Securely Improving Performance in PoW Blockchains using Anchors

Hyperledger India Chapter
Women in Blockchain 2023

Ovia Seshadri

LinkedIn: @oviaseshadri
Twitter: @ovia_seshadri

Talk Outline

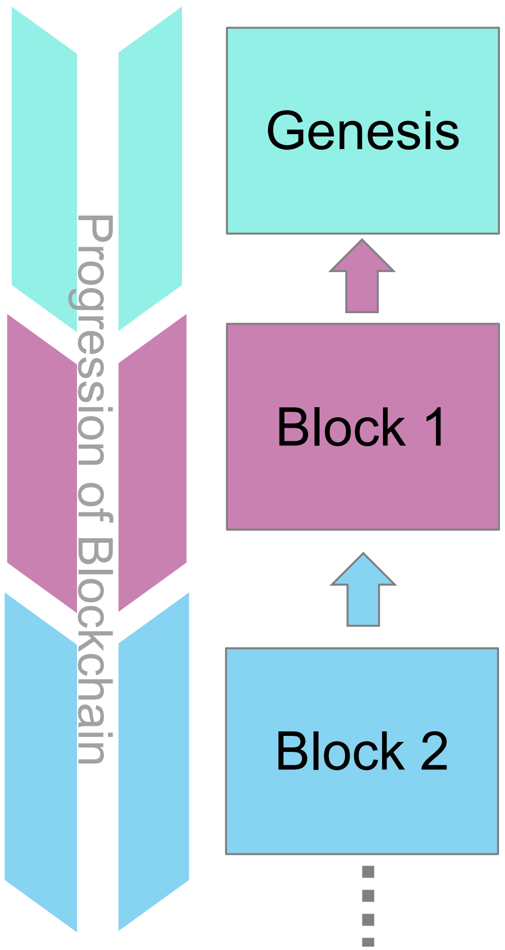
- Blockchain Background
- Problems in PoW Blockchains
- Goals
- Anchors
  - Features and Mechanism
  - Theoretical and Experimental Results

What is a Blockchain system?

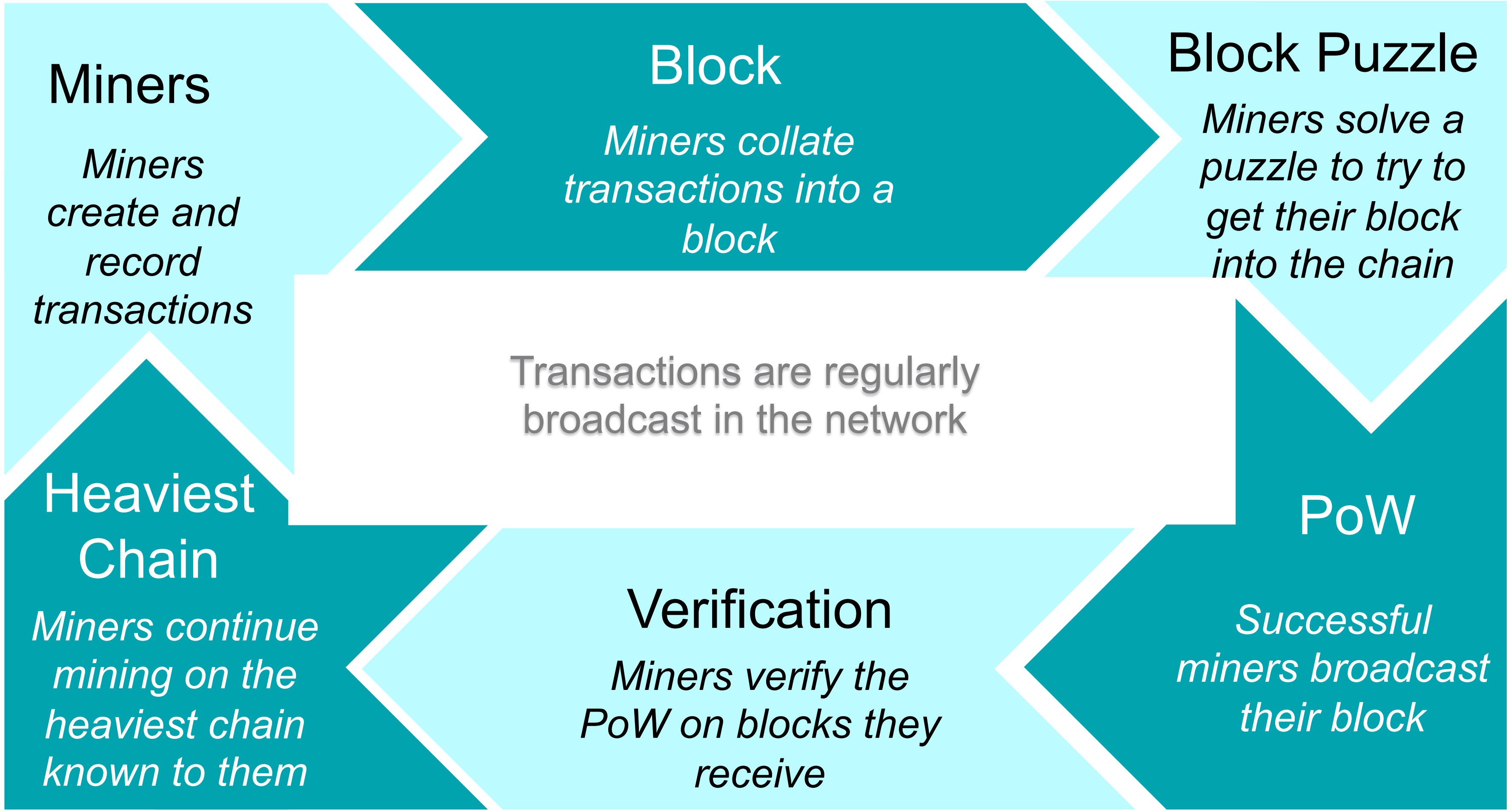
Features of Blockchain

- System where data can be stored and retrieved
- Single dataset, multiple copies, authoritative universal log
- Facts can be independently verified by anyone
- Data is guaranteed to be unaltered
- Decentralized and distributed
- Public-private key

Progression of Blocks



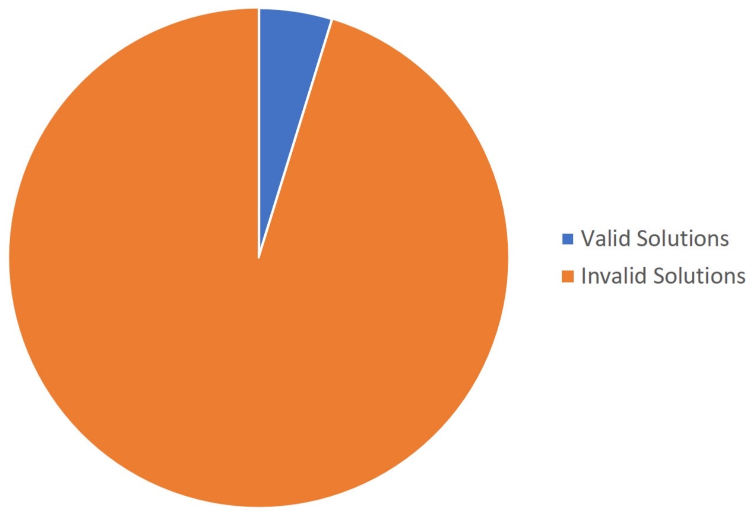
The PoW Blockchain workflow



What is Proof of Work?

- Election lottery based "Nakamoto" consensus
- Puzzles that need more work to solve than to verify.
- Non-precomputable
- Agreement on the amount of Computing power in the network
- Varying difficulty levels
- 40 zeros ~ 240 = 1 trillion trials for one solution

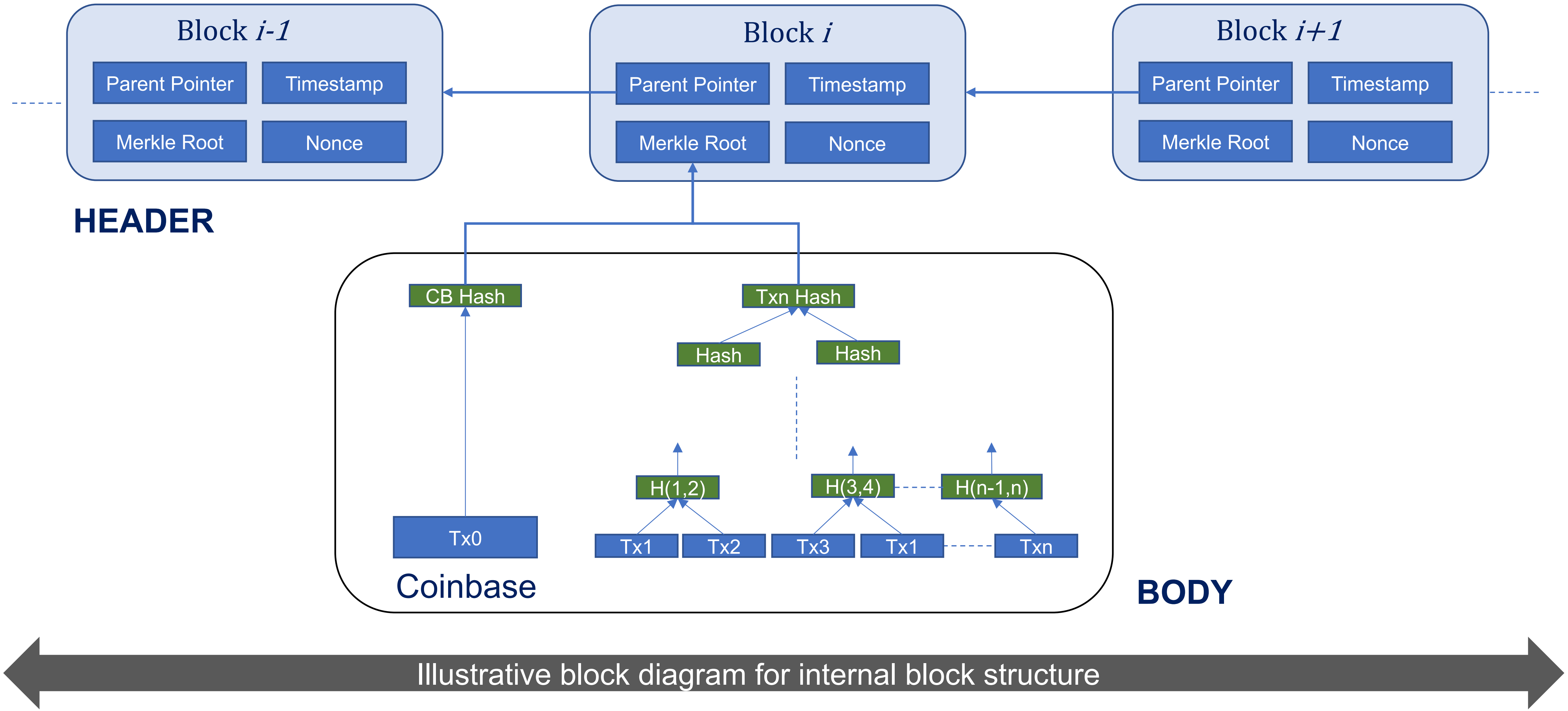
2^{256} Total Possible Block Solutions



SHA_256(Block Header) $\leq$ Target

PoW makes block generation a random process

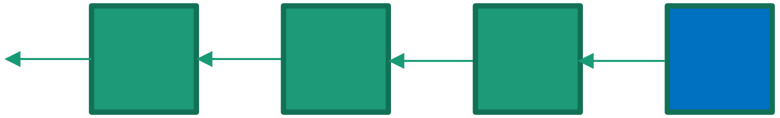
PoW Block Structure



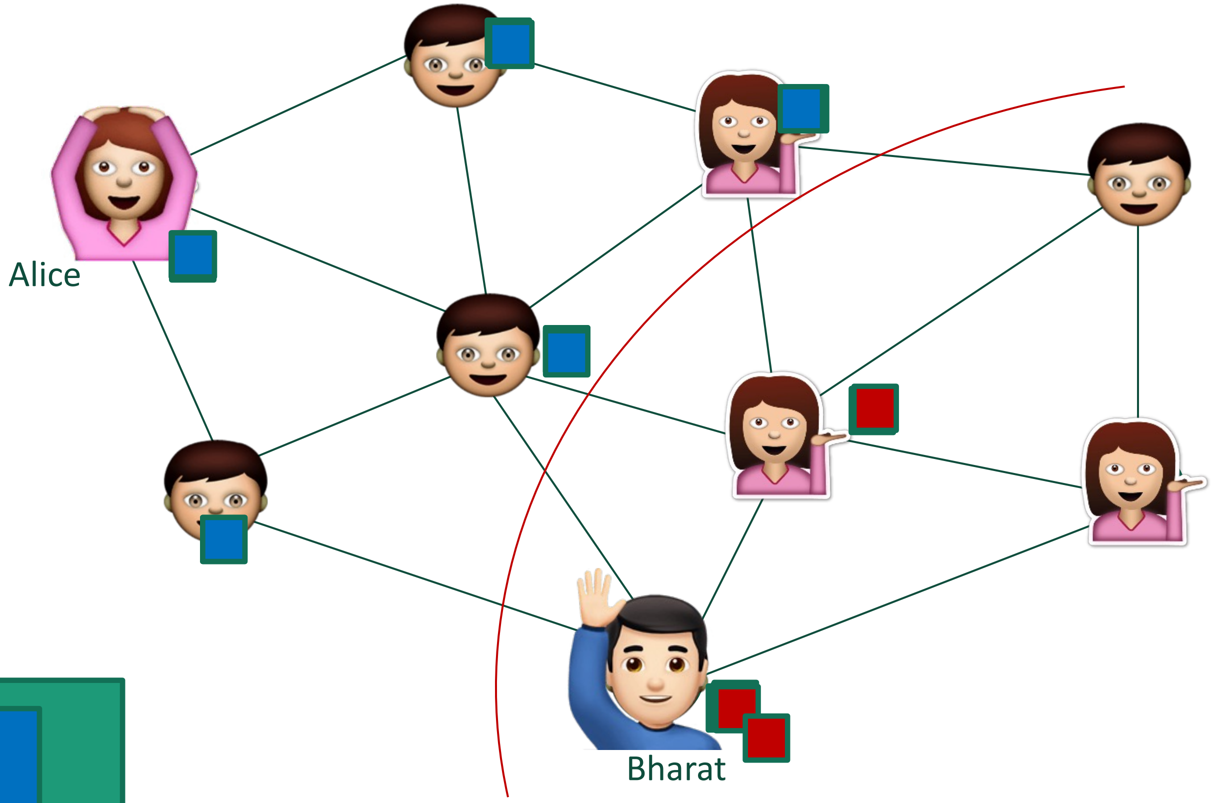
Talk Outline

- Blockchain Background
- Problems in PoW Blockchains
- Goals
- Anchors
  - Features and Mechanism
  - Theoretical and Experimental Results

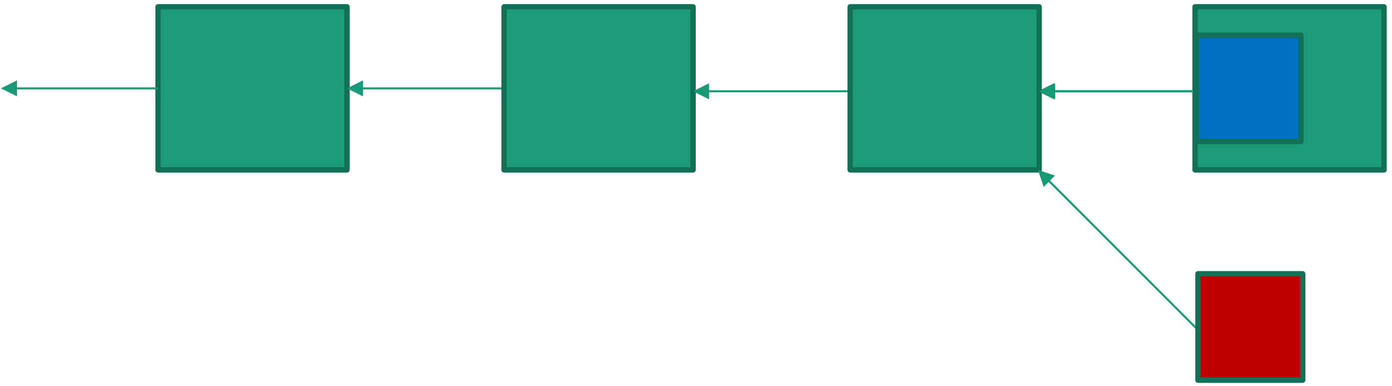
Forks and their effect on Chain Stability

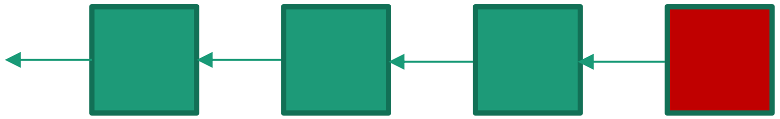


Alice’s view of the blockchain



Absolute view of the blockchain

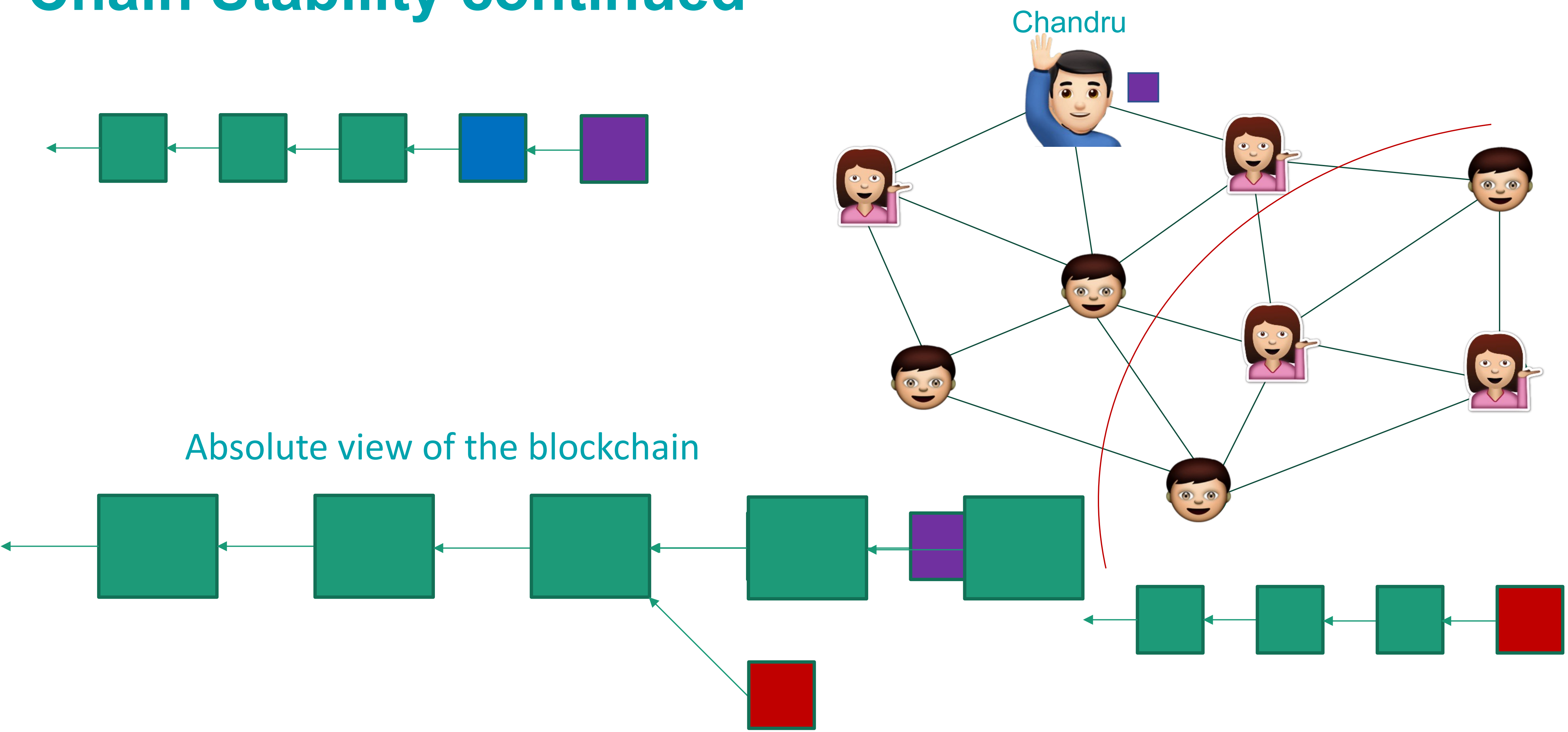




Bharat’s view of the blockchain

J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies,” in Security and Privacy (SP), 2015 IEEE symposium on. IEEE, 2015, pp. 104–121.

Chain Stability continued



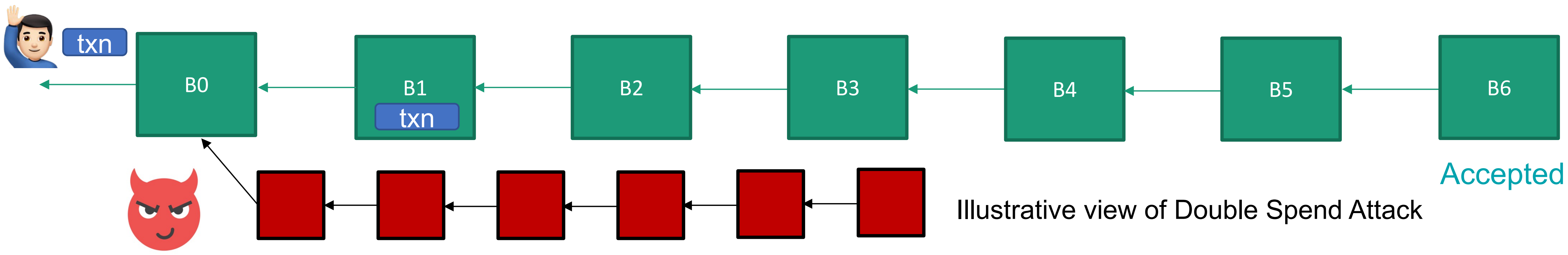
J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in Security and Privacy (SP), 2015 IEEE symposium on. IEEE, 2015, pp. 104–121.

Confirmation Time and Double Spends

Significance of Confirmation time

Confirmation time is the time for a transaction to be accepted by seller for him to safely release his goods or services.

Lower Confirmation times translates to fast payments and a practical system.



Illustrative view of Double Spend Attack

1. An adversary can secretly mine a chain after initiating txn before it enters a block
2. After txn enters a block he waits for it to be accepted while extending his private chain
3. Once txn is accepted, if his private chain is heavier, he releases it and orphans the chain containing txn
4. He is now free to double spend the coins used in txn

Satoshi suggested 6th block confirmation to guarantee committed transactions with probability of 0.99 in the presence of 10% adversary.

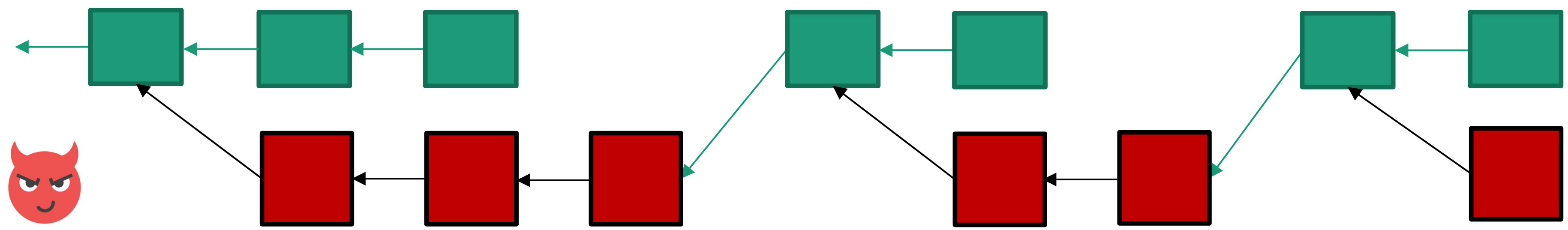
S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008 S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008

Selfish Mining

The adversary's goal is to gain more than their fair share of revenue and may deviate from honest protocol to do so.

The selfish miners achieve their goal by secretly forking the blockchain and selectively revealing their mined blocks or links to invalidate honest miners' work and claiming unfair rewards.

Illustrative view of Selfish Mining Attack



1. An adversary mines a secret chain from any block and tries to maintain a lead
2. He waits for the honest chain to catch up and releases his private chain when they are almost caught up
3. Since adversary has more weight on his chain, he claims unfair rewards of the orphaned chain
4. If the adversary is unable to hold a lead, he tries to catch up to the honest chain and releases his chain.
5. If the honest miners pick and extend the adversary chain in the fork, he wins.

I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. In FC. Springer, 2014.

Issues with PoW blocks

Problem	Effect
Blocks are generated in random wide intervals	Unsteady chain weight growth
	High Confirmation Time
Blocks are large in size, hence have large network delay	High fork resolution Time
	Security and Performance problems

A. Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, and S. Capkun. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 3–16. ACM, 2016.

Effort so far

Performance matters

Security matters

Trade-off between performance and security in blockchains

Small block interval

- More Forks
- Waste of Computational energy and Mining rewards

Large block interval

- High Confirmation Time
- Lower transaction throughput

Hierarchical Blockchain/ Multi Blockchains

- Not an incremental approach
- loss of simple Linear structure
- Additional Security vulnerabilities

A. Gervais, G. O. Karame, K. W˙ust, V. Glykantzis, H. Ritzdorf, and S. Capkun. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 3–16. ACM, 2016.

Is Proof of Work still relevant?

- Demonstrated their resilience, durability, robustness and longevity since their inception
- Truly resistant to 51% attacks
- Resistant to centralisation
- Widely adopted with high TVL
- Vibrant ecosystem and developer communities
- New Innovations – BRC20

Goals

Honest chain must grow at a steady, fast rate

1

Reduce confirmation time at the fixed transaction throughput

2

Reduce number of natural forks and the weight orphaned by them

3

In case of natural or adversary forks, resolve them faster to improve chain stability

Low propagation delays and lower weight orphaned at each fork

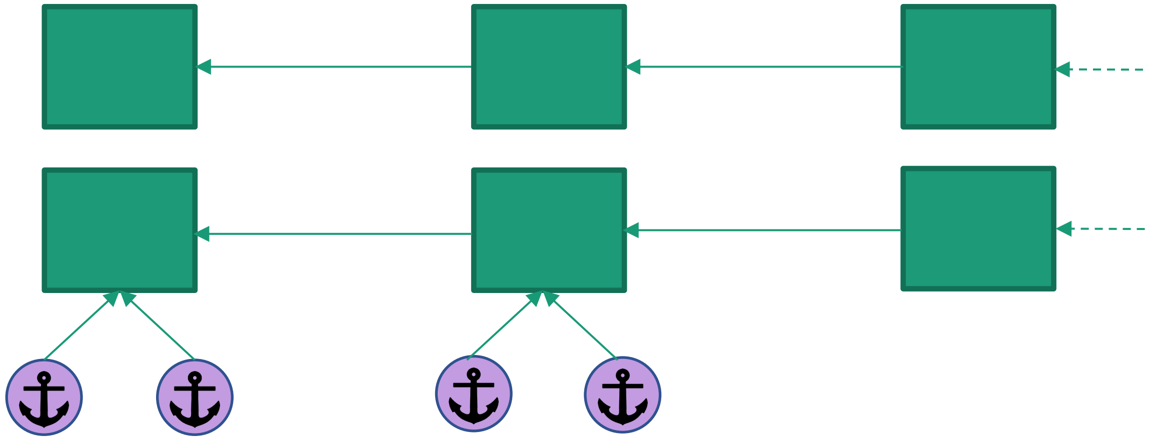
With minor modifications to architecture such that it benefits new and existing PoW blockchain platforms

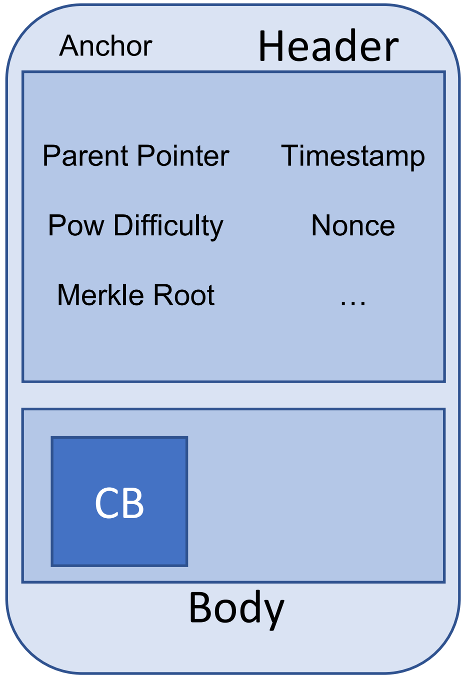
Talk Outline

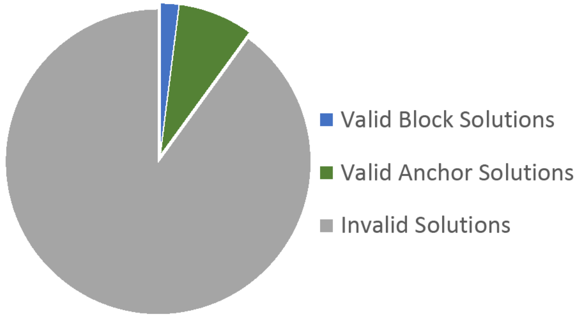
- Blockchain Background
- Problems in PoW Blockchains
- Goals
- Anchors
  - Features and Mechanism ⚓
  - Theoretical and Experimental Results

What are Anchors?

Anchors are block headers that are mined with less PoW than blocks. They contain no transactions in the body except the Coinbase and are mined on blocks.



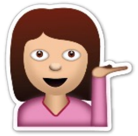




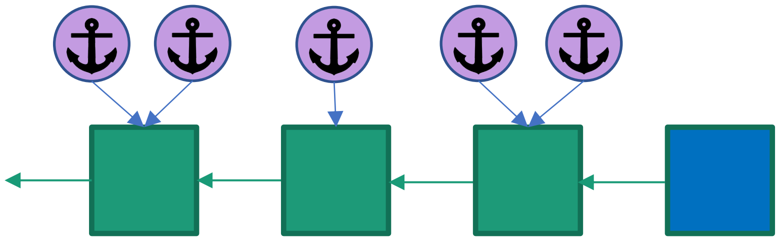
- Faster, smaller and more frequent to blocks
- Reusable Solution, Negligible Overheads
- Cannot create forks, can prevent forks by blocks

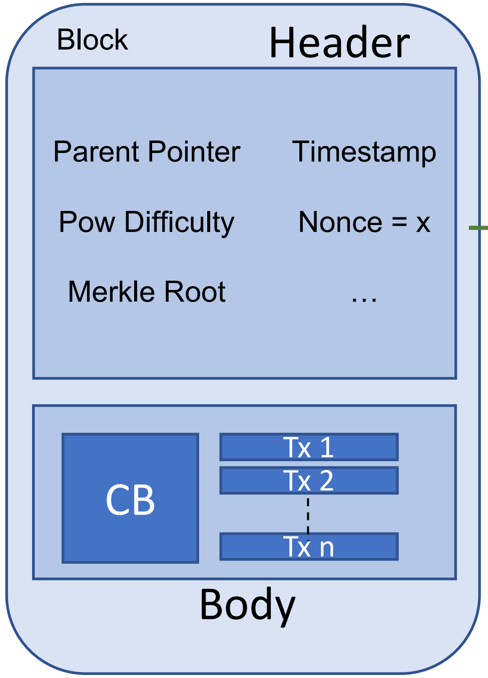
O. Seshadri, V. J. Ribeiro, and A. Kumar. Securely boosting chain growth and confirmation speed in pow blockchains. In 2021 IEEE International Conference on Blockchain (Blockchain), pages 140–149, 2021.

Generation of Anchors

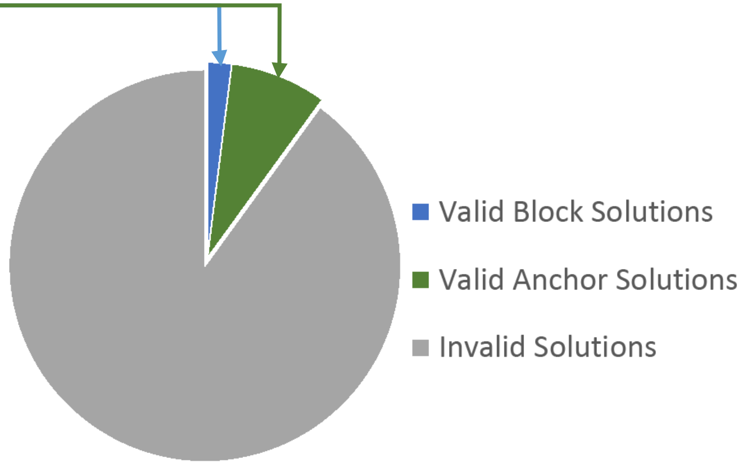


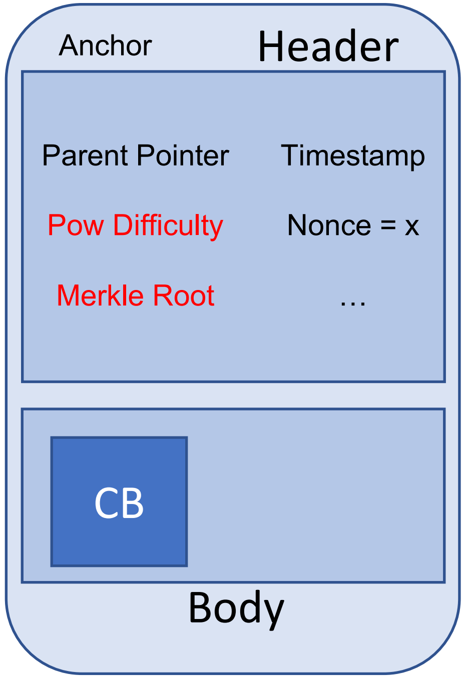
Alice creates a block B on the heaviest chain known to her

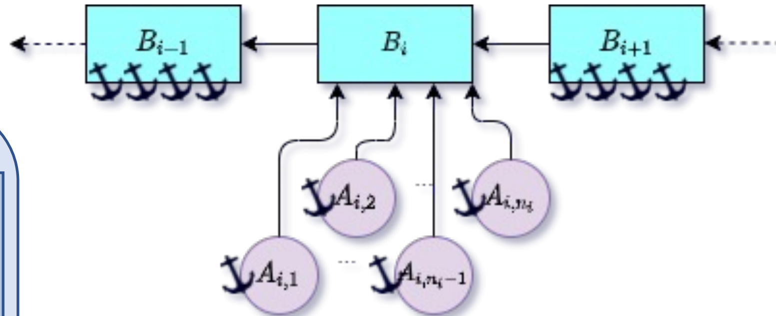




SHA_256(SHA_256(Block Header)) ≤ Block Target / Anchor Target







B_i = i^{th} block on the blockchain

n_i = Number of anchors created on the i^{th} block

$A_{i,j}$ = j^{th} anchor of the i^{th} block

Weight of a blockchain of N blocks

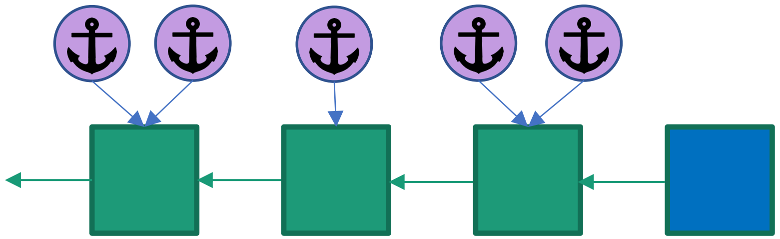
$$\sum_{i=1}^{N}\left[w(B_i) + \sum_{j=1}^{n_i} w(A_{i,j})\right]$$

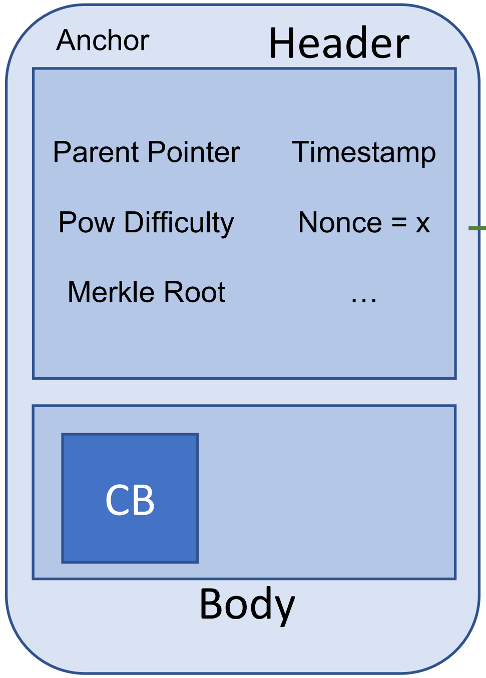
$w(.)$ denotes the weight of a block or anchor

$w(B_i) = 1; w(A_{i,j}) = \alpha$

Processing of Anchors

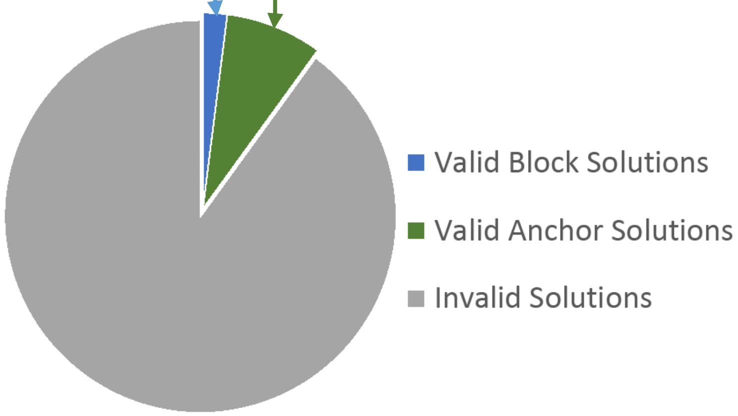
Bharat receives an entity E on his entity tree





SHA_256(SHA_256(Block Header)) ≤ Block Target

SHA_256(SHA_256(Block Header)) ≤ Anchor Target



If addition of new anchor creates a new heaviest chain, Bharat must shift mining on the parent of the new anchor

+ Txn Hash

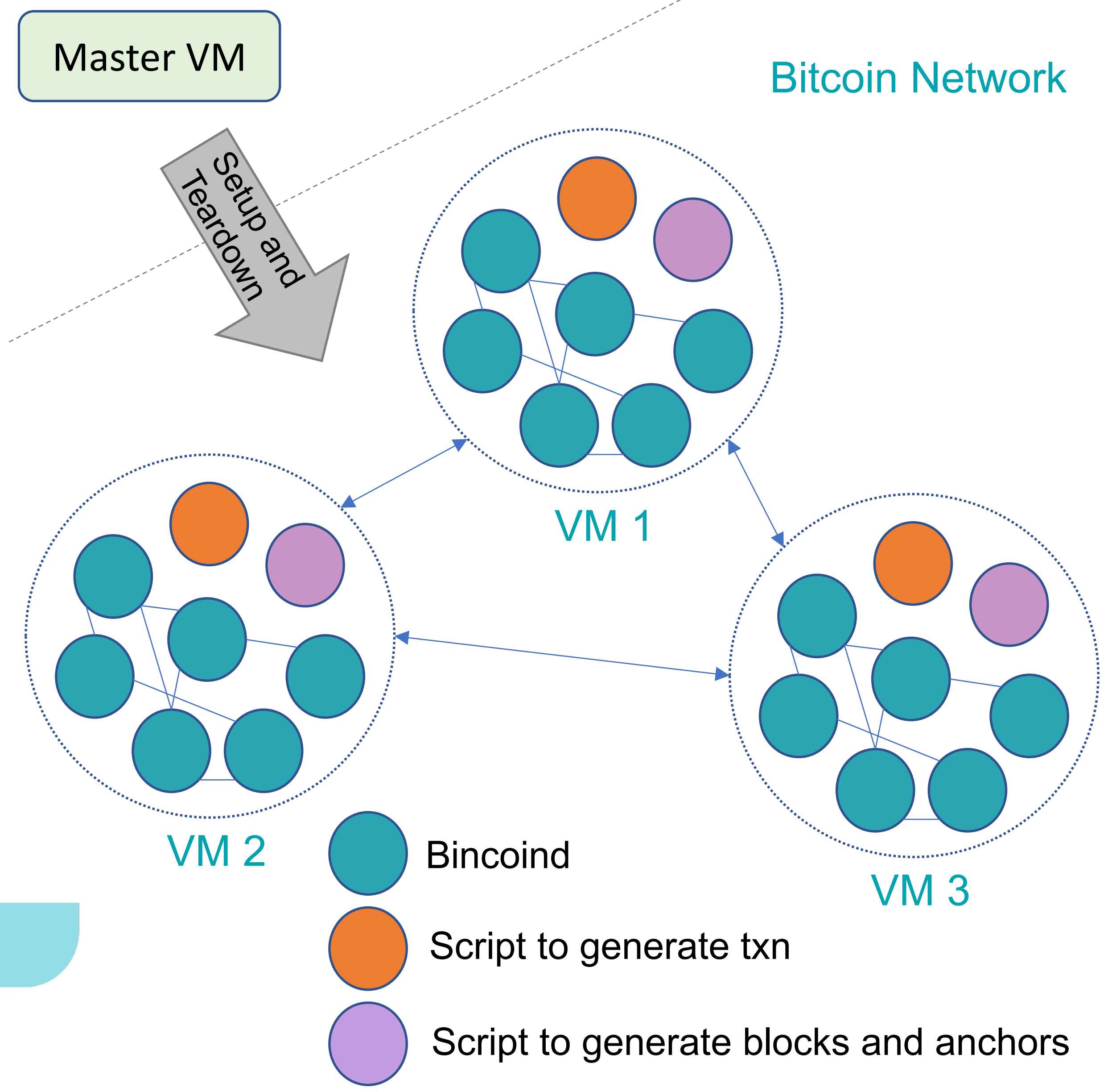
SHA_256(SHA_256(CB)+Txn Hash) = Merkle Root

Talk Outline

- Blockchain Background
- Problems in PoW Blockchains
- Goals
- Anchors
  - Features and Mechanism
  - Experimental and Theoretical Results ⚓

Emulation Setup

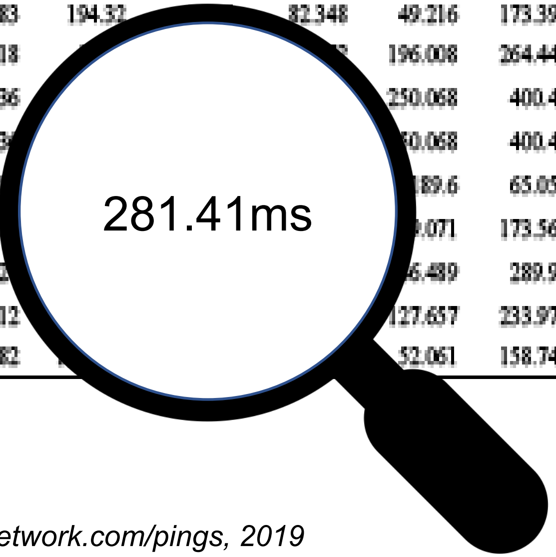
- 36 Virtual Machines on cloud
- 35 VMs * 6 bitcoind = **210 nodes**
- Real World Latencies



The Bitcoin Core Developers Satoshi Nakamoto. Source Code - Bitcoin Core v0.16. 2018. URL: https://github.com/bitcoin/bitcoin/.
Protocol documentation - Bitcoin Wiki. 2019. URL: https://en.bitcoin. it/wiki/Protocol_documentation.

Intercity delay of our test-bed

City	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Adelaide (1)	0	322.478	324.752	217.291	158.629	221.814	301.07	240.907	359.966	443.586	241.13	318.534	179.417	339.143	396.119	228.227	327.753	19.457	230.093	328.809
Amsterdam (2)	322.408	0	229.02	98.18	215.336	190.816	13.271	81.857	71.874	161.2	76.24	12.127	141.875	239.652	298.991	164.633	25.048	286.033	87.729	15.269
Bangkok (3)	318.713	216.251	0	251.168	67.833	202.647	247.368	252.748	243.547	111.188	286.555	204.941	193.722	153.847	230.445	65.303	306.793	217.937	273.725	200.744
Chicago (4)	216.845	97.568	274.366	0	213.579	98.319	87.777	23.371	149.923	221.461	23.475	96.012	51.536	198.451	287.763	223.594	112.26	201.674	16.294	116.801
Hong Kong (5)	158.519	215.473	68.942	219.217	0	129.538	242.317	196.769	279.746	250.772	223.08	281.747	156.216	120.274	210.75	33.895	220.697	158.827	244.335	270.929
Honolulu (6)	221.763	189.393	235.195	98.295	129.377	0	180.113	117.127	222.317	253.609	117.076	191.236	59.781	198.957	273.476	189.597	200.265	202.78	116.792	194.694
London (7)	301.743	13.097	259.359	86.029	242.261	180.063	0	80.87	51.311	138.12	75.404	5.186	161.183	292.729	247.463	172.112	25.601	281.339	90.545	25.198
Montreal (8)	240.935	81.883	274.188	24.029	196.744	117.096	80.795	0	127.48	236.042	9.459	81.731	72.789	273.287	238.298	234.766	106.4	258.365	8.287	96.553
Moscow (9)	359.862	71.974	259.511	142.76	279.799	222.334	51.424	127.191	0	182.3	131.194	48.871	195.967	347.679	262.81	189.566	19.086	346.504	127.585	51.951
New Delhi (10)	443.114	161.511	130.483	222.377	250.787	253.687	138.195	241.518	182.245	0	207.956	145.391	264.517	401.264	421.59	70.416	173.42	289.307	233.755	158.673
New York (11)	241.1	76.191	297.35	22.569	218.884	116.982	75.443	9.442	131.177	207.915	0	74.249	70.354	247.133	234.047	247.402	95.822	213.626	11.978	103.882
Paris (12)	313.009	17.616	203.92	91.485	244.683	194.32	[illegible]	82.348	49.216	173.393	84.873	0	144.178	264.478	259.406	245.792	30.398	279.41	87.528	13.669
San Francisco (13)	179.411	142.018	234.571	51.785	156.318	[illegible]	[illegible]	[illegible]	196.008	264.446	70.331	144.255	0	167.629	164.349	168.186	164.309	152.079	63.375	166.86
Shanghai (14)	368.599	257.577	241.753	335.279	132.536	[illegible]	[illegible]	[illegible]	250.068	400.41	242.636	294.528	167.619	0	30.528	168.186	264.322	332.21	259.428	166.86
Shenzhen (15)	368.599	330.459	241.753	335.279	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	400.41	242.636	294.528	167.619	0.044	0	168.186	264.322	309.734	259.428	166.86
Singapore (16)	228.315	164.687	51.543	220.171	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	65.057	247.449	242.467	168.158	265.77	390.675	0	188.129	93.93	241.711	170.708
Stockholm (17)	327.663	25.06	314.189	112.901	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	173.567	95.956	28.783	164.304	266.964	241.32	188.123	0	308.59	109.8	33.014
Sydney (18)	19.364	286.342	203.229	202.69	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	289.99	213.652	279.966	152.022	323.34	307.296	92.903	308.34	0	213.521	309.075
Toronto (19)	230.057	87.712	287.936	15.838	242.712	[illegible]	[illegible]	[illegible]	127.657	233.971	11.985	87.653	63.415	248.021	298.331	241.611	109.85	213.545	0	129.925
Zurich (20)	328.837	15.328	219.488	115.708	270.982	[illegible]	[illegible]	[illegible]	52.061	158.741	103.925	13.534	166.92	292.636	218.718	170.628	33.069	308.965	129.792	0



Global Ping Statistics - WonderNetwork. https://wondernetwork.com/pings, 2019

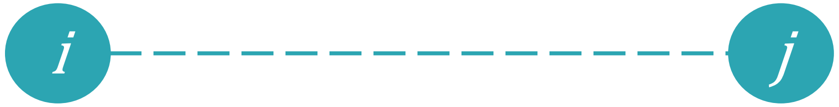
Delay Model

Anchors being fixed small structures, have low broadcast latency.

M Size of message

$C_{i,j}$ Bandwidth

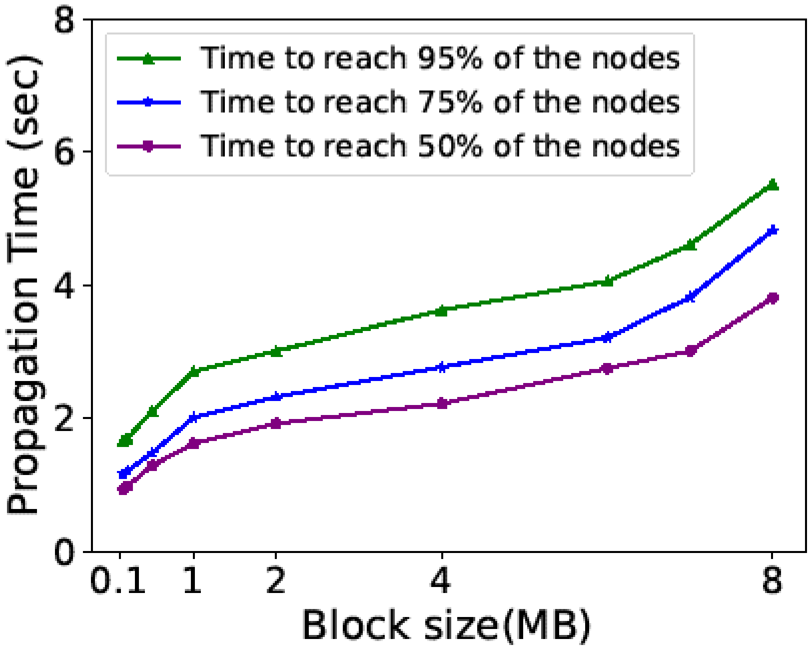
$D_{i,j}$ Speed of light delay



$$total\ time = D_{i,j} + \frac{M}{C_{i,j}} + kM$$

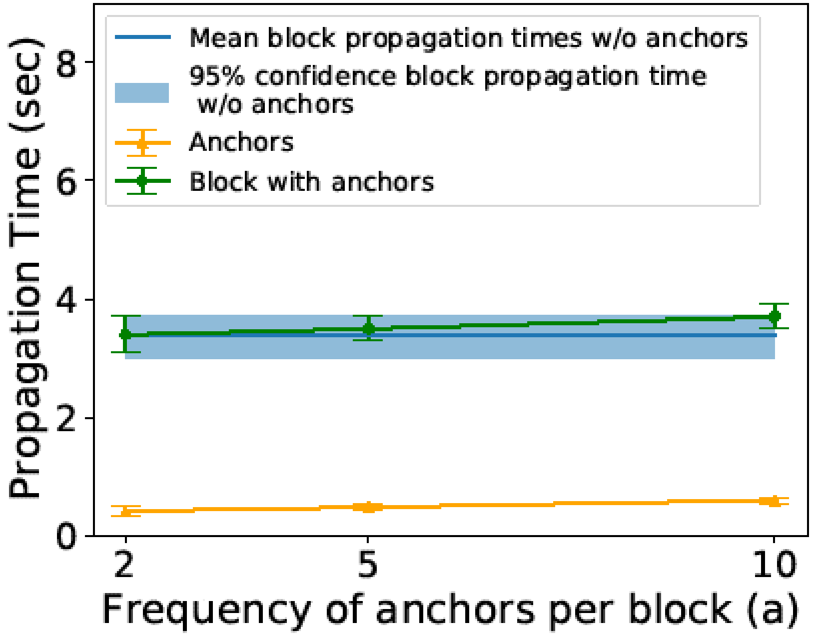
Time for first bit + time for rest of the message + verification at ‘j’

Experiment 1: Propagation Time

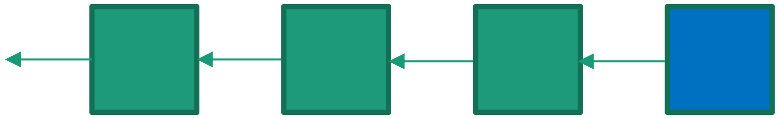


- Network delay for block increases linearly with increase in block size
- Anchors of 264 bytes propagate at an avg of ~0.5 secs across the network.
- Anchors are 3x faster that blocks of 100KB size.
- Anchors are 10x faster that blocks of 8MB size.
- Anchors propagate faster than all block sizes considered.

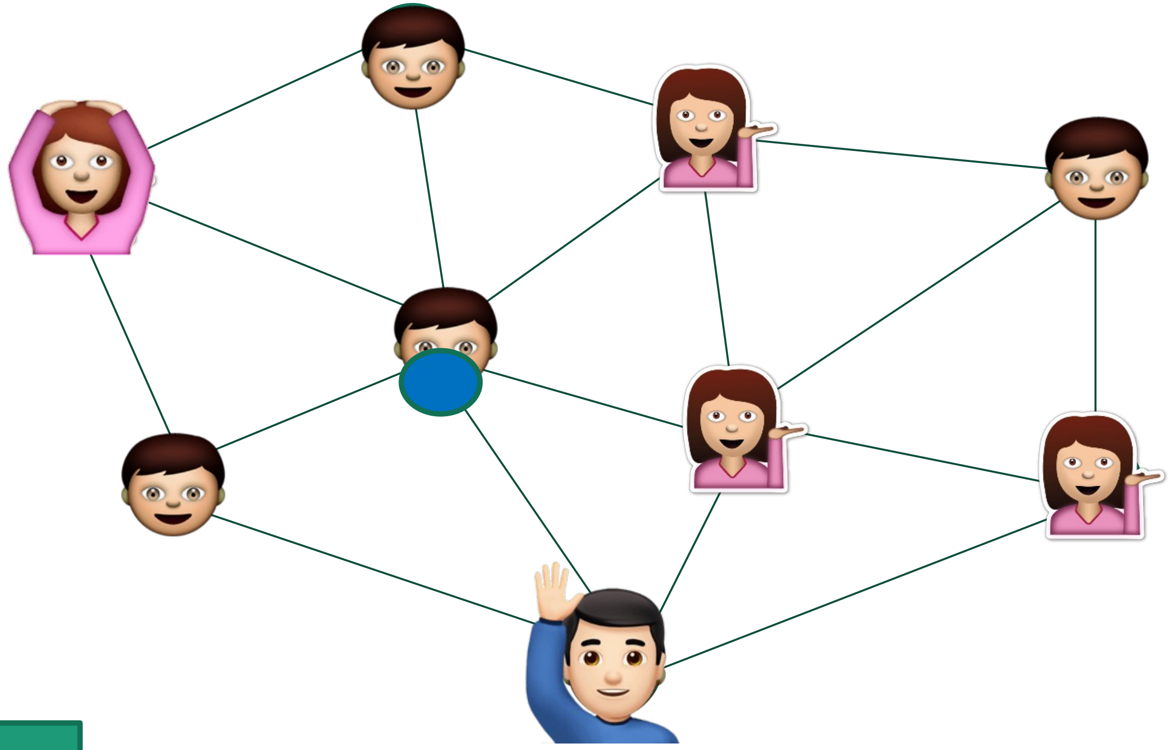
- Block Size ~1.2MB and Anchors are fixed 264 bytes
- Anchors' mean prop time was 0.45 secs
- Avg delay for blocks was 3.46,3.52 and 3.7 secs for a = 2,5,10 respectively
- Anchors are at least 5 times faster than blocks
- Anchors work well without creating significant bandwidth or latency overheads



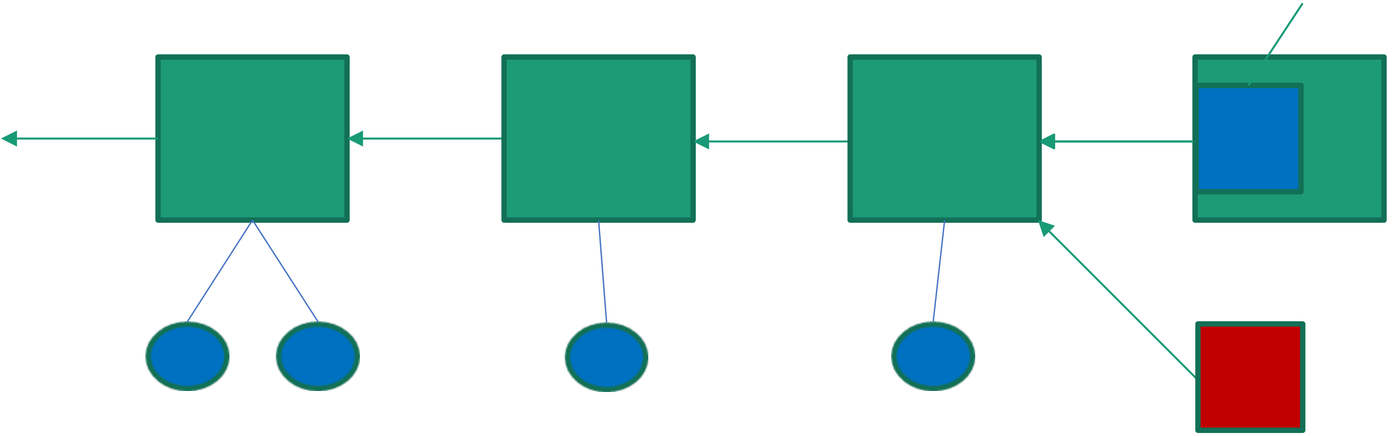
Fork Resolution with Anchors

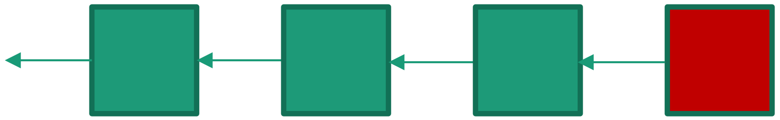


View 1 of the blockchain



Absolute view of the blockchain

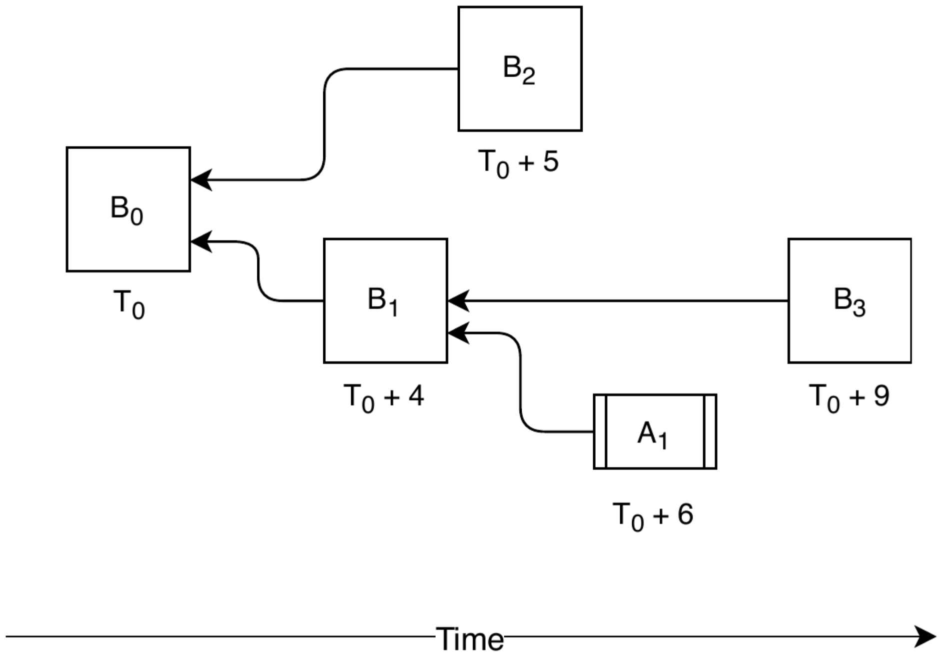


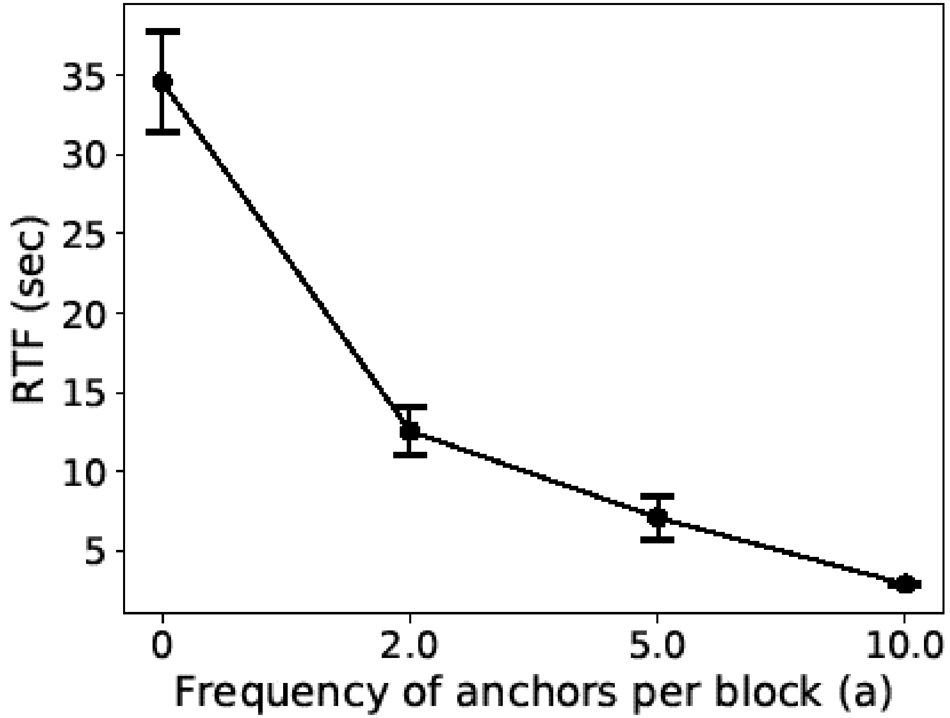


View 2 of the blockchain

Experiment 2: Fork Resolution

G3





Fork created by B2.

In a system without Anchors, it is resolved by B3.
In a system with Anchors, it is resolved by A1.

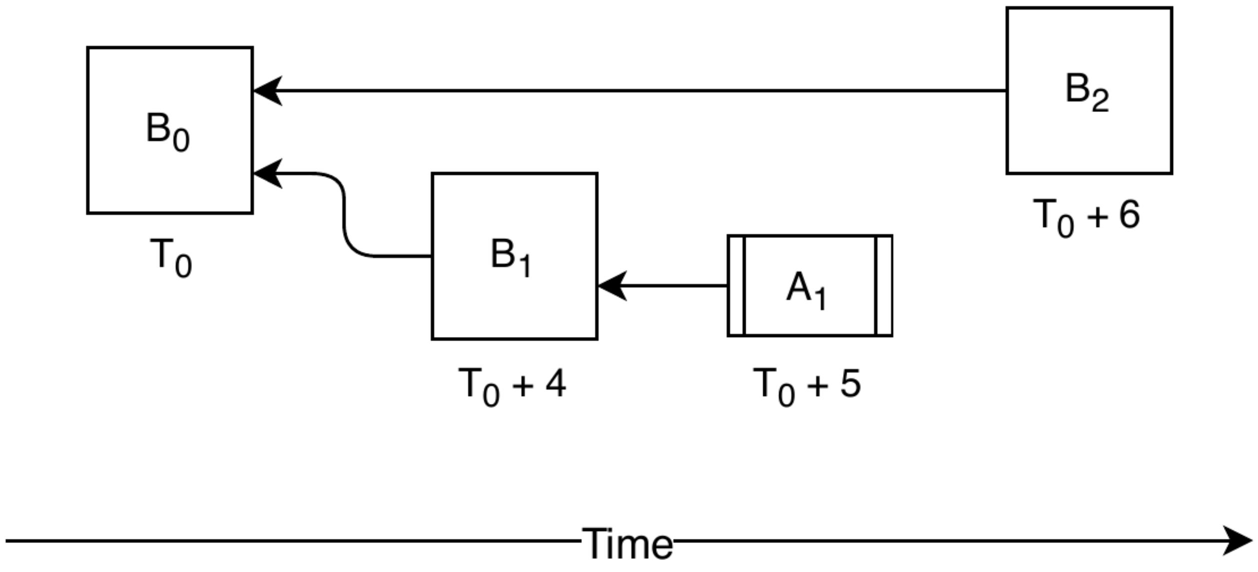
64% improvement in RTF for a=2 over a=0

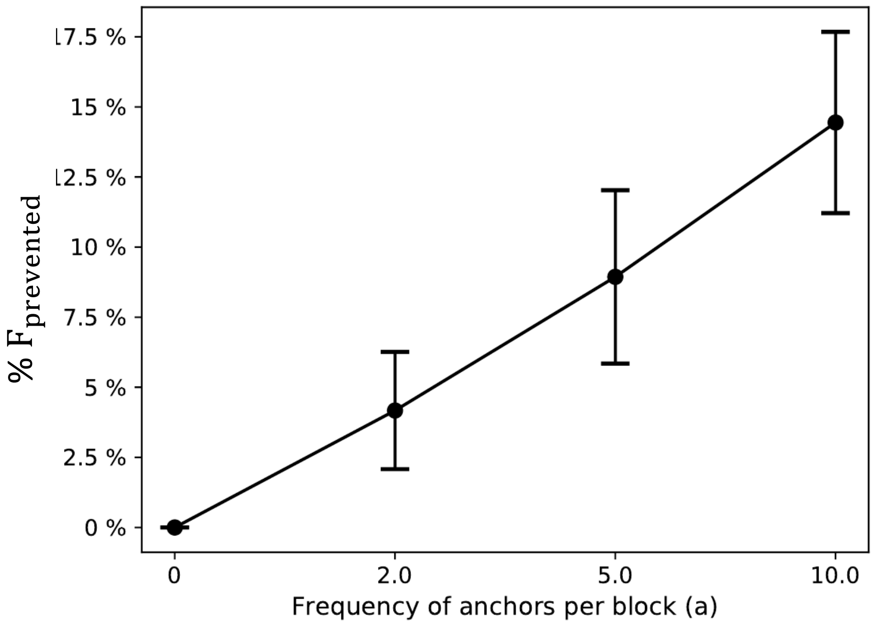
80% improvement in RTF for a=5 over a=0

91% improvement in RTF for a=10 over a=0

Experiment 3: Fork Prevention

G2





In a system without Anchors, B2 would cause a Fork.
In a system with Anchors, the fork never really happens since A1 arrived and was accepted before B2.

B1's chain already has more weight and is the final chain.

$$F_{prevented} = \frac{f_{prevented}}{f_{prevented} + f_{occurred}}$$

$f_{prevented}$ is the number of forks prevented in the network.

$f_{occurred}$ is the number of fork occurrences in the network.

$F_{prevented}$ is the ration of forks prevented in the network.

Notations and Assumptions

Partially synchronous network

n Number of miners in the network

Δ_b Maximum network delay for Blocks

α Weight of an anchor. $\alpha \leq 1$

q Fraction of the network controlled by adversary. $q < 0.5$

Δ_a Maximum network delay for Anchors. $\Delta_a < \Delta_b$

a Frequency of anchors per block $= 1/\alpha$

G Probability of an honest block at a time instant

Chain Growth with Anchors

Chain growth is the minimum weight all honest miner's chains must have gained in a time interval.

We study chain growth in weight as opposed to length in prior work.

υ is the lower bound honest weight gained in unit time in a system with anchors.

Lower bound growth per round of PoW systems without anchors (υ_{pow}) is found by Pass et. Al.

For any interval [s,s+t] where t>2 Δ_b rounds, system with anchors achieves an honest chain growth of at least υt in weight except with negligible probability. Honest growth rate parameter per round is,

$$\upsilon_{pow} \; \upsilon = \frac{G}{G\Delta_b + 1}$$

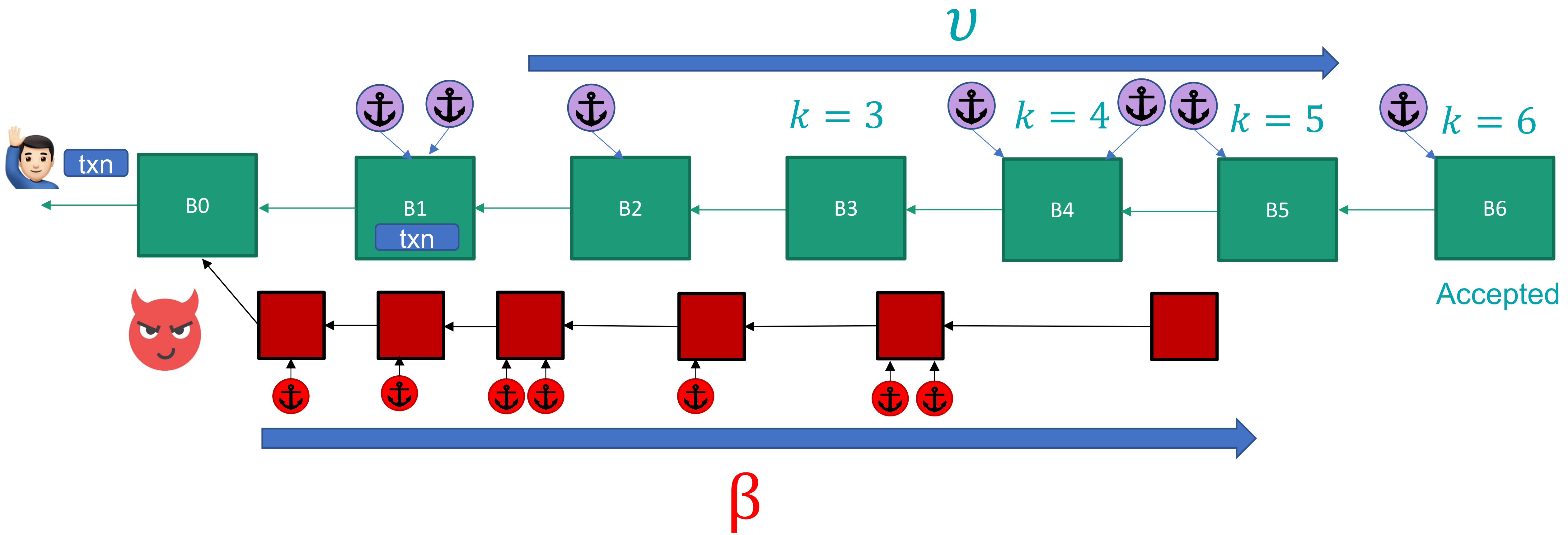
We find that $\upsilon_{pow} \leq \upsilon$, therefore, a system with anchors has better chain growth.

R. Pass, L. Seeman, and A. Shelat. Analysis of the blockchain protocol in asynchronous networks. In EURO-CRYPT. Springer, 2017.

Intuition behind the double spend with anchors

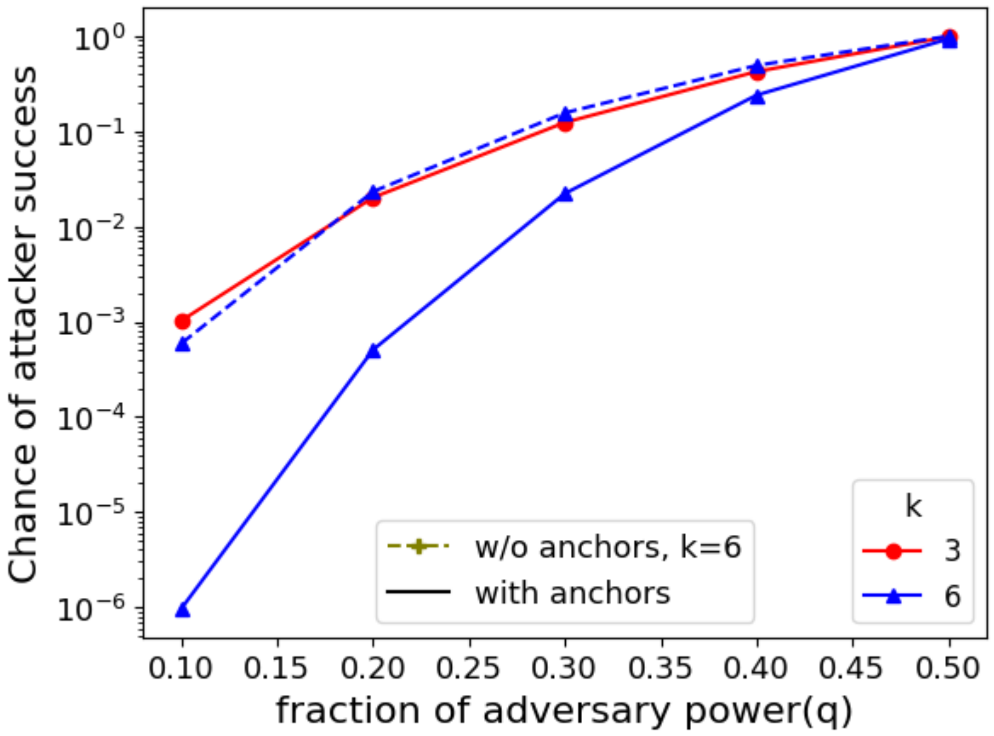
υ is the lower bound honest weight gained in a time round in a system with anchors.

β is the upper bound adversary growth in a time round in a system with anchors. Assume $\upsilon > \beta$.



Confirmation Time with Anchors

G1



$\upsilon > \beta$

a Frequency of anchors per block = 2

k Number of confirmation blocks

Anchors reduce the chance of a double spend attack in Bitcoin by over 2 orders of magnitude.

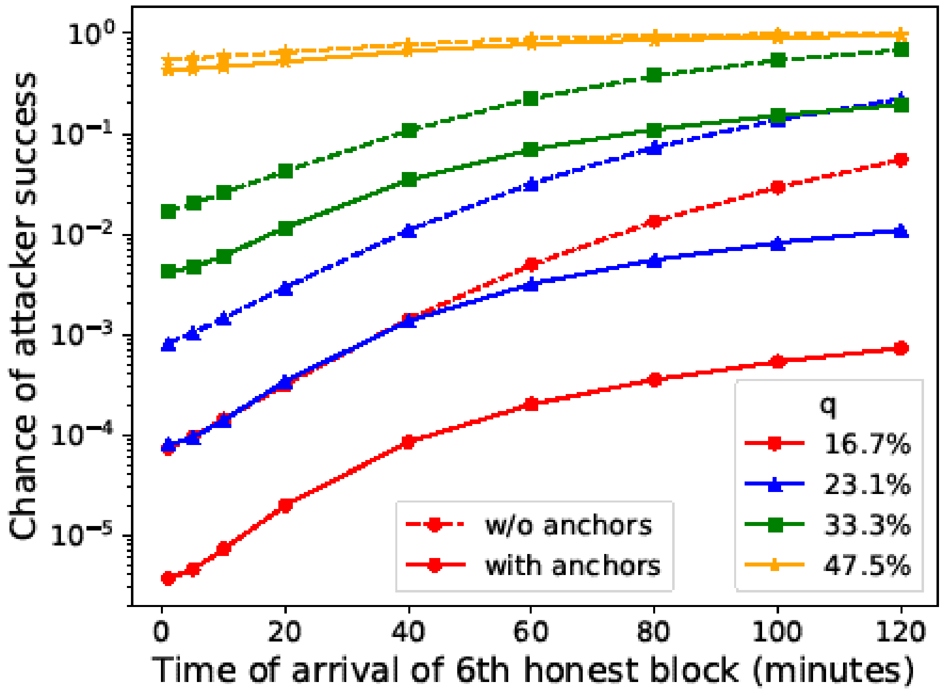
Alternatively, they can reduce the confirmation time by half for the same security guarantee

S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008 S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008

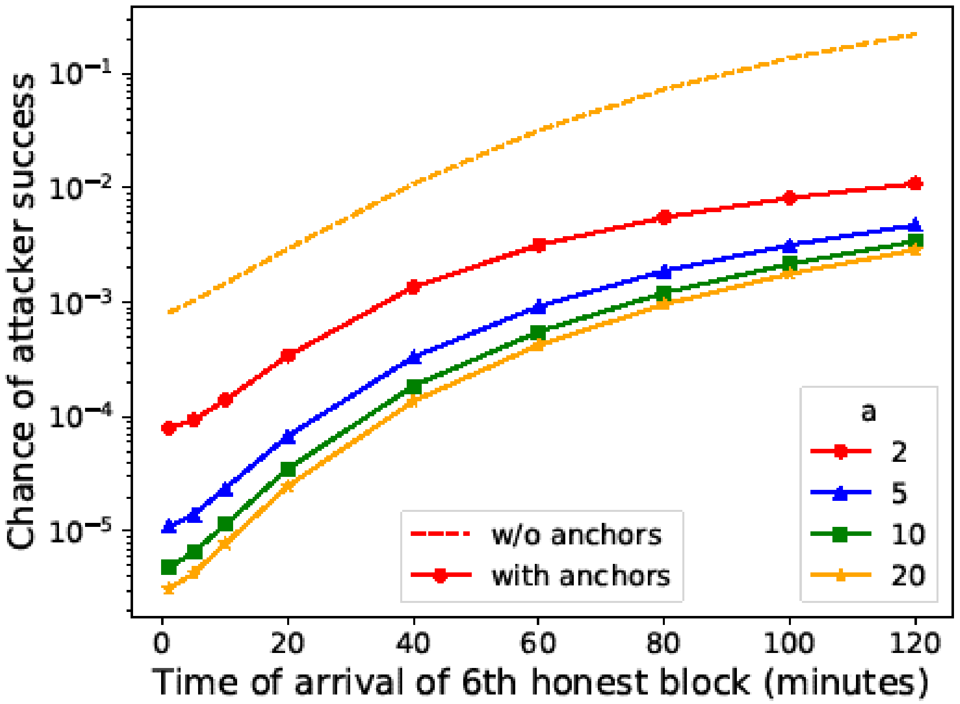
M. Rosenfeld. Analysis of hashrate-based double spending. arXiv preprint arXiv:1402.2009, 2014.

Confirmation Time with Anchors (Time Variant)

a = 2



q = 23%



k = 6

C. Pinz´on and C. Rocha. Double-spend attack models with time advantage for bitcoin. Electronic Notes in Theoretical Computer Science, 329:79–103, 2016.
S. Neumayer, M. Varia, and I. Eyal. An analysis of acceptance policies for blockchain transactions. IACR Cryptology ePrint Archive, 2018

Summary

G1 G2 G3

Reduces confirmation time by half in Bitcoin with no security compromise

Fast signaling mechanism of mining power division in case of forks

Five times faster propagation than bitcoin blocks

Benefits of Anchors

Reduces fork resolution time and Prevents fork occurrences

Provides stability by steady weight addition to the chain

Versatile solution to new or existing Blockchains with minimal modifications

Thank You! Questions?

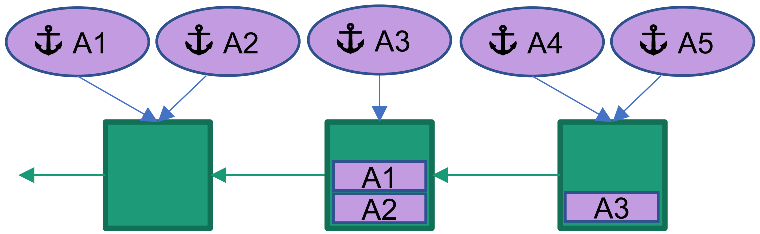
LinkedIn: @oviaseshadri

Twitter: @ovia_seshadri

Additional slides

Anchor Rewards

- Anchors can be rewarded by including its header in later blocks.
- This can help chains with anchors define its weight unambiguously
- Anchor header without CB is 80 bytes
- When a=2 this is 160 bytes addition to a block's body on avg.



$r_c(n)$ Creation reward for including anchors in a block at a length of 'n' from its parent

$r_i(n)$ Inclusion reward for including anchors in a block at a length of 'n' from its parent

Block reward is 1
Anchor reward is α.

- Miners get smaller more timely payouts
- Disincentivizes the need to join mining pools
- Reduces ambiguity in chain weight.

Chain Quality with Anchors

Chain Quality is the minimum honest weight contributed on any miner's chain in a time interval.

υ is the lower bound honest weight gained in a time round in a system with anchors.

Let β be the upper bound adversary growth in a time round in a system with anchors. Assume $\upsilon > \beta$.

We found that a system with anchors satisfies a lower bound chain quality of

$$1 - \frac{\beta}{\upsilon}$$

Lower bound chain quality found by Pass.et.al is $1 - \frac{\beta_{pow}}{\upsilon_{pow}}$ for PoW systems without anchors.

Here, υ_{pow} is the lower bound growth rate of PoW systems without anchors and β_{pow} is the upper bound adversary growth per round in PoW system without anchors .

R. Pass, L. Seeman, and A. Shelat. Analysis of the blockchain protocol in asynchronous networks. In EURO-CRYPT. Springer, 2017.

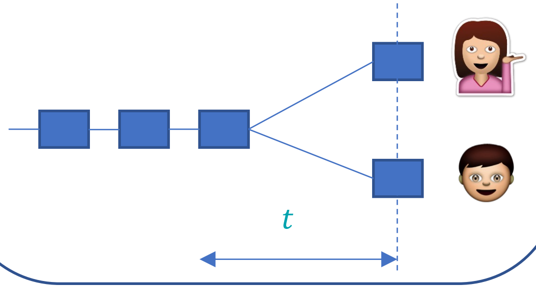
Consistency with Anchors

Consistency is a theoretical security guarantee that shields the system from any type of adversary attack if he owns power less than a threshold.

Consistency is achieved when the system can guarantee with high probability two properties:

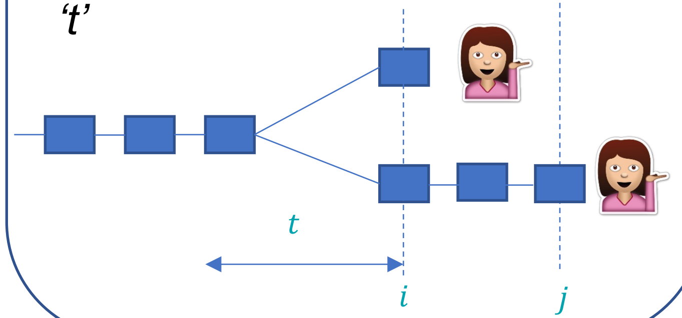
Common Prefix

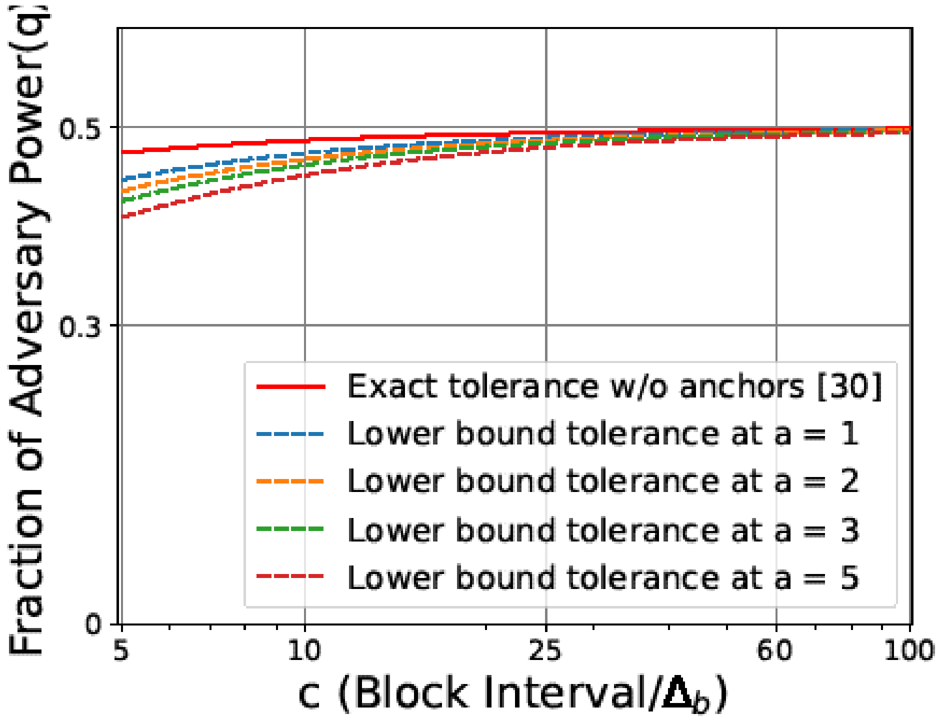
The chains of any two honest players at any time instant must have common ancestors of entities except for the last ‘t’ rounds with high probability in ‘t’



Future Self Consistency

The chains of any honest player at any two time instants “i” and “j” where “i<j” must have common ancestors of entities except for the last ‘t’ rounds before “i” with high probability in ‘t’





$\upsilon > \beta$

[7] A. Dembo, S. Kannan, E. N. Tas, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni. Everything is a race and Nakamoto always wins. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pages 859–878, 2020

[36] P. Gaˇzi, A. Kiayias, and A. Russell. Tight Consistency Bounds for Bitcoin. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, CCS ’20, pages 819–838, New York, NY, USA, 2020. Association for Computing Machinery