

# シンプルMyブロックチェーン・ネットワークを作る

土屋 健

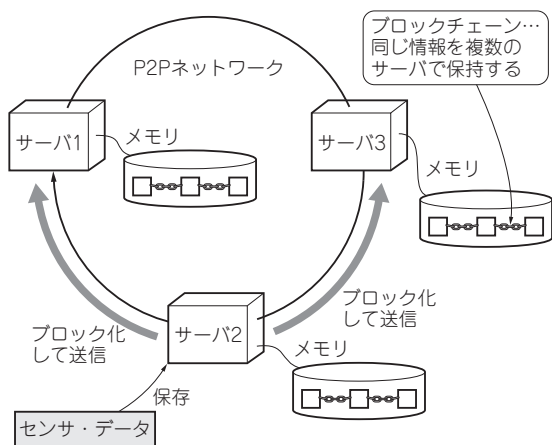


図1 安全でシンプルに使えるネットワークI/O環境を手に入れる

Myブロックチェーンを使ったセンサ・データの保存やデータ値からアクションが起こせる自由で堅牢な制御システム

### ● IoT的な使いどころ

ブロックチェーンそのものはビットコインとともに表に出てきたので、暗号通貨を実現するための仕組みだと思われがちですが、そうではありません。

アプリケーション部分を取り替えば、さまざまなサービスを実現でき、世の中にもブロックチェーンを基盤とした暗号通貨以外のサービスもあります。

ブロックチェーンを基盤とした暗号通貨以外のサービスとして以下が考えられます。

1. センサ・データやマイコンのログの保存
2. 制御コマンドやその応答の保存
3. カメラ画像の保存
4. 農産物や制作物のトレース
5. データの売買(スマート・コントラクト)

本章で作るのはこれらの土台となるブロックチェーンです。

### 作るもの

ここでは簡易なブロックチェーンを作って動作させ

てみます(図1)。ブロックチェーンは一般的に以下の要素で構成されています。

- P2Pネットワーク(通信の基盤)
- ブロックチェーン(ブロック、チェーン管理、コンセンサス)

実際のシステムはもっと複雑な構造となっていますが、ブロックチェーンそのものとしては最低限これだけあれば実現できます。また、その他の要素技術としては、公開鍵暗号や署名の仕組みもありますが、それらはブロックチェーン固有のものでもありませんし、ブロックチェーンそのものに必須という訳ではないので、今回は除いています。

### ●仕様

シンプルな仕様のMyブロックチェーンを作ってみます。

- ブロックには1つのデータだけ保存する
- P2Pネットワークへのサーバ追加だけをサポートし、削除はできない
- 1つのサーバ・プロセスでマイニングは同時実行しない
- チェーン競合の回避はタイム・スタンプで判断<sup>注1</sup>
- コンセンサスは簡易的なPoW(Proof of Work)
- チェーンにつなげなかったブロックに含まれているデータは破棄する<sup>注2</sup>
- ブロックはメモリ上に保存される(ディスク・アクセスがないので高速だが、プロセスを止めるとデータがなくなる)

これは、一般的なブロックチェーンの全ての機能を網羅しているわけではありませんが、ブロックチェー

注1: 実際にはチェーンが長い方が採用されるアルゴリズムが良いが、今回はそこまで実装していない。P2Pノードへの途中参加もないし、悪意ある集団もないので、そこは割り切った。

注2: 本来は再度マイニングから始めてデータを記録するのが、その仕組みはブロックチェーンより上位のアプリケーションで実施するのが好ましいので、今回はそこまで実装していない。