Kadena

SOLVING THE TRILEMMA: SCALING PROOF OF WORK

DOUG BEARDSLEY

ROUGHLY SPEAKING

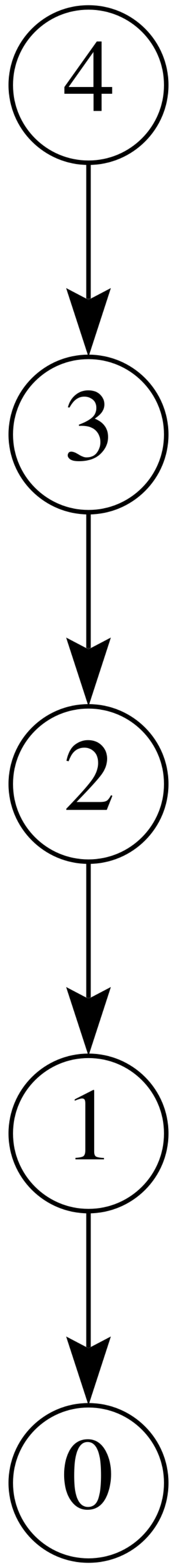
ALL SINGLE-CHAIN POW BLOCKCHAINS HAVE THE SAME PERFORMANCE

They have the same fundamental physical limitations

EXPLAINED

1. SPEED OF LIGHT
2. NETWORK BANDWIDTH
3. TRANSACTION EXECUTION TIME

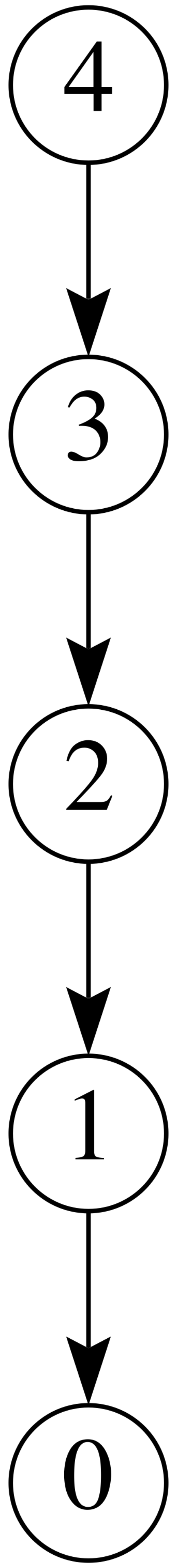
5 TPS (APPROX.)



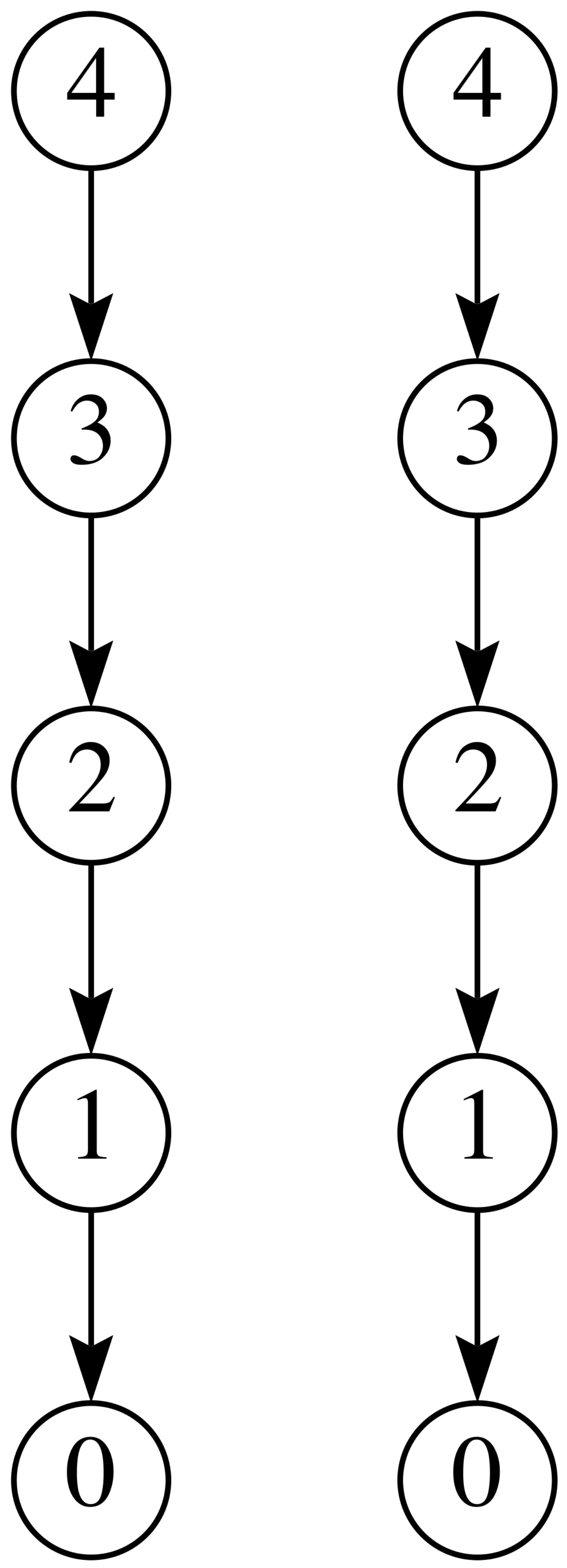
WE CAN SCALE WITH A "MULTI-CORE" BLOCKCHAIN

MULTIPLE CHAINS
JUST LIKE COMPUTERS USE
MULTIPLE CORES

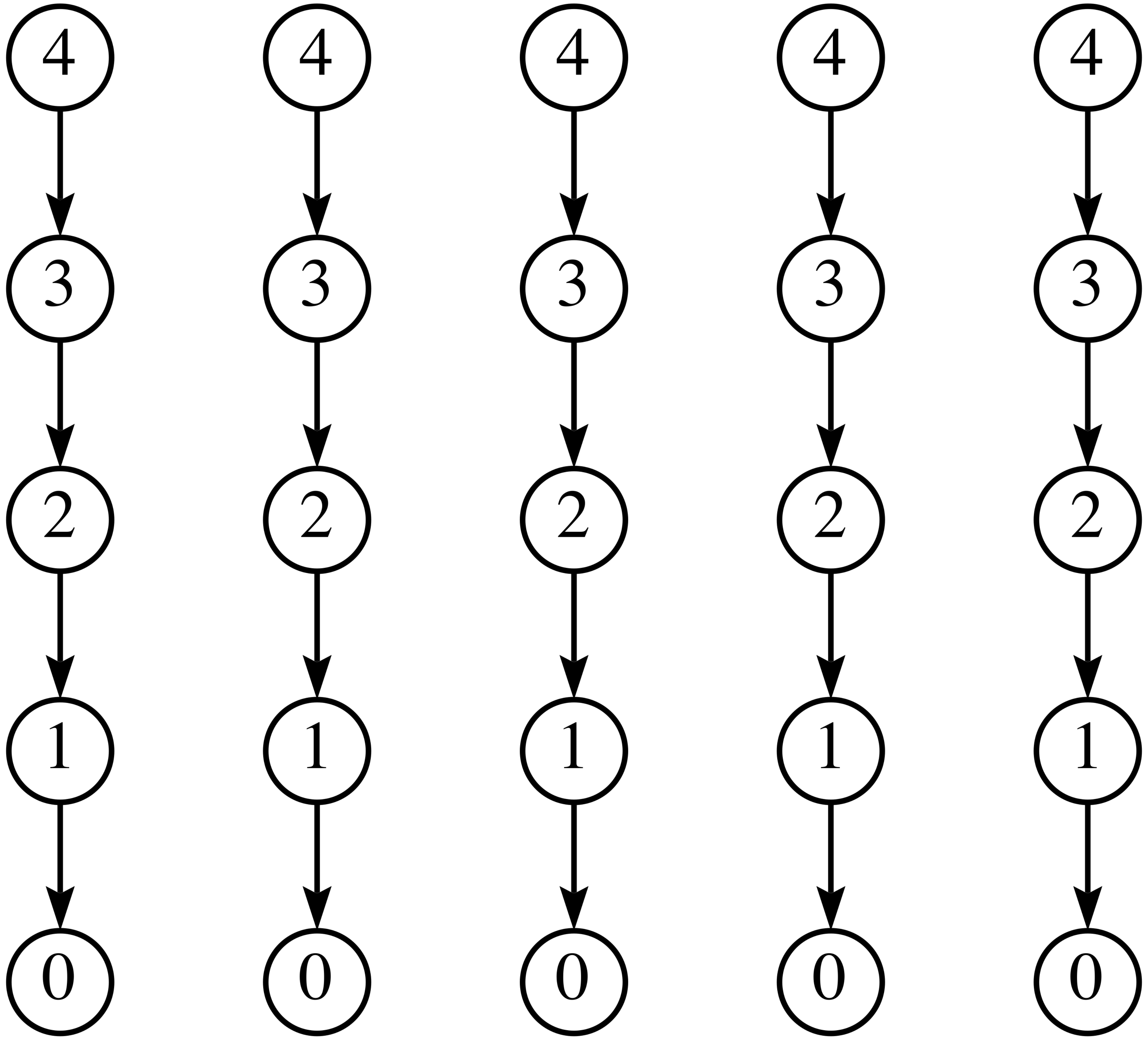
1 CHAIN = 5 TPS



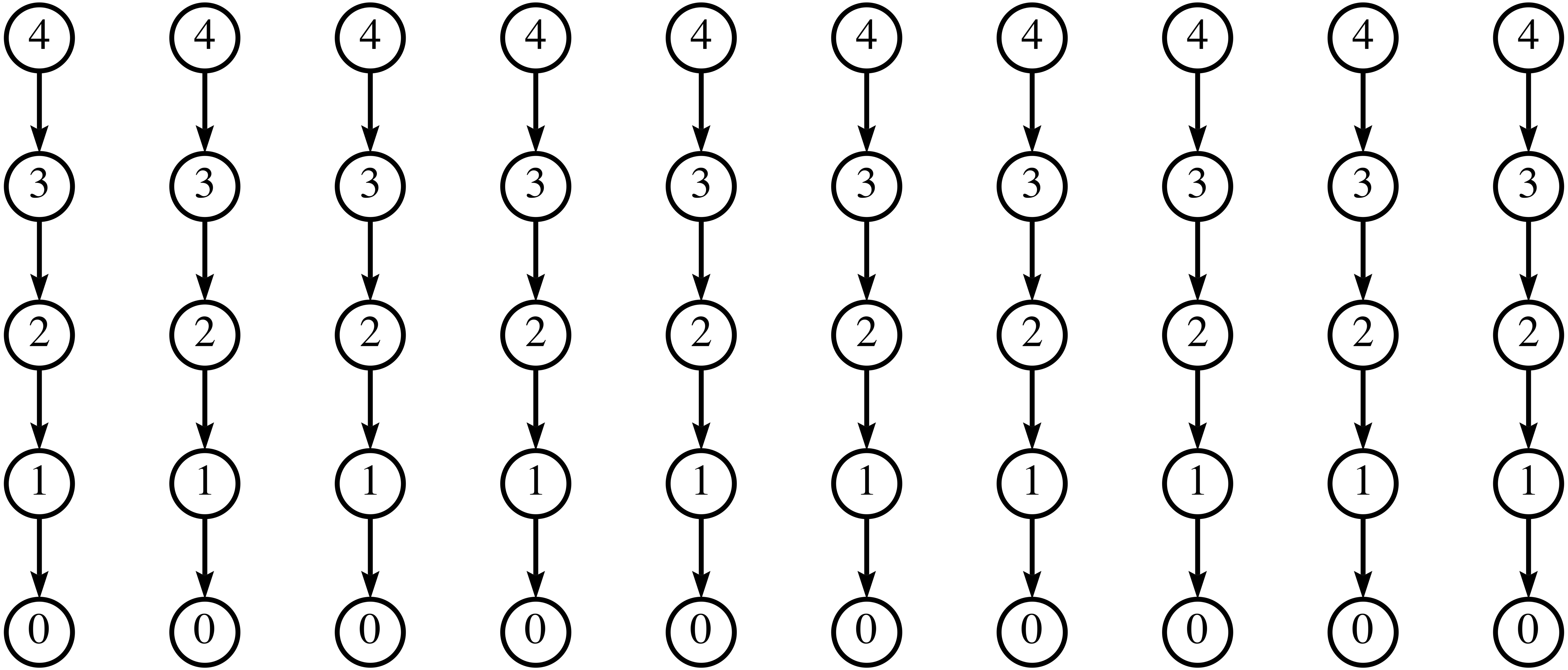
2 CHAINS = 10 TPS



5 CHAINS = 25 TPS



10 CHAINS = 50 TPS



NAÏVE APPROACH HAS TWO CHALLENGES

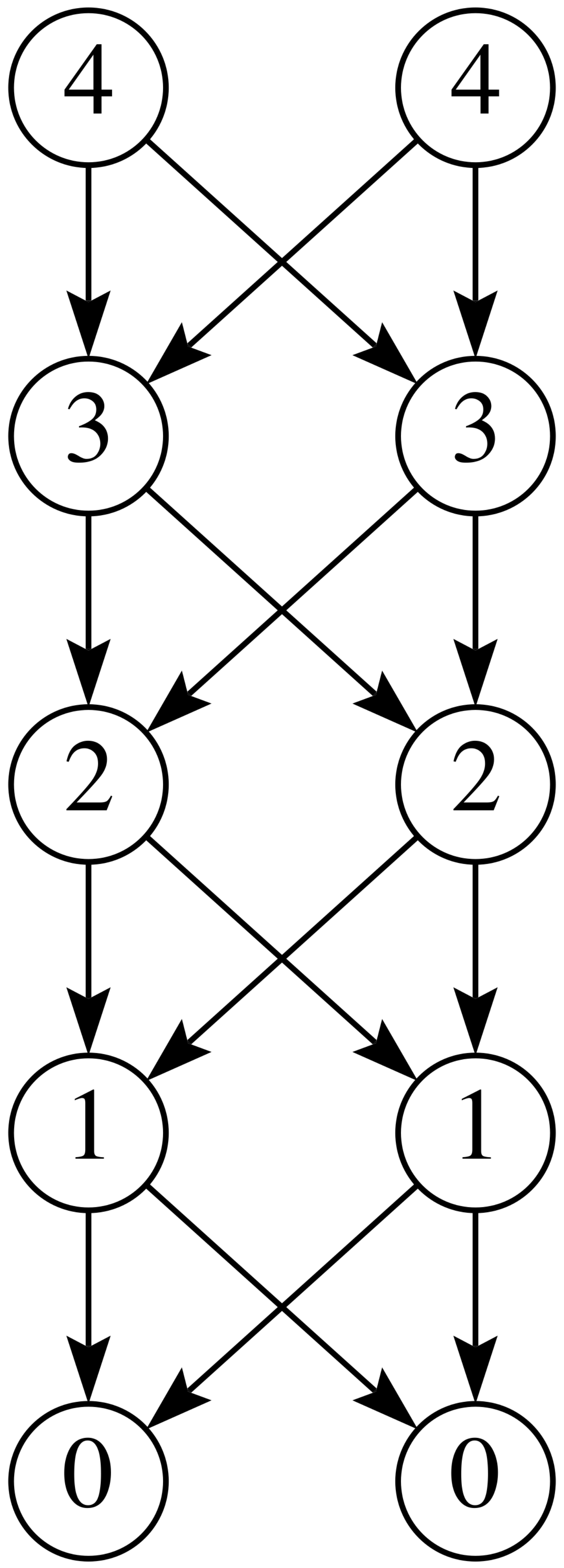
+ 10 SEPARATE BLOCKCHAINS GIVES US 10 DIFFERENT CURRENCIES

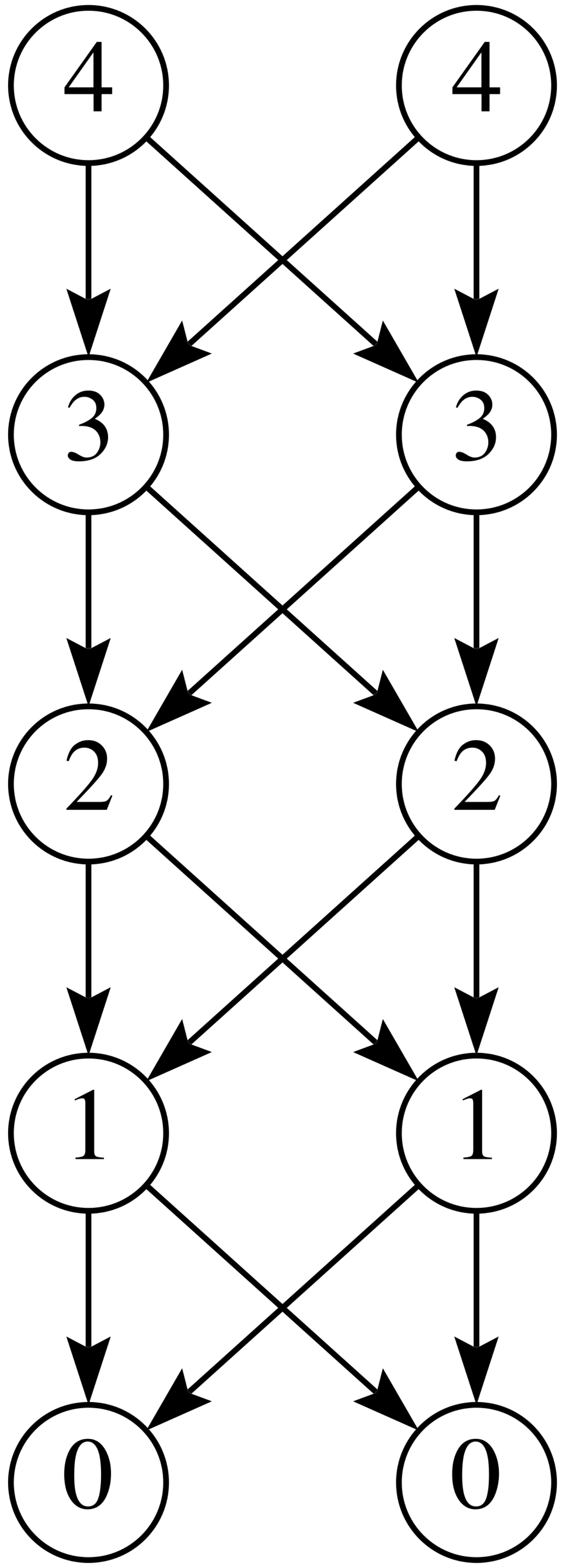
+ A 51% ATTACK BECOMES A 5.1% ATTACK

SOLUTION

BRAID THE CHAINS TOGETHER

2 CHAINZ





BRAIDING SOLVES BOTH PROBLEMS

BLOCK INCLUDES ADDITIONAL HASH

In addition to including the hash of the previous block on the same chain, you also have it include the hash of the previous block on the other chain.

SOLVES 5.1% ATTACK PROBLEM

If you wait one block after your transaction, it will require the full hash power of both chains to do a 51% attack on that block.

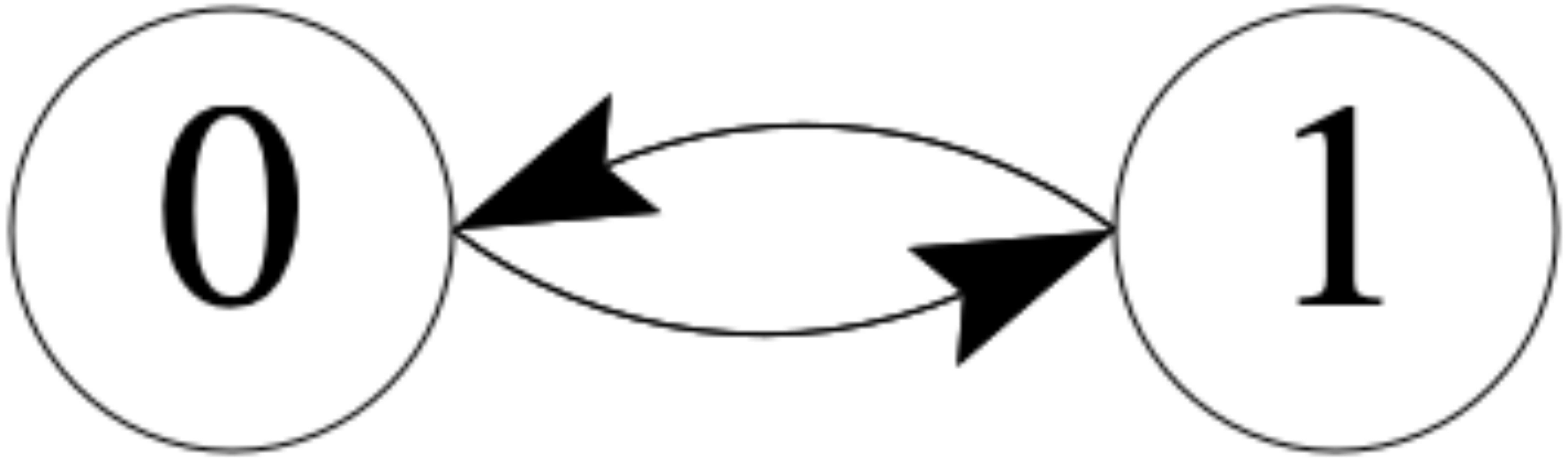
SINGLE CURRENCY

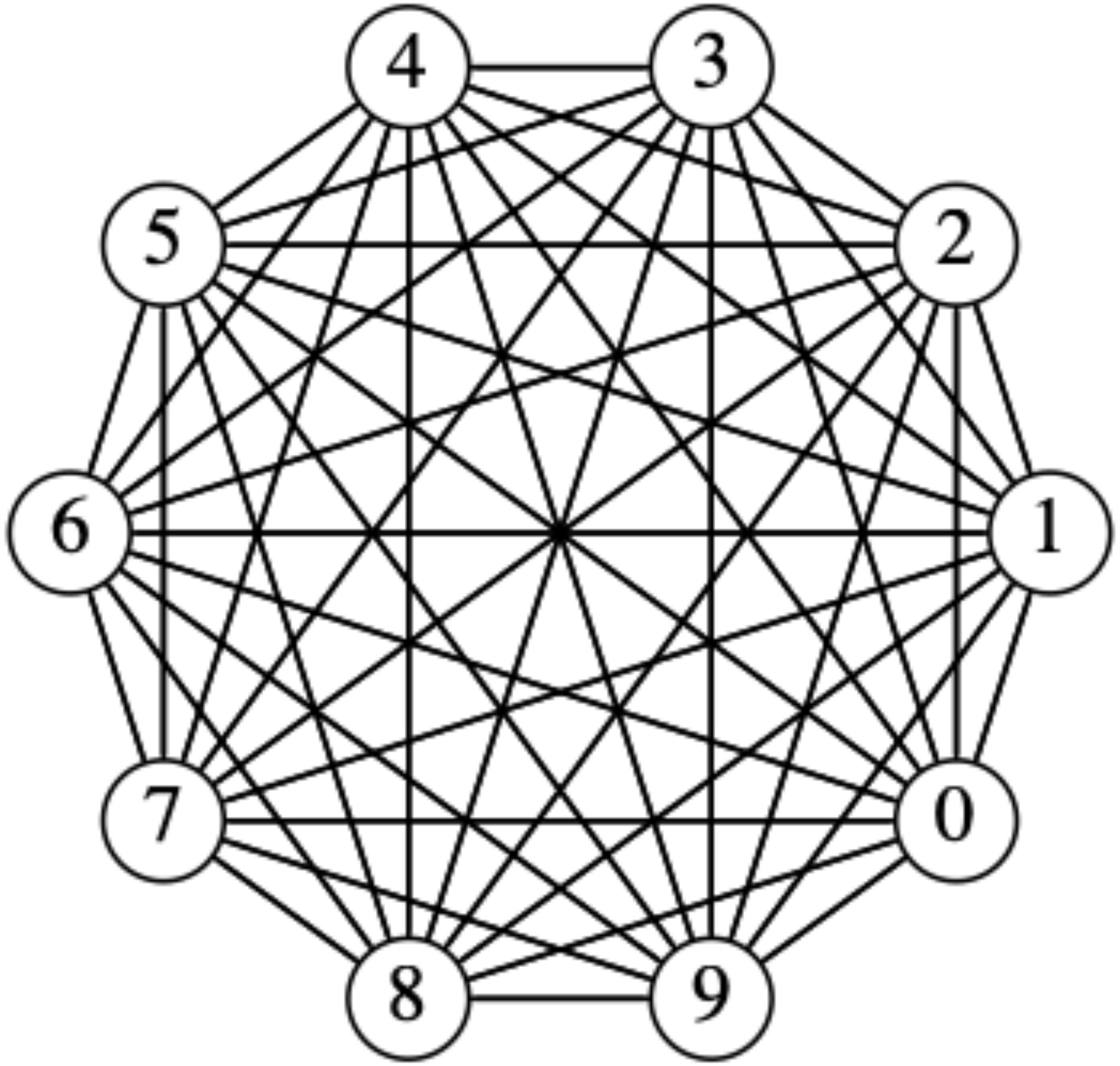
Hash braiding lets us do trustless cross-chain transfers, yielding a single currency across both chains. Transfer across chains happens by burning on one chain and submitting the proof to create the coins on another chain.

2 CHAINS ISN’T ENOUGH

HOW DO YOU SCALE FURTHER?

2-CHAIN GRAPH





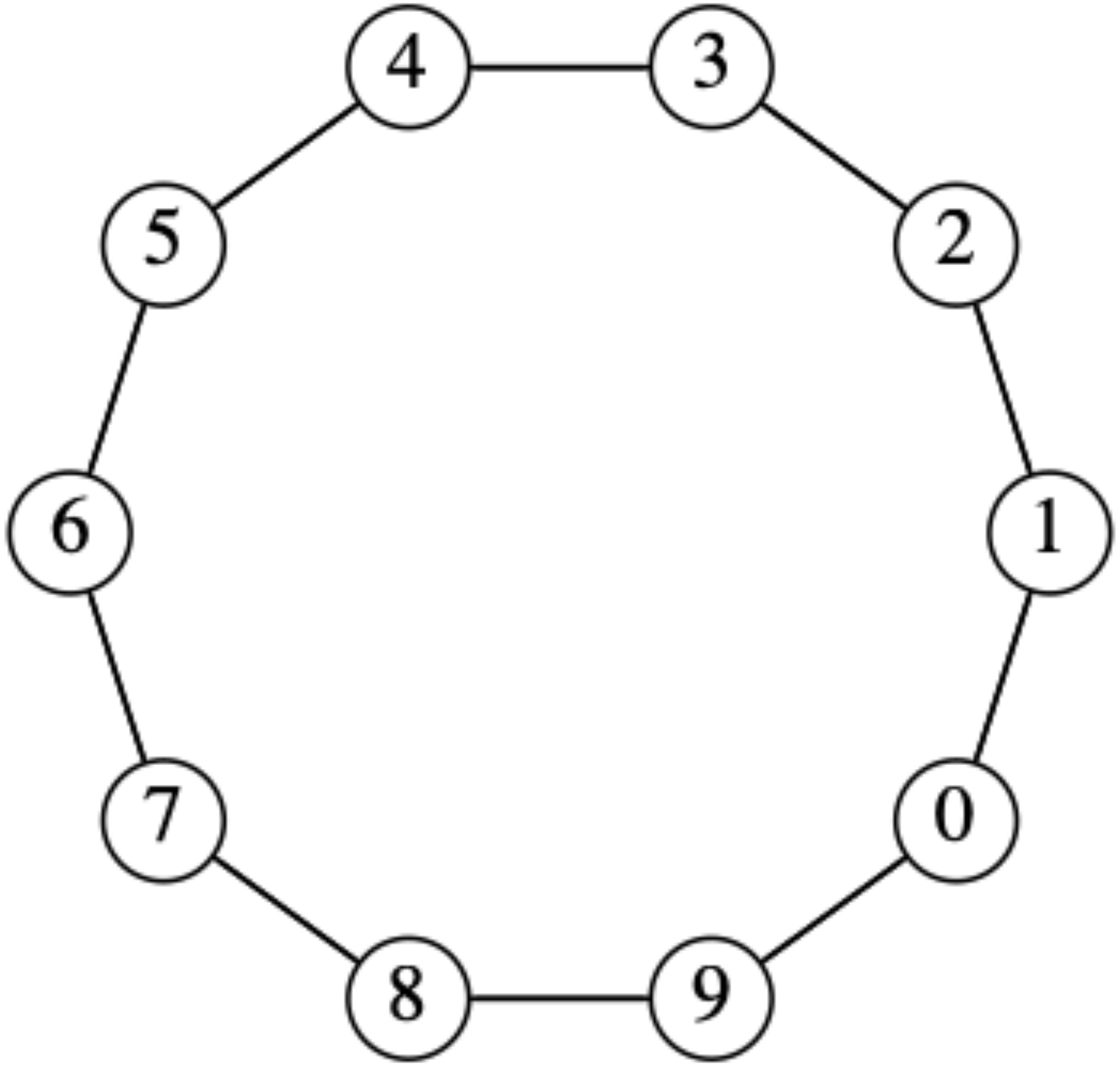
HOW DO YOU CONNECT 10 CHAINS TOGETHER? METHOD 1

1 HOP TO FARTHEST CHAIN

Fastest possible cross-chain operations. Only have to wait one block. Stays the same as you scale higher.

9 EXTRA HASHES PER BLOCK

Requires too much space. Gets way worse as you scale higher.



HOW DO YOU CONNECT 10 CHAINS TOGETHER? METHOD 2

5 HOPS TO FARTHEST CHAIN

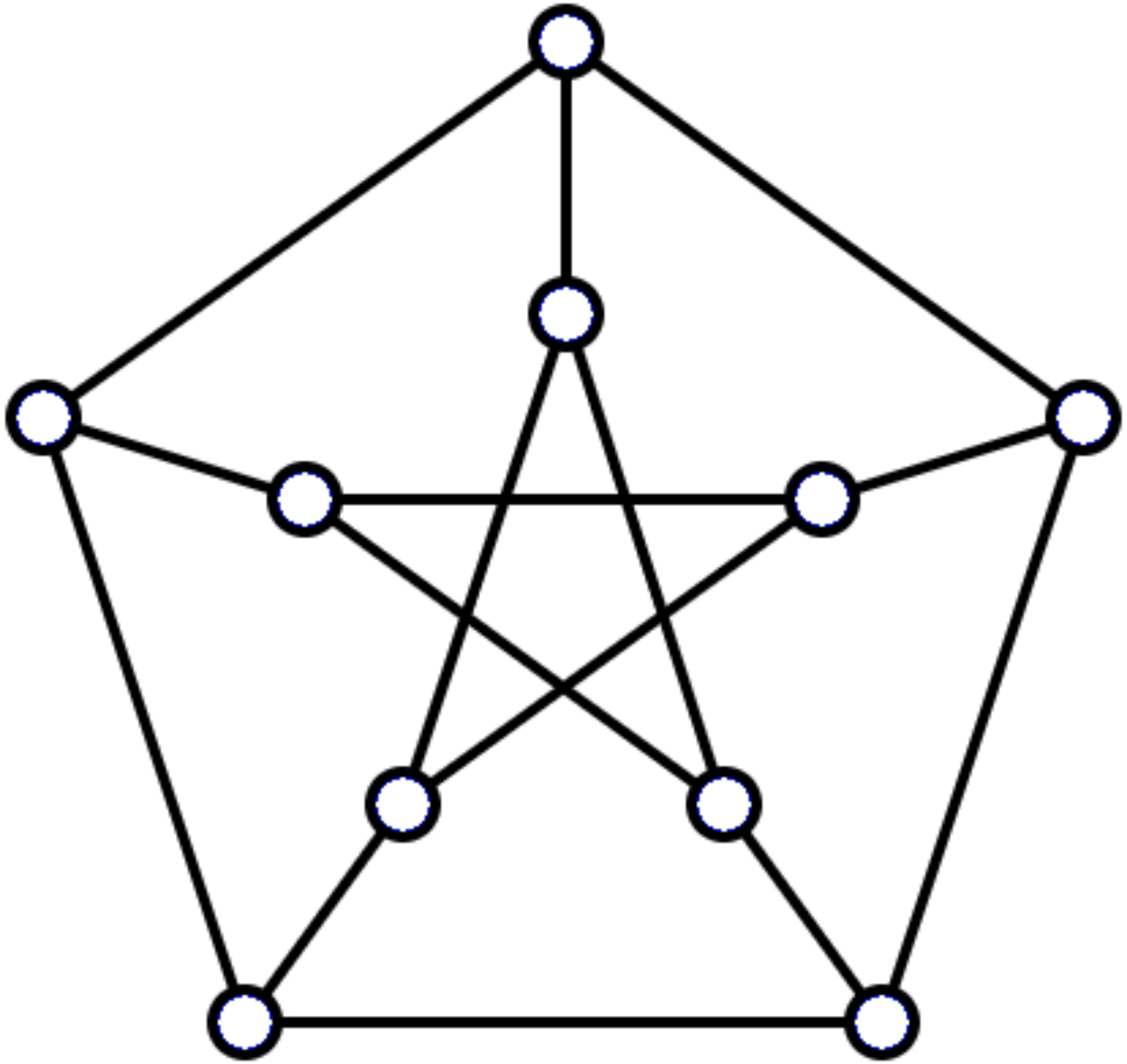
Have to wait 5 blocks for cross-chain operations. With 100 chains it would be 50 blocks…too long.

2 EXTRA HASHES PER BLOCK

Great on space. Doesn’t get worse as you scale higher.

GRAPH THEORY SAVES THE DAY!

DEGREE-DIAMETER PROBLEM



HOW DO YOU CONNECT 10 CHAINS TOGETHER? THE ANSWER

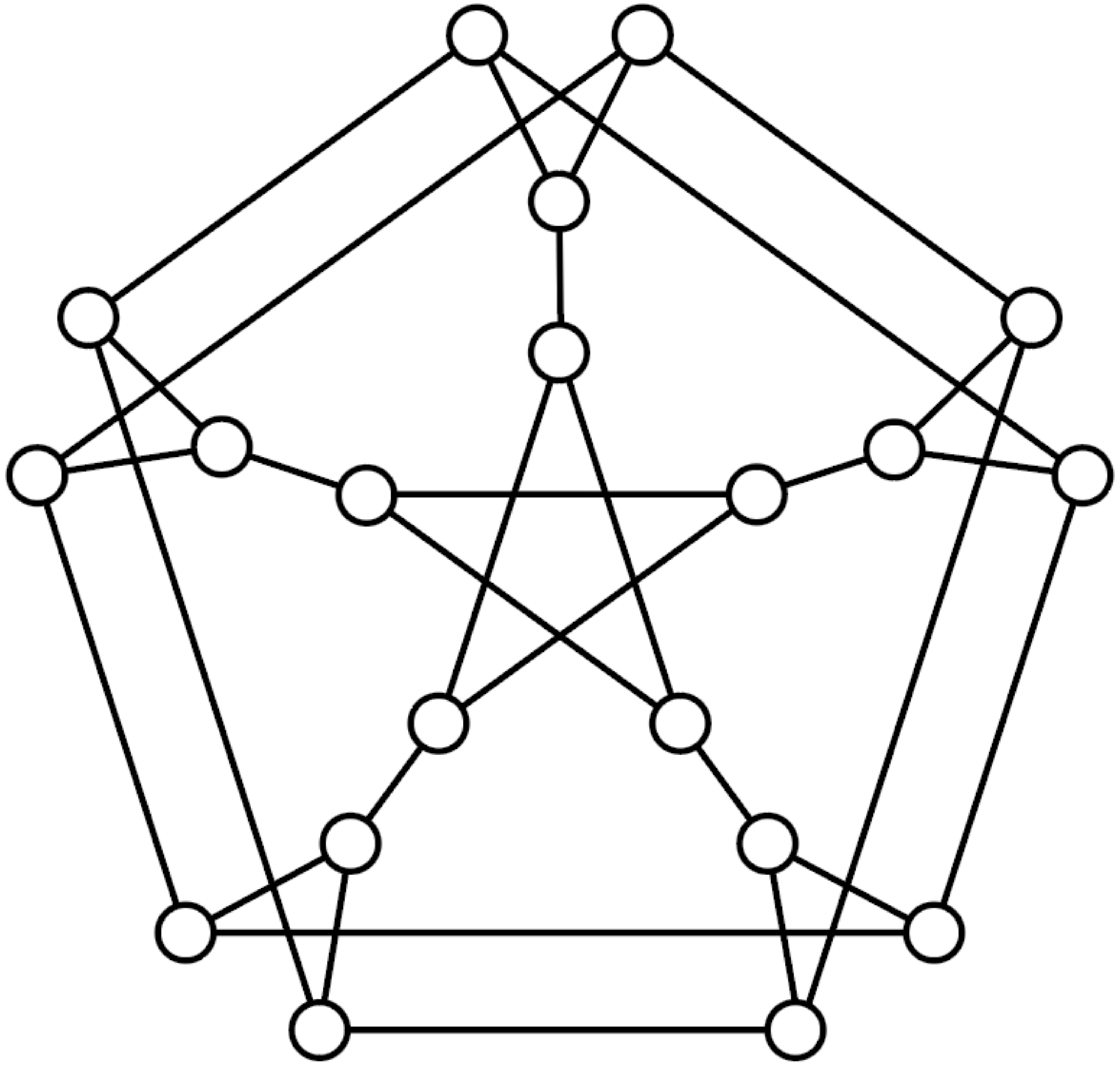
2 HOPS TO FARTHEST CHAIN

Fast cross-chain operations.

3 EXTRA HASHES PER BLOCK

Reasonable space requirements.

20 CHAINS



3 HOPS TO FARTHEST CHAIN

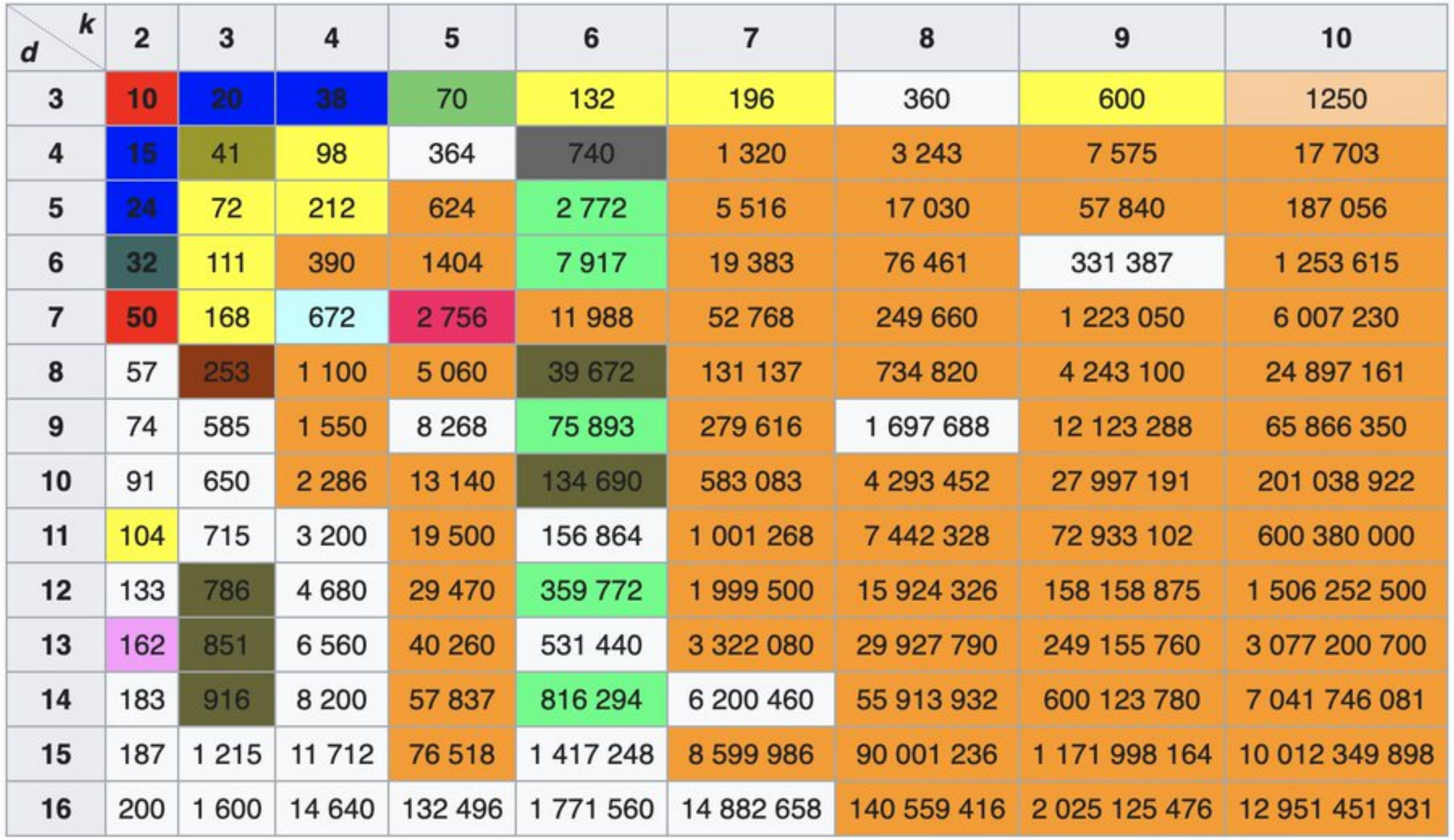
Fast cross-chain operations.

3 EXTRA HASHES PER BLOCK

Reasonable space requirements.

WHAT ABOUT MORE THAN 20 CHAINS?

KADENA SCALES WITH DEGREE-DIAMETER SOLUTIONS



k d	2	3	4	5	6	7	8	9	10
3	10	20	38	70	132	196	360	600	1250
4	15	41	98	364	740	1 320	3 243	7 575	17 703
5	24	72	212	624	2 772	5 516	17 030	57 840	187 056
6	32	111	390	1404	7 917	19 383	76 461	331 387	1 253 615
7	50	168	672	2 756	11 988	52 768	249 660	1 223 050	6 007 230
8	57	253	1 100	5 060	39 672	131 137	734 820	4 243 100	24 897 161
9	74	585	1 550	8 268	75 893	279 616	1 697 688	12 123 288	65 866 350
10	91	650	2 286	13 140	134 690	583 083	4 293 452	27 997 191	201 038 922
11	104	715	3 200	19 500	156 864	1 001 268	7 442 328	72 933 102	600 380 000
12	133	786	4 680	29 470	359 772	1 999 500	15 924 326	158 158 875	1 506 252 500
13	162	851	6 560	40 260	531 440	3 322 080	29 927 790	249 155 760	3 077 200 700
14	183	916	8 200	57 837	816 294	6 200 460	55 913 932	600 123 780	7 041 746 081
15	187	1 215	11 712	76 518	1 417 248	8 599 986	90 001 236	1 171 998 164	10 012 349 898
16	200	1 600	14 640	132 496	1 771 560	14 882 658	140 559 416	2 025 125 476	12 951 451 931

5 HASHES, 5 HOPS
Hundreds of chains

6 HASHES, 6 HOPS
Thousands of chains

7 HASHES, 7 HOPS
Tens of thousands of chains

8 HASHES, 8 HOPS
Hundreds of thousands of chains

MORE THAN ENOUGH FOR GLOBAL TX LOADS!
Architecture is no longer a limiting factor.

WHEN WILL THIS BE READY?

Kadena has already launched, proved the concept, and scaled.

EXPLAINED

1

OCTOBER 2019

Mainnet genesis blocks mined with a 10-chain network.

2

JANUARY 2020

Full smart contract launch

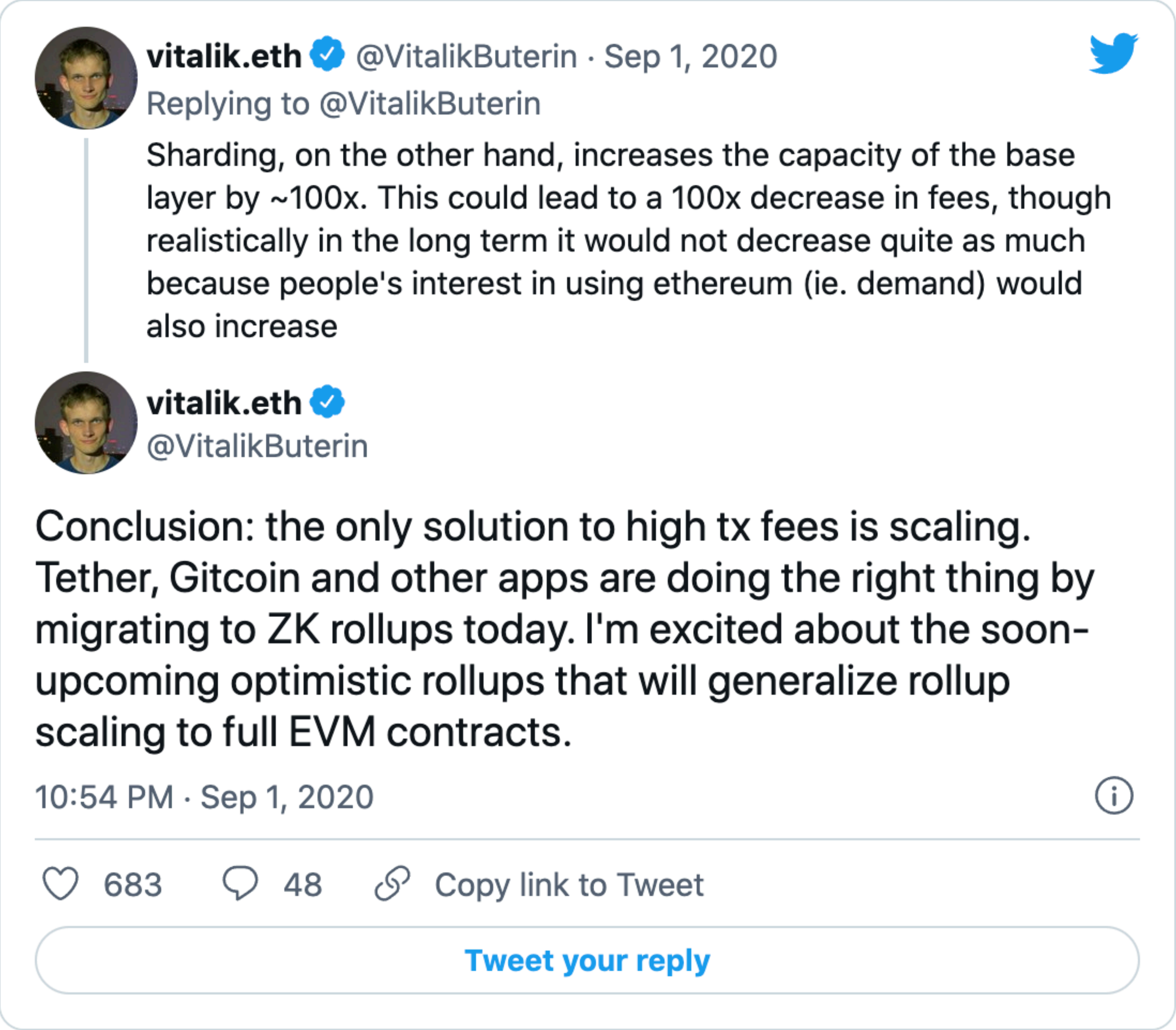
3

AUGUST 2020

Doubled network capacity to 20 chains while running in production!

WHAT DOES SCALING GET US?

LOW GAS FEES



vitalik.eth @VitalikButerin · Sep 1, 2020

Replying to @VitalikButerin

Sharding, on the other hand, increases the capacity of the base layer by ~100x. This could lead to a 100x decrease in fees, though realistically in the long term it would not decrease quite as much because people's interest in using ethereum (ie. demand) would also increase

vitalik.eth
@VitalikButerin

Conclusion: the only solution to high tx fees is scaling. Tether, Gitcoin and other apps are doing the right thing by migrating to ZK rollups today. I'm excited about the soon-upcoming optimistic rollups that will generalize rollup scaling to full EVM contracts.

10:54 PM · Sep 1, 2020

HIGH GAS FEES

HARM THE INDUSTRY
MORE THAN WE THINK

EXAMPLES OF HIGH GAS PROBLEMS

+ ConstitutionDAO

+ Miner Extractable Value (MEV)

+ Smaller addressable market

HIGH GAS: CONSTITUTION DAO

Most users lost substantial fractions of their donation to fees, which had to be paid a second time to get money out after the auction bid failed.

$50-90	$217	$1.2M
Fees to donate to the DAO	Median donation	Total spent on gas fees

HIGH GAS: MINER EXTRACTABLE VALUE

Uniswap V2 fees as of 2021-11-30

$137

Swap

$332

Supply Liquidity

$150

Remove Liquidity

HIGH GAS: MINER EXTRACTABLE VALUE

+ Alice submits a trade, someone sees and pays a miner to put another transaction ahead of it, profiting from the knowledge that it will happen.

+ Alice doesn’t want to cancel the trade because the > $100 fee will be wasted.

+ Low fees allow Alice to construct trades that will cancel if a front-runner moves the price too much.

+ This would significantly reduce the profitability of MEV.

HIGH GAS: SMALLER ADDRESSABLE MARKET

+ You’ll never be able to buy coffee with cryptocurrency if fees are > $20.

+ Small in-game NFT purchases

+ Several hundred dollars to mint an NFT excludes many artists, especially more speculative projects.

+ Hurts adoption in many other ways that are hard to imagine because it’s an unknown unknown…we literally don’t know what we’re missing.

LAYER-2 DOESN’T COMPLETELY SOLVE THE PROBLEM

+ Rollups often end up being app-specific. You still have to pay high fees to move back through the layer-1 chain to interact with other dapps.

+ Other layer-2 solutions like Lightning sacrifice decentralization and the flexibility of smart contracts.

+ Layer-2 has a place, but is not a substitute for layer-1 scaling.

CONCLUSION

KADENA

+ Scalable layer-1 blockchain

+ Mainnet started in 2019

+ Doubled capacity in 2020

+ You can use it today and be liberated from high gas fees

BUILD ON A SCALABLE FUTURE… KADENA

LET’S TALK

Doug Beardsley https://kadena.io/
Scaling Proof of Work
twitter.com/BlockchainDoug

Kadena