Inclusive protocol

- 이 논문은 블록의 크기가 크거나 블록이 자주 생성될 때에 적합한 블록체인 메커니즘을 연구한다.

- 비트코인의 경우 fork choice rule로 longest chain을 채택함.

- 이더리움의 경우 변형된 GHOST 프로토콜 사용.

- fork choice는 이중지불을 당할 수 있다.

- 이전의 연구는 블록 생성률, 블록크기가 증가하면 블록생성시간이 길어지고 이는 포크가 많이 발생함을 의미.

- 공격에 취약해지고 탈중앙성을 위태롭게함.

블록크기 증가, 블록 생성률 증가 문제

- 악성 공격에 대한 프로토콜의 보안적 문제가 생김

- 블록의 크기를 늘리는 것이 트랜잭션 처리량을 선형적으로 증가시켜주지는 않는다.
- 적은 수의 마이너들을 불리하게함. 보상이 적어지고 탈중앙성이 적어짐.

- 따라서, 이더리움의 변형된 GHOST프로토콜과 longest chain rule 에 추가적인 수정안을 제시한다.

- 이는 어떤 프로토콜과도 연동되어 잘 작동한다.

- 블록 DAG 및 inclusive 프로토콜을 통해 모든 트랜잭션을 로그에 담을 수 있도록 블록체인을 DAG 구조로 재구성할것임.

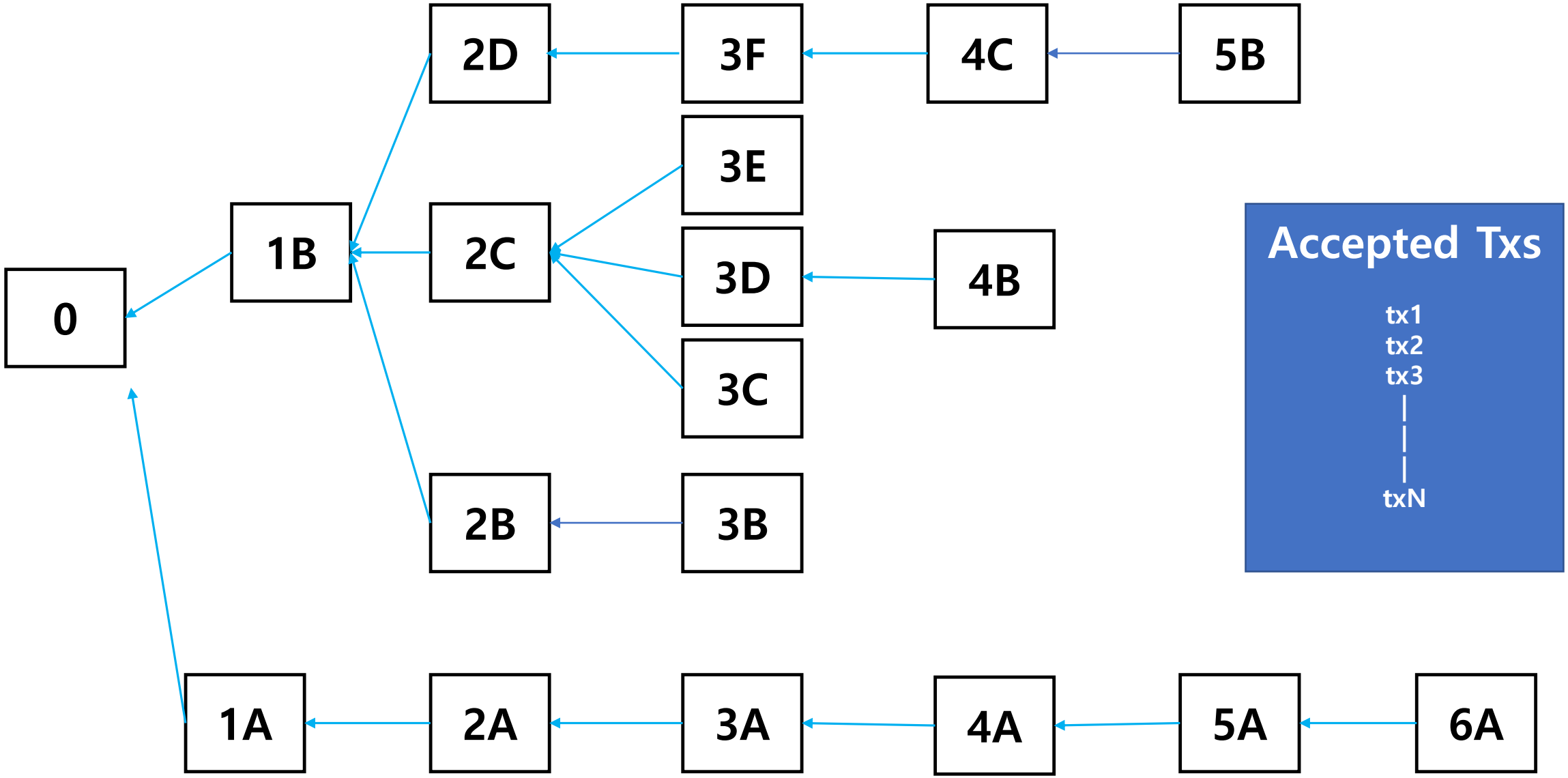
- Inlcusive 프로토콜의 중요한 점은 블록이 메인체인의 일부가 아니어도 블록을 만든사람에게 수수료를 보상으로 준다는 것이다.

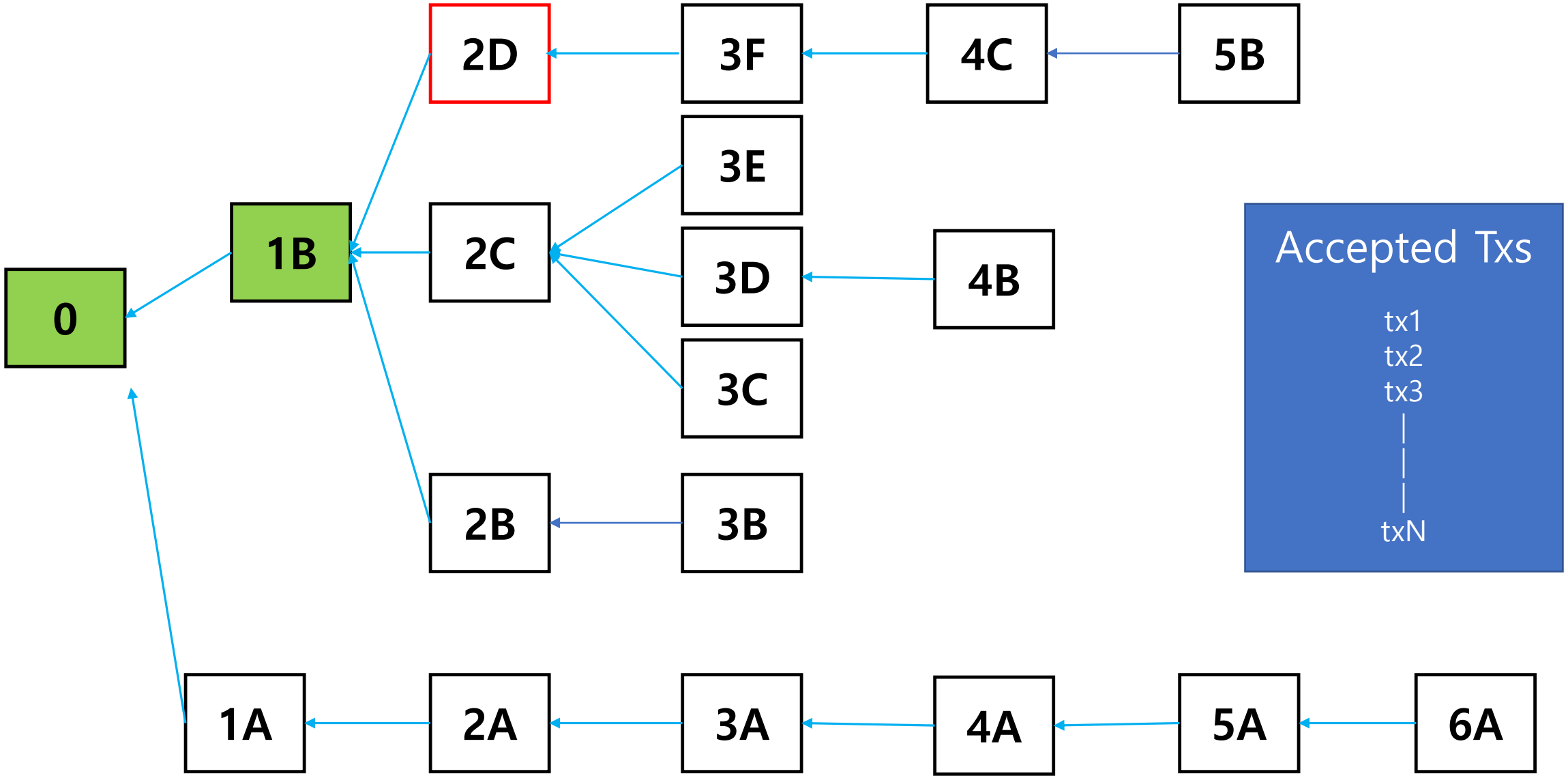
- 게임이론, 노드의 충돌을 최소화 ---

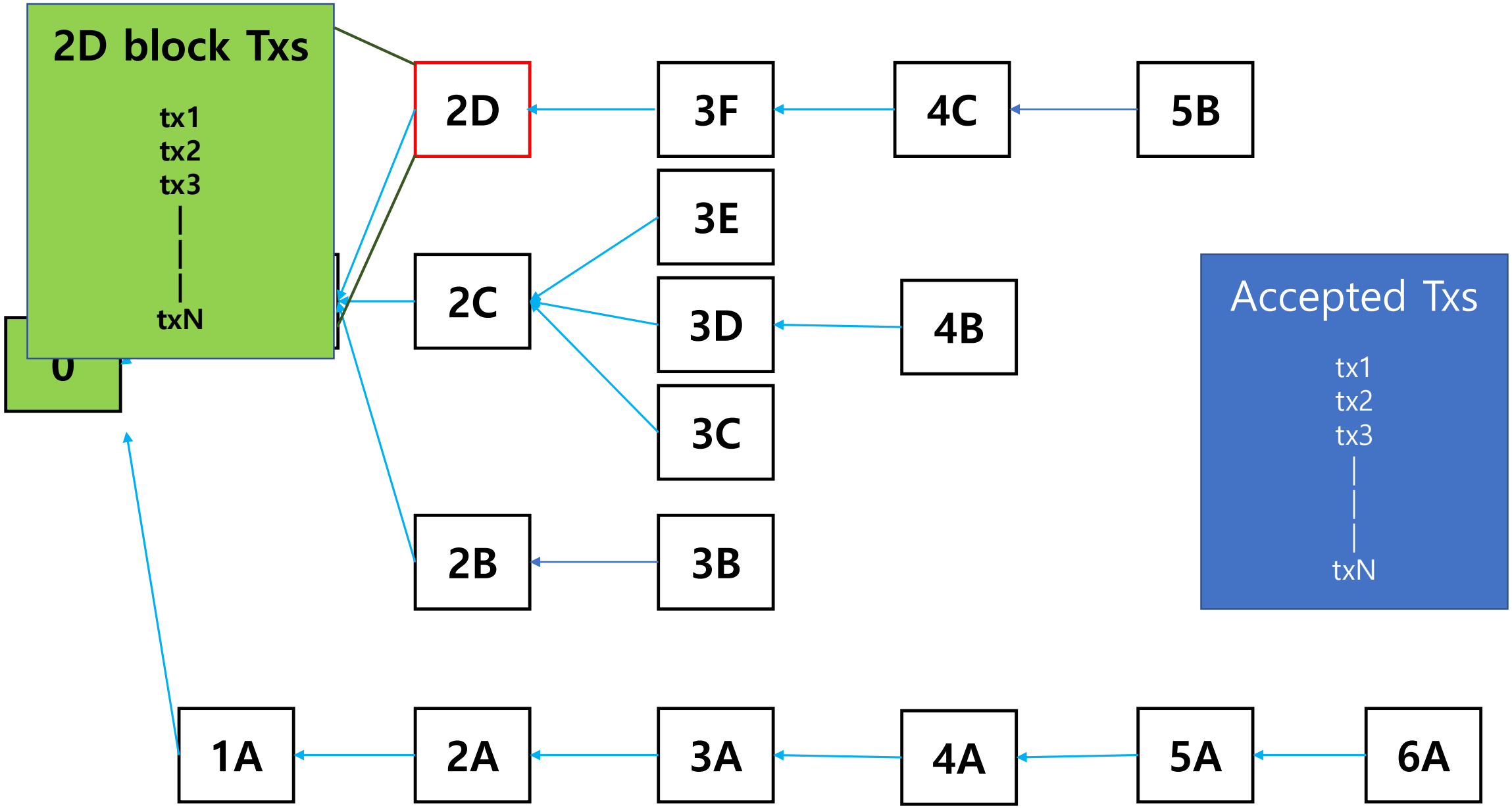
- 비순환 구조의 블록 그래프를 통해 모든 블록의 내용을 로그에 통합함.
- 게임이론적 모델을 제공함.
- 게임 이론적 솔루션으로 프로토콜의 성능을 개선한다.
- 이중지불에 대한 문제를 해결하면서 탈중앙화와 보안성을 잃지 않는것이 목표.

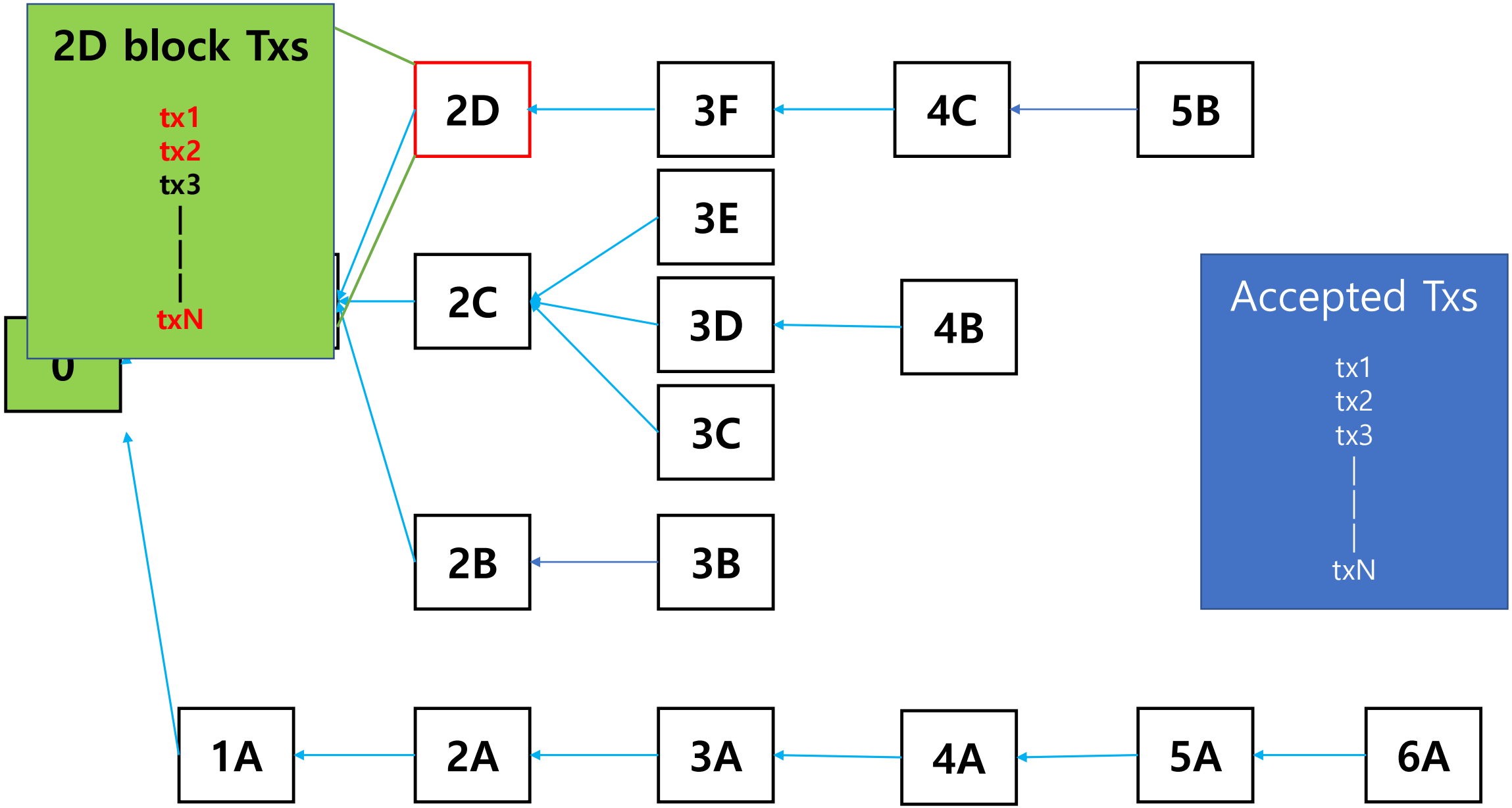
- 블록은 포크가 발생하므로 DAG구조 가 형성됨.

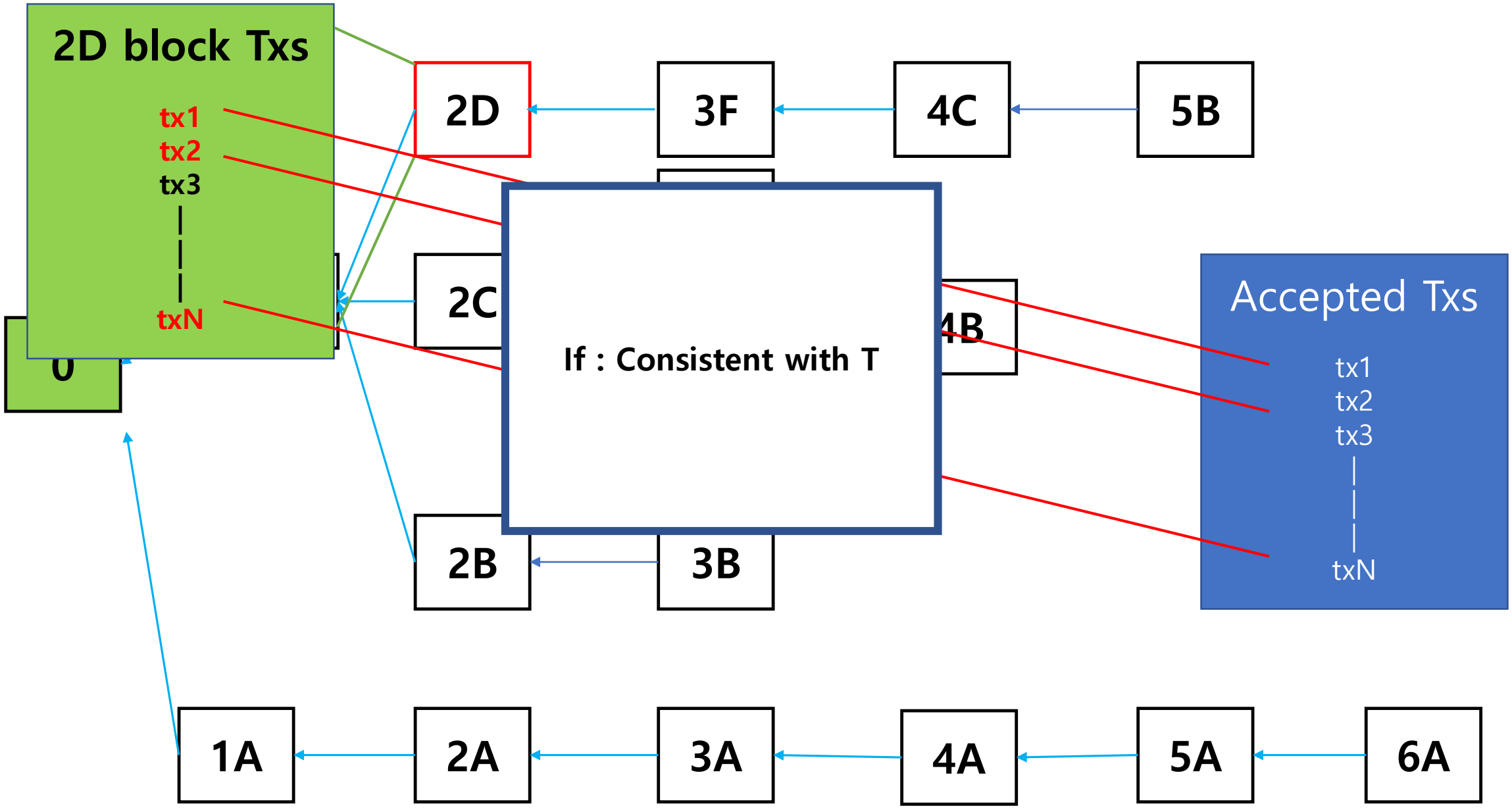
- 블록을 타고가면서 해당 블록에 들어있는 트랜잭션이 T에 속하지 않으면 T에 포함시키는것을 반복.

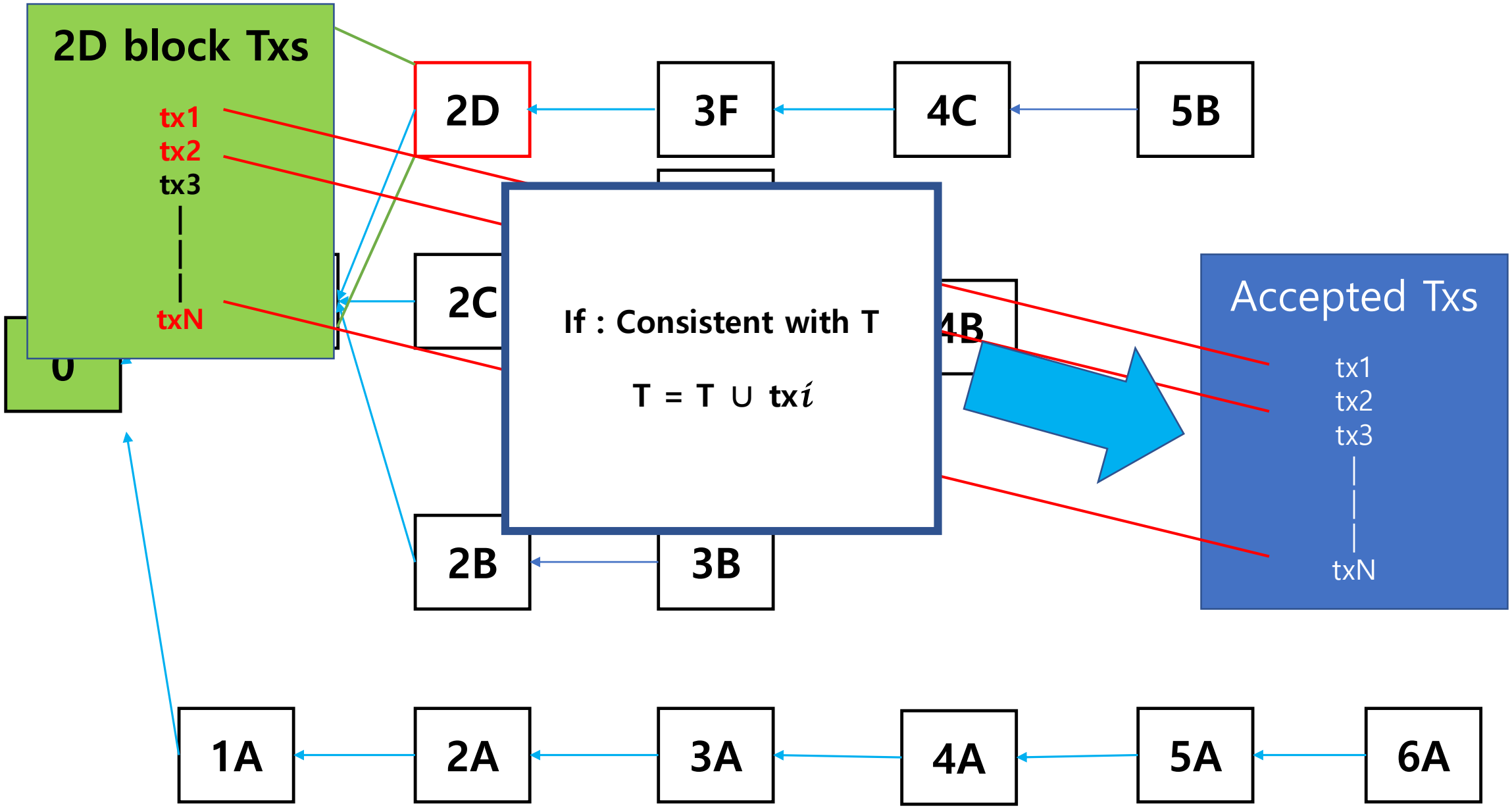

0
1B
2D
3F
4C
5B
2C
3E
3D
4B
3C
2B
3B
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A

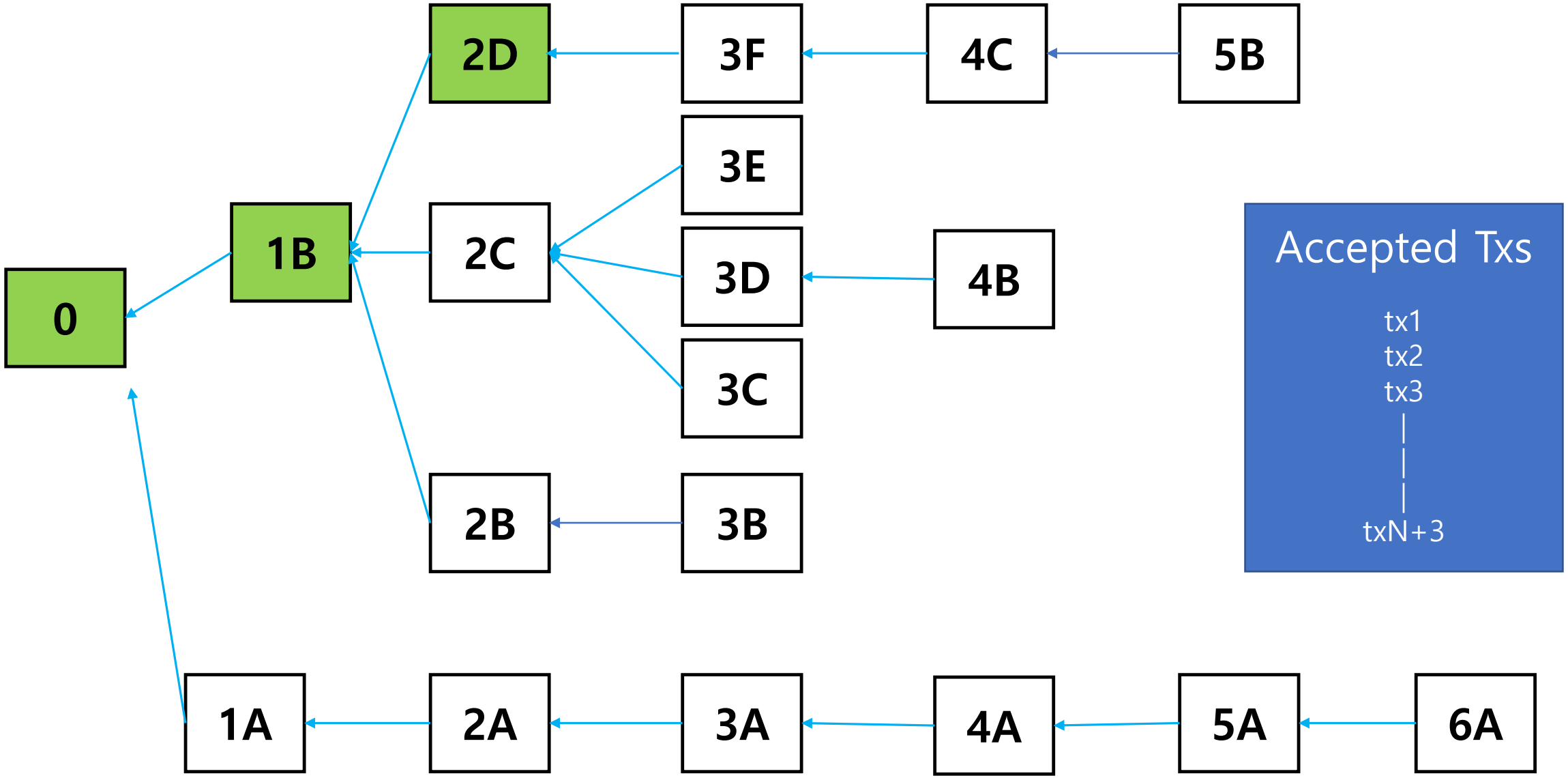

0
1B
2D
2C
2B
3F
3E
3D
3C
3B
4C
4B
5B
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A

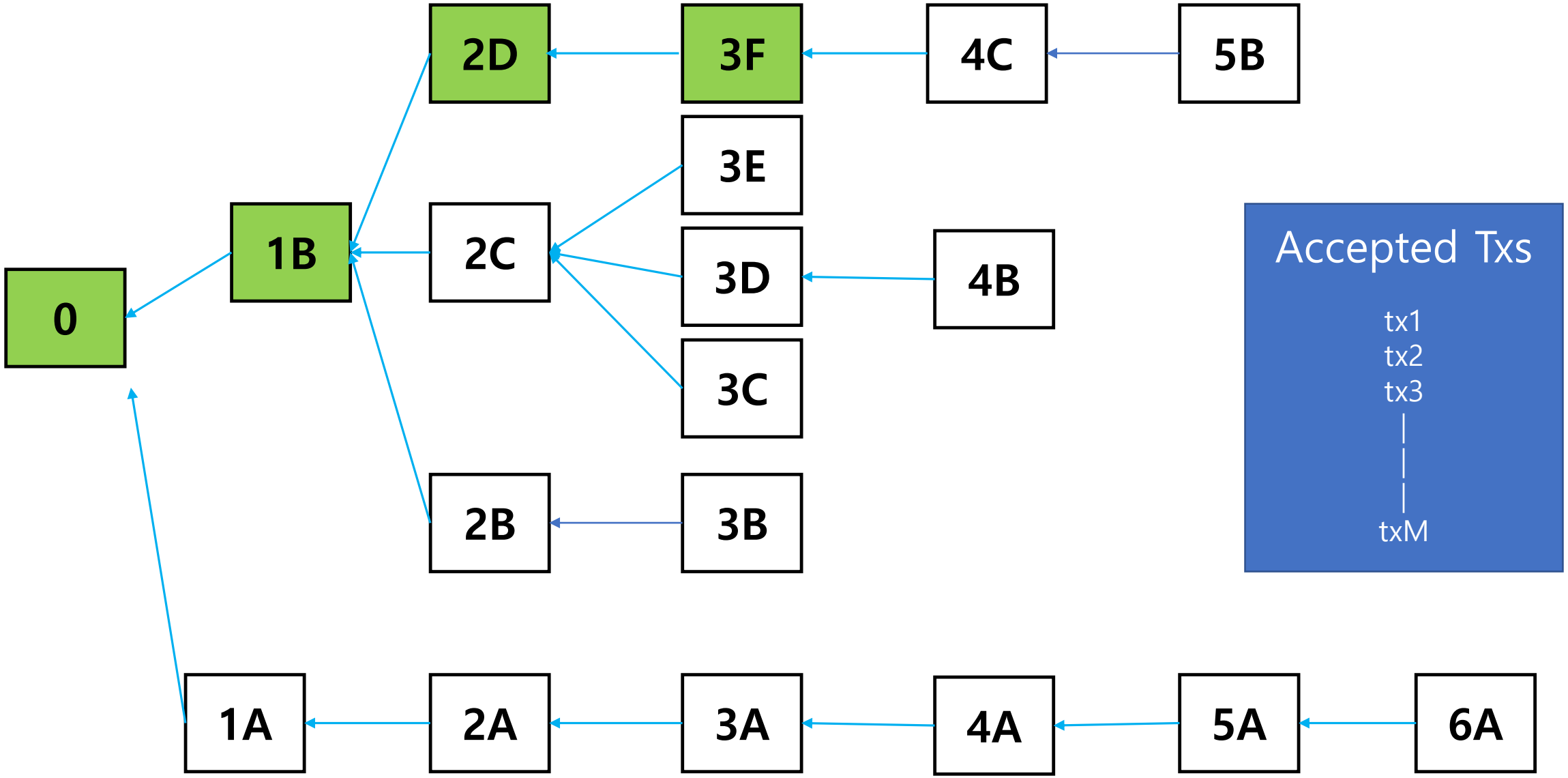

2D block Txs
tx1
tx2
tx3
txN
0
2D
3F
4C
5B
3E
2C
3D
4B
3C
2B
3B
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A

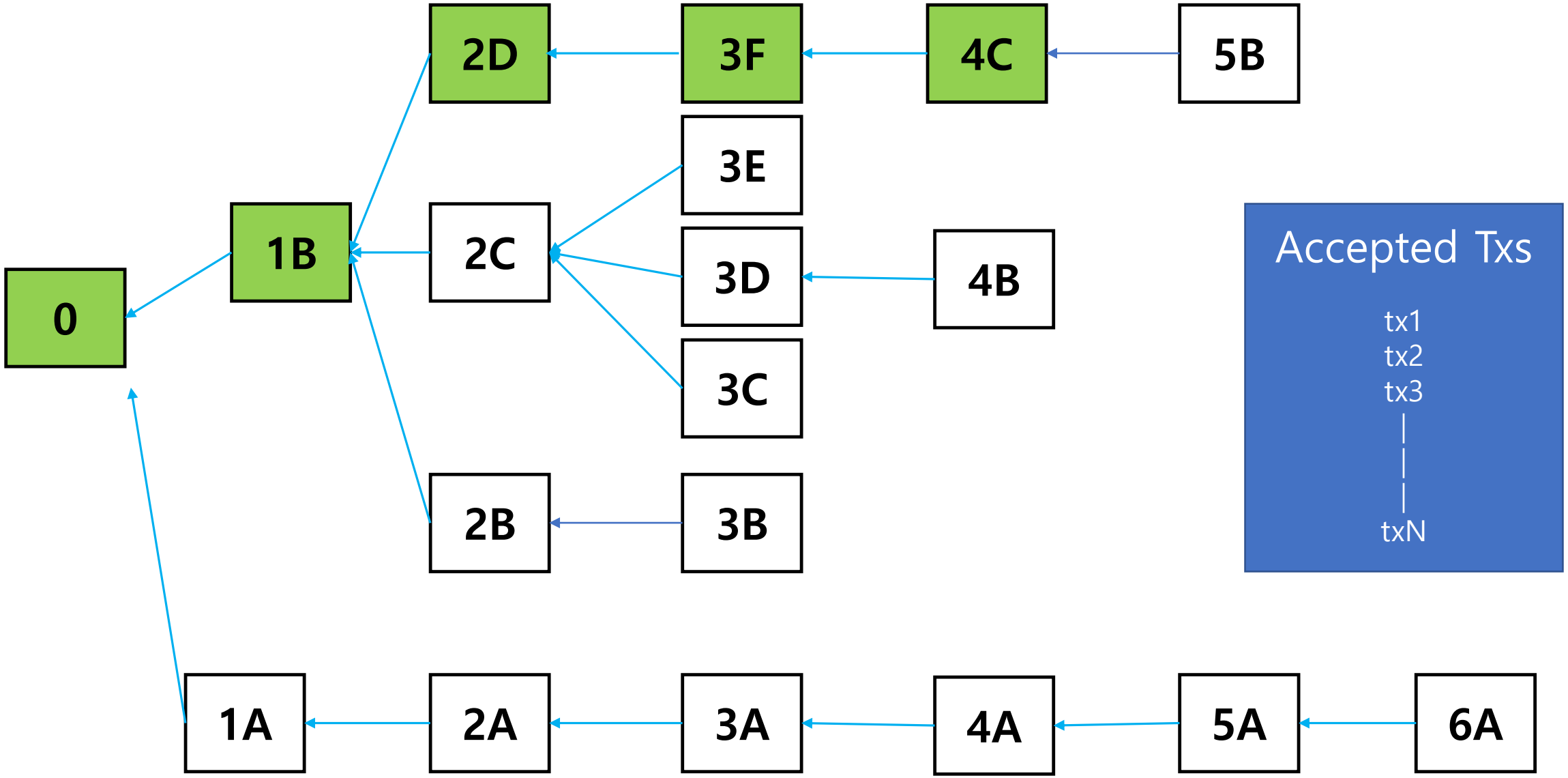

2D block Txs
tx1
tx2
tx3
txN
0
2D
3F
4C
5B
3E
2C
3D
4B
3C
2B
3B
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A

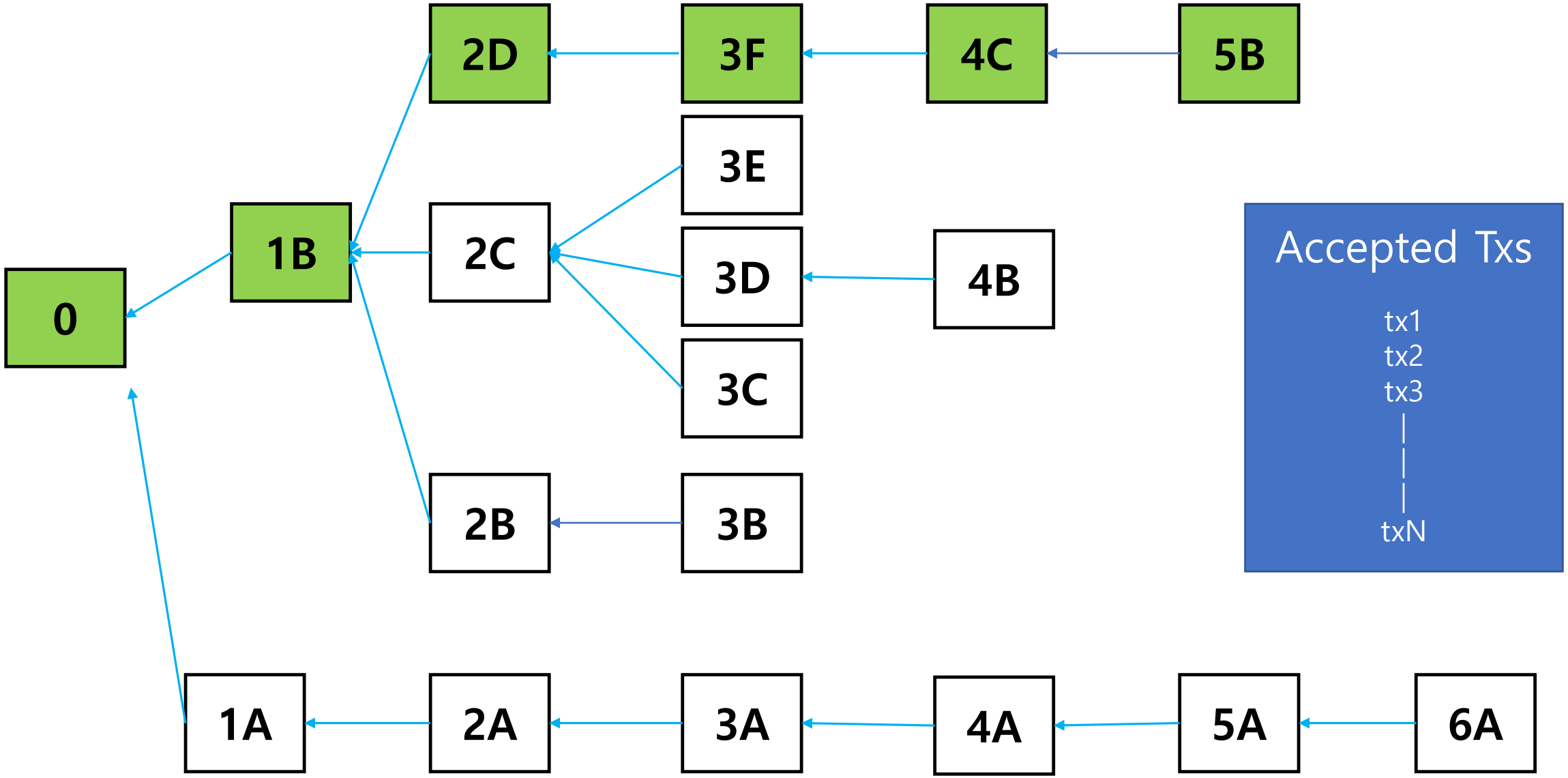

2D block Txs
tx1
tx2
tx3
txN
2D
3F
4C
5B
2C
4B
If : Consistent with T
Accepted Txs
tx1
tx2
tx3
txN
2B
3B
1A
2A
3A
4A
5A
6A

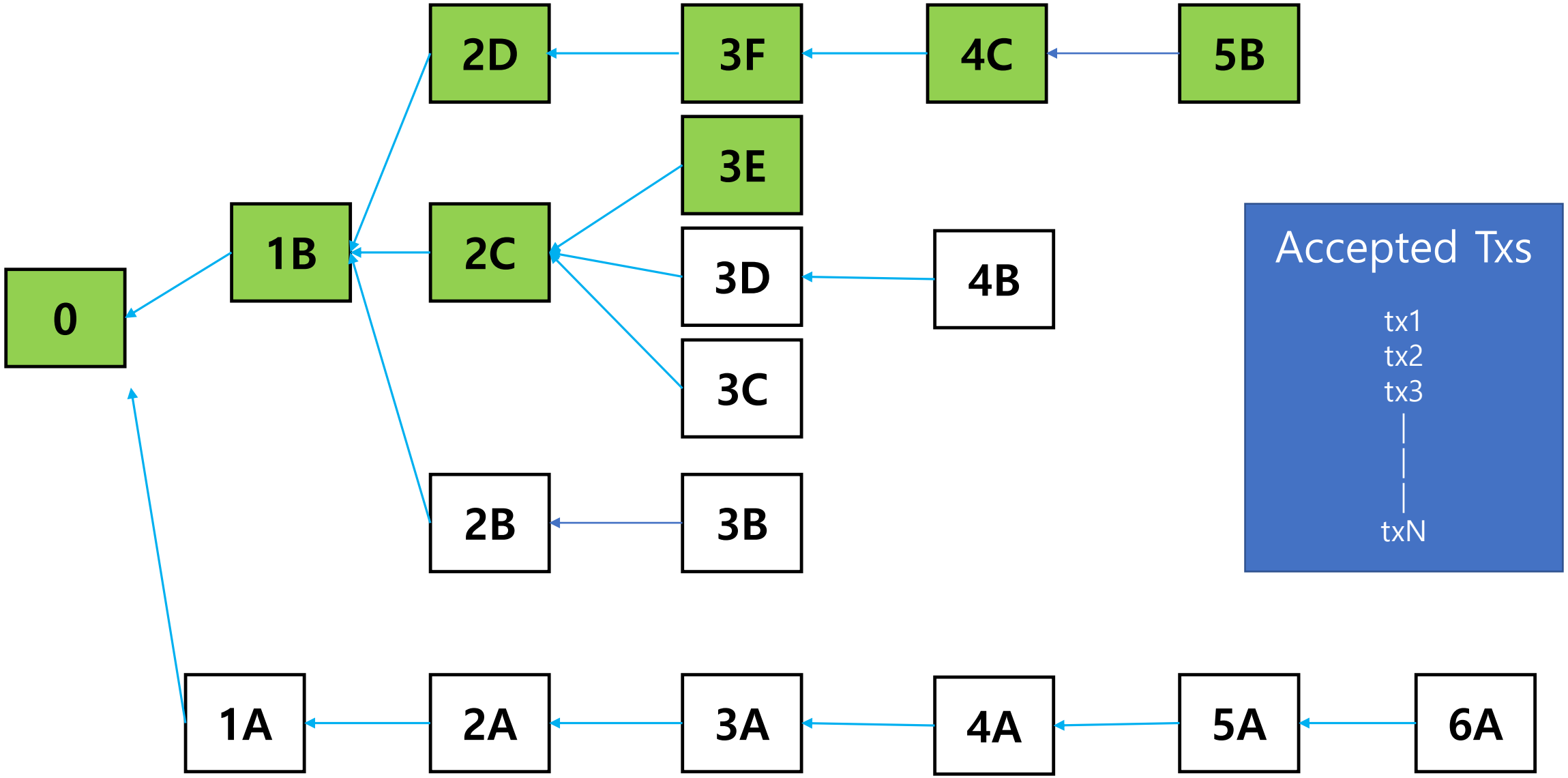

2D block Txs
tx1
tx2
tx3
txN
2D
3F
4C
5B
2C
4B
2B
3B
0
If : Consistent with T
T = T ∪ tx$i$
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A

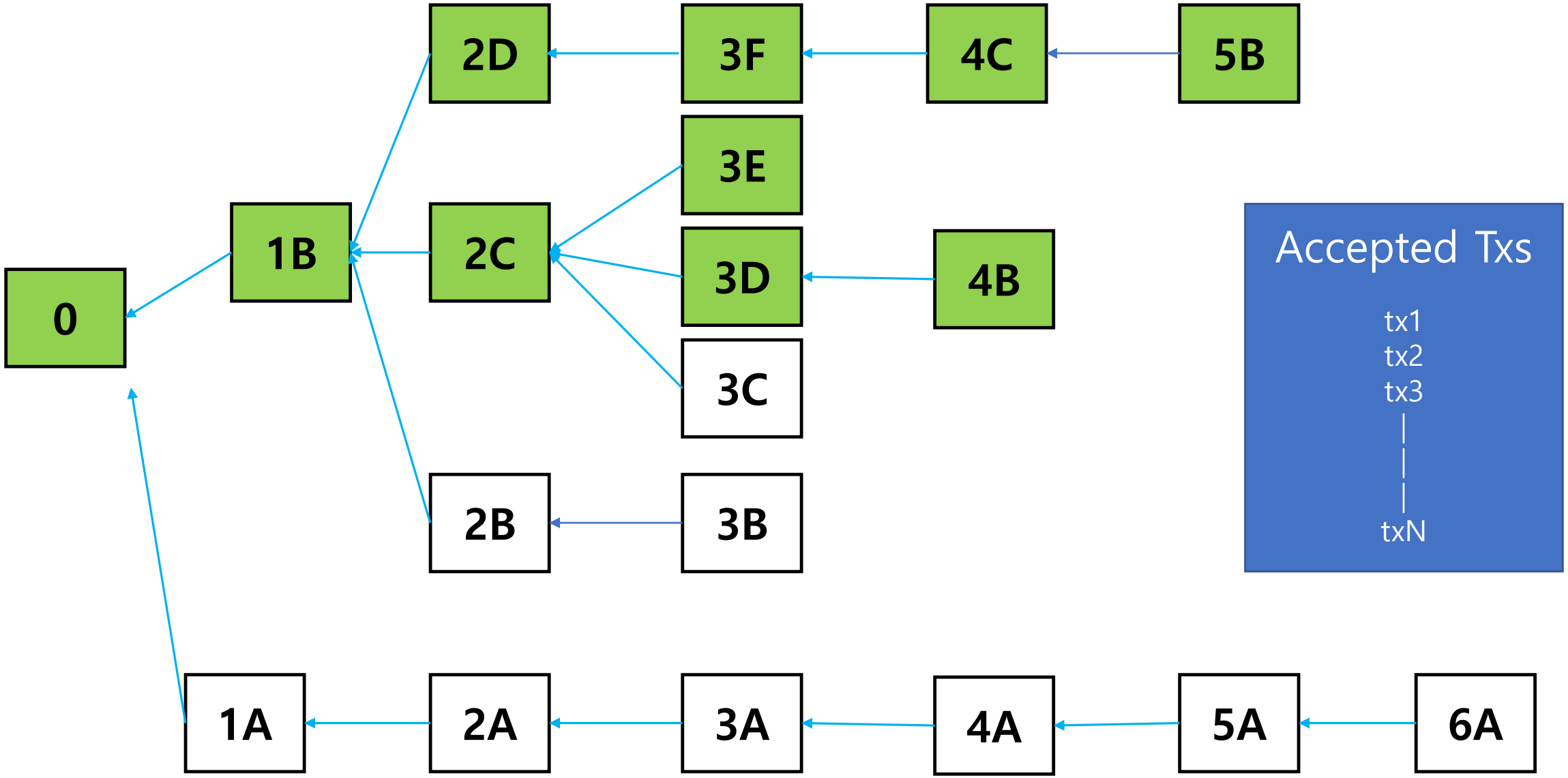

0
1B
2D
2C
2B
3F
3E
3D
3C
3B
4C
4B
5B
1A
2A
3A
4A
5A
6A
Accepted Txs
tx1
tx2
tx3
txN+3

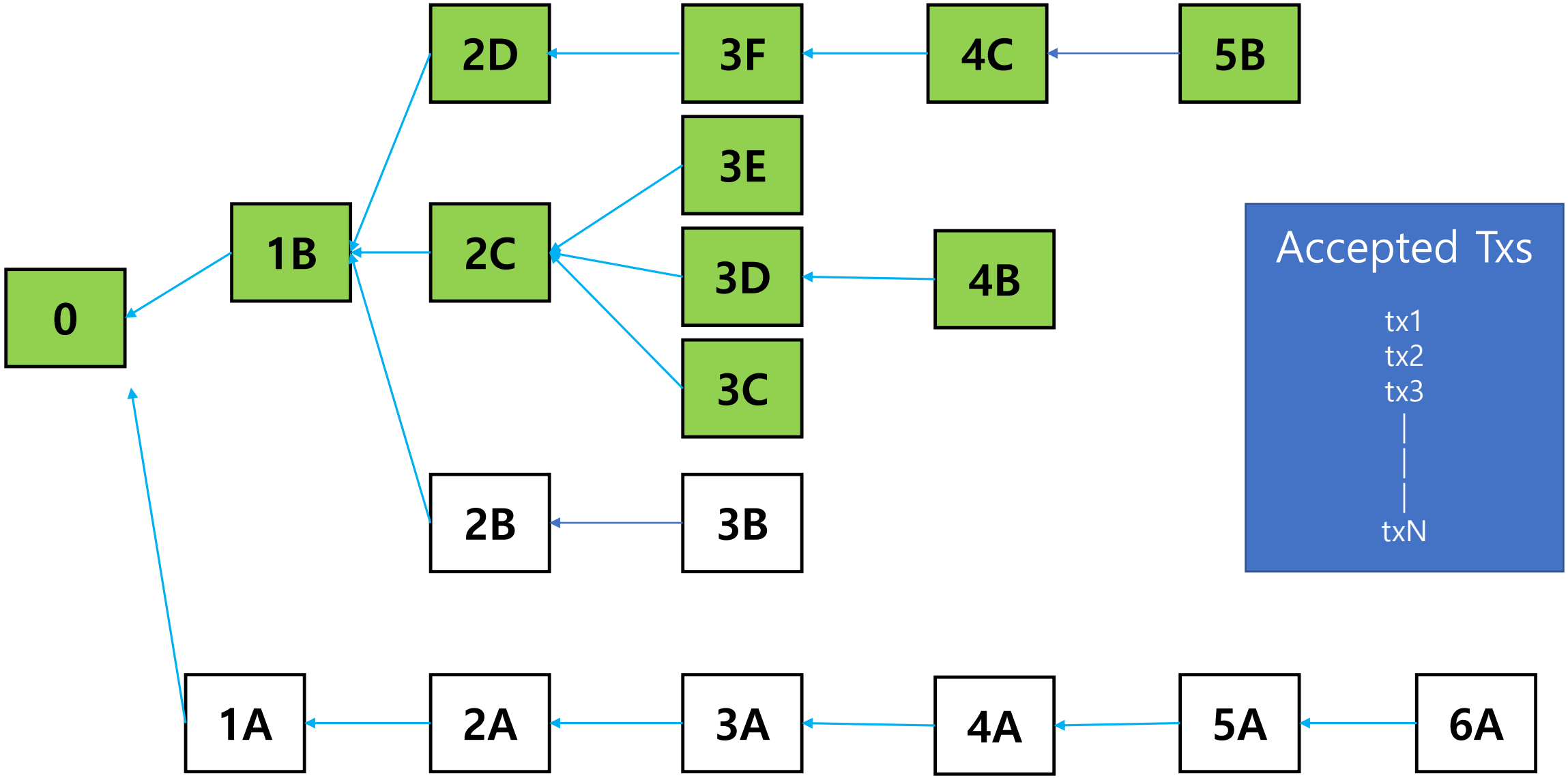

2D
3F
4C
5B
3E
1B
2C
3D
4B
0
3C
Accepted Txs
tx1
tx2
tx3
txM
2B
3B
1A
2A
3A
4A
5A
6A

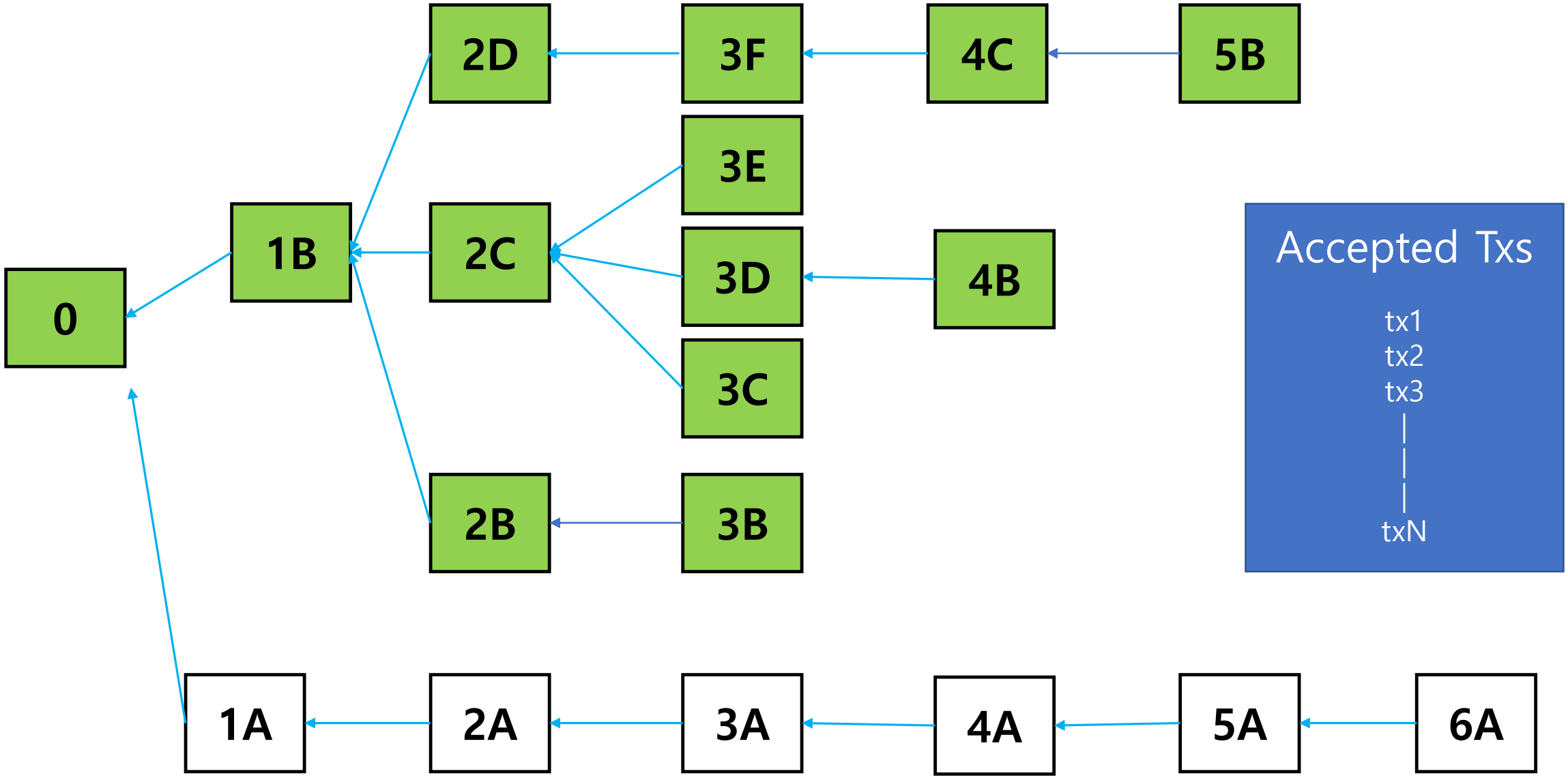

0
1B
2D
3F
4C
5B
3E
2C
3D
4B
3C
2B
3B
1A
2A
3A
4A
5A
6A
Accepted Txs
tx1
tx2
tx3
txN

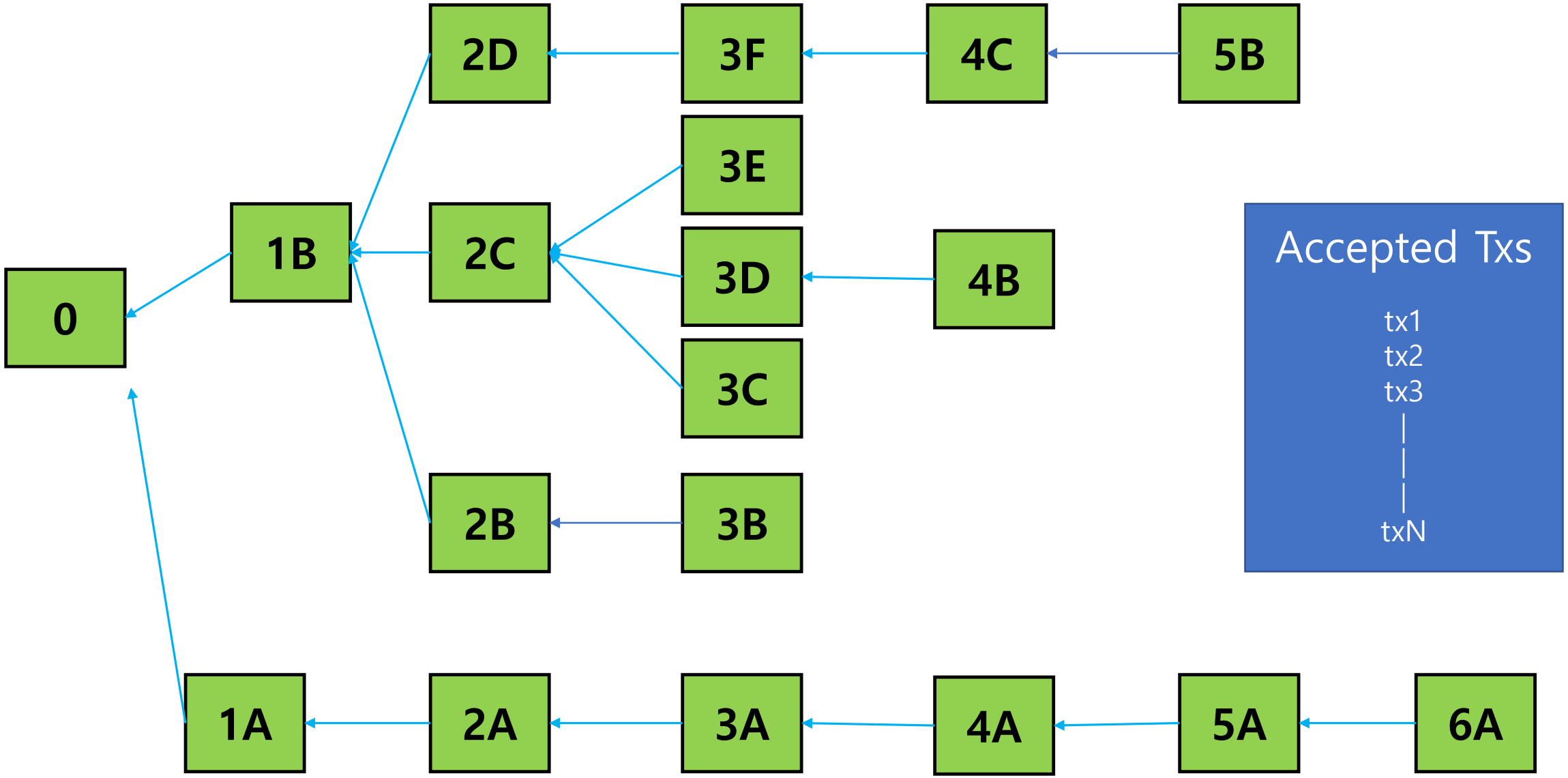

2D
3F
4C
5B
3E
1B
2C
3D
4B
0
3C
2B
3B
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A

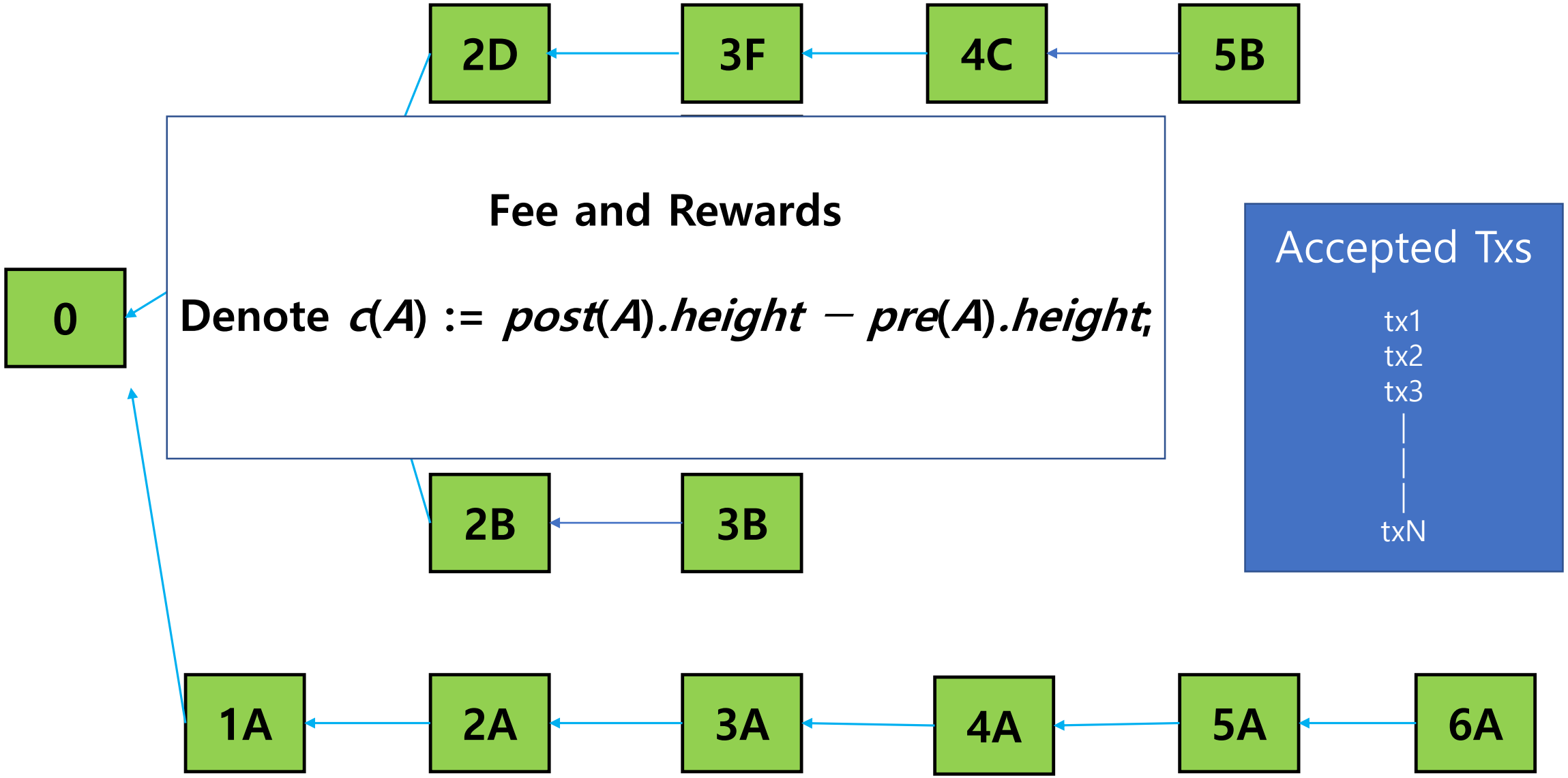

2D
3F
4C
5B
3E
1B
2C
3D
4B
0
3C
2B
3B
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A


2D
3F
4C
5B
3E
1B
2C
3D
4B
0
3C
2B
3B
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A


2D
3F
4C
5B
3E
1B
2C
3D
4B
0
3C
2B
3B
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A


2D
3F
4C
5B
3E
1B
2C
3D
4B
0
3C
2B
3B
Accepted Txs
tx1
tx2
tx3
txN
1A
2A
3A
4A
5A
6A


0
1B
2D
3F
4C
5B
2C
3E
3D
4B
3C
2B
3B
1A
2A
3A
4A
5A
6A
Accepted Txs
tx1
tx2
tx3
txN


2D
3F
4C
5B
Fee and Rewards
Denote c(A) := post(A).height − pre(A).height;
0
Accepted Txs
tx1
tx2
tx3
txN
2B
3B
1A
2A
3A
4A
5A
6A

Longest-chain과 비교 공격의 가능성

Table 1. The minimal double-spend (normalized by blocks' expected rewards, *val*) needed in order for an attack to be profitable in expectation, as a function of the number of confirmations and the attacker's computational power.

q	1	2	3	4	5	6	7	8	9	10
2%	0	0	$9.3 \cdot 10^2$	$1.2 \cdot 10^5$	$1.1 \cdot 10^7$	$8.3 \cdot 10^8$	$5.8 \cdot 10^{10}$	$3.8 \cdot 10^{12}$	$2.4 \cdot 10^{14}$	$1.3 \cdot 10^{16}$
6%	0	0	79	$3.1 \cdot 10^3$	$8.7 \cdot 10^4$	$2.1 \cdot 10^6$	$4.5 \cdot 10^7$	$9.1 \cdot 10^8$	$1.8 \cdot 10^{10}$	$2.9 \cdot 10^{11}$
10%	0	0	22	$4.8 \cdot 10^2$	$7.5 \cdot 10^3$	$9.9 \cdot 10^4$	$1.2 \cdot 10^6$	$1.4 \cdot 10^7$	$1.5 \cdot 10^8$	$1.4 \cdot 10^9$
14%	0	0	8.5	$1.3 \cdot 10^2$	$1.3 \cdot 10^3$	$1.2 \cdot 10^4$	$9.4 \cdot 10^4$	$7.1 \cdot 10^5$	$5.1 \cdot 10^6$	$3.2 \cdot 10^7$
18%	0	0	4.0	44	$3.3 \cdot 10^2$	$2.1 \cdot 10^3$	$1.2 \cdot 10^4$	$6.8 \cdot 10^4$	$3.6 \cdot 10^5$	$1.6 \cdot 10^6$
22%	0	0	2.0	18	$1.0 \cdot 10^2$	$5.1 \cdot 10^2$	$2.3 \cdot 10^3$	$9.7 \cdot 10^3$	$3.9 \cdot 10^4$	$1.4 \cdot 10^5$
26%	0	0	1.1	7.9	37	$1.5 \cdot 10^2$	$5.3 \cdot 10^2$	$1.8 \cdot 10^3$	$5.7 \cdot 10^3$	$1.6 \cdot 10^4$
30%	0	0	0.63	3.8	15	49	$1.4 \cdot 10^2$	$4.0 \cdot 10^2$	$1.0 \cdot 10^3$	$2.4 \cdot 10^3$
34%	0	0	0.36	1.9	6.4	18	45	$1.0 \cdot 10^2$	$2.3 \cdot 10^2$	$4.6 \cdot 10^2$
38%	0	0	0.20	0.92	2.8	6.9	15	30	58	$1.0 \cdot 10^2$
42%	0	0	0.10	0.43	1.2	2.6	5.2	9.3	16	25
46%	0	0	04	0.16	0.40	0.82	1.5	2.5	3.9	5.6
50%	0	0	0	0	0	0	0	0	0	0

Longest-chain과 비교 공격의 가능성

- 서비스 지연 공격의 경우 만약 A라는 블록을 지연시키려면, A가 그래프에 포함되지 않는 블록을 생성해야함..
- 블록을 만들어야하므로 공격자의 비용이 크다.
- 따라서, 정직한 네트워크는 이러한 공격에 저항성이 있음.

Longest-chain과 비교 공격의 가능성

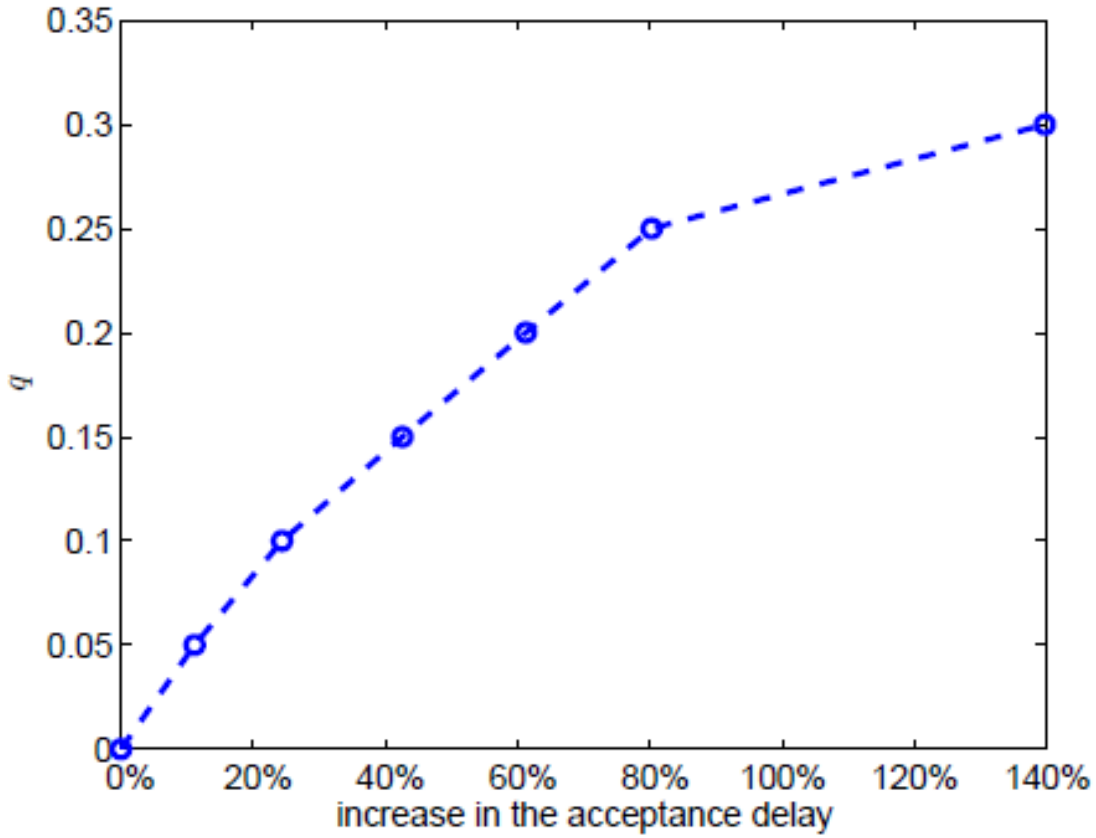


Fig. 1. The fraction of computational power an attacker needs to hold as a function of the increase in waiting time it aims to induce.

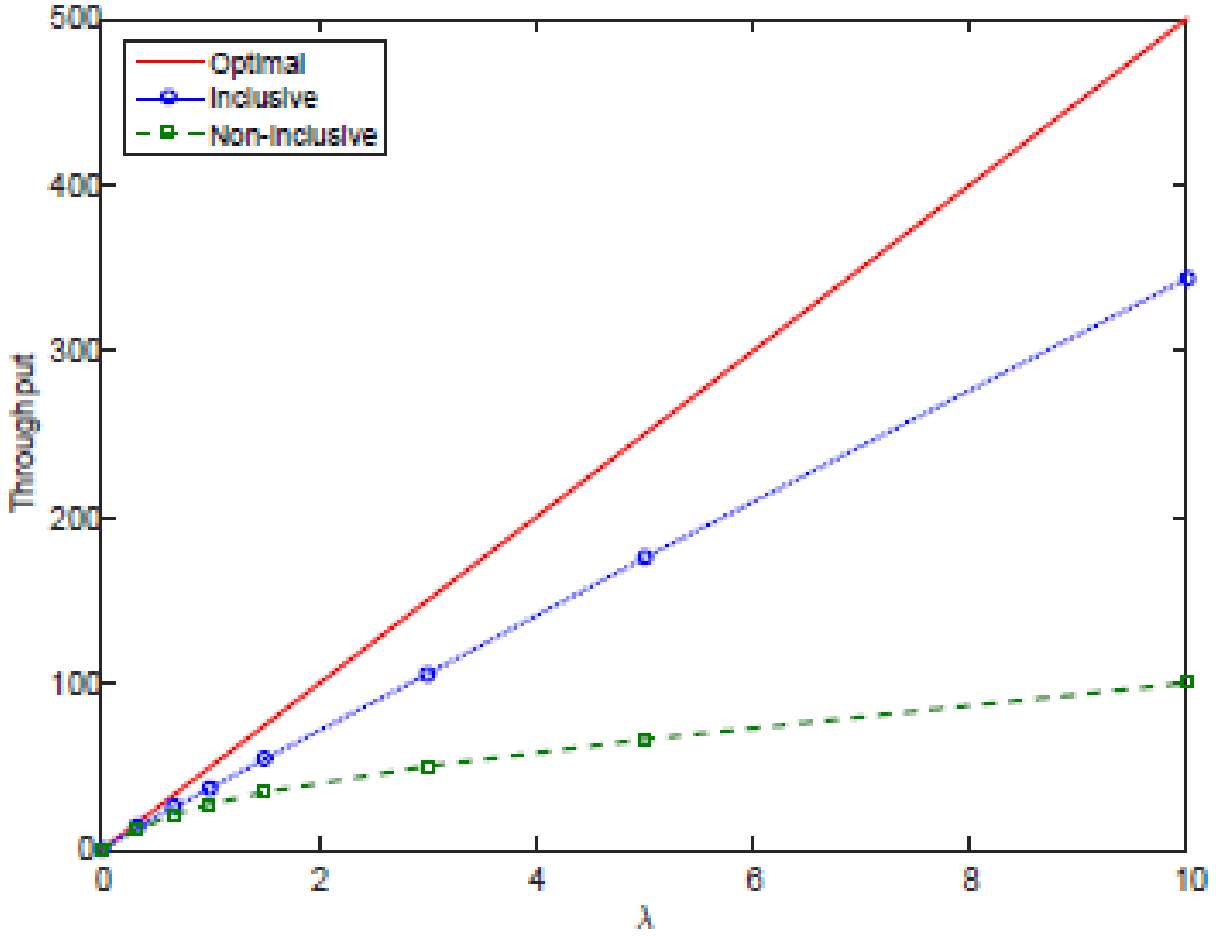


Fig. 2. The fraction of optimal throughput achieved in Inclusive and non-inclusive longest-chain protocols.