第3章 ハッシュ・ハッシュ・ハッシュ…暗号化&検算の仕組みをかい間見てみる

ブロックチェーン台帳のデータ構造

佐藤 聖

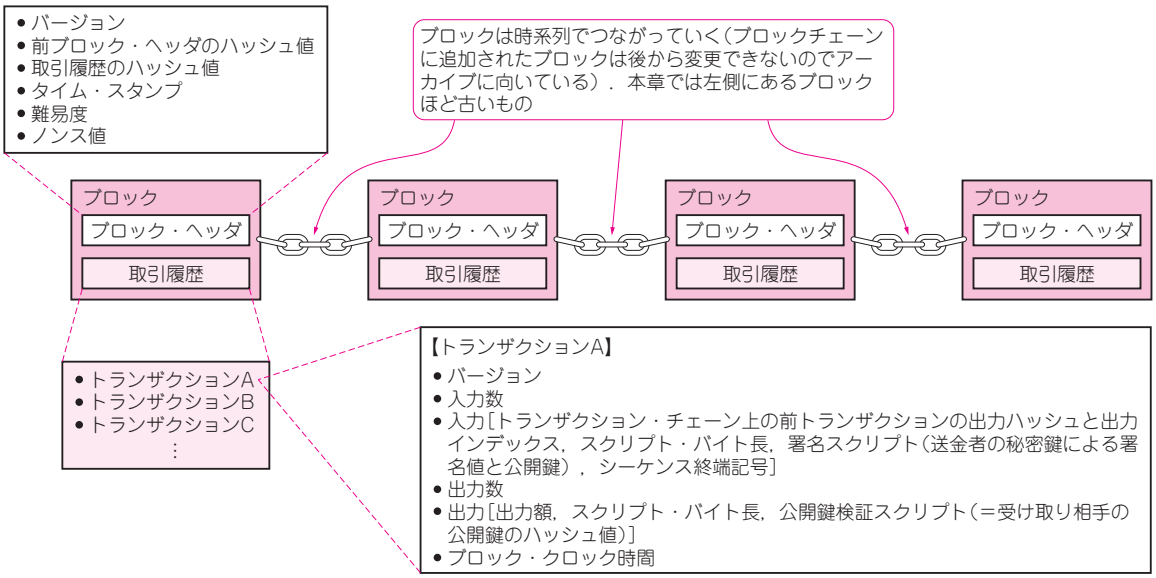

図1　台帳には取引データやセキュリティ・データが書き込まれている

台帳の基本構造

ブロックチェーンはトランザクションを格納し記録する台帳です（**図1**）．この台帳は各ノードがそれぞれ保有しており参照や更新を行います（**図2**）．ブロックチェーンは，複数のブロックがチェーンのようにつながったイメージです．例えば「Proof of Work：PoW」（暗号通貨によく利用される）による計算で作られるブロック［**図3**（**a**）］は主に，ブロック・ヘッダと取引履歴とでできています．

ブロック・ヘッダ［**図3**（**b**）］の中には，前ブロック・ヘッダのハッシュ値，取引履歴のハッシュ値，ノンス値，その他ヘッダが含まれます．

ヘッダの中身①…前ブロック・ヘッダのハッシュ値

「前ブロック・ヘッダのハッシュ値」は，前ブロックとの論理的なつながりを保持します．これによって前ブロックと現ブロックとのつながりの正しさを検証できます．

ヘッダの中身②…取引履歴ツリーのルート・ハッシュ値

● 取引そのものはブロック内に残っていなくてもよい

ブロック・ヘッダには，取引データから算出されたハッシュ値［**図4**（**c**）］[注1]が格納されていて，マークル・ツリーのルート・ハッシュといいます．

ハッシュ値を格納しておくことで，取引データそのものはブロック内に格納しておかなくても，取引データがブロックの要素として正しい組み合わせであることを検証できます．

取引履歴のハッシュ値は，取引の不正や整合性を確

注1：ハッシュ値は，ハッシュ関数を使って作ります．ハッシュ関数は，任意長のビット列から規則性のない固定長のビット列を生成してくれます．詳しくは第5章で解説しています．

編集部注：ノンス（nonce）の読み方について．ノンスともナンスとも言われます．特集ではノンスで統一しました．

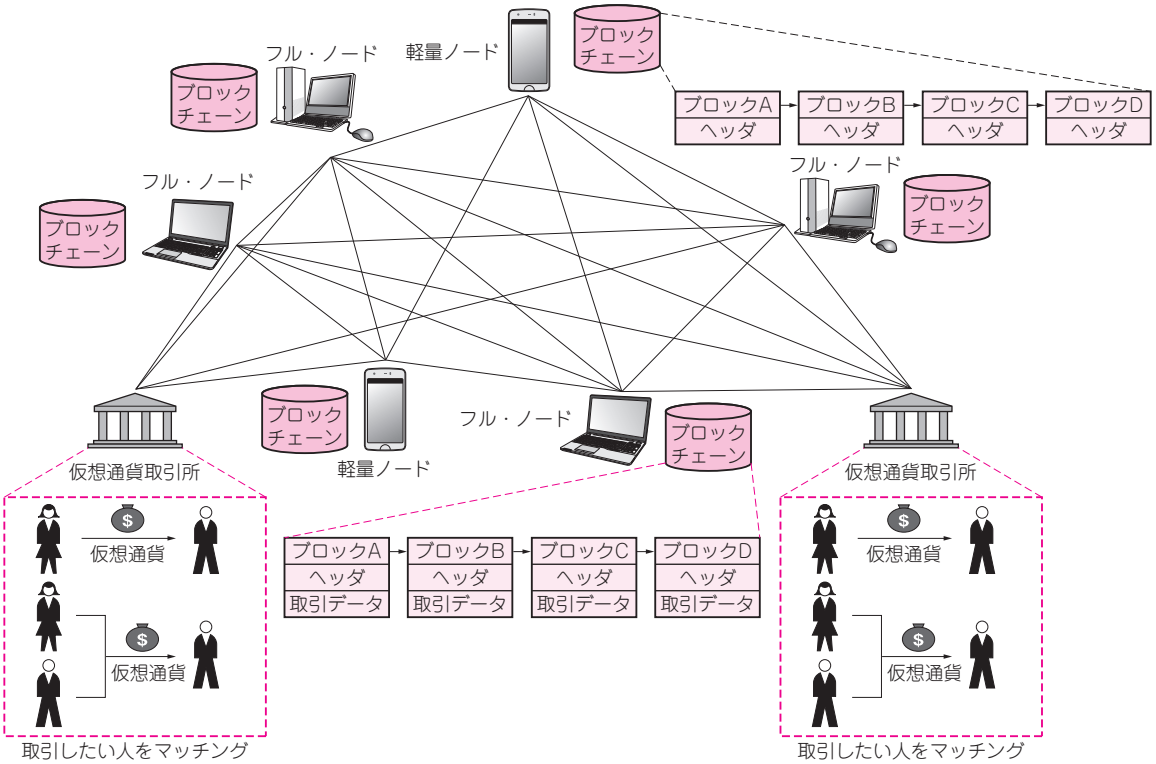

図2　台帳は各ノードがそれぞれ保有しており参照や更新を行う

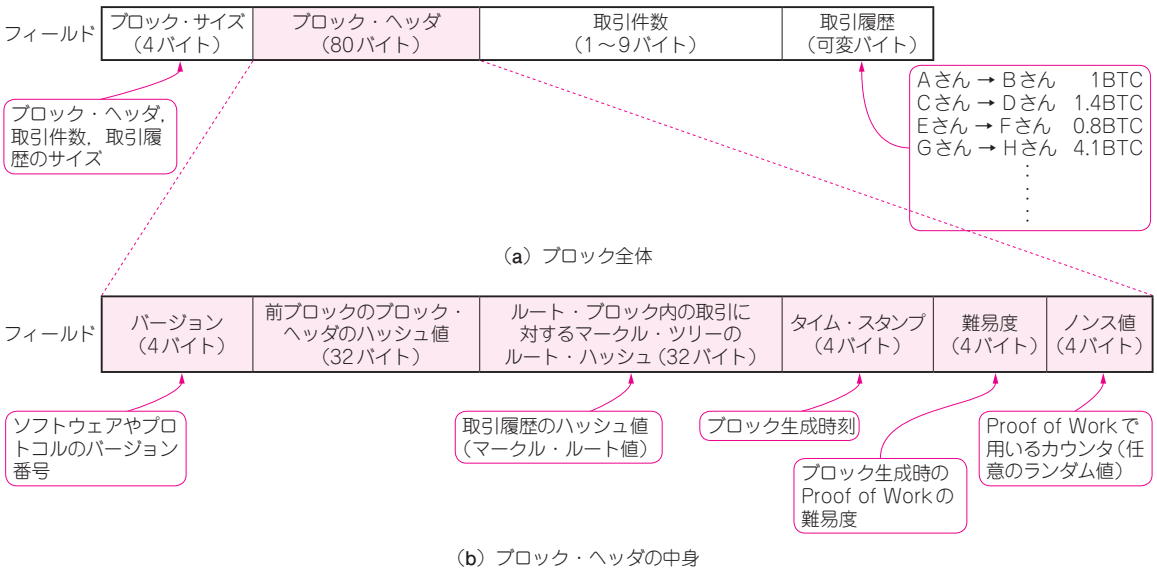

図3　台帳（ブロック）の構造

認するために利用されます．ブロック・ヘッダと取引履歴とをつなげる重要な情報です．ブロック・ヘッダにルート・ハッシュを書き込むことで，軽量ノードは一部の取引履歴だけを保持していればよく，過去から現在までの全ての取引データを保持する必要はありません．

● 過去の取引を検証できるメカニズム

軽量ノード利用者が，過去の取引データを検証する方法を通貨の例で示します．まず，P2P通信によってウォレット内の取引履歴を他ノードに伝えます．フル・ノードA（例えばAとしただけ）は，ブルーム・フィル