, 残りの分岐は無かったものとして切り捨てられる. この要素はとても重要なので, よく頭に入れておく必要がある.

2.3　ブロック

ブロックは, ブロックヘッダーと取引の記録やその個数, ブロックのサイズなどが書かれている. ブロックには容量が 1 MB あり, それを超えない限りはいくつでも取引を入れることが出来る.

2.4　ブロックヘッダー　ハッシュ値編

ブロックヘッダーとは, 6 つの要素が含まれている. この中で最も重要な要素は, 現在の 1 つ前のブロック内にあるブロックヘッダーハッシュ値である. これは, この 6 つの要素が入った情報を, ハッシュ関数によってハッシュ化してまとめたものであり, これ 1 つあれば, 前後の情報の正しさが証明でき, これはハッシュ値の節を読めば納得できるのでそちらを読んでほしい. ブロックチェーン技術では, このハッシュ値を各ブロックに入れることで, チェーンとして繋がっていることを示せる. 次の要素は, 現在のブロック内にあるトランザクションハッシュ値である. トランザクションは取引記録で, このブロックで行われた取引が承認されたことを示すハッシュ値である.

2.5　ブロックヘッダー それ以外編

まず, ブロックのバージョンと, 取引が決まったら書かれるタイムスタンプがある. 次に, ターゲット（採掘難易度）がある. 本稿ではビットコインのブロックチェーンを見ているため, このような要素も含まれている. ビットコインは, １０分に 1 回取引が承認される仕組みになっていることから, 採掘難易度を調整しておよそ１０分になるような仕組みになっている. １０分より早く掘られすぎると採掘が難しくなり, 一方１０分よりかかりすぎると簡単になる. こうして取引の時間を一定に保つことで急激な取引による価格の急暴落対策をしている. 最後にナンスだが, これもビットコインの Proof of Work という仕組みのために導入されている. これは採掘者と呼ばれる人が, 取引の承認となるハッシュ値を探すときに使う任意の文字列のことである. 一度その文字列を入力すると, ハッシュ関数によってハッシュ値が算出されるのだが, この時に出てくるハッシュ値には何の規則性もないため, 取引を承認できるか否かの 2 択のみである. よって, 取引が承認されない文字列を再び使うことがないため,Number used once（一度きりの数字）の頭文字をとって, ナンスと呼ばれる.

2.6　ハッシュ値

ハッシュ値とは, 任意の文字列 x に対して, 文字列の長さを変える規定を持つハッシュ関数 H に x を代入した値 H(x) のことを言う. なお, ハッシュ関数は, 任意の文字列を無作為に文字列の長さを変えるため, 似たような文字列を選択しても全く異なるハッシュ値が返される. そして, 重要な要素として, ある文字列 y から, ハッシュ値 z が出せても, ハッシュ値 z からある文字列 y を特定することはできない. これは, ブロックチェーン技術の要である要素である.

2.7　トランザクション

トランザクションは, ネットワーク取引の記録のことである. 主な流れを暗号通貨の一種である Bitcoin を例にとって考える.A さんが B さんに 1 BTC 送りたいとする. まず, これを transaction として取引内容が打ち出される. この後, 採掘者と呼ばれる人が, この transaction を選んで, 自分のブロックに追加していく. そして採掘作業を行い, その transaction の持っている特定のハッシュ値を当てたとき, この取引が承認されたことになり,A さんは 1 BTC 失い,B さんが 1 BTC 得たことになる.

2.8　ブロックチェーン技術の強み

特に Bitcoin で使われているブロックチェーン技術の良い点を紹介する. まず, 中央で通貨を管理するような特定の団体や人が存在しない. これを非中央集権型の分散型ネットワークと呼ぶ.Peer-to − Peer という仕組みを利用することで, よりブロックチェーンを用いた信頼性を強化することができる.Peer-to − Peer とは, ある人がある人に何か情報を流すと, そこからまた別の誰かへと情報が伝わり, 最終的に全ユーザに情報が伝わるシステムである.transaction の伝達や取引承認の際に利用されている. また, 全ユーザが, 全員の取引記録を見ることが出来るため, 不正をすぐに見抜くことが出来る. そして, 重要なのは改ざんが結果的に不可能な点である. ここについては詳しく説明する.

2.9　改ざんの不可能なブロックチェーン

n ブロック目と n+1 ブロックについて見る.n ブロック目には,n-1 番目のブロックヘッダーハッシュ値 aaa と,n 番目の取引記録 A,n 番目のトランザクションハッシュ値 bbb がある.n+1 番目のブロックには,n 番目のブロックヘッダーハッシュ値 ccc と,n+1 番目の取引記録 B, 及び n+1 番目のトランザクションハッシュ値 ddd がある. この状態を考える.

分かりやすく, 取引記録 A は, アリスがボブに 1 BTC 渡す取引としよう. そして, ドロシーはこの取引を改ざんし, アリスがドロシーに 1 BTC 渡す取引を行いたいとする. まず, ドロシーは n ブロックの取引記録 A を C に変える. すると,n 番目のトランザクションハッシュ値が xxx に変わってしまう. 次にこの値が変わると,n+1 ブロックにある n 番目のブロックヘッダーハッシュ値が yyy に変わる. これは, ブロックヘッダーには, 前回の取引承認で使われたトランザクションハッシュ値が変わったためである. さらに,n+2 ブロック目を見ると n+1 番目のブロックヘッダーハッシュ値が zzz に変わってしまった. ブロックヘッダーには, 前回のブロックヘッダーハッシュ値も含まれているためである. ドロシーが実行している改ざん行為は分岐によって, 既存のチェーンよりも改ざんのチェーンを長くすることで達成することが出来る. ゆえにここから先, ドロシーはこの操作をひたすら繰り返し, 改ざんチェーンを既存チェーンより長くするまで続けなければならない.

実際問題, これは不可能ではないが, 既存のチェーンの莫大な長さ, 及び正当なブロックチェーンは１０分に１つずつ増えていること, そして改ざんにかかる演算は莫大なエネルギーを必要とすること. これらを考えると, 一つの取引データを改ざんすることよりも, 正当に採掘をする方がより効率的に Bitcoin を集めることが出来るため, 改ざんをする必要がなく, また, よほどのスペックがない限り, 改ざんすること自体非常に困難である. よって, ブロックチェーンは改ざんにも強い, 安全性を備えていることが分かった.

3　ビットコイン

ここで, ブロックチェーン技術を最初に取り入れ, 暗号通貨の代表である Bitcoin について取り上げる.

Bitcoin は, 通貨ではなく, 決済システムである. ブロックチェーン技術の導入に加えて,Peer-to-Peer システムを用いることで, 取引の透明化を図った. これは transaction によって, ハッシュ値を探し当てたときのある文字列 x が, 本当に transaction が承認される文字列 x かを確かめるためのシステムである. 内容としては, ハッシュ値を探し当てた人から, 任意の誰かに探し当てた文字列 x が送信されて正しいことを確認, さらにその人から別の人へと承認を進める. そして全ユーザーの５１％以上が正しいと確認できた時, このブロックの transaction を承認したことになる. そうして Bitcoin は, 暗号通貨の中で最も問題視されていたダブルスペンディング問題を解決した.

他にも, 個人送金が可能になり, 海外への送金に関して, 海外の銀行を仲介せずに直接行うことができるようになった. その為, 従来比較すると, 取引速度が良くなり, 手数料も抑えられるようになった.

3.1　採掘者 (マイナー)

ブロックの中には１ＭＢまでの複数の transaction が入り, １０分に１回これは掘り出される.Merkle Tree[*1] の親にあたる, チェーンとして繋がる予定のブロックのハッシュ値を当てることで, そのブロックの全ての

[*1] データ構造の二分木を指す

transaction が承認される. そこで取引が成立して, 取引に書かれた額面の所有権が移る. ただし, ここで使われた Bitcoin は,Proof of Burn[*2]によって消滅する. そして, 受け手と送り手の差額分を, マイナーは取引手数料としてもらうことができ, さらにブロックを前のブロックと繋げた報酬として, 一定量の暗号通貨が与えられる.

3.2 Bitcoin の問題点解決策

3.2.1 Altcoin

Bitcoin には問題点がいくつかあり, それを解決すべく生まれたのが Altcoin である. 例えば,Ethereum という Altcoin は,Bitcoin のブロックチェーン技術を取り入れながらも, 独自の技術であるスマートコントラクトを持っている. これは, 売買の契約など, 契約に関することを自動化するシステムであり, 料金未払いや支払ったが商品が届かないなどといったトラブルを未然に防ぐことができる. また,Ripple という Altcoin は,Bitcoin とは異なる中央集権型かつ非ブロックチェーンであるが, 海外送金に当たる手数料と取引時間を大幅に改善した.

3.2.2 Bitcoin の分裂経緯

文責：浜田　和幸

Bitcoin の利用者が増え続ける一方, 送金に時間がかかるようになってしまった.Bitcoin は取引記録をまとめた台帳を分散管理することによって人々の資産を管理している. この台帳は 10 分ごとに更新される「ブロック」という単位で管理され, 新しく生成されたブロックは過去の取引記録を含む形で連鎖していく. 取引記録の検証には莫大な計算能力が必要になる.Bitcoin のブロックサイズは仕様上 1MB,10 分に更新されると決められている. つまり,10 分で 1MB のデータ相当の送金が可能という事である. 逆に言えば,10 分で 1MB のデータしか送金できず（スケーラビリティ不足）, 利用者が増えることにより送金時間が増えてしまった. また, 送金されない送金要求が詰みあがることにより予期しないエラーが発生することも考えられる. そこで Bitcoin の仕様を変更するべきだという勢力が生まれ,Bitcoin は分裂することになった.

3.2.3 ソフトフォークとハードフォーク

文責：山口　流星

ソフトフォークは, ブロックチェーンが分岐して 2 種類のシステムが使えるようになる. ソフトフォークに関しては, マイナーの９５％以上の同意がないとなされない. ソフトフォークは両方のシステムが存在するため, 同意率が高いのは従来の分岐型のチェーンが繋がってしまわないようにする必要があるからである. ブロックチェーンが長い方のシステムが採用されてしまうことと, 新型から従来型へとチェーン変更が起こった時に, ダブルスペンディング問題や transaction の消失が起こってしまうこともある.　ハードフォークは, 従来のブロックチェーンとの互換性が一切なく, 全く新しいシステムを導入してチェーンが繋がっていき, 完全に独立

[*2] 一度取引に使用された暗号通貨は消滅すること

した Altcoin になる. この時に, 従来型のシステムでマイニングをすることができない.

3.2.4 Bitcoin の分裂

Bitcoin の分裂について, はじめは 2 つの提案がなされていた.1 つはジーハン・ウーが提唱した UAHF[*3], もう 1 つはユーザー側が提唱した UASF[*4]である. 分裂までの主な流れを説明すると, まずユーザー側は, ビットコインの新しい改案として UASF を提唱した. これは,SegWit[*5]という方法でスケーラビリティ問題を解決しようとした.SegWit は,transaction を圧縮してブロックに載せることでよりたくさんブロックに入れられる状態を作るシステムのことである. また,ASICBoost と呼ばれる非常にマイニング性能の高い機械でマイニングを行うことに不平等があるとして, これを用いてのマイニングを禁止するというものであった.

しかし, マイナー側はこれを反対し, 特に ASICBoost の特許を持っている Bitmain 社の社長のジーハン・ウーは反対し,UAHF を提唱した.UAHF システムは, ブロックの容量を 1 MBから 8 MBまで増やしてスケーラビリティ問題を解決しようとしている. 初め, ジーハン・ウーは SegWit システムによって ASICBoost が使えなくなることを恐れて, ハードフォークを行うことで自由に採掘できるようにしたのだと筆者は考えていた. しかしこのように考えると不可解な点がある. まず,BCH（Bitcoin Cash）は UAHF のシステムをそのまま利用しているため,Bitmain 社と関係があるように思えるが, ここのサイト[*6]によると, 関係を正式に否定していることが分かる. つまり,UAHF を提唱することは別の意味で対策をしていると考えた. すると UASF の支持率がそこまで高くなかったため, これではソフトフォークした後にまた従来のチェーンが戻ってしまう可能性があり, これによって取引の消失などを恐れたのではないかと考える. しかし,UAHF と UASF での分裂は決まらず均衡が続いていた.

3.2.5 第三の案　SegWit2x

これを破ったのがバリーの SegWit2x 案である. これはいずれ将来ハードフォークをすることは示唆されているが, ユーザー側の UASF の内容の SegWit が含まれていて, また,SegWit2x が実際に施行されると, マイナー側は ASICBoost を使って掘れる可能性があるため, 両者に SegWit2x の採用にメリットがあった. これによって SegWit2x の合意投票が行われる前に非常に高い支持を得ており, 7 月 2 3 日に SegWit のアクティベートが実施された. これは,SegWit のシステムをこの先することを確定しただけで, まだ施行はされていない状態である. この後, 2 週間ほどかけて SegWit の施行に向けて準備を進めていき, 8 月 9 日～遅くとも 2 2 日までに施行されることが予定されている.

これとは別に, 8 月 1 日に Bitcoin のハードフォークが施行され, 新たな暗号通貨,Bitcoin Cash（BCH）が生まれた. これは,Bitmain 社が提唱した案 UAHF をそのまま引き継ぎながらも,ViaBTC が施行に踏み切った. 本来,Bitmain 社が打ち出した UAHF は,UASF が施行される場合にのみ半強制的に案を施行するものだった. 実際 UASF の案は施行されなかったために, ハードフォークは行われないと考えられていたため, これは

[*3] User Activated Hard Fork
[*4] User Activated Soft Fork
[*5] Segrigated Witness
[*6] http://btcnews.jp/2e9qo5hr11898/

異例の事態だった. ただ,BCH は Bitcoin とは完全に別通貨として扱われるため, 直接関係しないことから, それほど問題として挙がらなかった. この一連の分裂問題によって, 相場の不安定が予想されたが, 相場は逆に急騰を見せた. 以上の流れを説明したチャートが図 1 である.

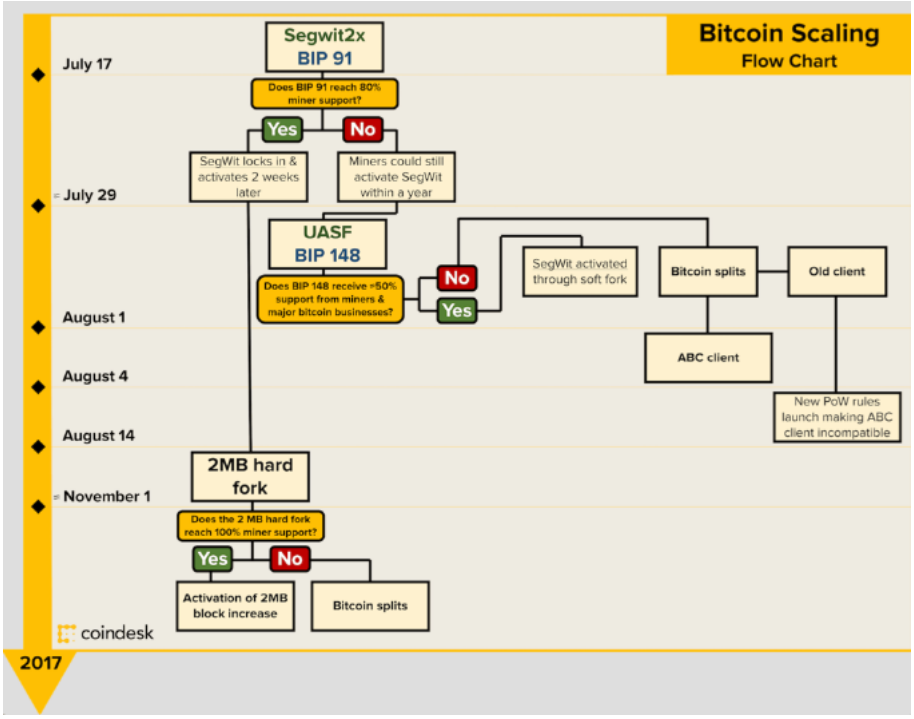

図 1　https://www.coindesk.com/happen-bitcoin-visual-guide-scaling-outcomes/

4　考察

分裂騒動に関して,Bitcoin の不安定さに加えて, 様々な分裂の場合分けが考えられたため, 不安定要素がより大きくなり価値が低下すると予想していたのだが, 実際は真逆の動きをした. ここで, 価値の変動が起きる要因を 4 つ考察してみる.1 つ目は, 誰かもしくは集団で大きな額の取引を一気に行うとすぐに変動しやすいこと. 2 つ目は, ソフトフォーク・ハードフォークによる将来の見通しが立たず, 不安定になること. 3 つ目は, 経済不況による法定通貨の信用下落による影響を受けること. 4 つ目は需要と供給のバランスが安定せず, 暴落と暴騰を繰り返しがちであること. よって, 今回価値の変動に影響を強く与えたのは, 1 つ目と 2 つ目の要因であると考える. 特に 2 つ目に関していうと, 起こるとされていたソフトフォークが, 数ある選択肢の中で最も安定する場合のものが選ばれた. そのため, より早く信頼性を回復でき, 一気に Bitcoin を購入する人が増え, 価値が上昇したと考える. まだまだ暗号通貨は増減の幅が大きく, 背景に何があったのかをとらえることは非常に重要である.

5　活動を通して得られたこと

・会内でブロックチェーン技術と Bitcoin の認知度が上がったこと
・Bitcoin の分裂問題に関する深い洞察が得られた.
・普通ではできないガチマイニングに挑戦でき, また自作ＰＣの知識も深めることができた.（この知識はコラムで紹介する）
・錬金術の楽しさと, チャートを見る楽しみが増えた.

6　次回に向けて

・実際にブロックチェーン技術を実装する
・各種暗号通貨の論文を読む時間を増やす

7　終わりに

文責：前川　彰

このプロジェクトを通して, 次世代技術であるブロックチェーン技術についての知識を深めることができた. これからも情報収集を続けるとともに, 会内やＳＮＳを通じて積極的に知識を発信していく. まだまだ難しい語句や仕組みも多いため, より一層の学習に励むことを目標にしていきたい.

最後にブロックチェーンに当てはまる, 未来科学者ロイ・アマラ氏の”アマラの法則”を引用して本稿を終える. どのように当てはまるかは読者の判断に委ねたい.

我々は, 技術について短期的な影響を高く見積もりすぎ, 長期的な影響を低く見積もりすぎる.[*7]

参考文献

[1] ・仮想通貨の教科書　日経ＢＰ　アーヴィンド・ナラヤナン, ジョセフ・ボノー, エドワード・W・フェルテン, アンドリュー・ミラー, スティーヴン・ゴールドフェダー　著　長尾高弘　訳
[2] 暗号技術入門第３版　ＳＢ Ｃｒｅａｔｉｖｅ　結城浩　著
[3] Bitcoin : A Peer-to-Peer Electronic Cash System link : www.cryptovest.co.uk Satoshi Nakamoto 著 October 31 , 2008
[4] ETHEREUM : A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER EIP-150 REVISION DR. GAVIN WOOD 著
[5] Ripple : Overview and Outlook Frederik Armknecht , Ghassan O. Karame , Avikarsha Mandal , Franck Youssef , and Erik Zenner 著
[6] Bitcoin news http://btcnews.jp/2e9qo5hr11898/　山崎大輔　著 2017,7,24 記 2017,8,6　取得

[*7] [Amara's law] "We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."

[7] UASF のリスク検証「2017 年 8 月 1 日, ビットコインは分裂するのか？」 https://innovation.mufg.jp/detail/id=180 著者不明 2017,7,7 記 2017,8,6 取得
[8] ビットコインの分裂問題. ここまでの流れ全部書く」タナカシゲルの仮想通貨ブログ https://t.co/vRdNqsDZUN 2017,7,22 記 2017,8,7 取得
[9] What Could Happen to Bitcoin? A Visual Guide to Scaling Outcomes https://www.coindesk.com/happen-bitcoin-visual-guide-scaling-outcomes/ Alyssa Hertig 著 2017,7,18 記 2017,8,7 引用
[10] SEGWIT LOCK-IN PERIOD https://www.xbt.eu/ 2017,8,8 最終閲覧
[11] bitcoinwiki-Blockhttps://t.co/Du2BUjiaKj 取得日 2017,8,9
[12] bitcoinwiki-Block hashing algorithm https://t.co/WVoOnszih4 取得日 2017,8,9

コラム –マイニング–

文責：前川　彰

このコラムでは活動を通して得られた, マイニング PC の推奨構成を紹介する.

しかしながらその前に一般に広く流布するマイニングに関する誤解を解いておく必要がある. マイニングは電気を無駄に費やす行為ではない. マイニングとはブロックチェーンをつなげるために計算リソースを提供する行為であり, その提供の見返りに暗号通貨を報酬として得る行為である. つまりこれはブロックチェーンに対する貢献行為である. 本稿でも解説したとおりブロックチェーンは長くなればなるほど改竄耐性が増加し, 計算リソースの提供はまさにこの改竄耐性の増加に貢献しているのである.

さてここからは固いことは抜きにして, はじめて PC を自作する人でも重要な点が分かるようにまとめる. まず自作 PC を作るためには各 PC パーツを自分で全て集める必要がある. 以下に必要なパーツをマイニングに関連する簡単な説明を交えながら全て挙げる.

マザーボード

各種パーツを全て接続するために必要なボードである. 特にマイニングにおいては PCIe という端子の数が重要となる. 平均的なマザーボードは PCIe が 3 つほどであるが, マイニングに適したマザーボードは PCIe が 6 つ以上のものである. また PCIe 端子には x1,x4,x8,x16 という種類の端子がある. マザーボードの大きさは大別して ATX と miniATX があるが,GPU を多く使うことが原因でケースを使うことは少ないため説明しない.

CPU

CPU(Central Processing Unit) は PC の頭脳と呼ばれるがマイニングにおいては重要ではない. マイニングにおいて必要なのは GPU による高速な並列計算能力であり,CPU は最小限度の性能を持つもので十分である.CPU には付属品として CPU クーラーがついており熱を逃してくれる.

メモリ

メモリは主記憶装置と呼ばれるものであるが, マイニングにおいては重要ではない.8GB 程度あれば十分である. メモリで最も注意すべきことは DDR3,DDR4 を間違えないことである. マザーボードの差し込み口の形状が DDRx によって違うことに注意していただきたい.

ストレージ

ストレージは補助記憶装置と呼ばれる.OS をインストールしたりマイニングをするためのソフトを保存することができる. 容量は 120GB あれば十分である. ストレージには SSD と HDD との 2 種類があるが SSD の方が速度が早くオススメである.

GPU

マイニングにおいて最重要の部品は GPU(Graphical Processing Unit) である. 高速な並列計算を容易にできるという特徴があり, この GPU の性能が高いほどハッシュをより多く見つけることができる.GPU はマザーボードと接続する際に PCIe 端子を使用する. ミドルレンジ以上の GPU はその大きさによる制約や PCIe x16 の数の制限により端子に直接接続できない場合が多い. その場合はライザーケーブルという PCIe x1 to x16 のケーブルを用いて接続する.

マザーボード

PCIe という拡張パーツを接続するケーブルである. 変態ケーブルと呼ばれ, マイニング以外で用いることはあんまりない. ただし, マイニングにおいては必須である.

電源

電源は PC の全てのパーツに電力を供給するパーツである. 電源は供給可能電力ごとに種類があり, マイニング PC では最低でも 800W 以上のものを使うのが一般的である. また, 電力効率の良さに関する指標として「80PLUS」がある.STANDARD から TITANIUM までの 6 種類があり,TITANIUM に近いほど電力効率が良い. ただし, 電源の壊れにくさなどの質を保証するものではない. 電力供給をするために電源の裏面からケーブルがでている. 各 GPU はマザーボードからだけでなく, 電源からも直接電力を得ているため配線が煩雑にならないように努力する必要がある.

-マイニング PC 構成例-

以下, マイニング PC の構成に必要な部品を価格と Amazon.com の購入リンクを合わせて示す. 価格については 6 月後半現在のものである. 変更されている可能性はあるが参考にしていただきたい.

CPU

Intel CPU Celeron G3900 2.8GHz 2M キャッシュ 2 コア/2 スレッド LGA1151
￥5,381 必要数:1
https://www.amazon.co.jp/gp/product/B01B2PJRPA/ref=oh_aui_detailpage_o08_s00?ie=UTF8&psc=1

マザーボード

BIOSTAR LGA 1151 プロセッサ対応 Intel B250 チップセット搭載 ATX マザーボード TB250-BTC
￥12,722 必要数:1
https://www.amazon.co.jp/gp/product/B072LXX4NF/ref=oh_aui_detailpage_o07_s00?ie=UTF8&psc=1

メモリ

CFD 販売 デスクトップ PC 用メモリ PC4-19200(DDR4-2400) 4GBx2 枚 288pin (無期限保証)(Crucial by Micron) W4U2400CM-4G

￥7,272 必要数:1

https://www.amazon.co.jp/gp/product/B01L6OC5HE/ref=od_aui_detailpages00?ie=UTF8&psc=1

GPU

玄人志向 ビデオカード GEFORCE GTX 1060 搭載 GF-GTX1060-6GB/OC/DF

￥28,652 必要数:複数

https://www.amazon.co.jp/gp/product/B01IOPM1TK/ref=od_aui_detailpages00?ie=UTF8&psc=1

ライザーケーブル

YIKESHU(一本樹)　新型　二重ポート　USB3.0 PCI-E Express 1x-16x 拡張ライザーアダプターカード　ビットコイン採掘　6Pin PCI-E と 15Pin SATA 電源ケーブル　60cm 延長ケーブル (3pcs)

￥1,000(1 つあたり) 必要数:GPU と同数

https://www.amazon.co.jp/gp/product/B0723DZZF2/ref=oh_aui_detailpage_o08_s00?ie=UTF8&psc=1

GPU

SAPPHIRE PULSE RADEON RX 580 8G GDDR5 OC グラフィックスボード VD6319 SA-RX580-8GD5PL001

￥33,433 必要数:複数

https://www.amazon.co.jp/gp/product/B06ZZPFM7L/ref=oh_aui_detailpage_o01_s00?ie=UTF8&psc=1

ストレージ

WD SSD 内蔵 SSD 2.5 インチ 240GB WD Green SATA3.0 6G / 3 年保証 / WDS240G1G0A

￥9,965 必要数:1

https://www.amazon.co.jp/gp/product/B01MDM3WI5/ref=oh_aui_detailpage_o04_s00?ie=UTF8&psc=1

電源

ENERMAX 80PLUS プラチナ電源 フルモジュラーケーブル採用 PLATIMAX 1375W EPM1375EWT

￥31,887　必要数:1

https://www.amazon.co.jp/gp/product/B01LXP2IHZ/ref=oh_aui_detailpage_o06_s00?ie=UTF8&psc=1

ホワイトボードマイニング

以上の部品を用いてマイニング PC を部室で構成した. なぜ”ホワイトボードマイニング”かを説明する. マイニング PC は GPU を多く使うためケースに入れることができず, 設置が難しい. そのため, 部室で構成するために最適な場所を考えたところ, ホワイトボードの下部にたどり着いた. それが”ホワイトボードマイニング”の由来である. 皆さんも是非よさそうな位置を見つけて, 新たな○○マイニングをしていただければ幸いである.

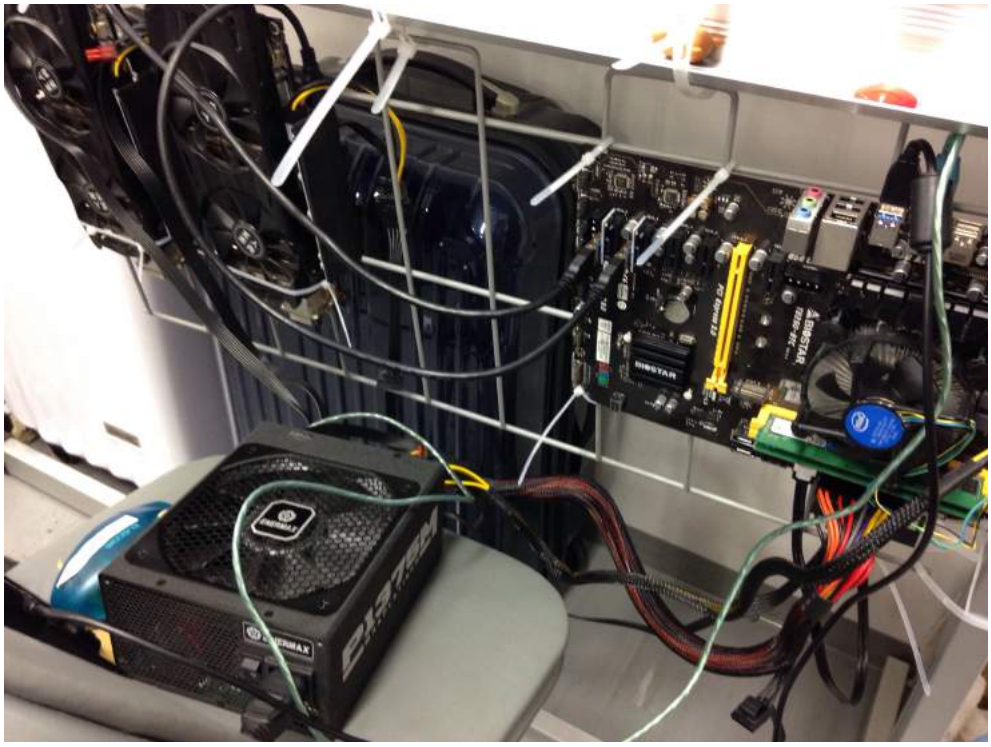

図 2　ホワイトボードマイニング