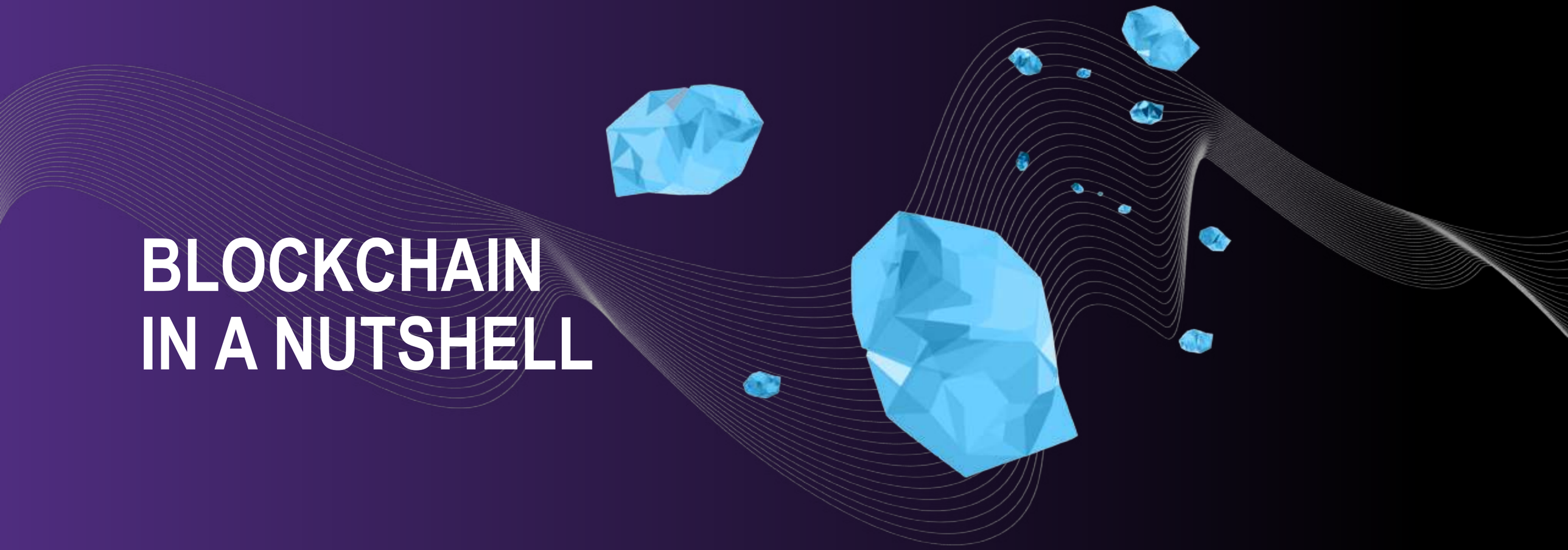
# BLOCKCHAIN IN A NUTSHELL



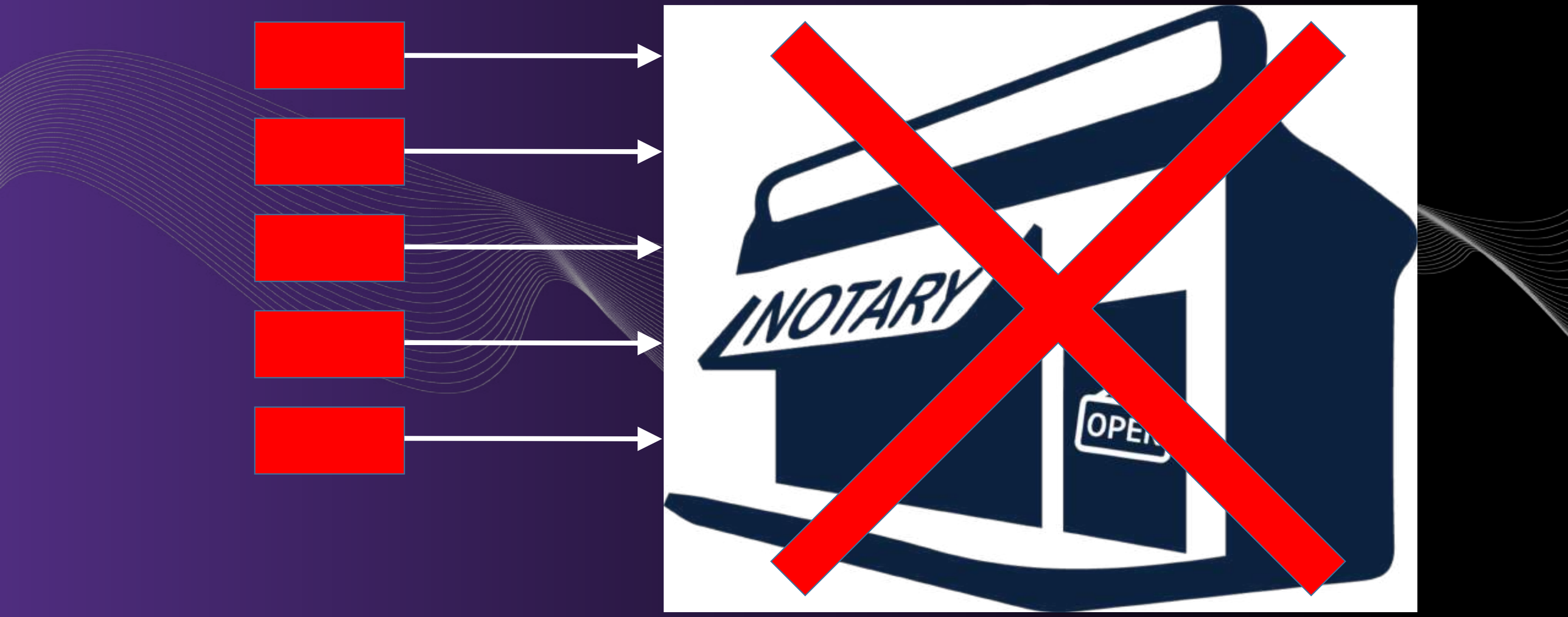
UNIVERSITY OF TWENTE. | DIGITAL SOCIETY INSTITUTE

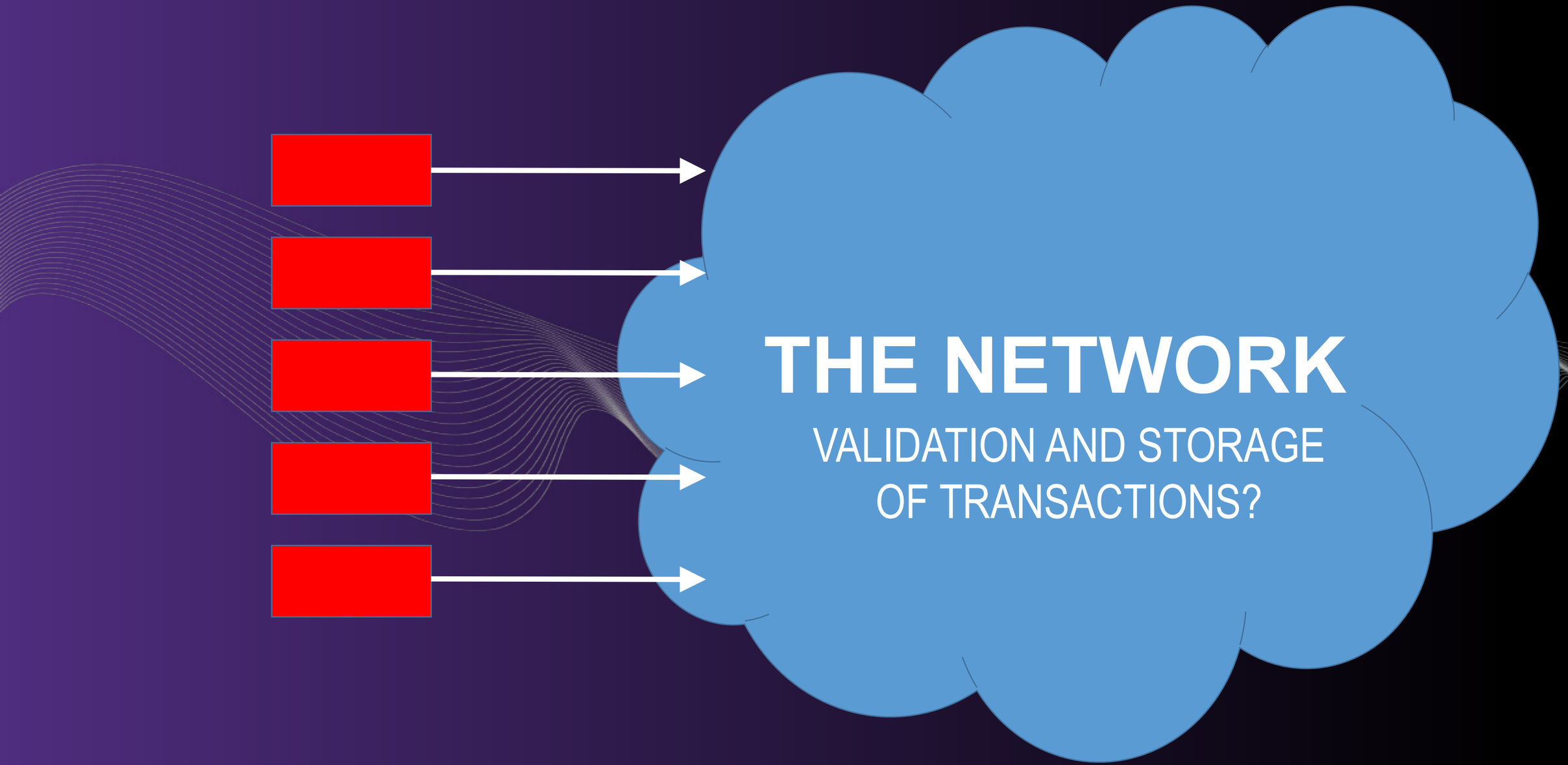
ALICE CREATES A TRANSACTION

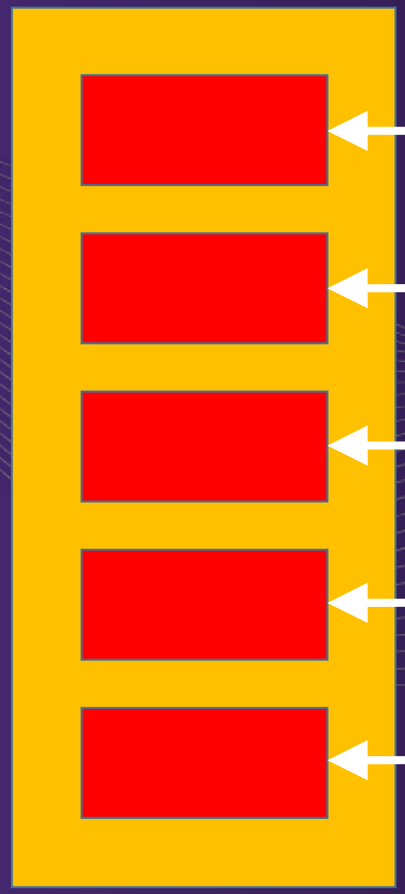
ALICE SIGNS THE TRANSACTION

SIGNED TRANSACTION NEEDS TO BE FINALIZED: VALIDATED AND IMMUTABLE

# VALIDATION AND STORAGE OF TRANSACTIONS




THE NETWORK
VALIDATION AND STORAGE
OF TRANSACTIONS?

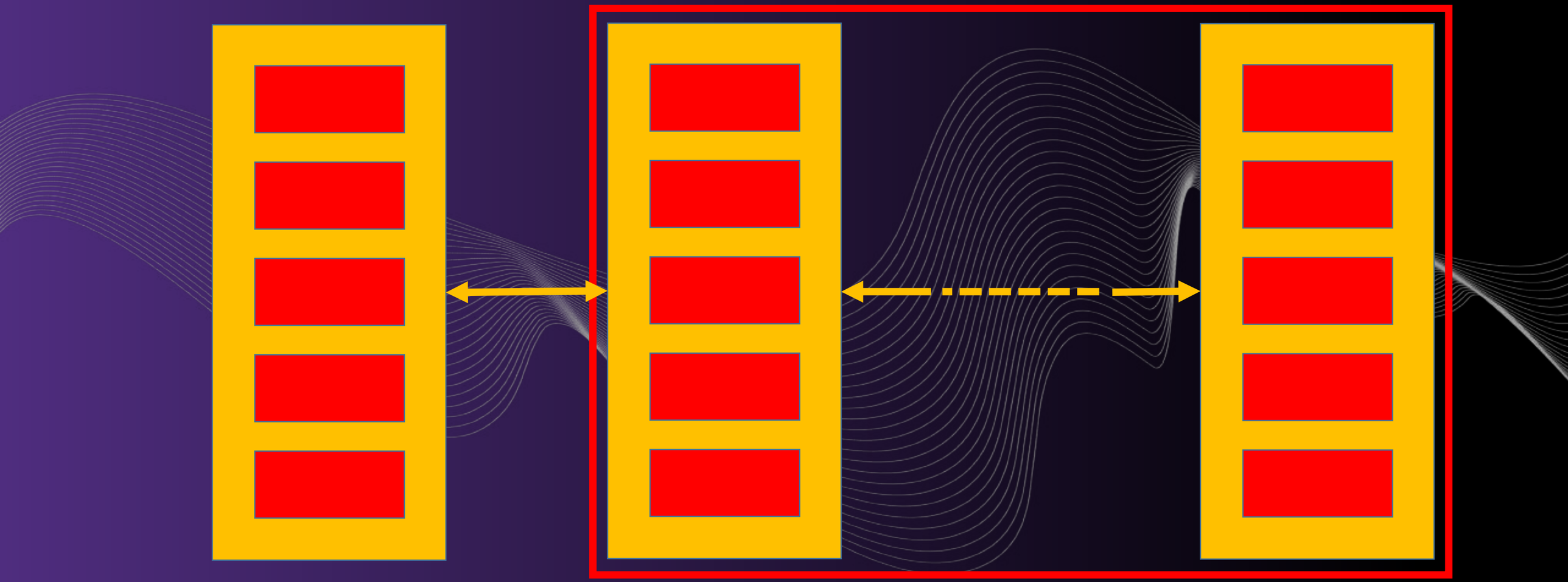


VALIDATOR COLLECTS &
VALIDATES TRANSACTIONS

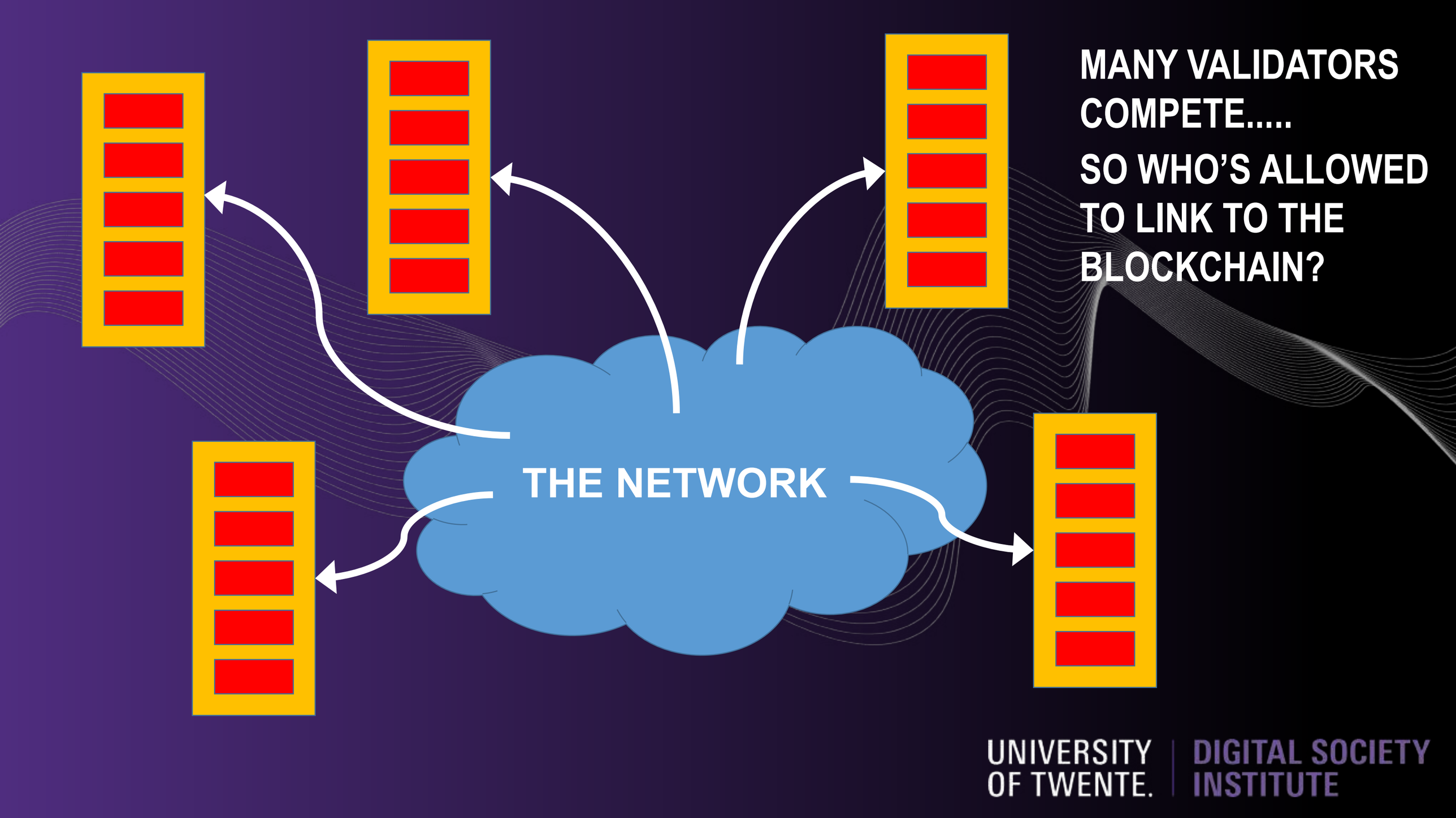
# THE NETWORK

VALIDATION AND STORAGE
OF TRANSACTIONS?

PUBLICLY ACCESSIBLE & DISTRIBUTED
BLOCKS OF VALIDATED TRANSACTIONS



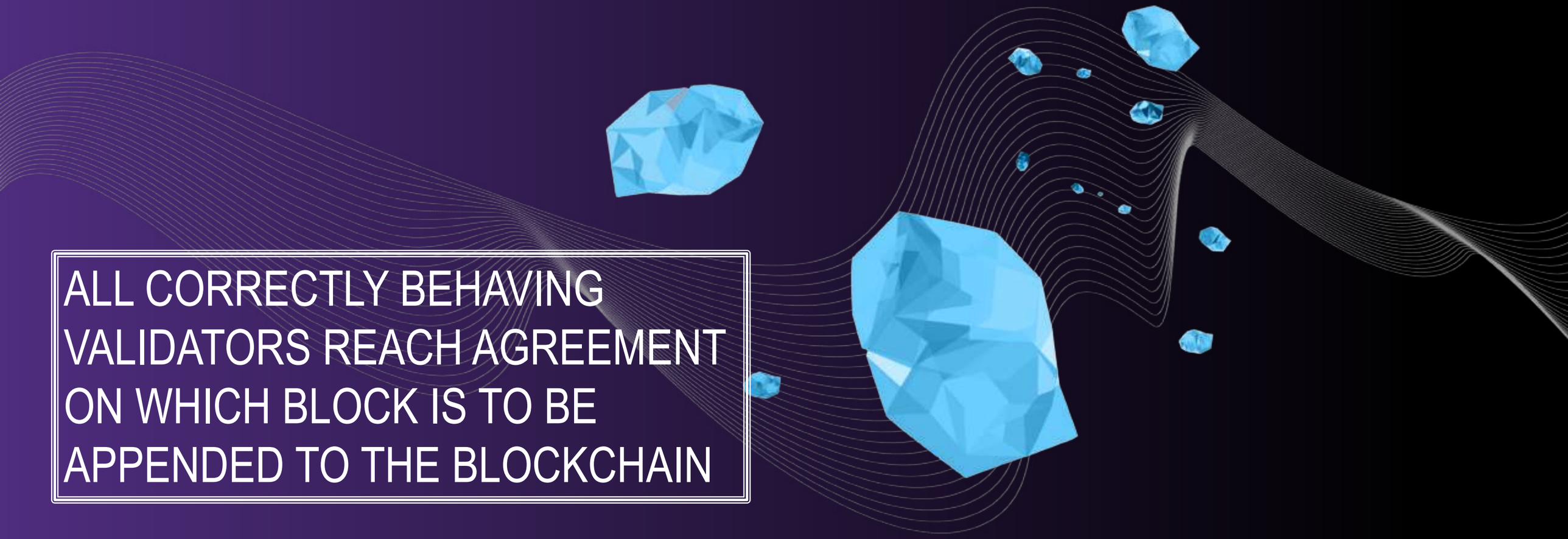
ATTEMPTS TO LINK TO
CURRENT BLOCK CHAIN




MANY VALIDATORS COMPETE.....

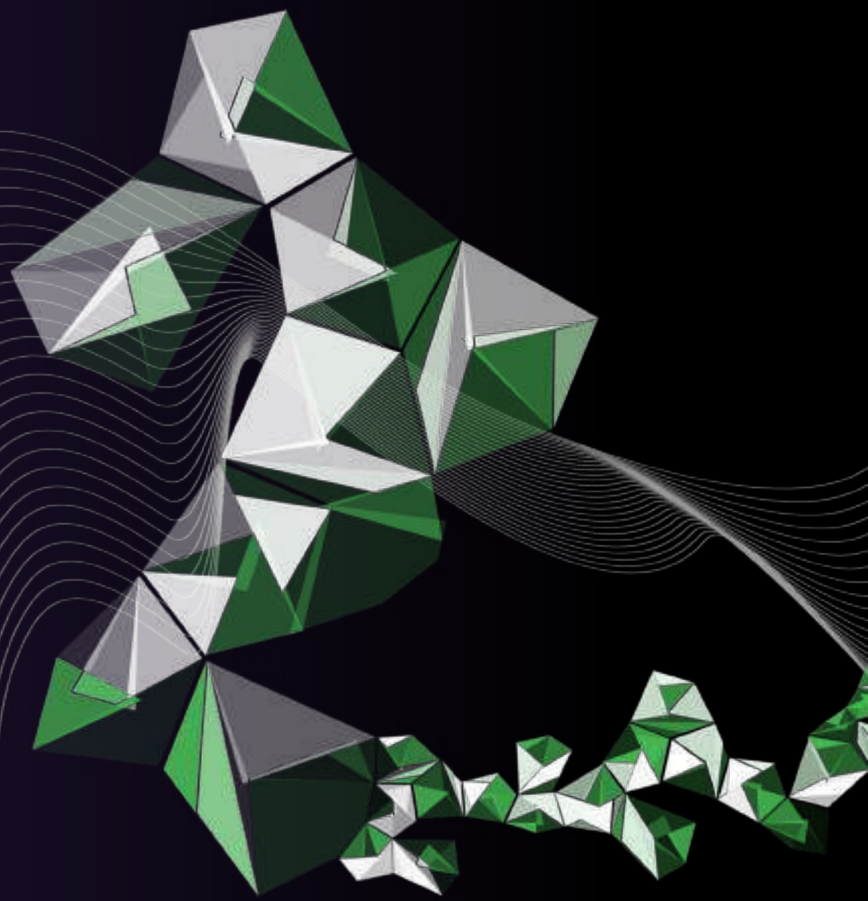
SO WHO'S ALLOWED TO LINK TO THE BLOCKCHAIN?

# WHAT DO WE MEAN BY CONSENSUS?

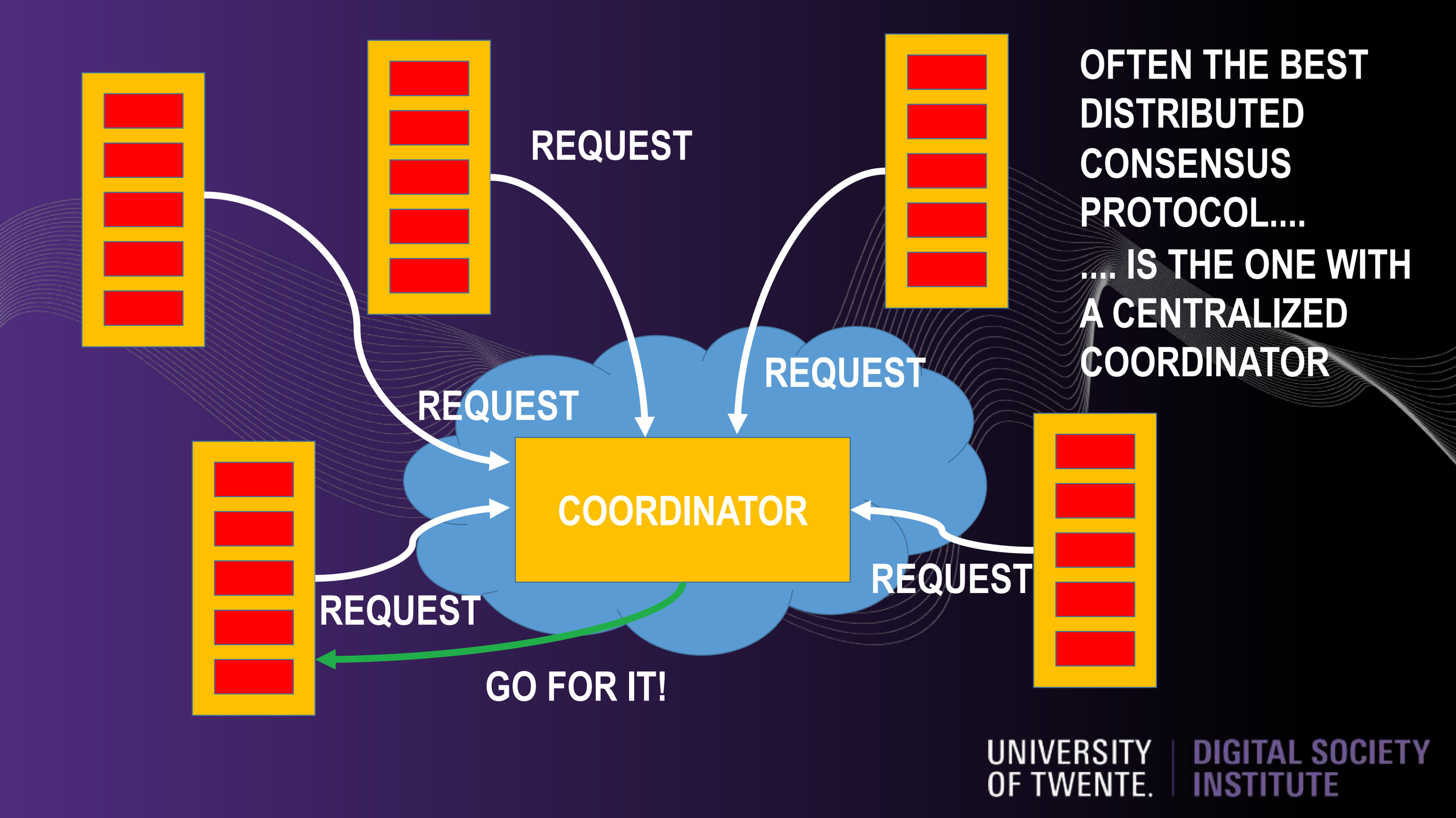


ALL CORRECTLY BEHAVING VALIDATORS REACH AGREEMENT ON WHICH BLOCK IS TO BE APPENDED TO THE BLOCKCHAIN

# DISTRIBUTED CONSENSUS PROTOCOLS

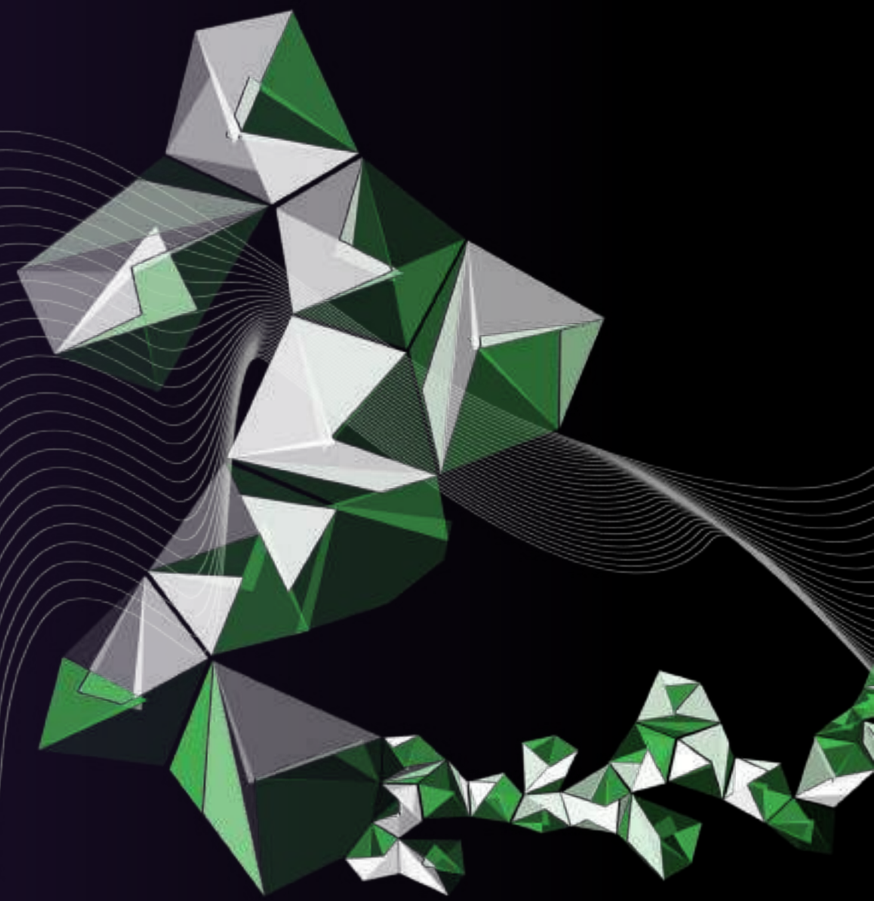


UNIVERSITY OF TWENTE. | DIGITAL SOCIETY INSTITUTE




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

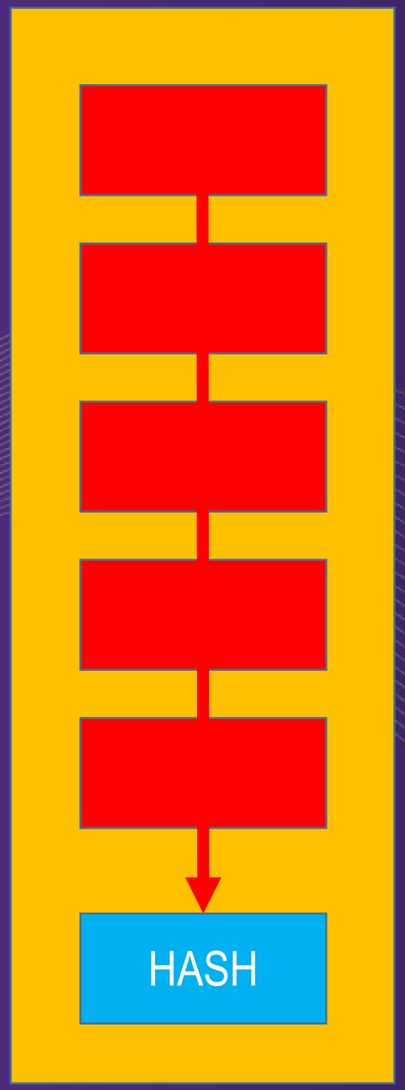
# REQUIREMENTS THAT HAVE BECOME PROMISES



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

# PROTOCOLS BASED ON RACING

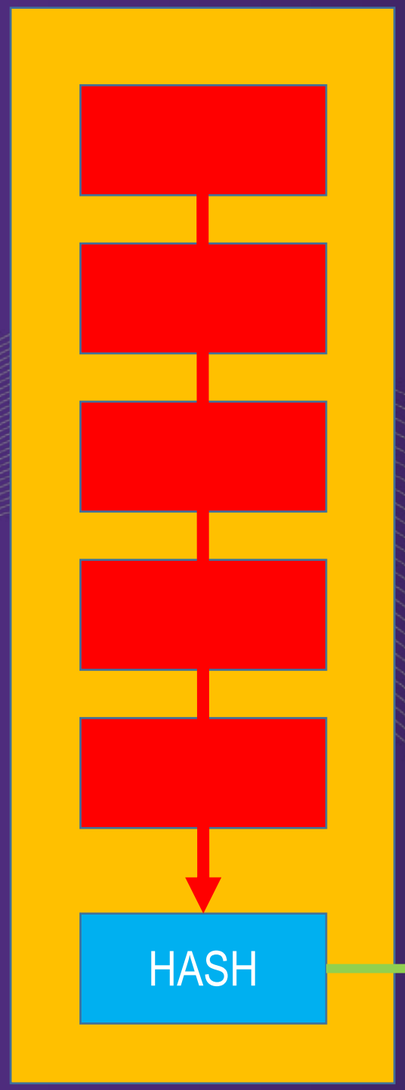
UNIVERSITY OF TWENTE. | DIGITAL SOCIETY INSTITUTE




COMPUTATIONALLY EASY

INPUT → HASHING → HASH

COMPUTATIONALLY HARD
(BRUTE FORCE NEEDED)



HASH

+

HASHING

HASH WITH K LEADING ZEROES

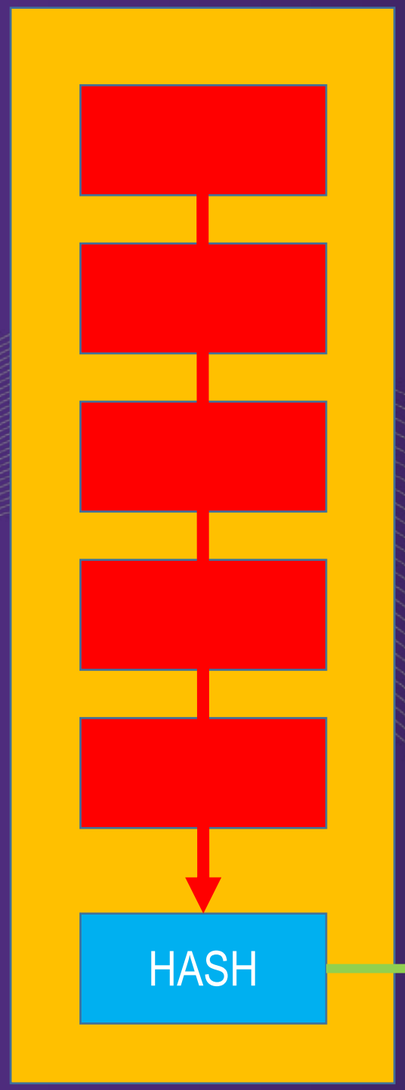
0000000000D6A8.....

N

FIND N

UNIVERSITY OF TWENTE. | DIGITAL SOCIETY INSTITUTE

- 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.




HASH WITH K LEADING ZEROES

FIND N

# 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



UNIVERSITY OF TWENTE. | DIGITAL SOCIETY INSTITUTE

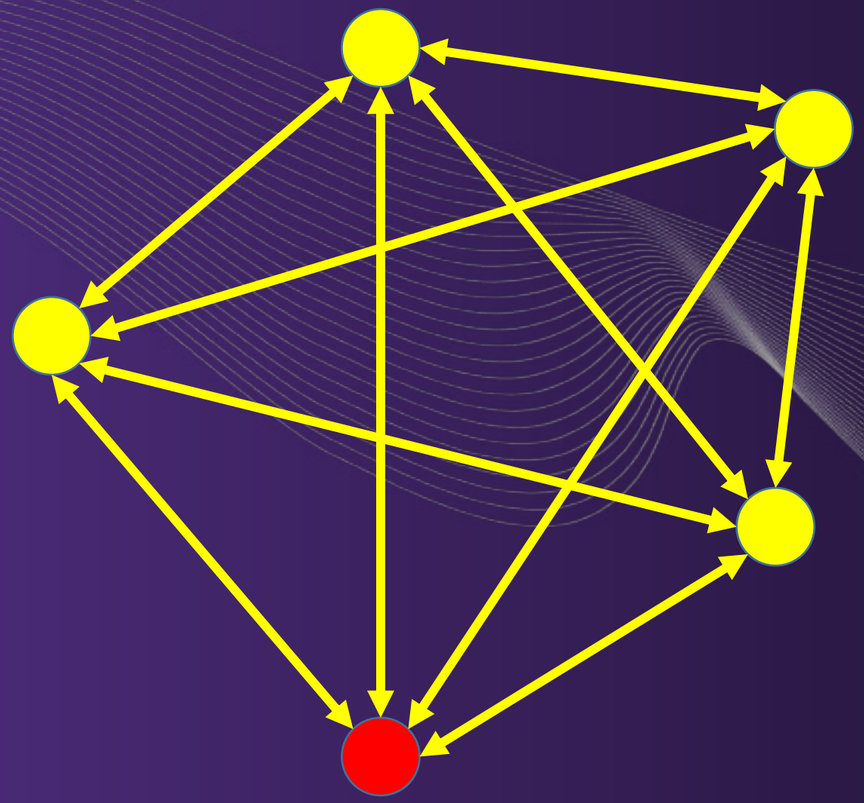
# FLOODING CONSENSUS



UNIVERSITY OF TWENTE. | DIGITAL SOCIETY INSTITUTE

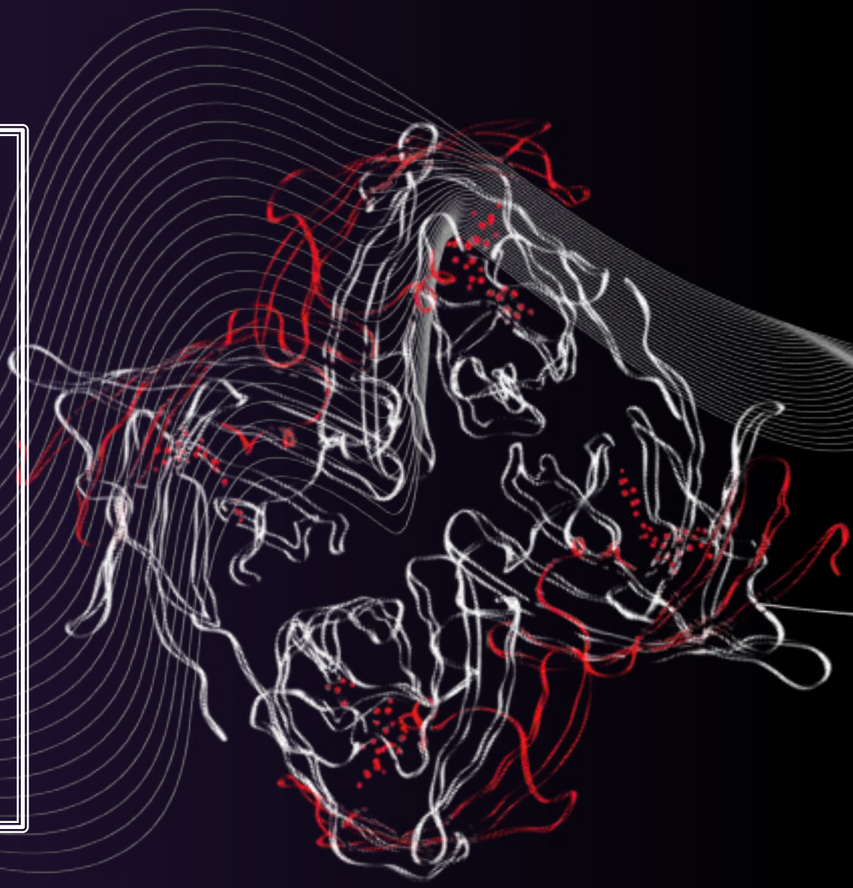
# FLOODING CONSENSUS

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



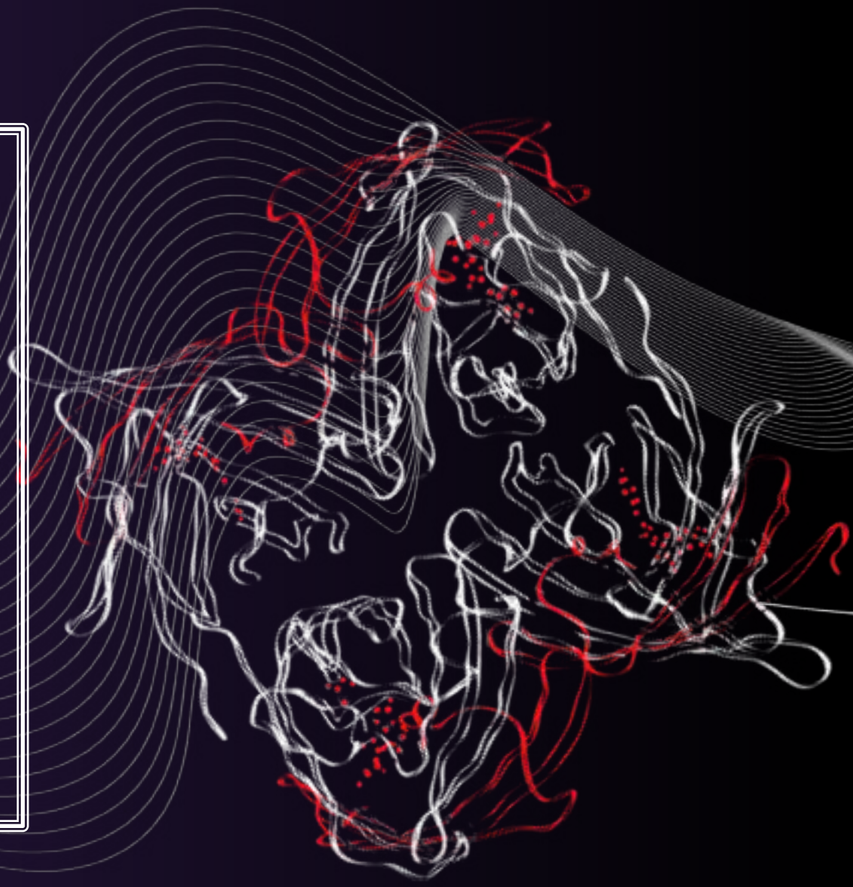
# NODES NEED TO BE TRUSTED?

- 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

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?