beyond-blockchain.org

報道関係者各位

日本発の新たなブロックチェーン基盤 BBc-1 (Beyond Blockchain One) を公開

一般社団法人ビヨンドブロックチェーン

2017 年 10 月 31 日

デジタル通貨 Bitcoin を成立させるために発明されたブロックチェーン[1]は、競争的マイニング[2]による改ざん耐性と、最も改ざんしにくい履歴[3]を全員が正史として採用するという「ナカモト・コンセンサス」により、通貨・証券をはじめとして、各種行政の手続きなど、社会の信用基盤をめぐって、中央の管理主体を不要とする新たな応用可能性の地平を拓いたことで評価に値します。しかし、この技術は、実時間性・秘匿性・スケーラビリティの課題や、暗号技術の危殆化への対応を含む、技術を進化させる上でのガバナンス上の課題、ネイティブ通貨の暴落による停止可能性など、さまざまな課題を未解決のまま持っています。

ビヨンドブロックチェーン株式会社 (東京都渋谷区) では、こうした従来のブロックチェーン技術がもつ諸々の課題を解決し、通貨やその他のフィンテック応用、各種証明機能といった社会信用基盤の自動化・高度化に寄与するべく、新たな基盤ソフトウェア「BBc-1 (Beyond Blockchain One)」を開発して参りました。このたび、10 月 31 日 (火) に同ソフトウェアのソースコードを一般公開し、新たに非営利法人として立ち上げた「一般社団法人ビヨンドブロックチェーン」(東京都渋谷区) にコードの管理を移管し、開かれた体制にて、無償のオープンソースソフトウェアとして開発・応用を推進することになりましたのでお知らせいたします。

BBc-1 とは？

BBc-1 (Beyond Blockchain One) は、従来のブロックチェーン技術が持つ諸々の課題への長期的な解決策を用意し、かつ短期的に控える実証実験や、その後の実用化に至るまでのアプリケーション開発を支援するための新たな基盤ソフトウェアです (図 1)。

[1] 【ブロックチェーン】記録の内容や存在を誰にも否定できないように保存・維持し、その正当性を誰もが確認でき、また、正当な記録が投入されることを誰も妨げることができないような分散台帳。

[2] 【競争的マイニング】Proof of Work (作業証明) によって、数学的くじを当てるまでの作業のコストを払ったと証明できる者だけが、記録を集めたブロックを生成するとともに新たなデジタル通貨の供給を受けられるという方式。

[3] 【履歴】ブロックチェーンでは競争的マイニングに勝ったと信じる者が自律的に履歴 (=チェーン) を形成していくため、頻繁に履歴が分岐する。ナカモト・コンセンサスでは、分岐した履歴のうち、最も改ざんしにくいもの (=作業証明に最も大きなコストが支払われているもの) を正しい履歴として採用する。

c/o BcH, 1F Yamazaki Bldg. 2-6-11 Ebisu Minami, Shibuya-ku, Tokyo 150-0022 Japan

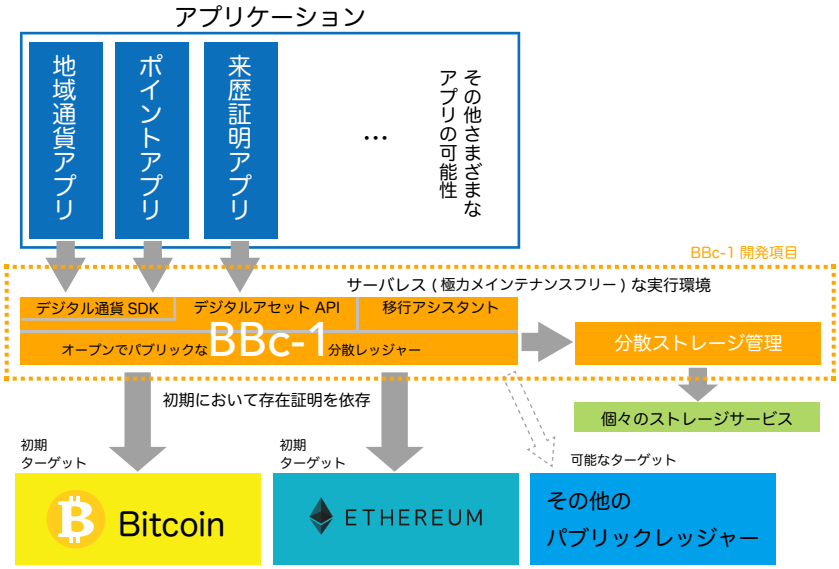

図 1: BBc-1 のアーキテクチャ

特徴：

- 既存のブロックチェーンよりも強固な改ざん耐性
- ブロック[4]や Proof of Work (作業証明) [5]といった、効率を損なう要因を取り払い、即時性、省資源およびスケーラビリティを達成できる設計
- データの共有範囲を設定し秘匿性を達成できる、「ドメイン」と呼ばれるサブネットワーク
- Bitcoin の考え方を踏襲した、(同一ドメイン内の) 第三者による検証可能性を担保したデータ構造
- プライベートな応用でもトランザクション[6]の証明機能を提供
  - 初期には Bitcoin や Ethereum といった既存のブロックチェーンと共に動作することにより達成
  - 中長期的には履歴交差[7]の考え方を応用した独自方式により達成
- ユーザ識別子と公開鍵を分離することにより、秘密鍵が失われた場合の回復手段を提供
- コア部ではベーシックな機能だけを提供することによる高度な拡張性

BBc-1 では、既存のブロックチェーン (Bitcoin および Ethereum) の存在証明の機能を利用することで、アプリケーションに対してトランザクションの証明機能を提供します。利用するブロックチェーンは動的に変更できることを想定しています。

[4] 【ブロック】トランザクションの集まり。
[5] 【Proof of Work (作業証明)】数学的くじ引きをして、それに当たったと証明すること。
[6] 【トランザクション】送金やデータの更新などの不可逆的な操作。
[7] 【履歴交差】無関係なトランザクションやデータ同士の間に暗号学的ハッシュ関数やデジタル署名による連結を埋め込むことで、過去のトランザクションやデータの存在・非存在を証明する方式。

現在、ブロックチェーンの応用には、大きく分けて通貨系 (「量」を移転する仕組み) とアセット系 (「量」を持つ実体の存在・来歴を証明し、かつ様々な権利を管理する仕組み) の 2 種類がありますが、BBc-1 では当面の応用型としてこれらの両方を想定し、そのための API[8] や SDK[9] の整備を進めています。

BBc-1 の運用では特定の管理者を不要にできるよう、いわゆるサーバレスな実行環境にデプロイされたノード群の自律分散協調動作により目的を達成できるように設計しており、また、BBc-1 におけるブロックチェーンの抽象化レイヤを発展させることにより、将来的には下位のレッジャー (台帳) への依存を無くし、ブロックチェーンそのものを置き換えることを狙っています。

ブロックチェーンハブ・コミュニティ[10]の優秀な研究開発者陣に恵まれ、17 年以上にわたる P2P・デジタル通貨の研究や、直近 4 年間のブロックチェーンの分析や実装の経験に裏付けられた、実用指向で確かな基盤技術と自負しております。当非営利法人には、すでに大手メーカーを含む企業がメンバーとして参加し、地域ポイントから宇宙開発までをも含む、さまざまな応用に向けた検討と実証実験システムの開発が進行しております。ぜひ、多くの方々にご活用をご検討いただきたく、広く報道をいただければ幸いです。

GitHub URL　https://github.com/beyond-blockchain/bbc1
団体 URL　https://beyond-blockchain.org

団体概要	
名称：	一般社団法人ビヨンドブロックチェーン
形態：	非営利
目的:	従来のブロックチェーン技術がもつ諸々の課題を解決し、通貨や各種証明機能といった社会信用基盤の自動化・高度化に寄与する一連のビヨンドブロックチェーン技術の開発とその応用促進を通して、社会の様々な課題の解決に貢献すること。
設立：	2017 年 9 月
代表理事：	斉藤 賢爾
住所：	〒 150-0022 東京都渋谷区恵比寿南 2-6-11 山崎ビル 1 階 BcH

お問い合わせ： office@beyond-blockchain.org (担当： 斉藤)

[8] 【API】Application Programming Interface の略で、アプリケーションがシステムの機能を使うためのインタフェース。
[9] 【SDK】Software Development Kit の略で、ソフトウェア開発のためのツールキット。
[10] 株式会社ブロックチェーンハブ (https://www.blockchainhub.co.jp/) により創業が支援された各ベンチャー企業や、その活動に賛同する企業支援者、および開発者のコミュニティ。