

第3部

Appendix 1

IoT入門としての最低限 [ご購入はこちら](#)

元祖も知っておこう… ビットコインの基礎知識

おがわ てつお

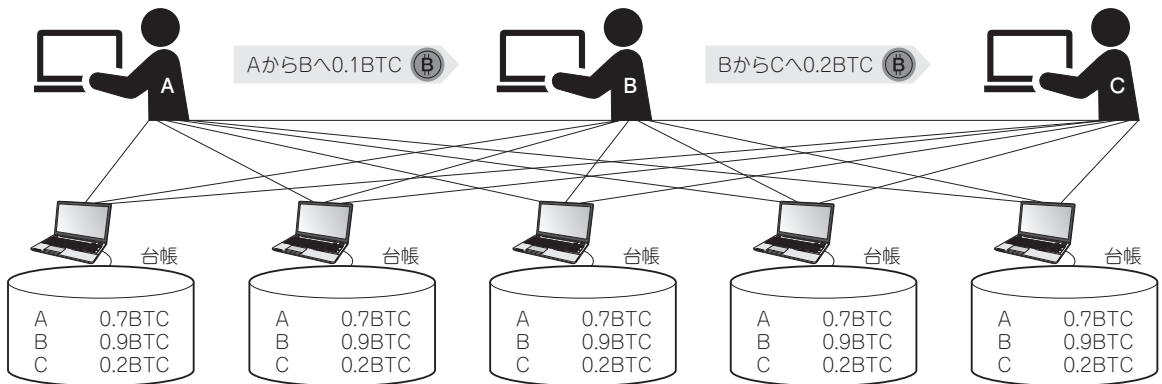


図1 全ての端末の台帳データは同期されている

● ビットコインの実態は取引データの集合体

まず初めにビットコインの実態について説明したいと思います。ビットコインの取引を行うためには、まず初めにウォレット・アプリを自身のPCまたはスマホ、タブレットに導入する必要があります。このウォレットに誰かからビットコインを送金してもらうと、ウォレット上に自身が所有するビットコインの量(単位はBTC)が表示されるようになります。

このとき、ビットコインはどこにあるのでしょうか。実は取引されたビットコインは、利用者のウォレット同士で取引データが送受信されているのではあ

りません。取引データはビットコイン・ネットワークと呼ばれる世界中にある何千台ものノードにブロードキャストされ、各ノードの中にある台帳に書き込まれます(図1)。

この台帳に書かれた取引データこそがビットコインの実態なのです。全てのノードの台帳は常に同期されているため、ウォレットがどのノードに接続しても同じ取引データを参照でき、送金が行われるとそれを利用者は認識できます。

● 発行上限は2100万BTC

ビットコインには中央銀行のような管理組織はありません。このためマイニングで無限にビットコインが発行されると、ビットコイン自体の価値が低下するいわゆるインフレになります。コア開発者Satoshi Nakamotoはこれを予測し、2100万BTCを発行上限とし、半減期という仕組みで徐々に発行量を減らすプログラムを組み込みました。これは4年ごと(≒21万ブロックごと)にマイニング報酬額を半分に減らすというもので、2140年ころに発行量はゼロとなるように作られています(図2)。

● 参加者

ビットコイン・ネットワークには特定の管理運営者や所有者はいません。世界中の開発者がビットコイ

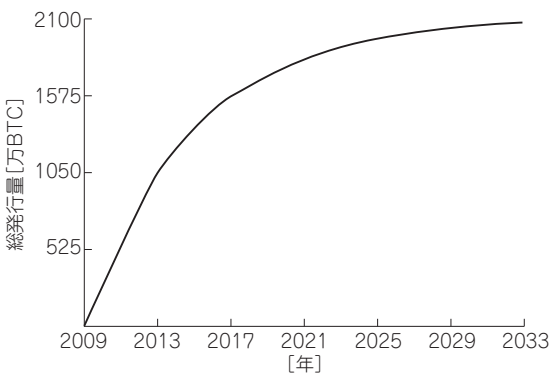


図2 ビットコインの発行量には上限がある