第5章　シミュレータの設計

本章では、第 4 章で述べた Bitcoin のネットワーク、そして個々のノードの振る舞い、データの伝搬のモデルを素にシミュレータの設計を行う

5.1 シミュレータの設計に含める情報の限定

本研究での Bitcoin の設計において、ネットワークを伝搬するオブジェクトは block、及び addr という情報構造体のみに限定し、決済情報等は省く事とする。

5.2 Bitcoin システム

節 4.2 において、Bitcoin システムを以下の要素

$b_h \in B$　block とそれらの block が連結して形成する blockchain

M　参加ノード群

L:M×M　それらのノード間のリンク

A　それらのノードのネットワークアドレスでありメッセージでもある addr

に抽象化した。これをオブジェクト指向モデリングにより図に表したのが図 5.1 となる。

図 5.1 シミュレータにおけるオブジェクト群

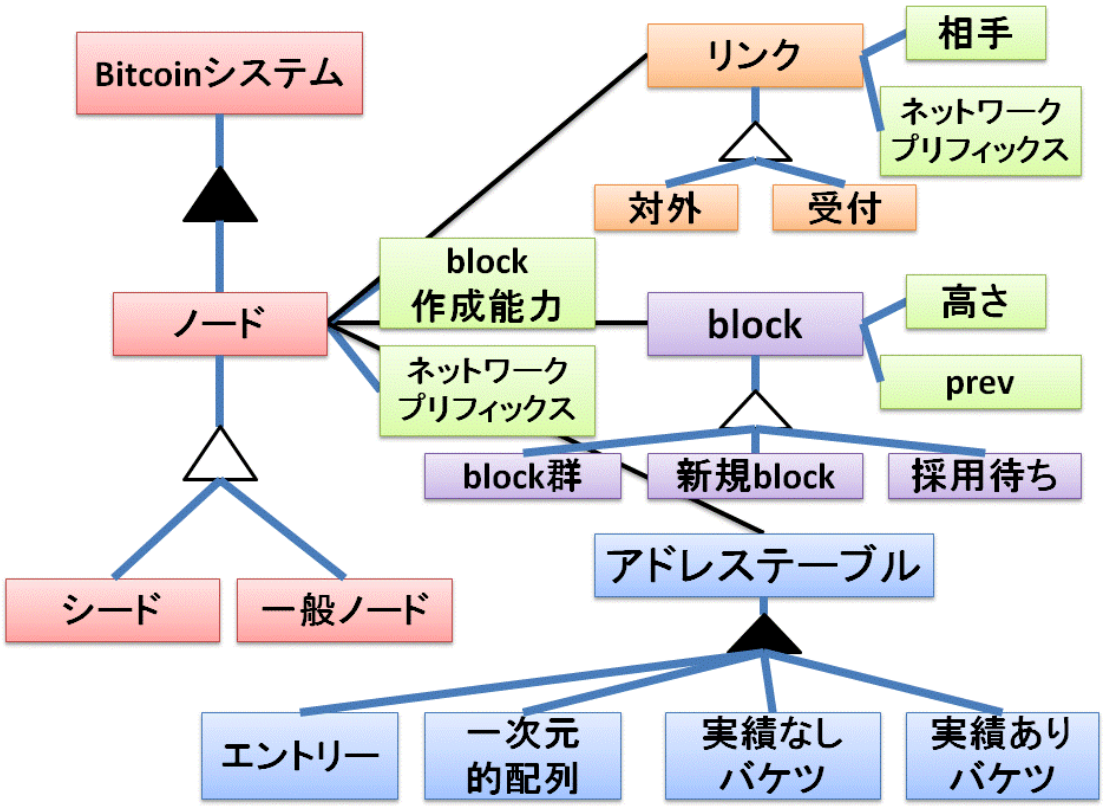

図 5.1 に示されている通り、当研究における Bitcoin のシミュレータ実装では、ノードを Bitcoin システム全体の根幹に据えており、リンク、block、addr 等の他オブジェクトはノ

ードが作成、伝搬、保持するような構造となっている。

5.3 個々のオブジェクトの構造

5.4 パラメーター一覧

本研究におけるパラメータの一覧を以下の表 1 に表す。

表 1. パラメーター一覧

表記	内容	値
N	常時最低存在ノード数	2000 台
hogehoge	時間経過による存在ノード数の変動	＊＊＊
これこれ	新規参入ノード数のレート	＊＊＊
あれあれ	永久離脱ノード数のレート	＊＊＊
何%	外部から接続を受け付けないノード数	何%
P_b	ネットワーク全体の block 作成確立	$\geq \frac{1\ \text{block}}{600\text{s}}$
このような分布	Block 作成能力の全ノードに対する分布	＊＊＊
	Block の受信と他ノードへの送信に要する時間	＊＊＊
	Addr の受信と他ノードへの送信に要する時間	＊＊＊

5.5 Bitcoin ノード群

5.6 リンク

5.7 他ノードへの接続

5.8 block 作成

個々のノードは、block 作成報酬を求め block 作成を試みる。実 Bitcoin システムでは、ネ

ットワーク全体で block が作成され blockchain に登録されるレートが 10 分に 1block となるように調整されており、その過程で作成されても不採用とされる block も存在する為ネットワーク全体で block が作成される確率は：

$$P_b \geq \frac{1\ \text{block}}{600s} \quad (\text{パラメータ})$$

と仮定される。(なお、正確な数値は検証、キャリブレーションにより調整する)
任意のノードxが block 作成に成功する確率 P_{xb} は、当該ノードの Bitcoin ネットワーク全体に占める block 作成能力を：

$$0 \leq r_x \leq 1$$

とした場合、シミュレーションにて個々のノードが block を作成出来る確率は、シミュレータ内の時間の 1 ユニットと 1 秒の対応を：

$$\frac{1s}{t_1}$$

とし、前回の block 作成挑戦からの経過仮想時間をt_aとした場合：

$$P_{xtb} = P_b \times r_x \times t_a \times \frac{1s}{t_1}$$

となる。なお、ノード群の個々に保有する block 作成能力値である r は、その総和が 1 となり、そのノード毎の block 作成能力値はこのような分布となる。(パラメータ)

5.9 block 伝搬、管理

5.10 addr の作成、伝搬、管理、利用