基般

❷ 対談：ビットコインコア開発の現場とは？ ―進化を続けるビットコイン―

Nicolas Dorier（ブロックチェーンハブ社）
本間善実（日本デジタルマネー協会）

本間（本）　自己紹介します．半導体業界，トラステッドコンピューティングの事業企画等を経て，2014 年 1 月に日本デジタルマネー協会を設立しました．ブロックチェーンがブームになる 2 年前から，ビットコインに関する調査と情報発信を続けています．

Nicolas（N）　私はメタコ社およびブロクチェーンハブ社の CTO で，ビットコインコア開発者の 1 人です．NBitcoin（マイクロソフト社の .Net Framework 向けという意味で冒頭に N を付けた）というビットコインの C# ライブラリを開発，メンテナンスしてます．

（本）　今日はビットコインに関する誤解，スケーラビリティ，プライバシー，サイドチェーン，カラードコイン等について話しましょう．

（N）　我々ビットコイナーはスケーラビリティやプライバシーを語りたがりますが，おそらく一般ユーザには無関係な話題なので，まず，ビットコインの魅力と利点を語りましょう．多くの人は，現金，クレジットカード，銀行を決済手段として利用しています．しかし，自分の資産を銀行に預けたり，決済に第三者機関を使うのは，実はリスクです．たとえ信頼できる第三者機関であっても．特に私のような外国人は，海外でクレジットカードや銀行を使う際に，不便を感じます．カウンタパーティリスクを，日本に住む日本人はあまり感じてないようですが，中央銀行や銀行を信用できない国もあります．すると，インターネットさえあれば使えて，カウンタパーティリスクのないピア・ツー・ピア（P2P）電子マネーは，大変便利で，かつ信頼できます．私は複数のクレジットカードを持っていますが，特に外国では使用できるとは限りません．ビットコインならば確実に使用できます．

ビットコインは，100% 自分の管理下にあり，ほかの誰も頼る必要ないことが最大の特徴です．中央銀行や銀行を信用できる場合は重要性が低いですが，国を出ると，これらとのコミュニケーションは困難であり，ビットコインの優位性が際立ちます．若い世代は，生まれながらに，インターネットとともに育っているので，ビットコインと相性が良いでしょう．

（本）　ビットコインは，すべての責任を自分で取ることができて，他者を頼る必要がないのが魅力，ということですね？

（N）　そうです．特に国境を越える人には魅力的です．9.11 事件の後は国際送金が困難でした．中央銀行と銀行は国際送金を規制することができます．ビットコインは，政府の規制を受けず，P2P 電子キャッシュであり続けることが重要です．カウンタパーティリスクを避けることが大事です．たとえば，私はフランスから日本に来た際に，クレジットカードを使えなかったことがあります．自分がクレジットカードの所有者と証明するために数日を要しました．自分のお金なのに，他者に利用を規制されるのは危険です．

（本）　Nicolas はサトシ・ナカモトのホワイトペーパー（信用できる第三者を必要としない電子キャッシュシステム）に忠実ですね？

（N）　私はプログラマで，お金や金融については無知でした．しかし，ビットコインの技術詳細を調べながら，同時にお金とは何だろうと考え始めて，『肩をすくめるアトラス』などの多くの書籍を読み，オーストリア経済学を学びました．私は日本に住み始めたところで，すでに国際送金周辺で問題を

抱えていて，私自身のお金の利用が困難だったので，ビットコインというソリューションは魅力的でしたし，深く調べて考えることができました．

もし，グローバル金融危機が再燃の場合，ビットコインはまだ全世界の決済を捌ききれませんが，数年後ならば，ライトニングネットワーク（ビットコインをスケールさせるための仕組み）で対応可能になるでしょう．

（本） グローバル金融危機に対する解になるにはスケールすることが必要で，ライトニングネットワークを実現するには，ビットコインコア開発の層で，ペイメントチャネル，ペイメントハブなど，何が必要ですか？

（N） コア開発だけでなくて，エクスプローラ，取引所，そのほか，さまざまな機能が必要で，時間がかかります．ビルを建てるには，基礎から作り，時間をかけて，作り込むように，ライトニングネットワークも同様の長い過程が必要です．

たとえば，ペイメントチャネルを使って，ある時間までに支払いされない場合，取引が解消されるような時間管理のプロトコルが必要です．

（本） ライトニングネットワークは，複数の要素技術の編集で実現されますが，これらは，どう発生したのでしょうか？

（N） オープンソースコミュニティには，さまざまなスキルセットを持つ才能が集まっています．漠然としたゴールに対して，複数の視点から議論を積み重ねることで，理論的にやれそうとの見込みを得て，各専門家が自分の得意領域で，具体化を進めていきます．

効率的なコミュニケーションを模索する中で，基本的なペイメントチャネル，ペイメントハブという概念が生まれました．しかし，ペイメントチャネルは一方向のみで，ペイメントハブは，TTP（信用できる第三者機関）が必要という問題がありました．ペイメントチャネルは双方向に発展しました．ペイメントハブは，もし TTP が失敗すると，意図通りの支払いが行われないという問題が発生します．時間管理可能な機能を盛り込むことで，意図通りの支払いがされない場合，取り戻すことができるようになりました．基礎的なプロトコルと細かな検証から，ライトニングネットワークに洗練されていきました．

（本） 幸運というか，奇跡的なチームで素晴らしいです．

（N） エンシュージアストが多数いるのが財産です．多くの人たちの熱心な貢献で日々洗練されてます．私自身は，ライブラリ開発が主たる役割で，Linux，C++ コミュニティで見かける暗号の専門家ではないので，それらの成果を利用して，C# でライブラリを開発する立場です．これらの環境を理解しながら，自分が貢献できる分野を見つけるのは楽しいです．Mike Hearn（元グーグル，現在 R3CEV 社所属の有名な開発者）が Java でやったことを，私は C# でやりました．つまり，暗号は下層で，私は，それを上層が利用しやすい環境を作ってます．私は暗号自体に貢献することはできず，暗号はブラックボックスとして使っています．

（本） breadwallet（最も人気あるスマホ用ビットコイン財布）は，Mike Hearn か Nicolas のライブラリを利用しましたか？

（N） 当時，iOS は objective C の利用が必須で，bitcoinj（Java ライブラリ）を使えなかったため，スクラッチから開発されました．その後，マイクロソフトが C# のクロスプラットフォーム化を進めたので，今では C# をさまざまな環境で使えます．

（本） ライトニングネットワークでビットコインがスケールすると，次はプライバシーが重要ですか？

（N） はい．ビットコインの問題はスケールとプライバシーですが，スケールよりもプライバシー，つまり fungibility（ファンジビリティ）が重要か

もしれません．

（本）　fungibility とは何ですか？

（N）　自由に交換できるという意味です．1 BTC（ビットコインの単位）は，どんな状況でも 1 BTC であるべきですが，ビットコインは全履歴を追えるので，ブラックマーケットで使われたビットコインを，たとえばコインベース社に預けると，（やる・やらないは別にして）同社は没収することができてしまいます．同じ 1 BTC でも悪い履歴の場合，安く扱われると問題です．事実，ブラックマーケットではビットコインよりも，モネロという匿名性に優れるアルトコインが使われ始めてます．

（本）　ミキシングをして，プライバシーを確保する解は有効ですか？

（N）　そのような外部サービスもありますが，外部サービスを頼るよりも，暗号通貨自体がプライバシーを持つ方が，暗号通貨として機能的です．モネロ，Zcash（開発中のアルトコイン）がビットコインの競合です．特に Zcash は fungibility を確保すると期待されてます．またライトニングネットワークは，スケールに貢献するだけでなく，副産物として，fungibility を解決します．

（本）　秘密トランザクションとは，何ですか？ Zcash と何が違うのでしょうか？

（N）　ビットコインは仮名であり，匿名ではないので，KYC（Know Your Customer= 顧客を知ること）を行う取引所から追跡が可能です．送り手と受け手の間のデータを秘密的にするのが，秘密トランザクションです．

　私は暗号についてはブラックボックスとして使っているので，Zcash の詳細は分かりませんが，おそらく Zcash は暗号レベルでプライバシーを実現していると推測してます．

（本）　秘密トランザクションが現実に機能するとベストな解でなくとも，Zcash は不要ですかね．Zcash は理論的には優れているのでしょう．さて，カラードコインの魅力は何ですか？

（N）　bitfinex（欧米人に人気ある香港の取引所）が，36% の資産を盗難されたのは悲劇ですが，盗難分を将来返済するためのトークンとして，bitfinex トークンをカラードコインで発行しました．もちろん 36% の資産を失ったのは bitfinex 側の過失ですが，それでも 64% の資産を引き出し可能で，弁護士に頼る従来的な処理よりも，早く 64% を利用できて，36% の回収の可能性があるのは，マウントゴックス社の事例より遥かに有利です．同社の場合，預け資産をまったく使えず，2 年以上経つので，それよりは，ユーザ側に有利です．少なくともブロックチェーンを利用する面白い実験と言えます．カラードコインはグローバルに無償で配布できますが，ほかの方法では高価のため，意義ある実験です．

（本）　カラードコインとサイドチェーンは競合する可能性がありますが，どう考えてますか？

（N）　カラードコインは現在使える解で，ペイメントハブとライトニングネットワークでスケール予定です．サイドチェーンは基盤層での開発が続いているので，将来は脅威となる可能性ありますが，現時点での比較は，市場に出ていないため評価困難です．

（本）　続いてビットコインコア開発の世界を知りたいのですが，ビットコインコア開発者は 17 名ですか？

（N）　リストされてるのは 17 名ですが，レポジトリにコードを投稿すればコントリビュータです．給与を貰ってフルタイムで貢献しているのはわずか 3 名で，多くの人は，メインの仕事をほかで持ちながら，空き時間に貢献してます．私は，取引所，財布，ペイメントプロセッサ，そのほかサービサーが使いやすい C# ライブラリ（NBitcoin）を開発してます．

（本）　人気あるライブラリを教えてください．

（N）　Java，JavaScript，C#，Python 等です．私は，C# ライブラリを開発，随時更新してますが，自分自身のライブラリを利用するエクスプローラ，財布，取引所も開発していて，そちらで稼いでいます．C# は Java や JavaScript よりも人気がないですが，C# ライブラリには自信を持っています．

C，C++ のライブラリもあるかもしれませんが，C，C++ プログラマは，上位層ではなくて，インフラ層で活躍してます．

ビットコインコアを分類すると，暗号層，コンセンサス層，プロトコル層，財布層，API（アプリケーションプログラムインタフェース）層からなります．私はコンセンサスライブラリも開発しています．コンセンサス層を分離，抽象化する仕事です．

サトシ・ナカモトのコードはバグが少なく，実用に耐えるモノで，ビギナーではないのですが，抽象化されたモジュールを使用せず，オブジェクト志向ではないオールドスタイルで解読困難でした．ある変更がほかにどんな影響を及ぼすのか検証が困難でした．CPU 周辺あるいはメインフレームのプログラマかもしれません．他人が扱いやすいモジュール化に意識がなかったのは明らかです．

Cory Fields と私が，抽象化（ライブラリ化）を進めてますが，すべての更新には検証が必要で，簡単ではないです．

（本）スクラッチから作り直すほうが，楽では？

（N） いえ．それは危険です．分散されたノードが合意できず，分岐する可能性があり，検証するのが大変です．

（本） 各コア開発者について解説してくださいますか？

（N） Wladimir J. van der Laan が主なメインテナーで，すべての貢献から，重要な貢献を選び出し，優先度を決めて，bitcoind を更新します．Jonas Schnelli は財布部分の責任者です．Marco Falke はユニットテストの責任者です．あらゆるバグを防ぎます．これら 3 人がフルタイムの貢献者です．

Dr. Pieter Wuille はすべての分野に精通してます． Cory Fields はソースコードのコンパイルの責任者です．複数プラットフォームでの稼働を保証するのは大変な仕事です．Gregory Maxwell は暗号に強く，プライバイシー確保に尽力してます．Luke-Jr もカバー範囲が広く，特にマイニングとブロック生成に精通してます．Jorge Timón もサトシのコードの抽象化，モジュール化に取り組んでます．上位層からコア開発に参加するには，コードの検証者として参加することです．私はライトニングネットワークのプロトコルが定まり，実装されたならば，N ライトニングというライブラリを開発予定です．

（本） Nicolas の活動と優先度を聞いていると，大変戦略的と思いました．

（N） オープンソースプロジェクトでは，自分の得意領域以外で貢献するのは難しいので，得意領域に活動範囲を限定してます．すべてをやることは不可能です．

（本） ライトニングネットワーク，サイドチェーンがレイヤ 2 で，ビットコインコアの外の活動とすると，ビットコインコアは，今後，どんな分野に取り組みますか？

（N） 暗号，署名領域です．プライバシーの確保，集合署名など．集合署名で，ブロックサイズはコンパクトになり，プライバシーも拡大します．これらは当分終わることなき領域です．

（本） 貴重なお話をありがとうございました．

（2016 年 8 月 31 日受付）

Nicolas Dorier dorier@blockchainhub.co.jp

メタコ社およびブロックチェーンハブ社の CTO．マイクロソフト社認定トレーナー．趣味としてオープンソースコミュニティに貢献した NBitcoin が評判となり複数社のコンサルを請け負う．Bitcoin Core と NBitcoin の 2 つにフルコミットしている．

本間善実 jimmyhomma@gmail.com

京都大学工学部物理工学科卒業．（一社）日本デジタルマネー協会代表理事．（株）debit 社外取締役．（株）breadwallet アドバイザー．ソラミツ（株）アドバイザー．（一財）ブロックチェーン技能認定協会 アドバイザー．