

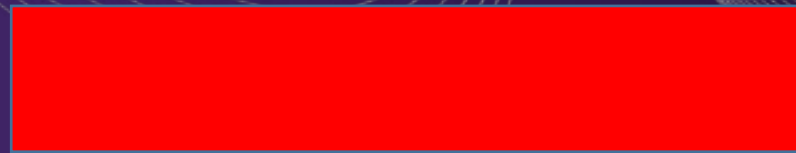
BLOCKCHAIN IN A NUTSHELL

An abstract graphic featuring several blue, faceted diamond shapes of varying sizes scattered across a dark purple background. White, wavy, concentric lines flow from the left side towards the right, creating a sense of motion and depth. The overall aesthetic is clean, modern, and tech-oriented.

ALICE CREATES A TRANSACTION

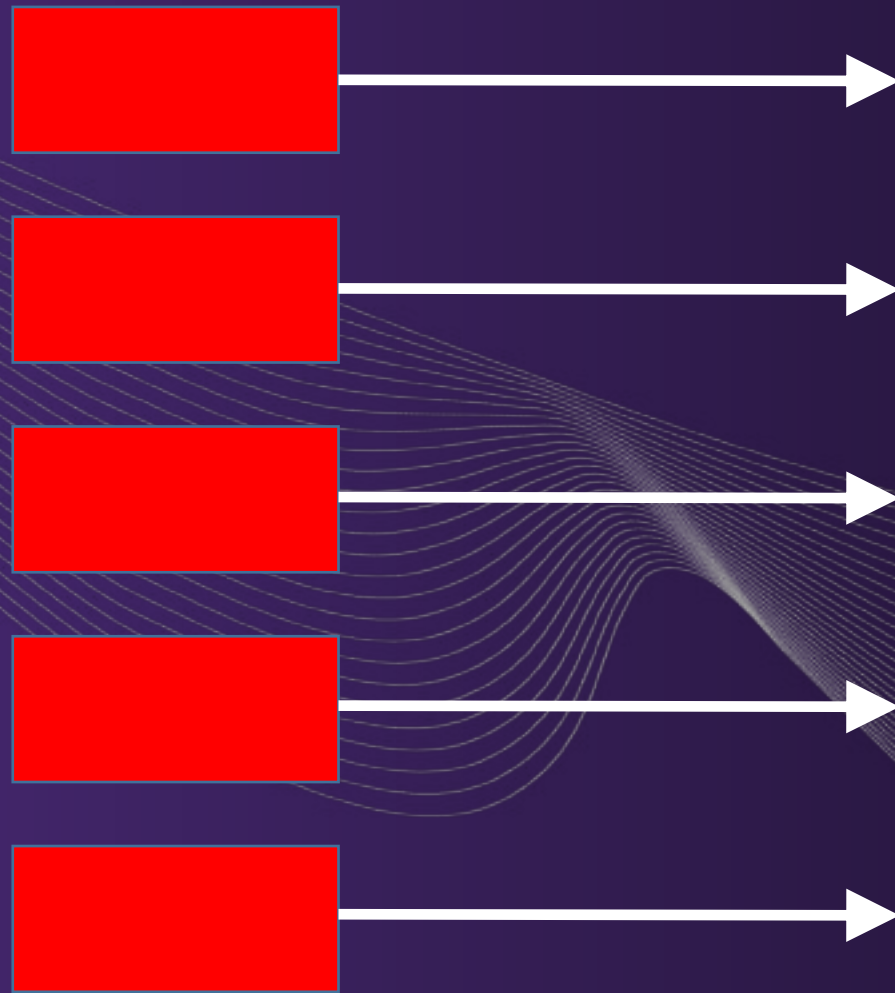


ALICE SIGNS THE TRANSACTION



SIGNED TRANSACTION NEEDS TO BE
FINALIZED: VALIDATED AND IMMUTABLE

VALIDATION AND STORAGE OF TRANSACTIONS





THE NETWORK

VALIDATION AND STORAGE
OF TRANSACTIONS?

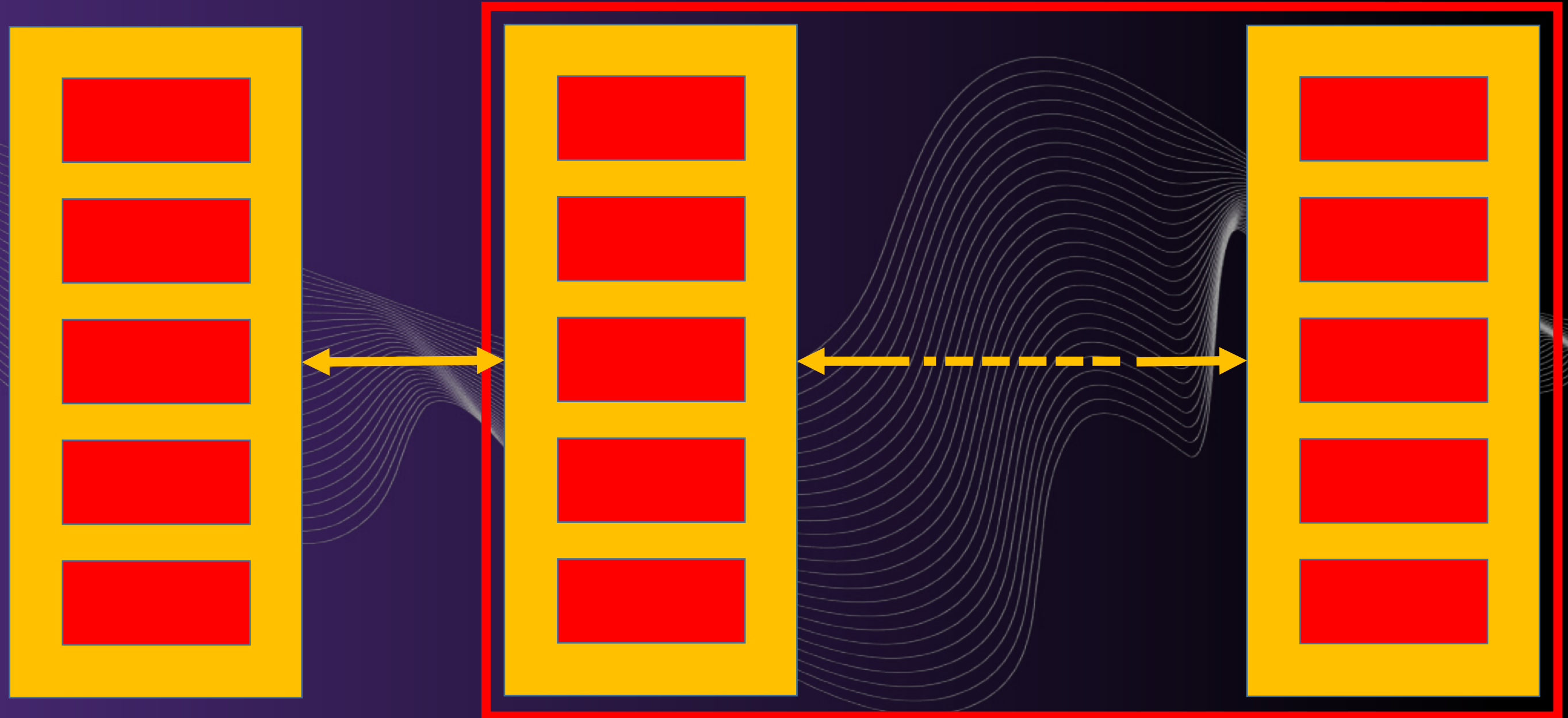
A diagram illustrating the flow of transactions from a network to a validator. On the right, a blue cloud contains the text 'THE NETWORK' and 'VALIDATION AND STORAGE OF TRANSACTIONS?'. Five white arrows point from the cloud to a vertical yellow rectangle on the left. Inside this rectangle are five red rectangles, representing a stack of transactions. The background is dark purple with faint white lines on the left and right sides.

THE NETWORK

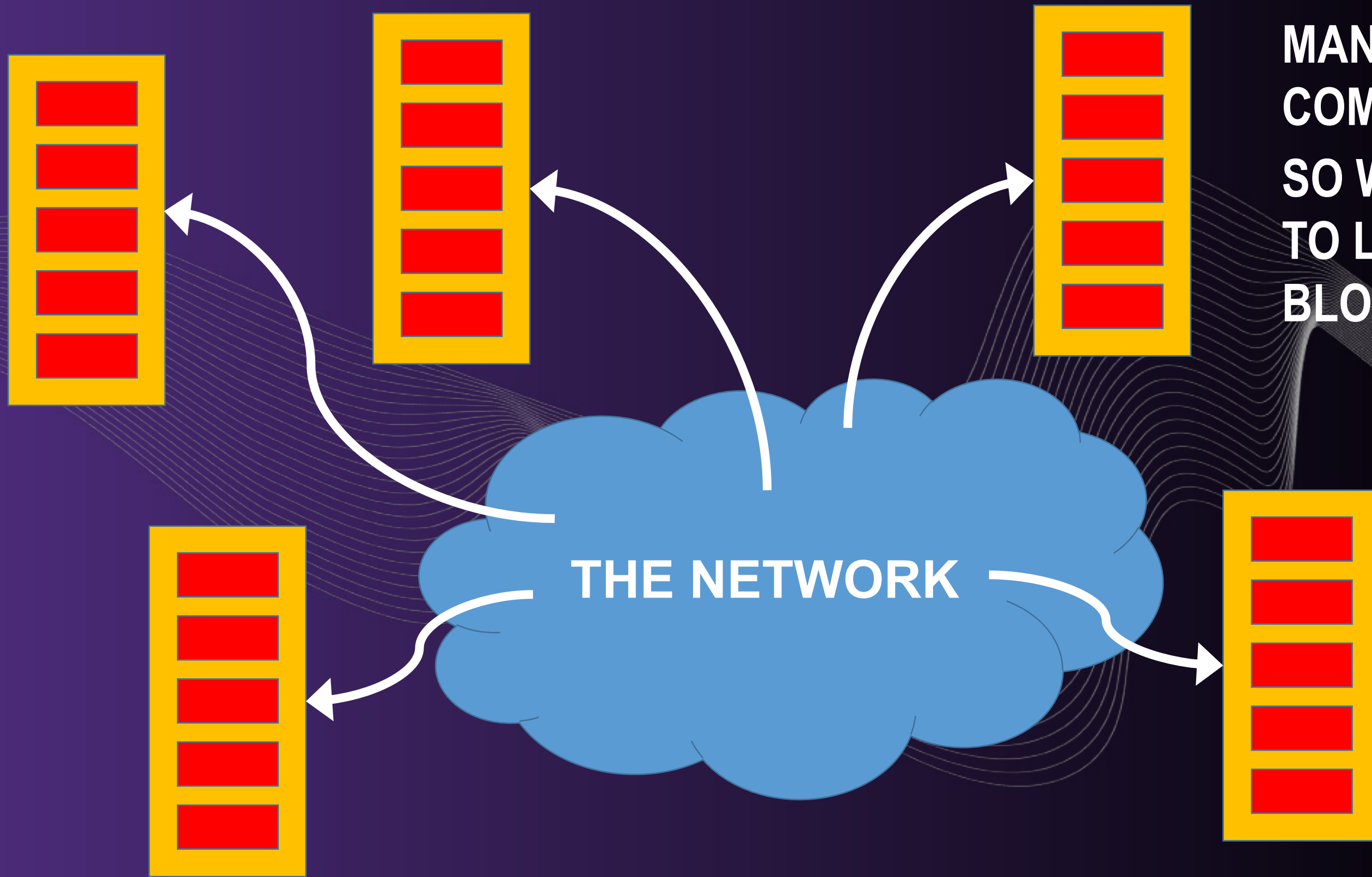
VALIDATION AND STORAGE
OF TRANSACTIONS?

VALIDATOR COLLECTS &
VALIDATES TRANSACTIONS

PUBLICLY ACCESSIBLE & DISTRIBUTED BLOCKS OF VALIDATED TRANSACTIONS



ATTEMPTS TO LINK TO
CURRENT BLOCK CHAIN

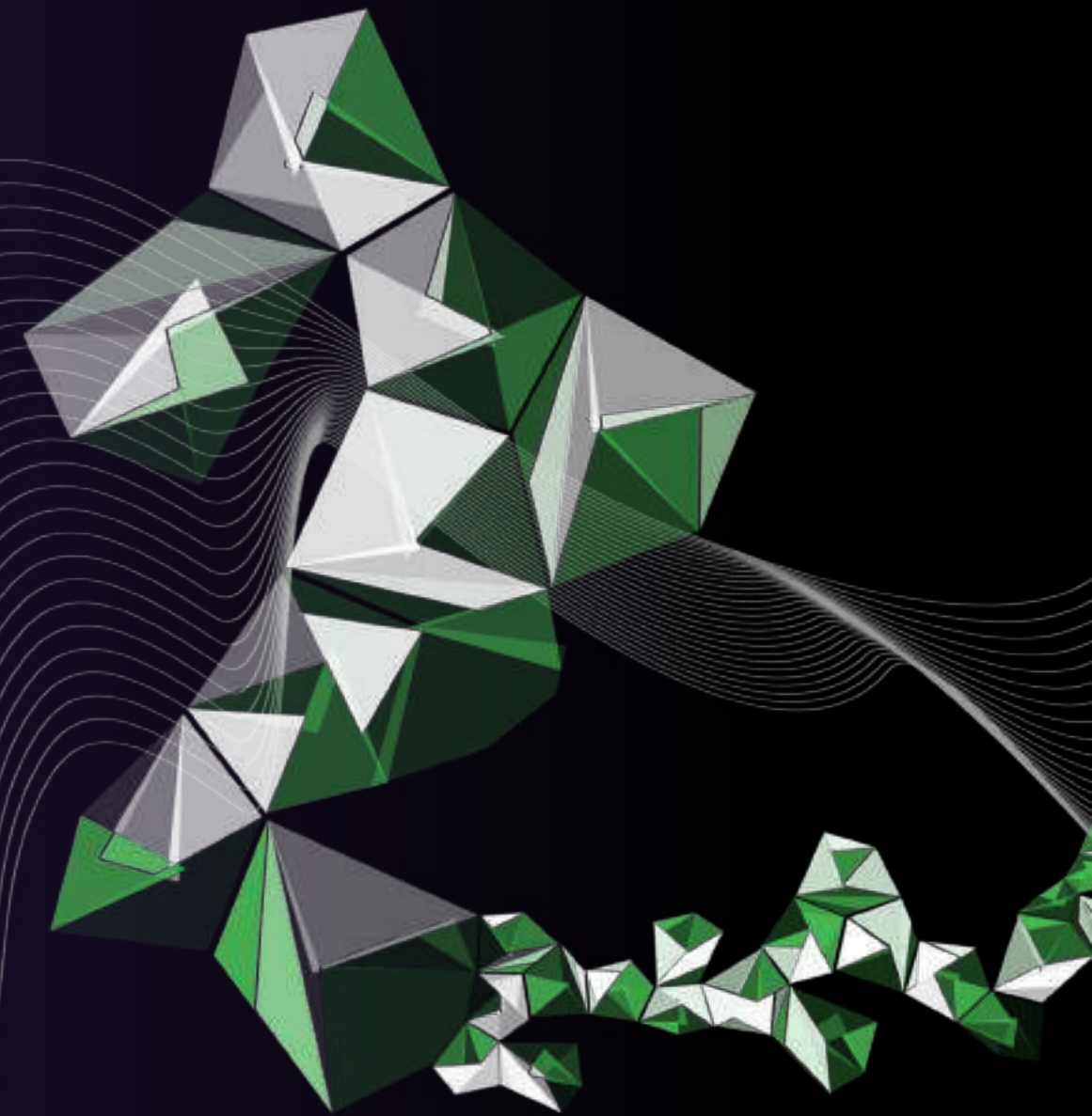


**MANY VALIDATORS
COMPETE.....
SO WHO'S ALLOWED
TO LINK TO THE
BLOCKCHAIN?**

WHAT DO WE MEAN BY CONSENSUS?

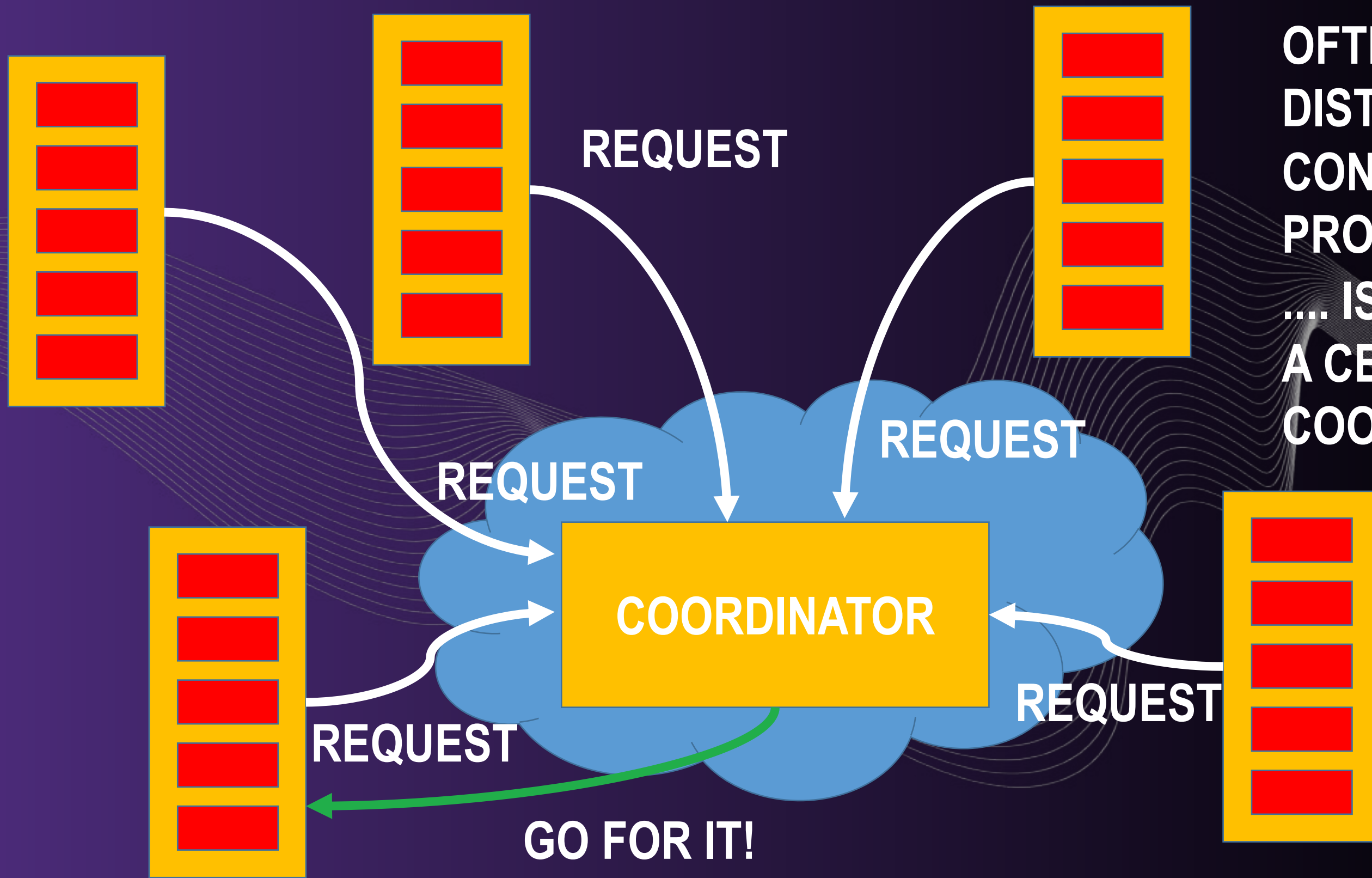
ALL CORRECTLY BEHAVING
VALIDATORS REACH AGREEMENT
ON WHICH BLOCK IS TO BE
APPENDED TO THE BLOCKCHAIN

DISTRIBUTED CONSENSUS PROTOCOLS



UNIVERSITY
OF TWENTE.

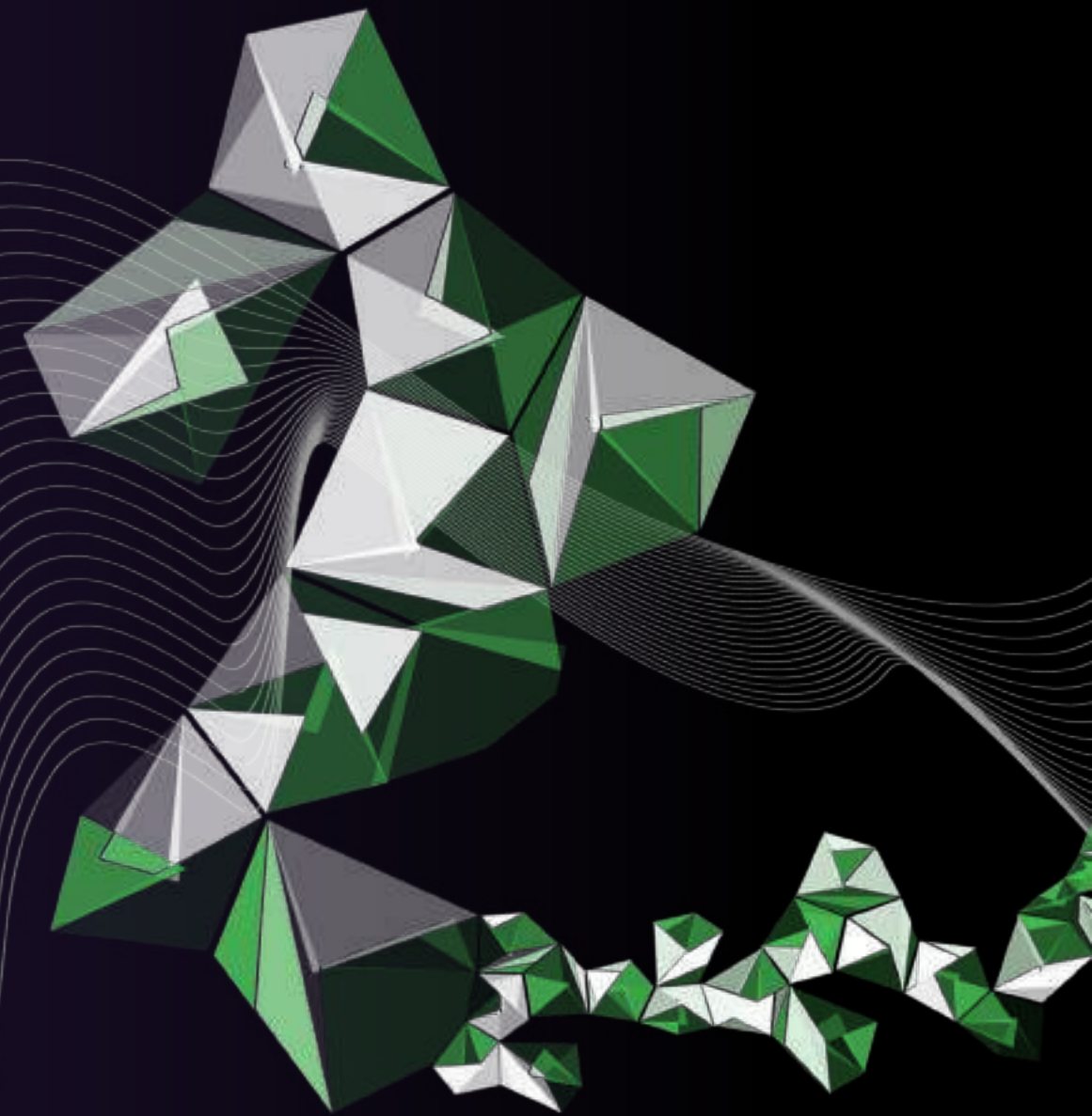
DIGITAL SOCIETY
INSTITUTE



OFTEN THE BEST
DISTRIBUTED
CONSENSUS
PROTOCOL....
... IS THE ONE WITH
A CENTRALIZED
COORDINATOR

REQUIREMENTS THAT HAVE BECOME PROMISES

1. HIGHLY SCALABLE
 - TRANSACTION PROCESSING CAPACITY
 - PARTICIPATING VALIDATORS
2. NO TRUSTED THIRD PARTY
3. COMPLETE CONSENSUS AMONG CORRECTLY BEHAVING VALIDATORS

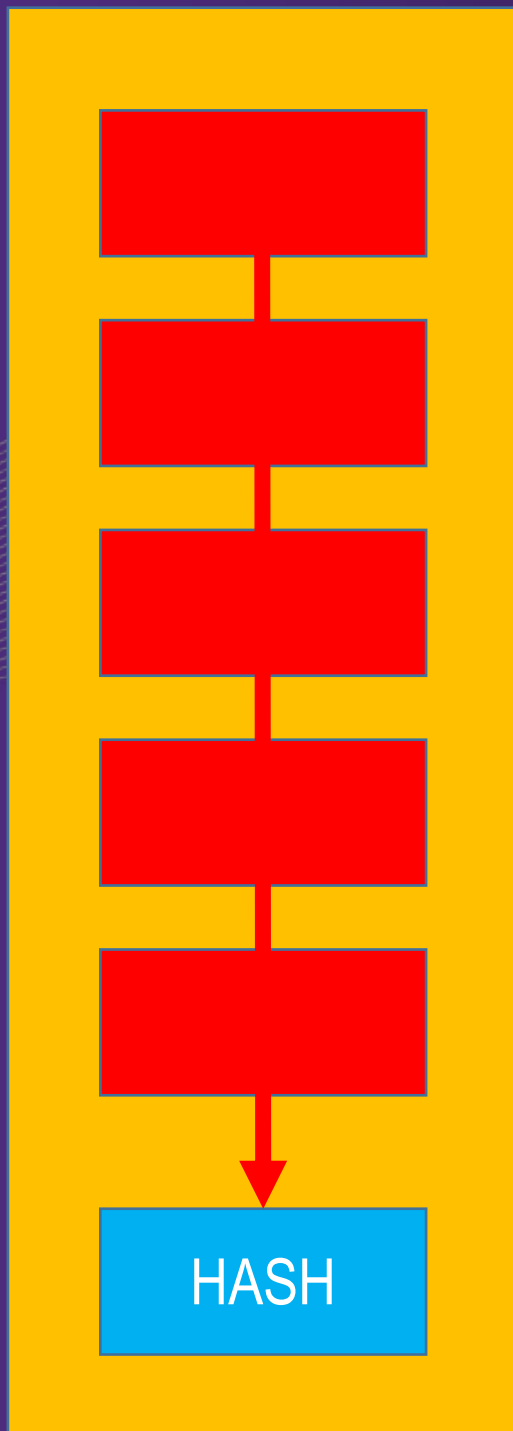




PROTOCOLS BASED ON RACING

UNIVERSITY
OF TWENTE.

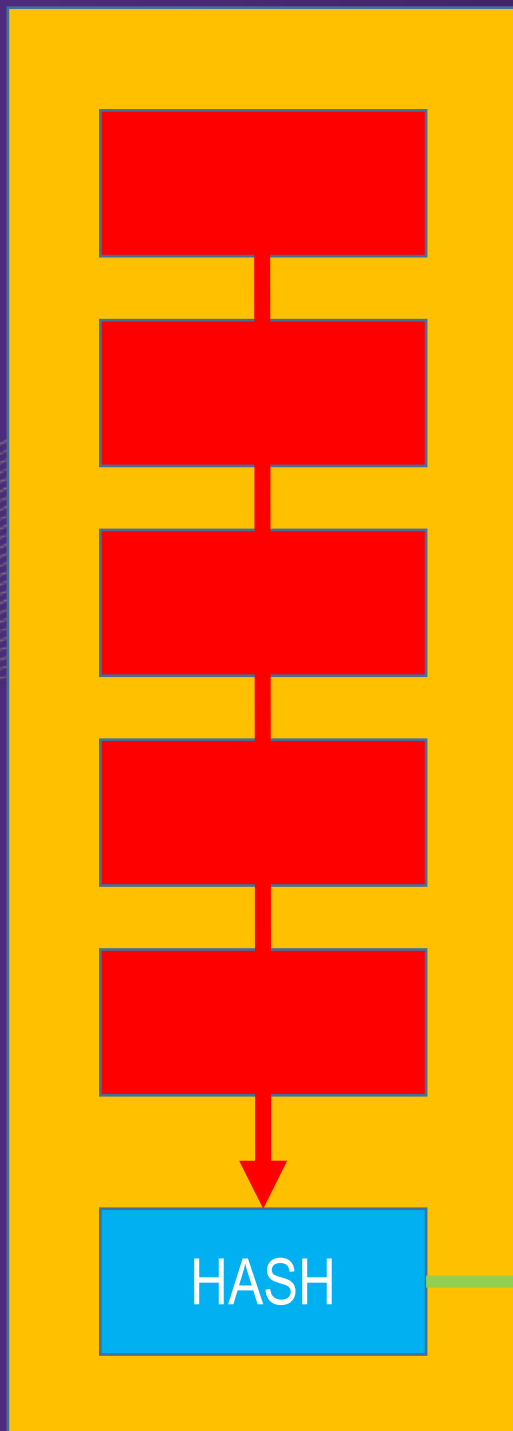
DIGITAL SOCIETY
INSTITUTE



COMPUTATIONALLY EASY



COMPUTATIONALLY HARD
(BRUTE FORCE NEEDED)



HASH



N

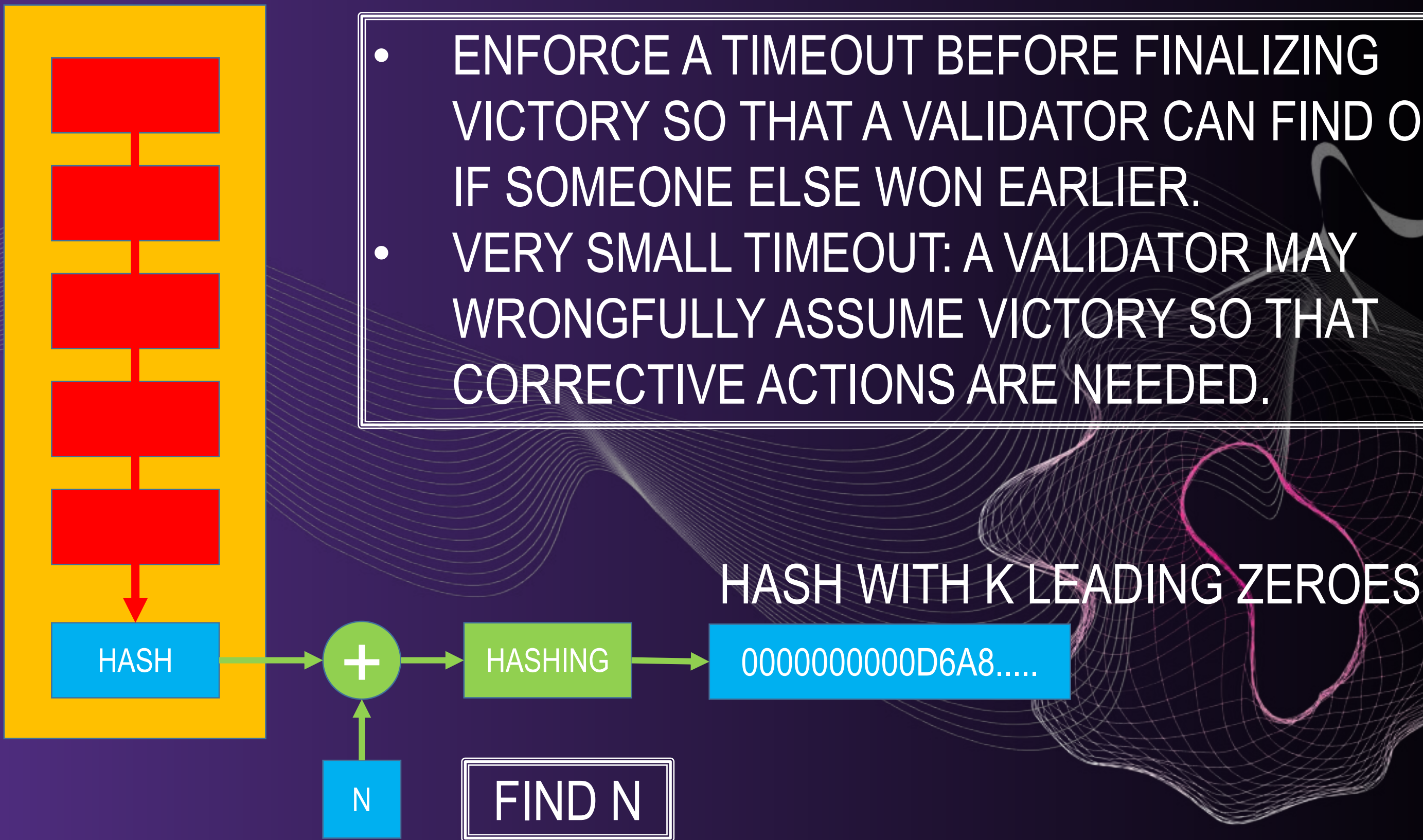
HASHING

FIND N

0000000000D6A8.....

HASH WITH K LEADING ZEROES

- ENFORCE A TIMEOUT BEFORE FINALIZING VICTORY SO THAT A VALIDATOR CAN FIND OUT IF SOMEONE ELSE WON EARLIER.
- VERY SMALL TIMEOUT: A VALIDATOR MAY WRONGFULLY ASSUME VICTORY SO THAT CORRECTIVE ACTIONS ARE NEEDED.

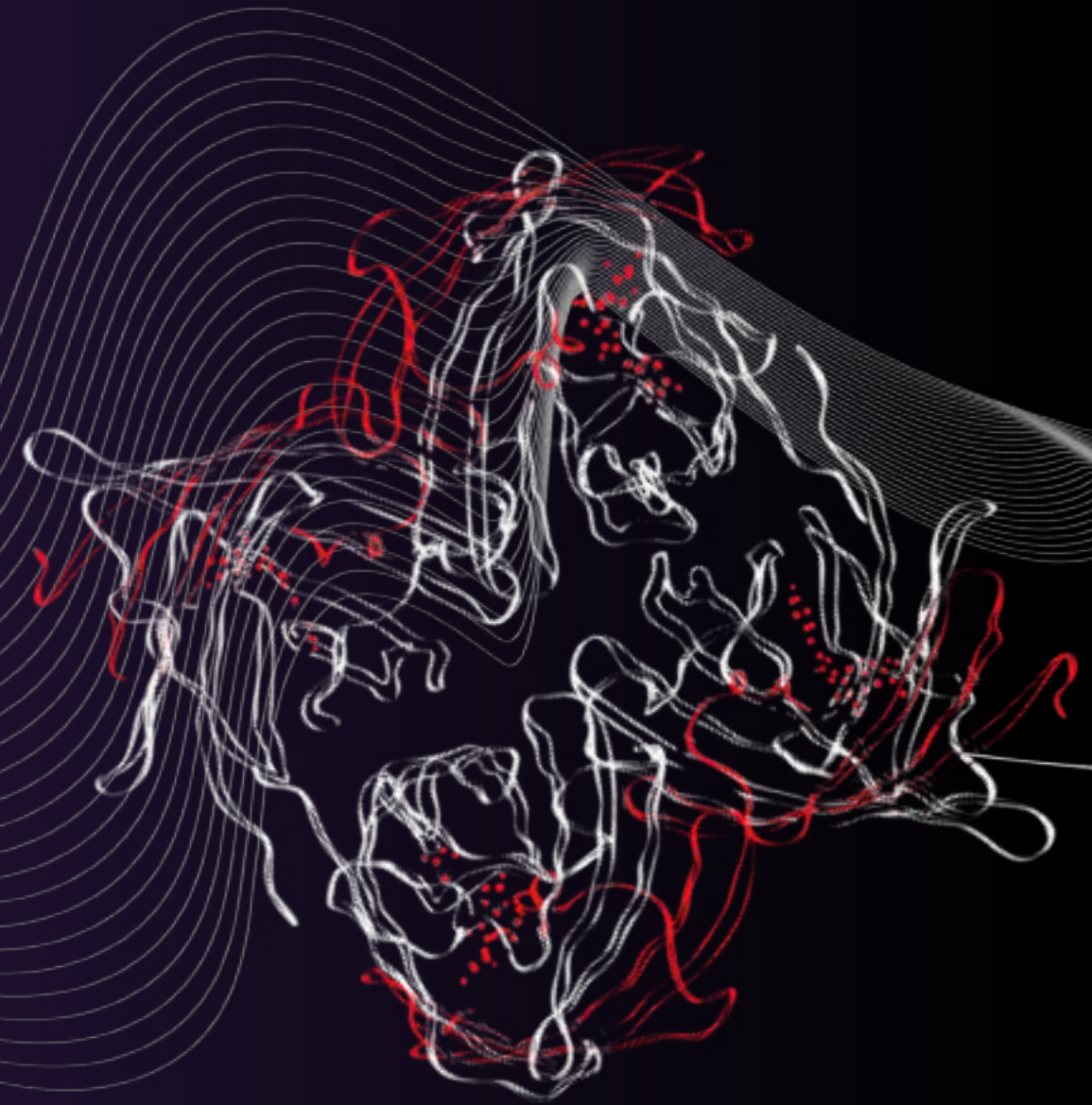


BOTTOM LINE

WE SHOULD CHALLENGE THE QUALITY OF HAVING **COMPUTATIONAL RACES** AS A DESIGN PRINCIPLE FOR BLOCKCHAINS:

- THEY WASTE ENERGY FOR THE SAKE OF RACING
- THEY INHERENTLY INCUR SCALABILITY PROBLEMS FOR TRANSACTION PROCESSING CAPACITY

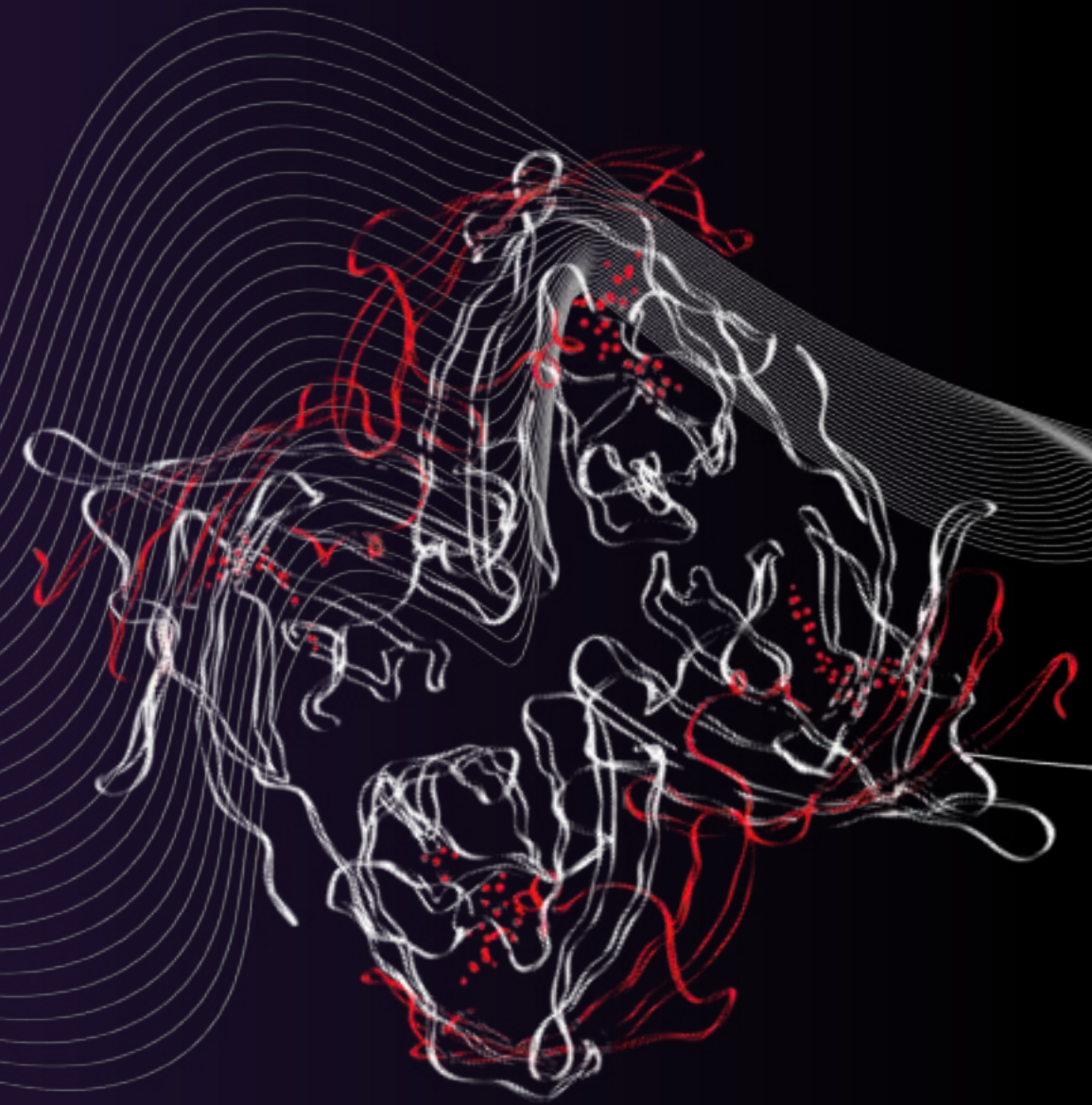
PROTOCOLS BASED ON TALKING



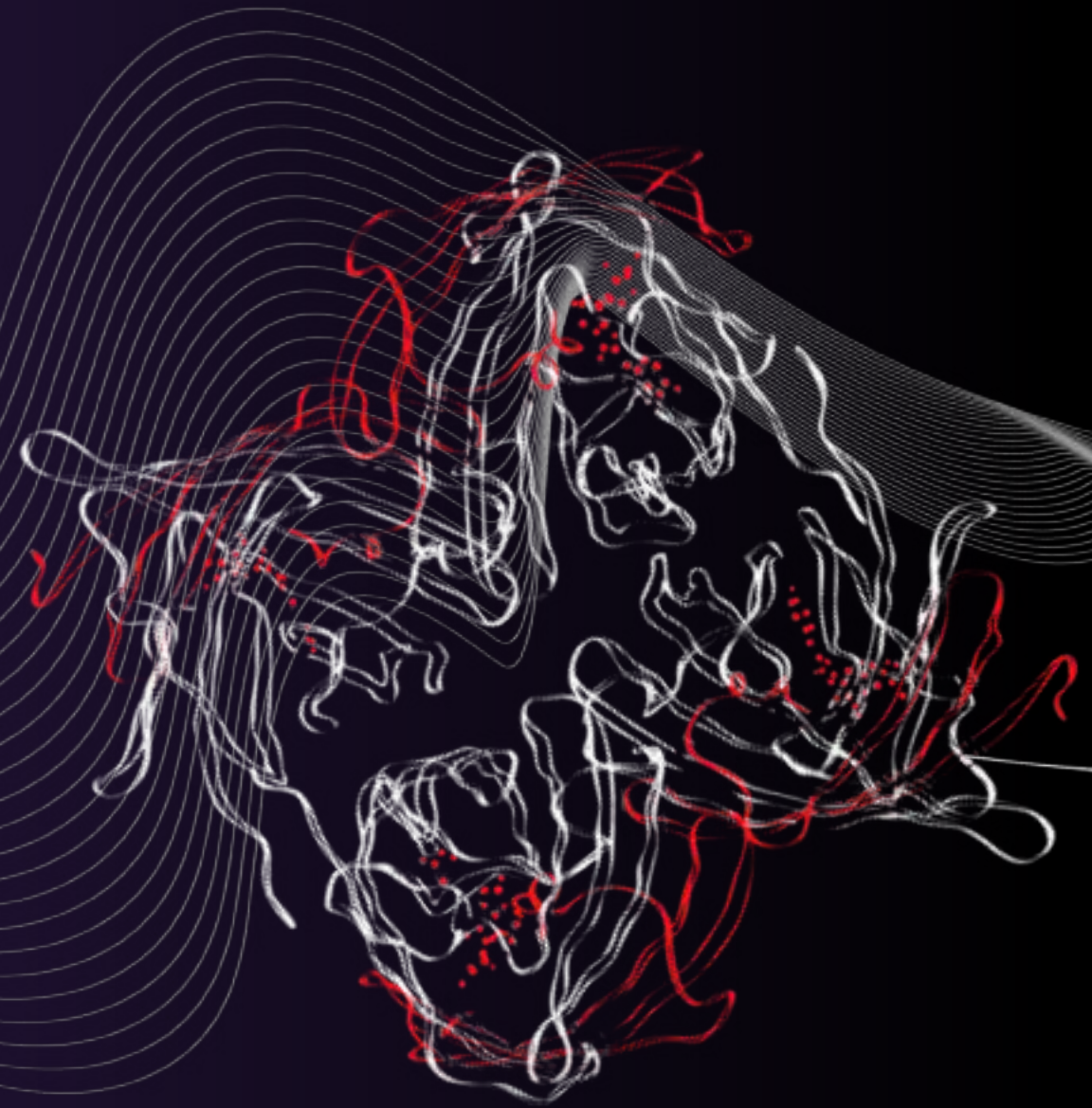
UNIVERSITY
OF TWENTE.

DIGITAL SOCIETY
INSTITUTE

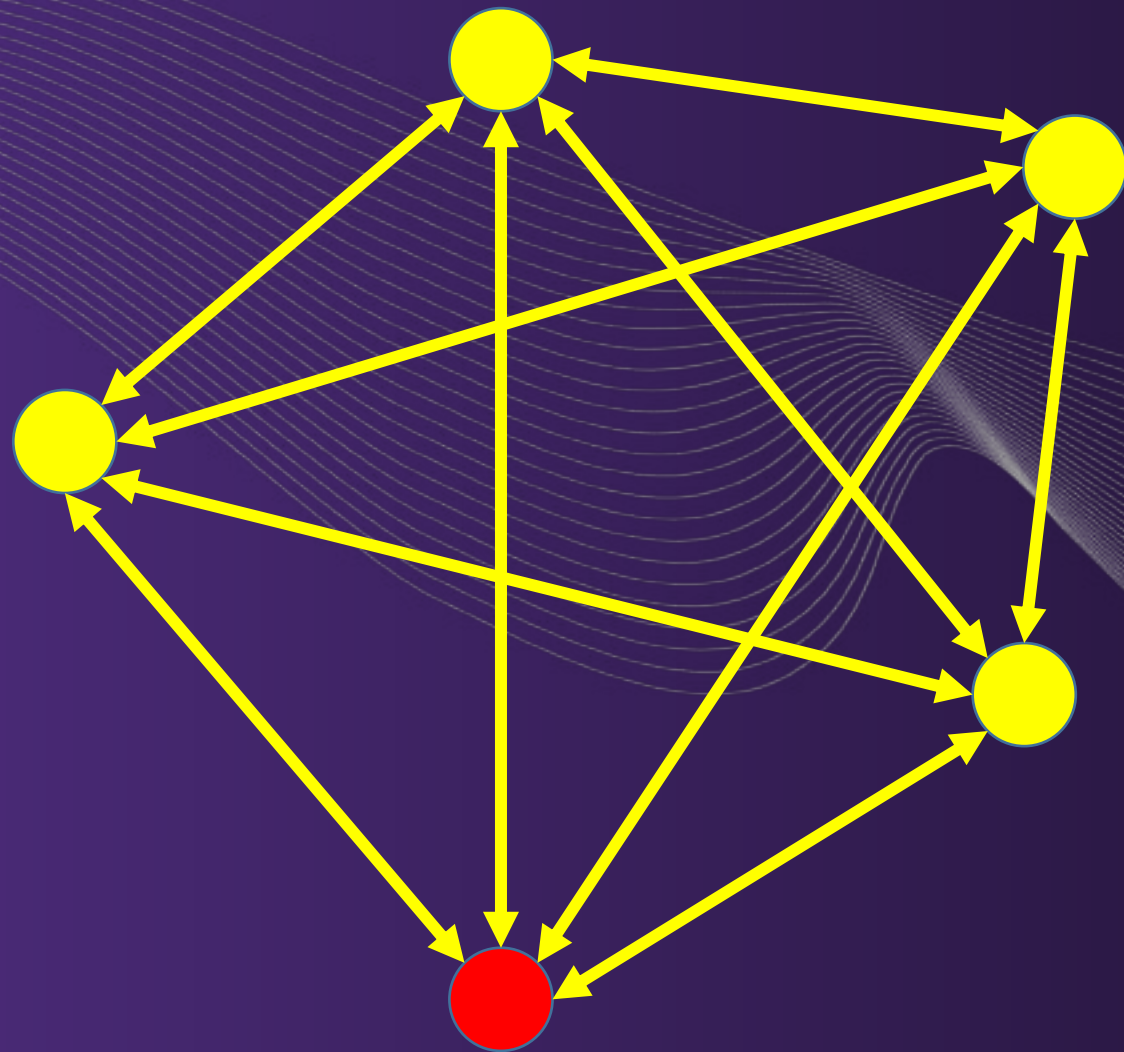
FLOODING CONSENSUS



FLOODING CONSENSUS



FLOODING CONSENSUS

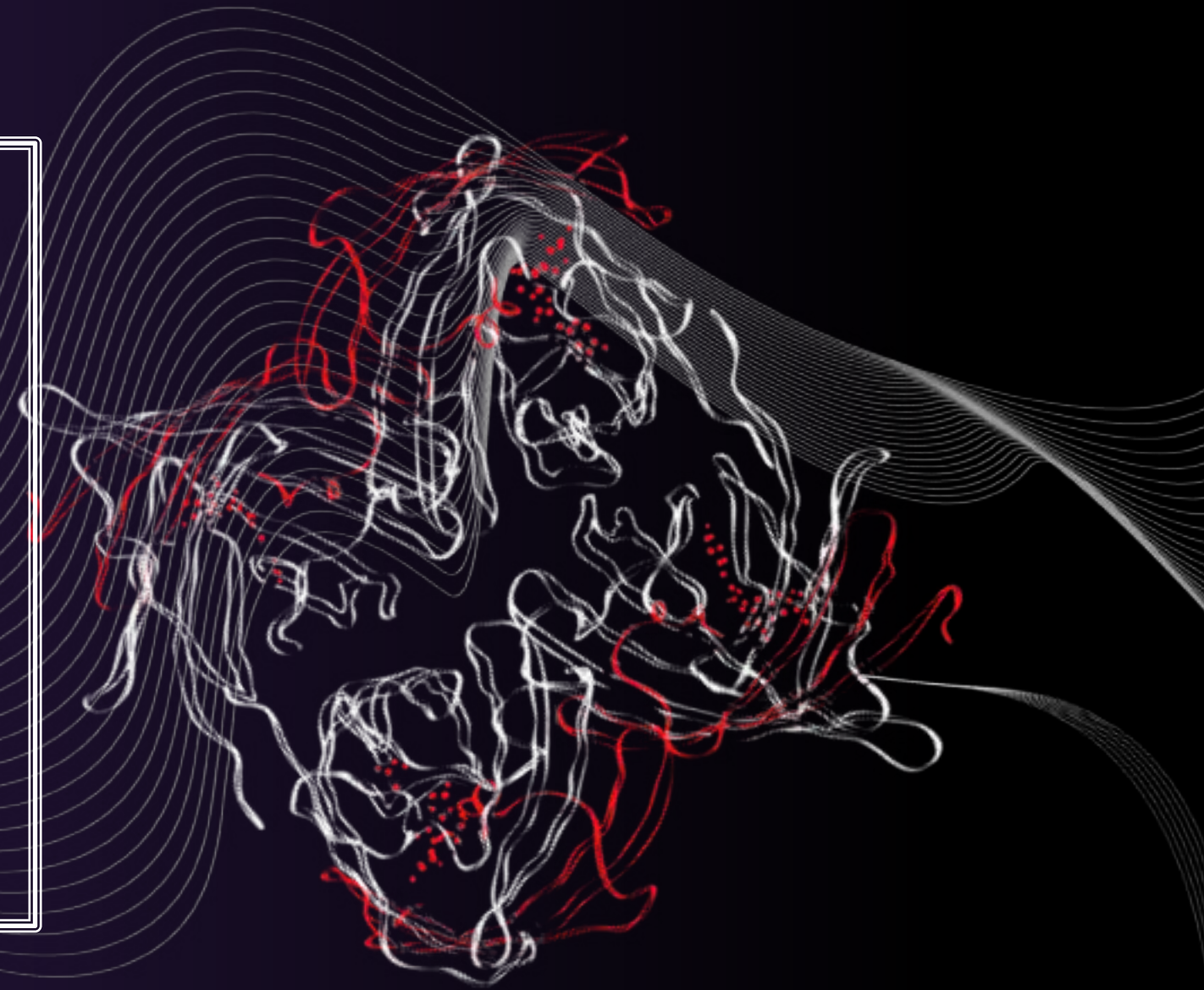


- NODES NEED TO BE TRUSTED
- CLOSED GROUP
- (FAILURES CAN BE HANDLED)



NODES NEED TO BE TRUSTED?

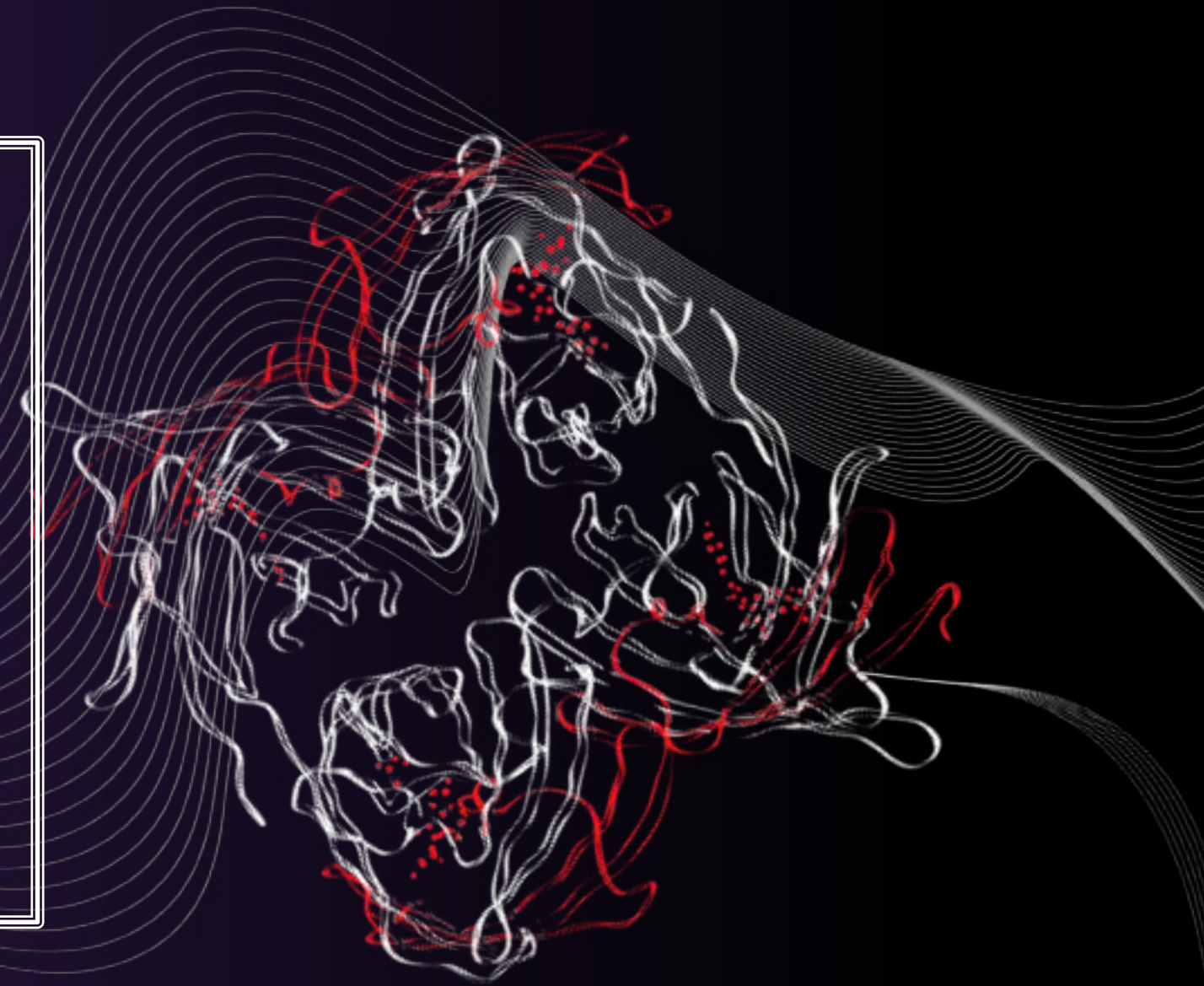
- WE NEED $2f + 1$ NODES TO TOLERATE f **CRASHING** VALIDATORS
- WE NEED $3f + 1$ NODES IF FAULTY VALIDATORS CAN PRODUCE **ARBITRARY** RESULTS (WHICH MAY GO UNDETECTED)



TALKING-BASED PROTOCOLS

- CLOSED GROUP
- SCALES IN THROUGHPUT
- DOES NOT SCALE IN NUMBER OF VALIDATORS
- HIGHLY FAULT-TOLERANT SOLUTION

CONSENSUS-AS-A-SERVICE



BOTTOM LINE

WE SHOULD CHALLENGE THE QUALITY OF HAVING **CONSENSUS-AS-A-SERVICE** AS A DESIGN PRINCIPLE FOR BLOCKCHAINS:

- THE SERVICE IS CENTRALIZED, LOGICALLY AS WELL AS PHYSICALLY
- THE SERVICE NEEDS TO BE TRUSTED

WORK TO DO

An abstract graphic featuring a series of white, wavy lines that flow from the left side of the frame towards the right. On the right side, these lines converge and form a complex, branching structure resembling a tree or a network of connections. The branches are rendered in a mix of white and orange colors, creating a sense of depth and movement. The background is a dark, solid color, which makes the white and orange elements stand out prominently.

UNIVERSITY
OF TWENTE.

DIGITAL SOCIETY
INSTITUTE

- Consensus in the age of blockchains
Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S. and Danezis, G.
arXiv preprint arXiv:1711.03936, 2017
- A consensus taxonomy in the blockchain era
Garay, Juan, and Aggelos Kiayias.
Cryptographers' Track at the RSA Conference, pp. 284-318. Springer, Cham, 2020.
- Distributed Systems book
H1, H7.2, H8.2, H9.1
- Essence: if reaching consensus is such a big issue, what would be good reasons to go for blockchains, and under which assumptions?