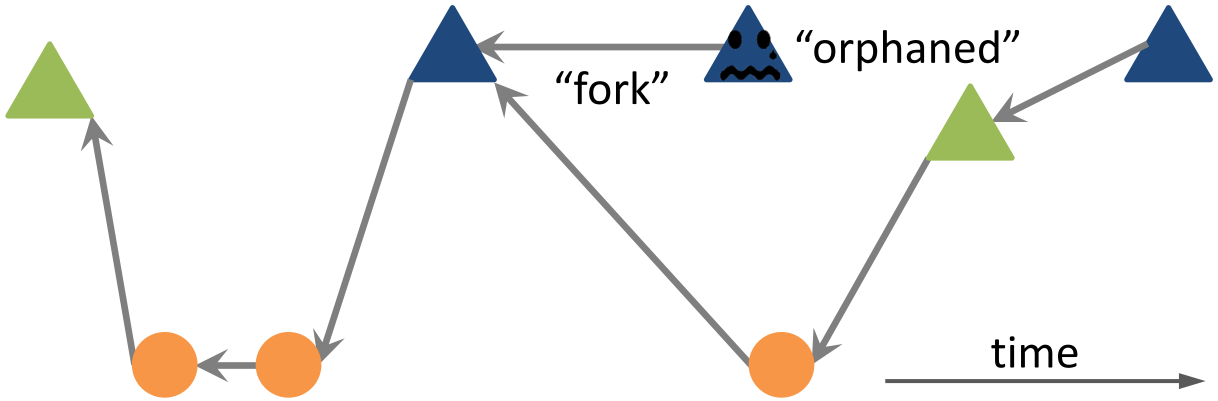
On the Necessity of a Prescribed Block Validity Consensus: Analyzing BU Mining Protocol

Ren Zhang & Bart Preneel
ren.zhang@esat.kuleuven.be
bart.preneel@esat.kuleuven.be

Bitcoin: Prescribed Block Validity Consensus



BVC — A block is either valid or invalid to all miners

Resolve Forks?
- Mine on the longest chain
- or the first received block during a tie

Rewards? — Blockchain blocks ✓; orphaned blocks ✗

(Once) Bitcoin Cannot Scale

	Transactions per second
VISA	2000
Alipay™	120000 (double eleven shopping festival, 2016)
bitcoin	< 4 (1 MB block/10 min)

People disagreed on how to fix it

bitcoinunlimited : no Prescribed Block Size

What?

- "A tool to raise the blocksize limit without splitting the network"

How?

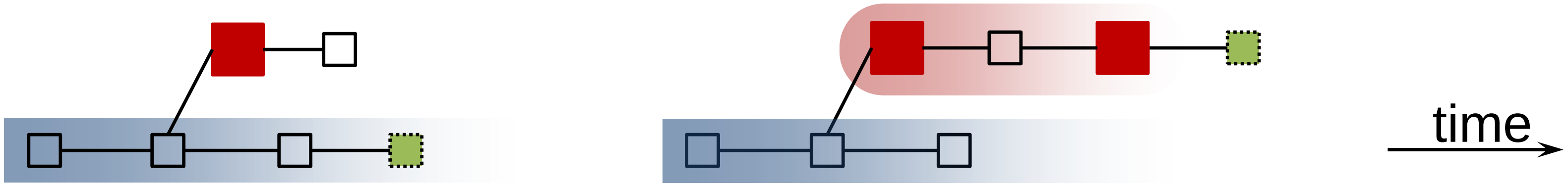
"the blocksize limit should never have been a consensus rule in the first place"

- Miners decide the block size limit collectively through a deliberative process

Who?

- Largest mining power support (40%) until late June, 2017

BU Mining Protocol



□ ≤ *EB* block

🟩 block that the miner tries to mine

🟥 > *EB* block

block size limit = *EB*

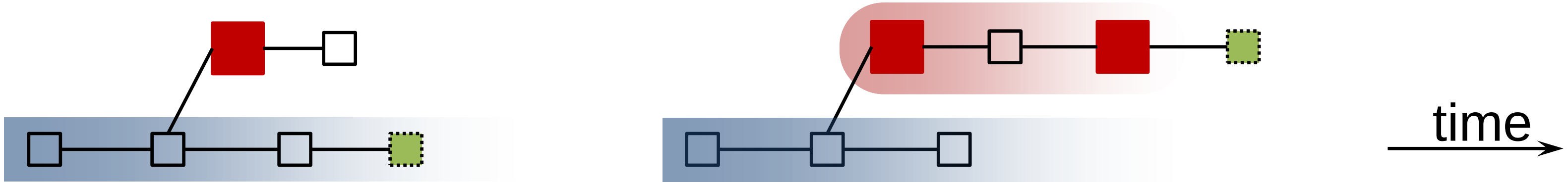
block size limit = 32MB

EB
- Maximum acceptable block size (of a miner, local)

AD (in figure: 3)
- Length of a chain starting with a "> *EB*" block before the miner accepts (local)

Sticky Gate
- Once *AD* is reached, opens *SG* and accepts large blocks until 144 consecutive "≤ EB" blocks appear

BU Mining Protocol: Rationale



Emergent Consensus

Economic factors can

- drive miners to the same EB
- which is the actual network capacity

Security?

- Attacks "cost the attacker far more than the victim"

Two Observations

BU supporters' different security claims

- Block validity consensus (BVC) is not necessary for security
- BVC will emerge on the run
- BVC will be formed/driven by attacks

Different incentive models

- Supporters: compliant & profit-driven
- Objectors: arbitrary

What We Did: Compare BU and Bitcoin

Incentive models \ Security claims	BU is secure when BVC is absent	BVC will emerge
Compliant & Profit-Driven		
Non-Compliant & Profit-Driven		Not meaningful
Non-Profit-Driven		

Is Consensus Necessary?
(Is BU secure when BVC is absent?)

Technical approach

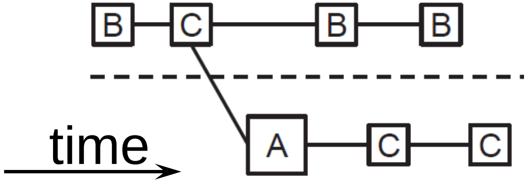
- For each incentive model, pick a most famous attack, define the attacker's goal/utility
- Evaluate effectiveness of these attacks in a most simple "BVC absent" setting: two different *EB*s, one small attacker
- Compute the optimal strategy and the utility of the attacker (math magic, see paper)
- Compare results with Bitcoin

Is Consensus Necessary?
(Is BU secure when BVC is absent?)

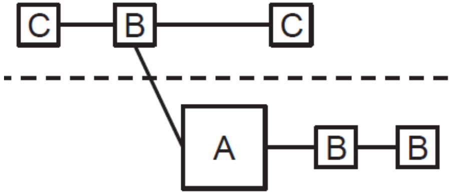
The setting:

- Three (groups of) miners Alice, Bob, Carol with mining power share $\alpha, \beta, \gamma; \alpha + \beta + \gamma = 1, \alpha \leq \min\{\beta, \gamma\}$
- Bob and Carol have the same *AD*=6, same block size = $EB_b<EB_c$
- Alice may mine blocks of size EB_b, EB_c or $>EB_c$, to strategically split Bob and Carol to different chains

Example:



(mine EB_c block)



(when Bob opens SG, mine $>EB_c$ block)

Is Consensus Necessary?

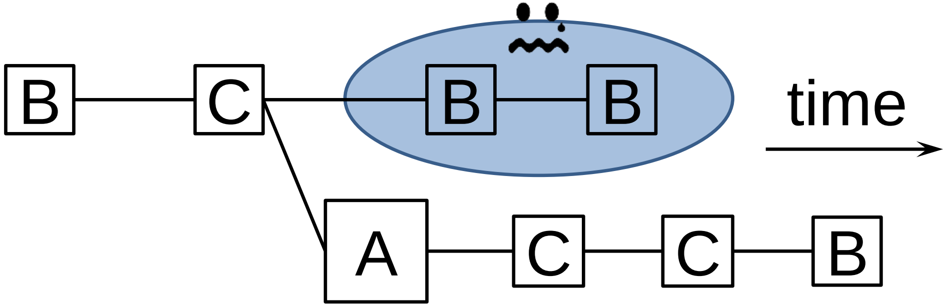
Compliant & Profit-Driven Alice

Goal

To maximize block reward share without deviating from the protocol (no selfish mining, no double-spending)

Typical execution

(AD=3)



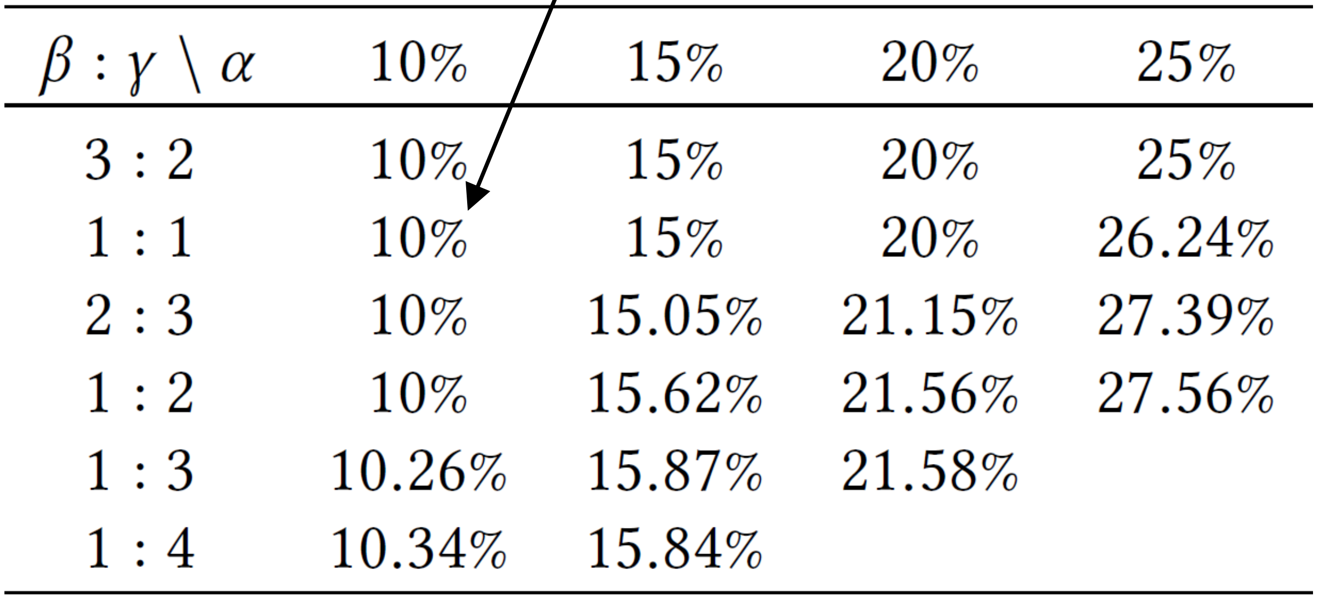
Alice orphans two Bob’s blocks by mining an EB_c block; relative block reward: 1/8 → 1/6

BU is Not Incentive Compatible

Compliant & Profit-Driven Alice

Results (optimal Strategy)

Alice 10%, Bob 45%, Carol 45%



$\beta : \gamma \setminus \alpha$	10%	15%	20%	25%
3 : 2	10%	15%	20%	25%
1 : 1	10%	15%	20%	26.24%
2 : 3	10%	15.05%	21.15%	27.39%
1 : 2	10%	15.62%	21.56%	27.56%
1 : 3	10.26%	15.87%	21.58%	
1 : 4	10.34%	15.84%		

Alice’s expected relative block reward

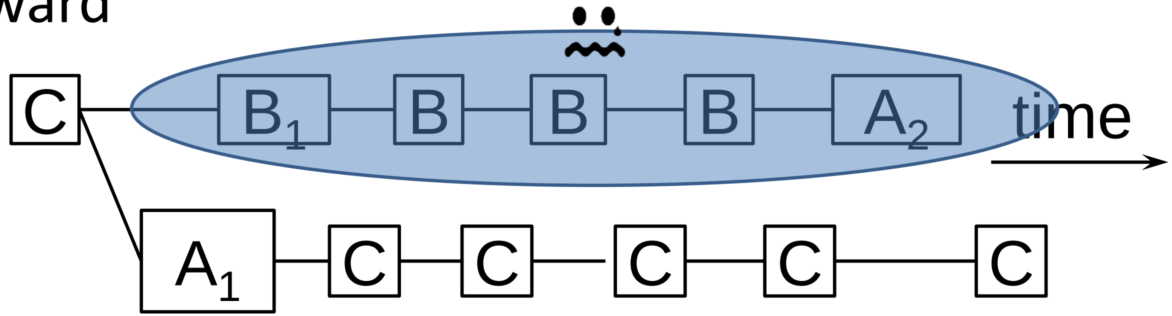
Is Consensus Necessary?

Non-Compliant & Profit-Driven Alice

Goal

to maximize block reward + double-spending reward

Typical execution



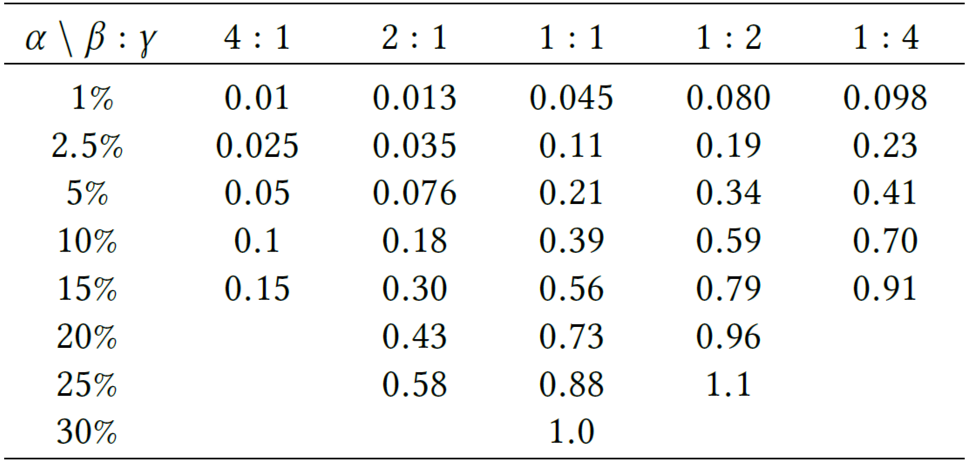
Alice bought something on B_1, the transaction is accepted at A_2; note that Alice mines a block A_2 on Bob's chain to help it reach 5* confirmations

*: due to a bug in my program, will be fixed later

Double-Spending is Easier and More Profitable

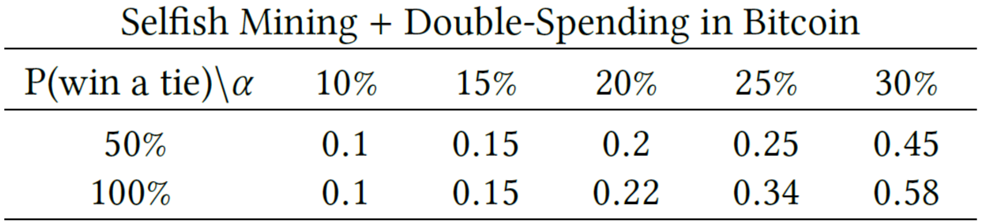
Non-Compliant & Profit-Driven Alice

Results (optimal Strategy, DS reward = block reward × 10)



$\alpha \setminus \beta : \gamma$	4 : 1	2 : 1	1 : 1	1 : 2	1 : 4
1%	0.01	0.013	0.045	0.080	0.098
2.5%	0.025	0.035	0.11	0.19	0.23
5%	0.05	0.076	0.21	0.34	0.41
10%	0.1	0.18	0.39	0.59	0.70
15%	0.15	0.30	0.56	0.79	0.91
20%		0.43	0.73	0.96	
25%		0.58	0.88	1.1	
30%			1.0		

Alice's expected mining+DS reward/10min (in block reward)



Selfish Mining + Double-Spending in Bitcoin

P(win a tie)$\setminus \alpha$	10%	15%	20%	25%	30%
50%	0.1	0.15	0.2	0.25	0.45
100%	0.1	0.15	0.22	0.34	0.58

(data might change after bug fix)

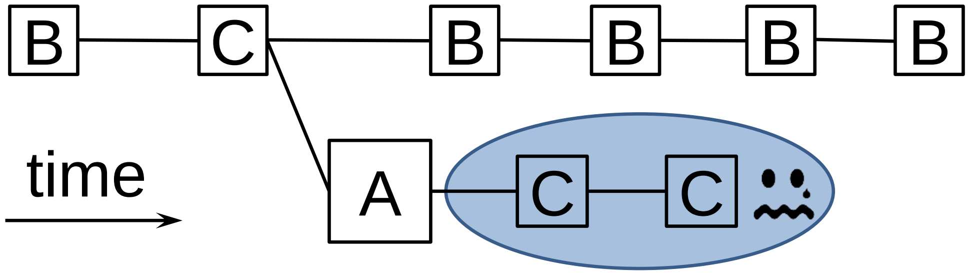
Is Consensus Necessary?

Non-Profit-Driven Alice

Goal

to orphan as many Bob and Carol’s blocks as possible with the least number of Alice’s blocks

Typical execution

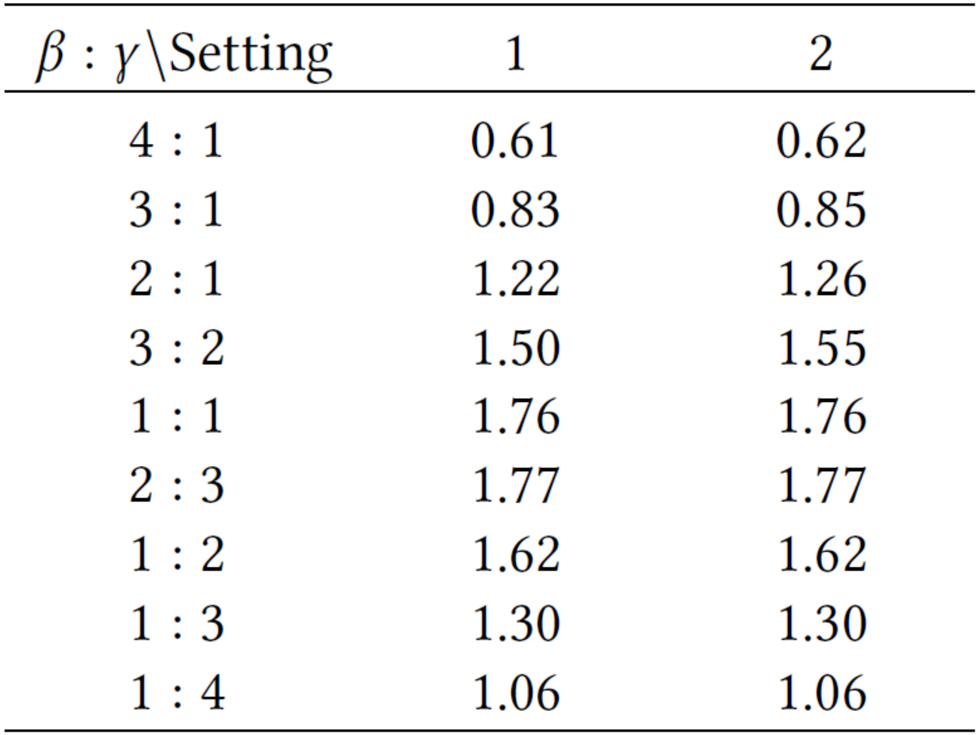


Alice orphans two Carol’s blocks with only one block

“Cost the Attacker Far More Than the Victim”

Non-Profit-Driven Alice

Results (optimal strategy, $\alpha = 1\%$)



$\beta : \gamma$\Setting	1	2
4 : 1	0.61	0.62
3 : 1	0.83	0.85
2 : 1	1.22	1.26
3 : 2	1.50	1.55
1 : 1	1.76	1.76
2 : 3	1.77	1.77
1 : 2	1.62	1.62
1 : 3	1.30	1.30
1 : 4	1.06	1.06

Expected # of Bob and Carol’s blocks orphaned by each Alice’s block

What We Did: Compare BU and Bitcoin

Incentive models \ Security claims	BU is secure when BVC is absent	BVC will emerge
Compliant & Profit-Driven	😭	
Non-Compliant & Profit-Driven	😭	Not meaningful
Non-Profit-Driven	😭	

Will BVC Emerge on the Run?

The EB choosing game: an imaginary world

Definition

- Miners choose from two EB values
- The EB value chosen by more than half of the mining power is the winner
- All rewards are shared among miners who chose the winner

Equilibrium

All miners choose the same EB

Implication

when all miners can choose any EB, there is a NE in which a consensus is reached

Will BVC Emerge on the Run?

The block size increasing game: moving closer to reality

Definition

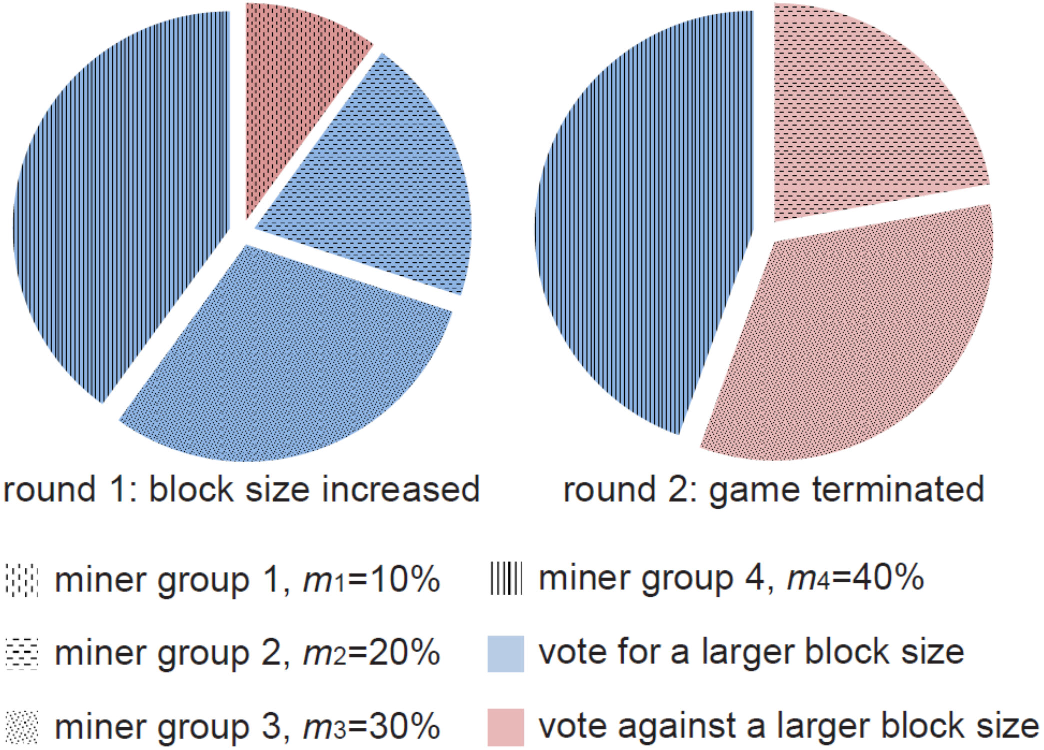
- Every miner has a maximum profitable block size (MPB); if most blocks >MPB, the miner is forced to leave the game
- Miners with large MPBs might form a coalition to raise the block size and kick others out; succeed if the coalition controls >50% mining power
- Rewards are shared among those who survive till the end

BU May Damage Decentralization

The block size increasing game: moving closer to reality

Termination State

($MPB_1 < MPB_2$
$< MPB_3 < MPB_4$)



round 1: block size increased

round 2: game terminated

In most initial settings, the block size will be raised

Results Summary

BU secure when BVC is absent?

No, new attack vectors in BU weakens Bitcoin’s security within all three incentive models

Will BVC emerge?

- BVC will not emerge in most occasions
- Even when a BVC is reached and all miners are compliant, the BVC is very fragile
- Strong miners have both the incentive and the ability to break BVC, raise the block size for higher reward share

bitcoinunlimited

release the potential **attacks**

We Are All Jon Snow

Is Prescribed BVC indispensable?

Maybe not, two approaches to let it go:

- Tolerate different topology views: SPECTRE
- Prove that the system is secure against 50% attacker

On consensus protocol

- Definition of decentralization, consensus
- Evaluation of consensus protocol security
- Design principles/elements, e.g., timestamp