第4章 新時代ネットワークの精神を理解する

ブロックチェーンで伝説「Satoshi Nakamoto論文」とは

小暮 淳

ビットコインを提唱したSatoshi Nakamotoの論文（形式の文書）はインターネットで以下のURLから入手できます．

Satoshi Nakamoto;Bitcoin: A Peer-to-Peer Electronic Cash System.
https://bitcoin.org/bitcoin.pdf

ブロックチェーンを語るには，まずは上記論文をあたるべきでしょう．しかし，初めから本論文だけでブロックチェーンを理解することは難しく，懇切丁寧な解説書も多数出版されているため，ここではその精神を理解する程度の引用に留めます．

● 中央集権から「分散管理」へ

ビットコインが従来の電子通貨と最も異なる点は，トランザクション・データを管理する中央集権が存在しないということです．即ちトランザクション・データを分散生成／処理／管理することによって世界中での流通を可能としました．これは中央集権システムの限界を突破することができなかった1990年代の電子通貨しか知らないものにとっては驚きのブレークスルーでした．

分散管理にもかかわらず，全てのデータを整合の取れたものとするためには，幾つかの仕掛けが必要です．まずは，おのおののトランザクション・データが正しいものであることを保証しなければなりません．

● 「電子署名」で取引データの正しさを保証

正しいとはどういうことでしょうか．ビットコインのシステムが扱うトランザクション・データは，単純化された形では，あるビットコイン口座から別のビットコイン口座へ何ビットコイン振り込むかというデータです．それはもちろん，振込元口座の持ち主が意図したものでなければなりません．それを保証するために用いられているのが電子署名の技術です．即ちトランザクション・データに振り込み元の口座の持ち主が電子署名を施すことによって，そのトランザクションは持ち主が意図したものであることを保証できます．論文2節「Transactions」を見てみると，冒頭に以下の記述があります．

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

これらの関係は**図1**のように示されています．

● 2重使用などの取引の不整合を防ぐ

電子署名は個々のトランザクション・データの真正性を保証しますが，これだけでは全体の整合性を保証することはできません．例えば署名者に悪意がある場合，2重使用を防ぐことはできないのです．このためビットコインでは，トランザクション・データを全て公開し，相互監視することによって，2重使用を含むデータ不整合をチェックし，不整合のあるデータはブロックチェーン上に登録しないようにします．論文には以下の記述があります．

The only way to confirm the absence of a transaction is to be aware of all transactions.（中略）

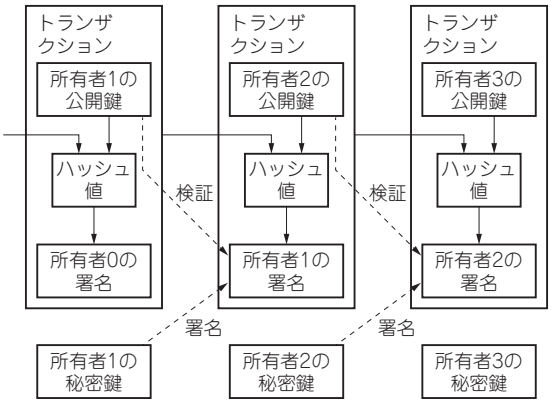

図1　トランザクション・データに振り込み元の口座の持ち主が電子署名を施すことによってそのトランザクションは持ち主が意図したものであることを保証する