“ZILLIQA /'ZILIKə/ ”

NEXT GEN HIGH-THROUGHPUT BLOCKCHAIN PLATFORM

DONG XINSHU, CEO

JIA YAOQI, BLOCKCHAIN ARCHITECT

“

SCALABILITY

OF PUBLIC BLOCKCHAIN

”

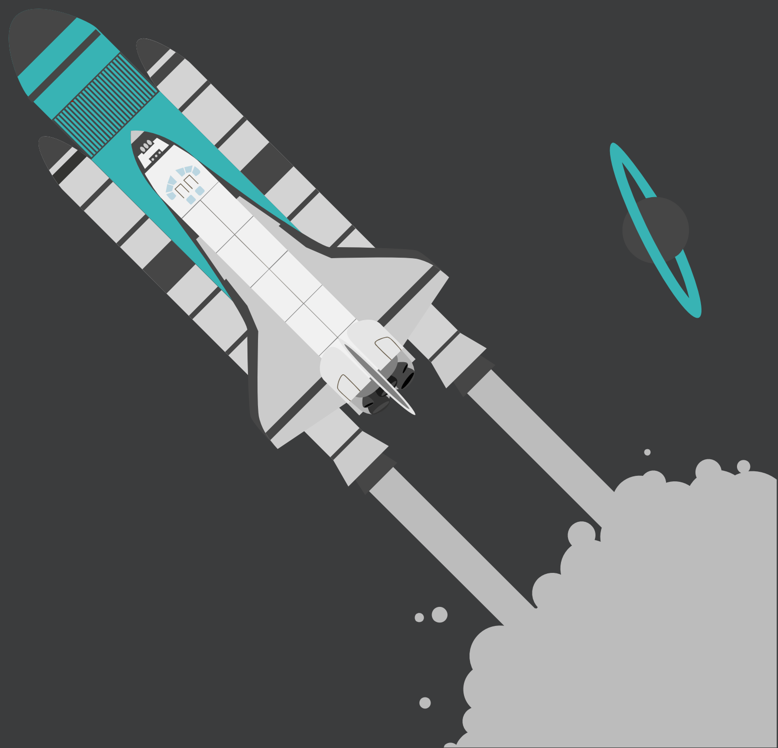
@ZILLIQA ZILLIQA.COM

BITCOIN
7 TX/S

ETHEREUM
10 TX/S

VISA
8000 TX/S

“SOME EXISTING SOLUTIONS”



“INCREASING BLOCK SIZE?”

NOT A 100X SCALING FACTOR, DUE TO COMPUTATIONAL AND BANDWIDTH LIMITATIONS

“ OFF-CHAIN TRANSACTIONS ”

Lightning Network

Scalable, Instant Bitcoin/Blockchain Transactions

Raiden Network

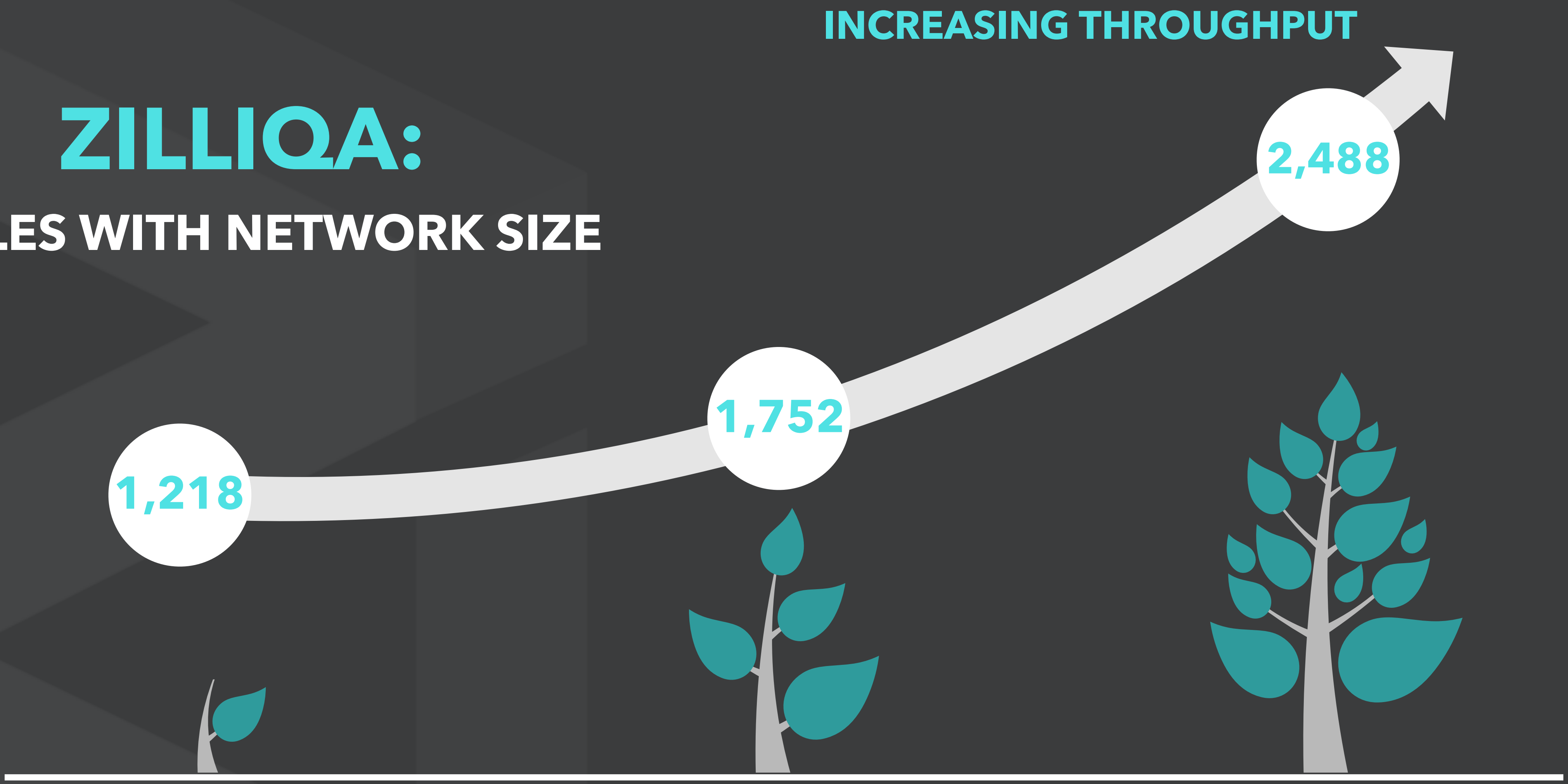
MORE APPLICABLE TO PAYMENTS

OPENNESS? TRANSPARENCY?

DECENTRALIZATION?

ZILLIQA:

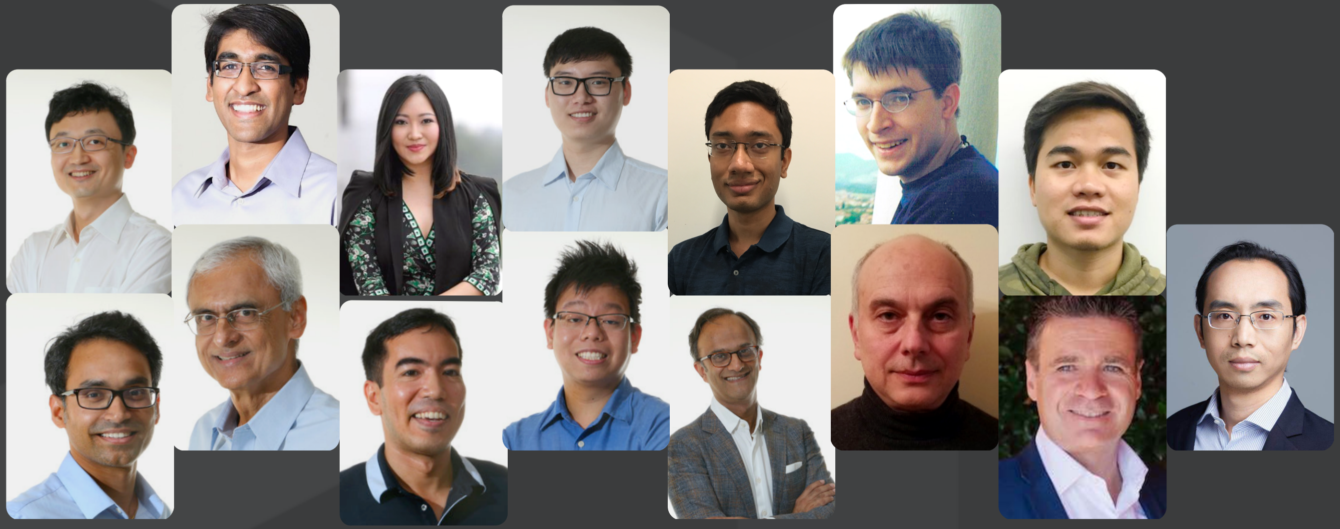
SCALES WITH NETWORK SIZE



3 SHARDS
1,800 NODES

4 SHARDS
2,400 NODES

6 SHARDS
3,600 NODES



“ DEEP TECH MEETS VENTURE CREATORS & FINANCIAL VETERANS ”

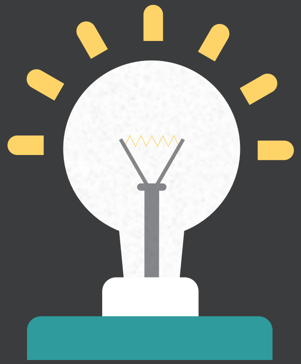
@ZILLIQA ZILLIQA.COM

“

A SECURE SHARDING PROTOCOL FOR OPEN BLOCKCHAINS (2015)

LOI LUU, PRATEEK SAXENA

”

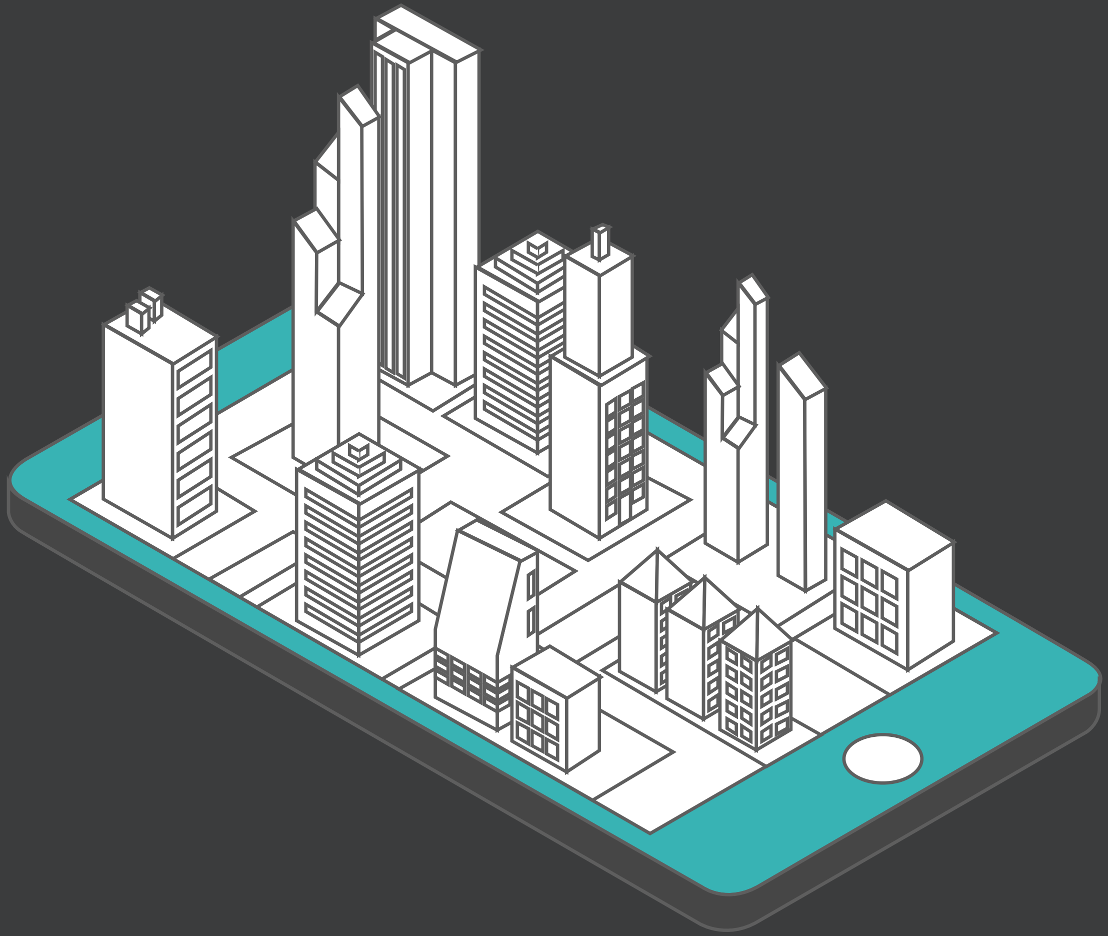


WE HAVE PUT THEORY INTO PRACTICE

PRIOR DEPLOYMENT

> "OTC TRADING: A TRIAL WITH A REGIONAL EXCHANGE & BANKS
>
> PRICE/PARTICIPANT DISCOVERY, SETTLEMENT, ANONYMITY"

> "DEPLOYING FOR AN E-COMMERCE APPLICATION IN SHIPPING
>
> INEFFICIENCY, DISPUTES, DELAYS"



“ ZILLIQA: A NEW PUBLIC BLOCKCHAIN ”

200X AND MORE HIGHER THROUGHPUT,
BUILT TO SCALE

DATA-FLOW & SHARDING-FRIENDLY
SMART CONTRACTS

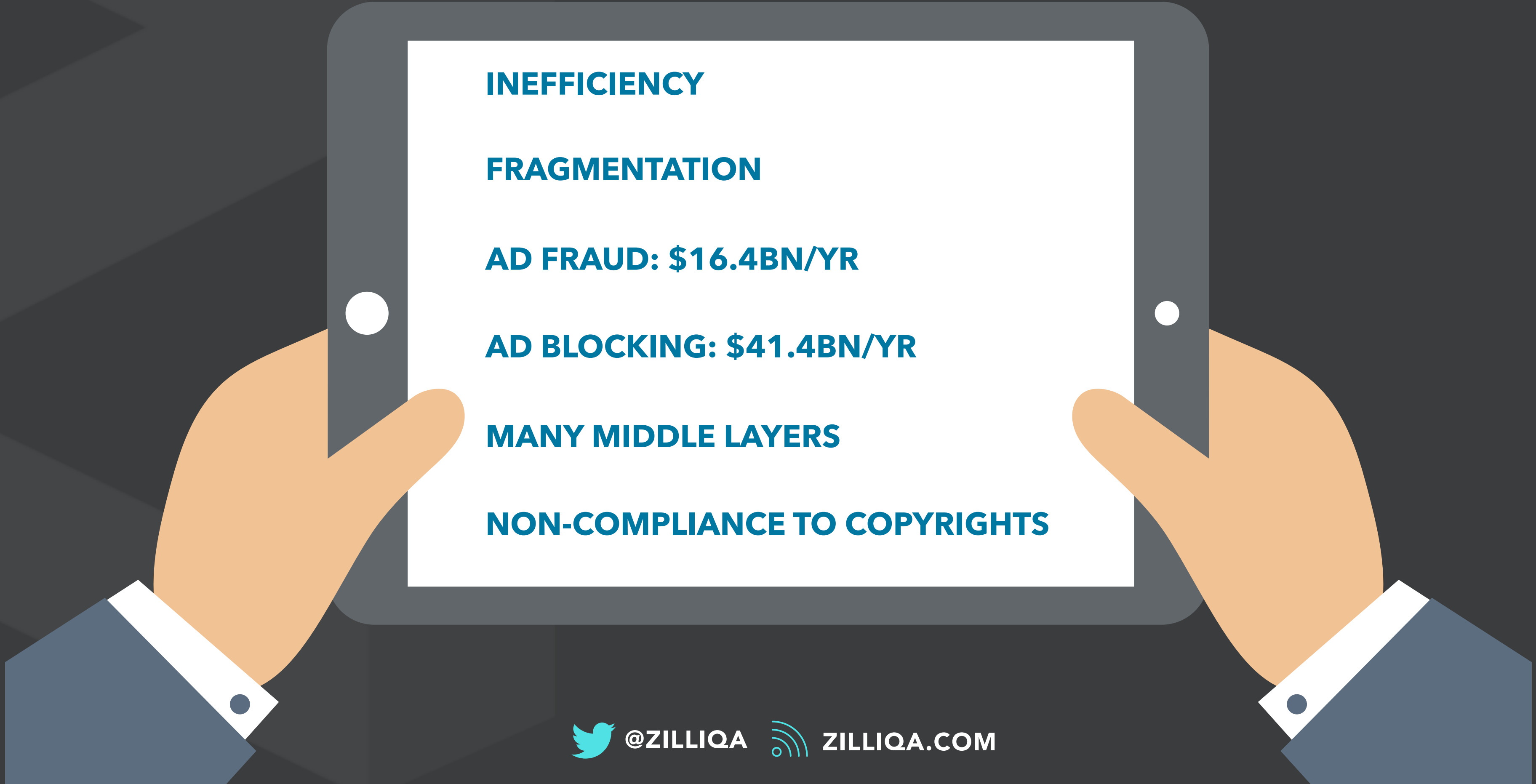
MINER FRIENDLY: LOWER COST,
STABLE REWARDS,
COMPATIBLE TO ETHASH

MUCH LOWER TX FEE FOR USERS

“ dAPPS ENABLED BY ZILLIQA ”

“DIGITAL ADVERTISING

MULTIPLE CHALLENGES, INCLUDING: ”



- INEFFICIENCY
- FRAGMENTATION
- AD FRAUD: $16.4BN/YR
- AD BLOCKING: $41.4BN/YR
- MANY MIDDLE LAYERS
- NON-COMPLIANCE TO COPYRIGHTS

“BLOCKCHAIN-BASED

ADVERTISING SUPPLY CHAIN”

PUBLISHERS SUPPLY SMART CONTRACTS

INVENTORY AVAILABLE
INVENTORY DESCRIPTORS

MARKETERS DEMAND SMART CONTRACTS

IMPRESSION VOLUME
DELIVER DEADLINE
TARGETED GROUPS OF USERS
GEOGRAPHIC RESTRICTIONS

SMART CONTRACTS ARE MATCHED AND AUDITED

IMPRESSIONS
SATISFACTION OF DEMANDS
PAYMENTS

“BLOCKCHAIN-BASED

ADVERTISING SUPPLY CHAIN BENEFITS ”

TRANSPARENT ADVERTISING NETWORK

OPEN MARKET ANALYSIS

RESPONSIBLE CONTENT DELIVERY

ACCOUNTABILITY

ENSURE TIMELINESS OF ADS CONTENT DELIVERY

“ REQUIREMENTS FOR BLOCKCHAIN ”

REAL TIME
PARALLEL BIDDING

HIGH VOLUME
TRANSACTIONS

CORRECTNESS &
FAIRNESS

VOLUME MISMATCH

BILLIONS OF ADS/DAY VS.
1 MILLION TXS/DAY ON ETHEREUM

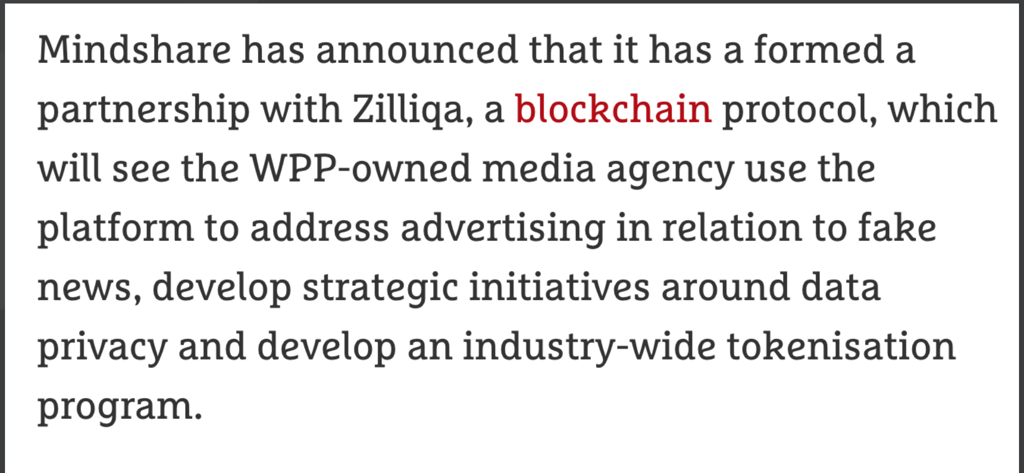
SMART CONTRACTS TOO COMPLEX TO
REASON ABOUT

SCALABLE THROUGHPUT
WITH NETWORK SHARDING

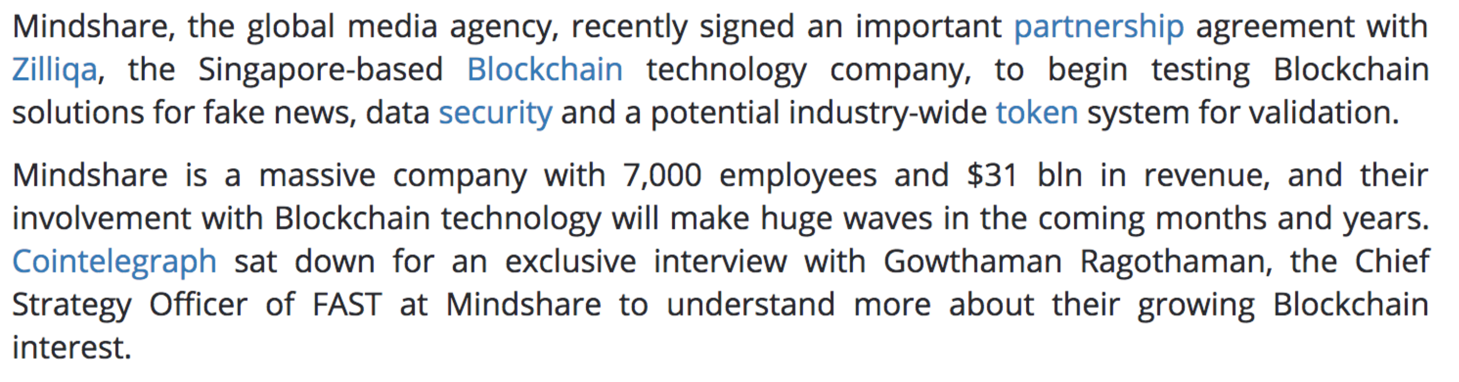
EFFICIENT PROCESSING
WITH COMPUTATIONAL SHARDING

DATA-FLOW SMART CONTRACTS
SIMPLE ABSTRACTIONS
AMENABLE TO VERIFICATION

“PARTNERSHIP WITH MINDSHARE„


Mindshare has announced that it has a formed a partnership with Zilliqa, a blockchain protocol, which will see the WPP-owned media agency use the platform to address advertising in relation to fake news, develop strategic initiatives around data privacy and develop an industry-wide tokenisation program.

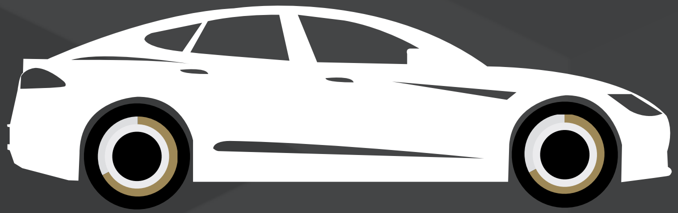
THE DRUM


Mindshare, the global media agency, recently signed an important partnership agreement with Zilliqa, the Singapore-based Blockchain technology company, to begin testing Blockchain solutions for fake news, data security and a potential industry-wide token system for validation.

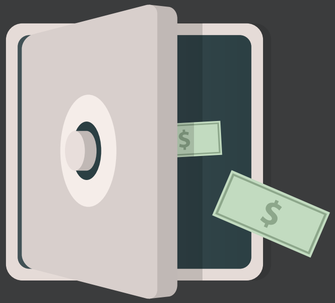
Mindshare is a massive company with 7,000 employees and $31 bln in revenue, and their involvement with Blockchain technology will make huge waves in the coming months and years. Cointelegraph sat down for an exclusive interview with Gowthaman Ragothaman, the Chief Strategy Officer of FAST at Mindshare to understand more about their growing Blockchain interest.

THE COINTELEGRAPH

“ OTHER dAPPS ”



SHARED ECONOMY



PAYMENT NETWORKS

PARALLEL AUCTIONS

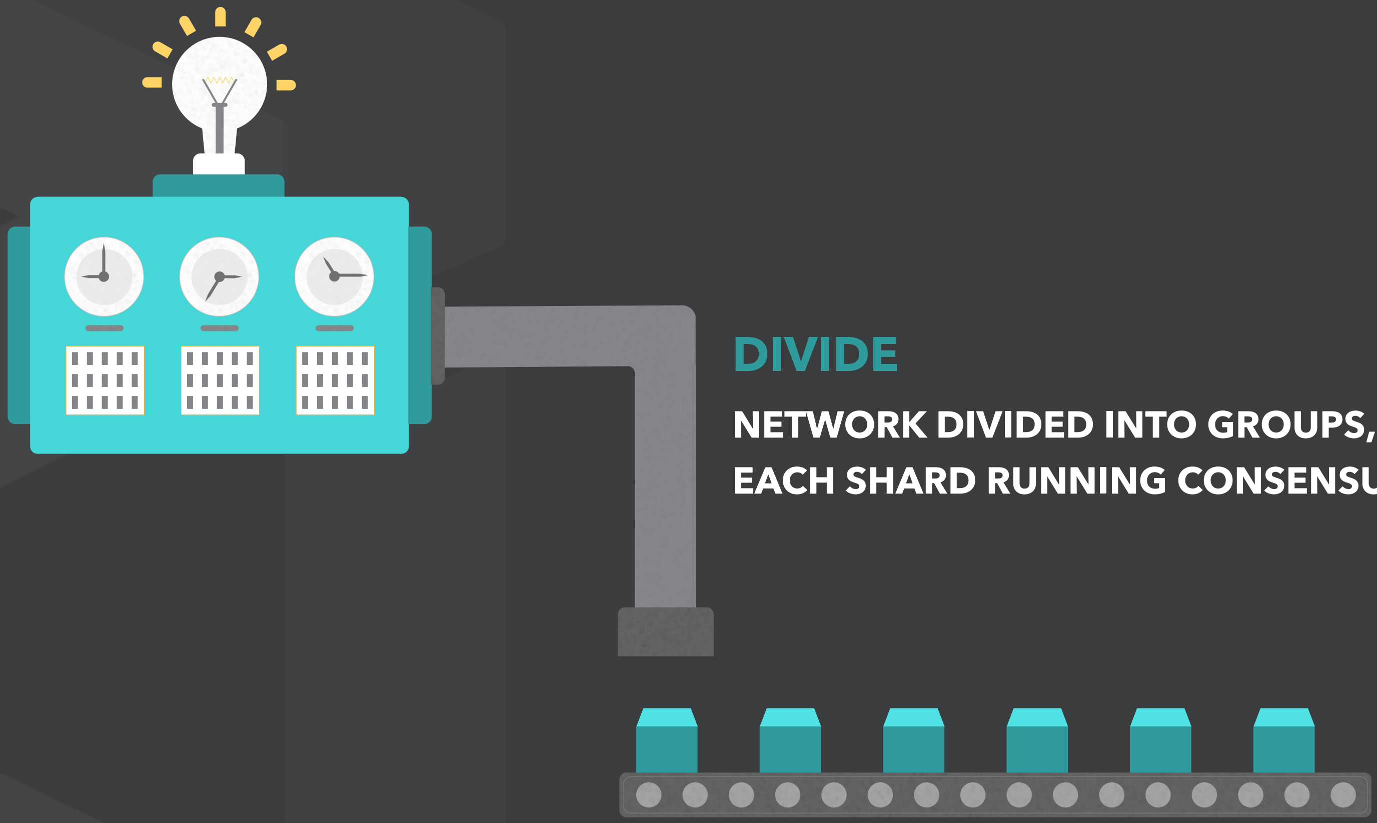
SCIENTIFIC COMPUTING

HIGH ASSURANCE COMPUTATION

“ TECH OVERVIEW ”

“ NETWORK SHARDING ”

DIVIDE AND CONQUER IN PARALLEL



DIVIDE

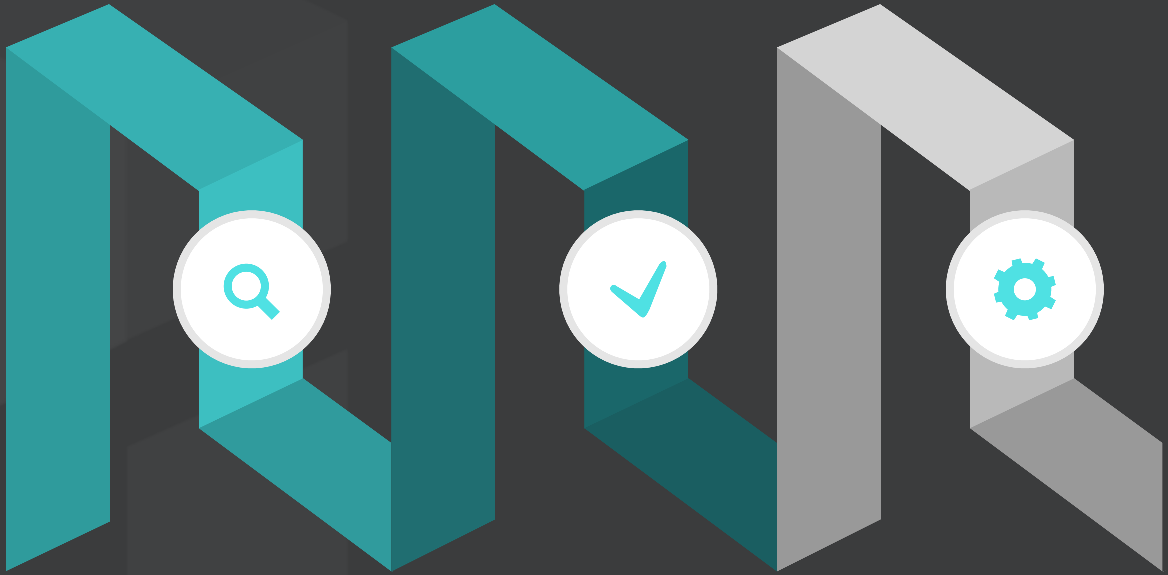
NETWORK DIVIDED INTO GROUPS, CALLED *SHARDS*
EACH SHARD RUNNING CONSENSUS PROTOCOL

CONQUER

A DEDICATED GROUP COMBINES OUTPUTS FROM EACH SHARD AND REACHES CONSENSUS ON IT.

“ SAFE & EFFICIENT CONSENSUS ”

KEY INGREDIENTS



01 PRACTICAL BYZANTINE FAULT TOLERANCE

Immediate finality of blocks
High message complexity

02 COLLECTIVE SIGNING

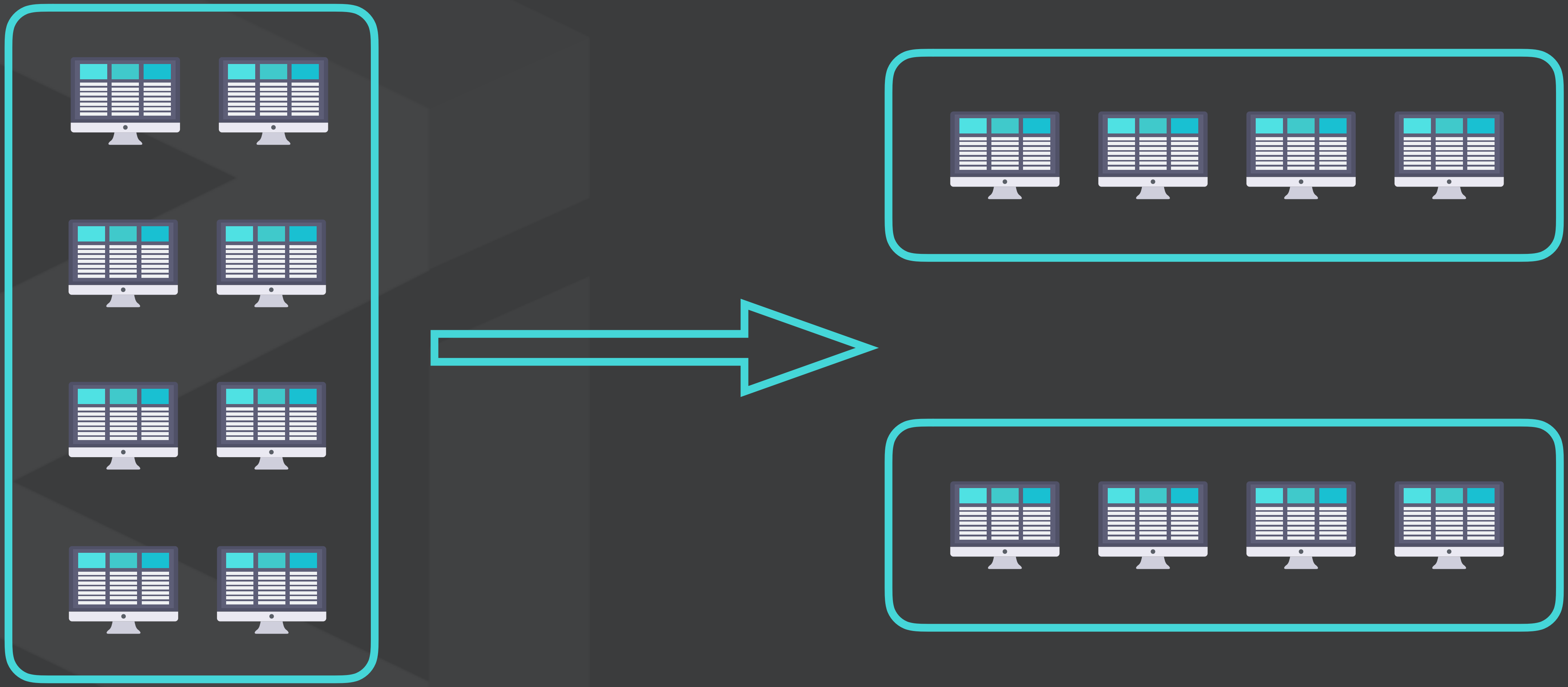
Highly efficient signature scheme for multiple parties
Same signature size for 1 or N parties

03 ZILLIQA’S CONSENSUS PROTOCOL

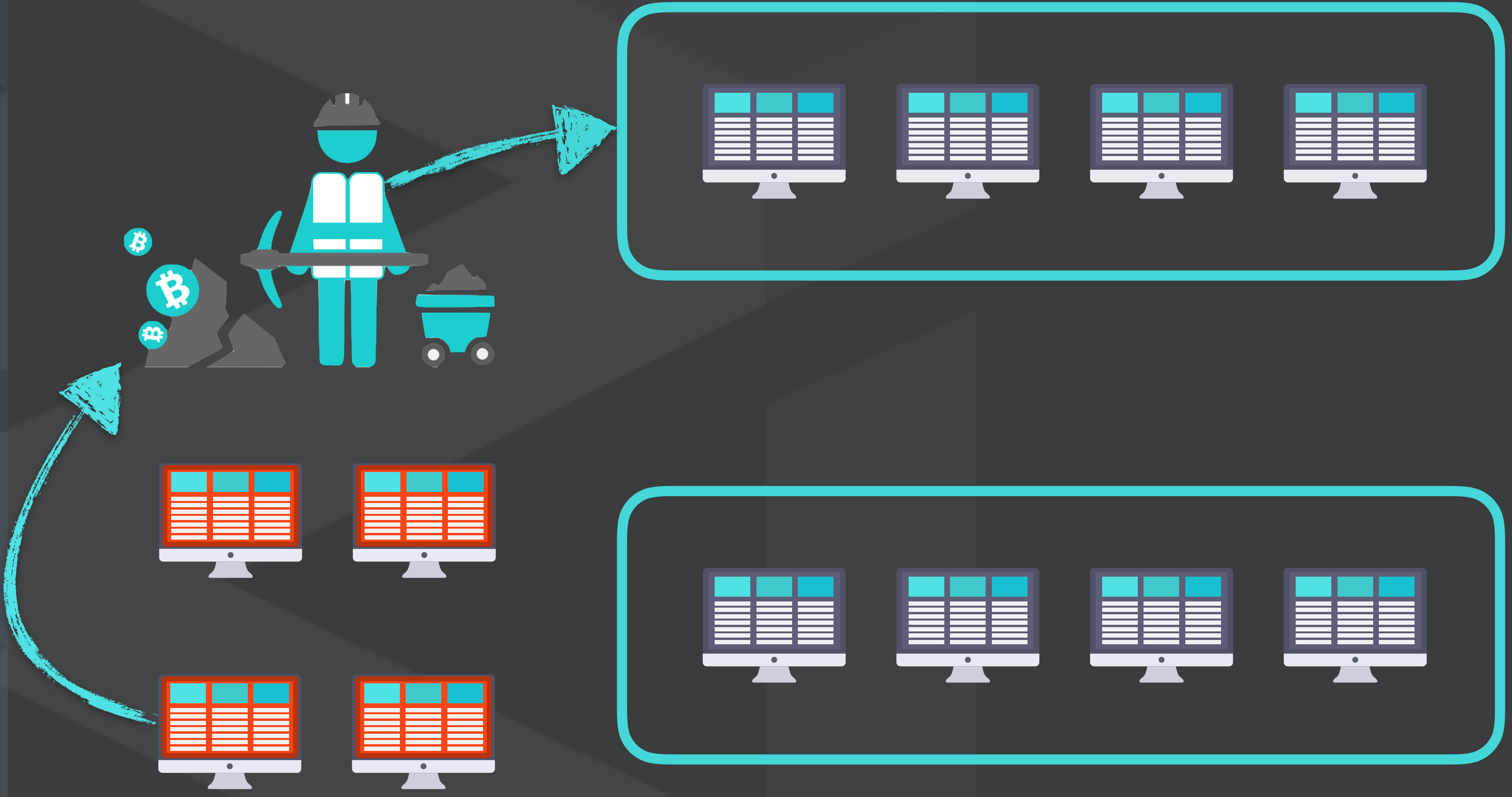
PBFT + Collective Signing
Security & performance enhancements

“Diving Deeper”

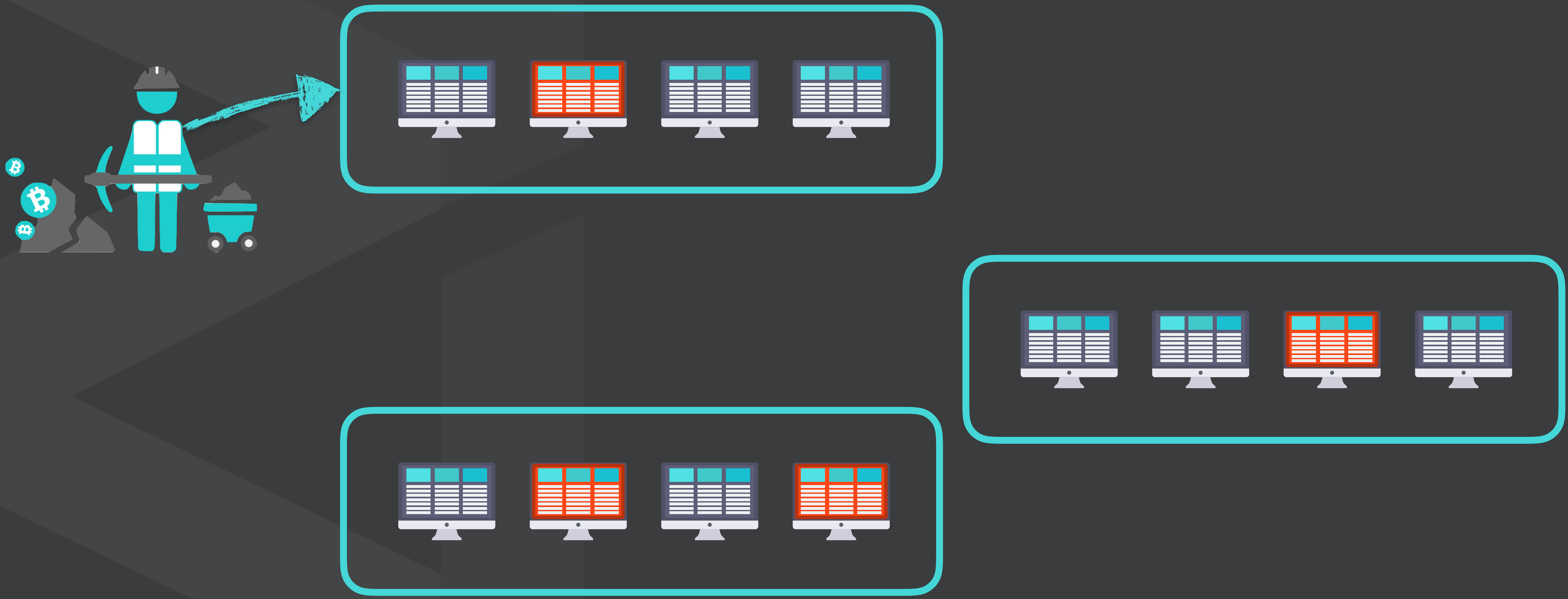
“ NETWORK SHARDING „



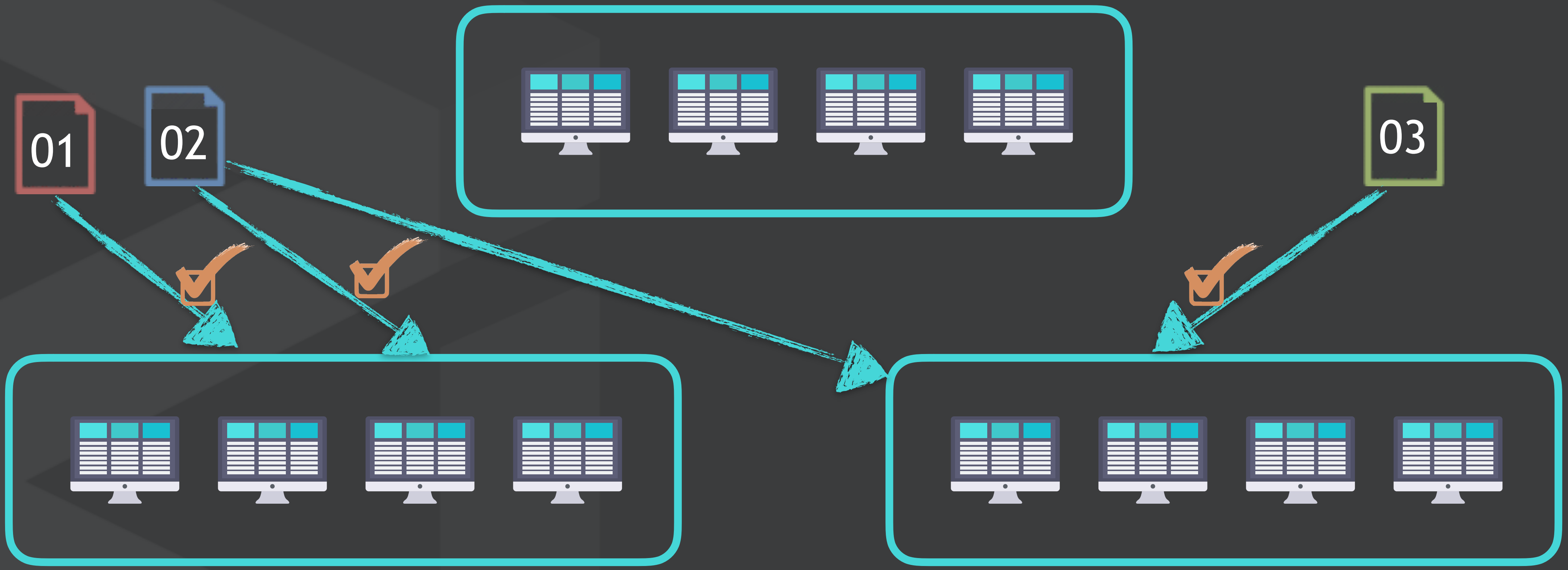
“MINE (POW) TO JOIN THE NETWORK”



“ NODES RANDOMLY DISTRIBUTED TO SHARDS ”

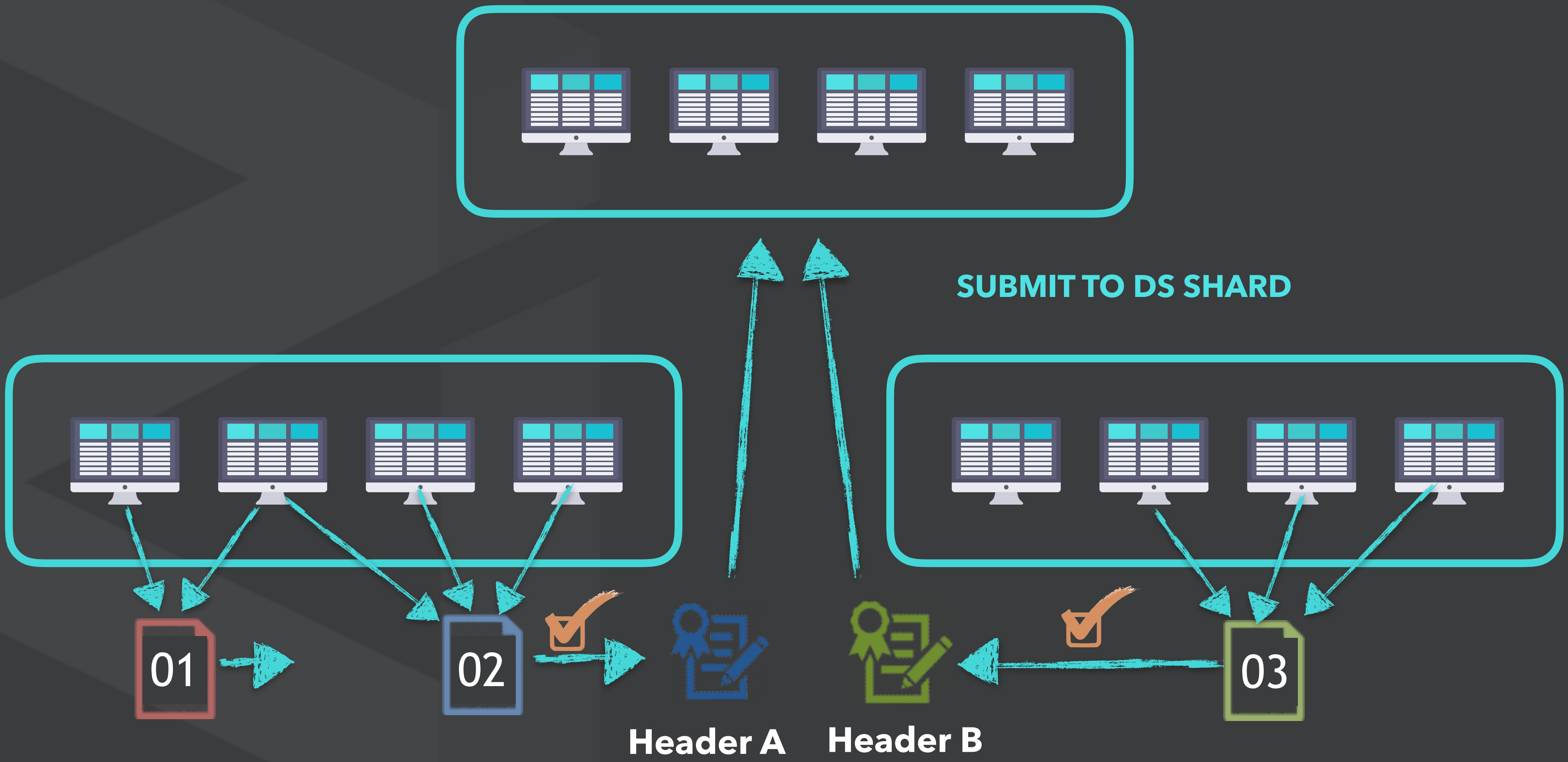


“TRANSACTION SHARDING „

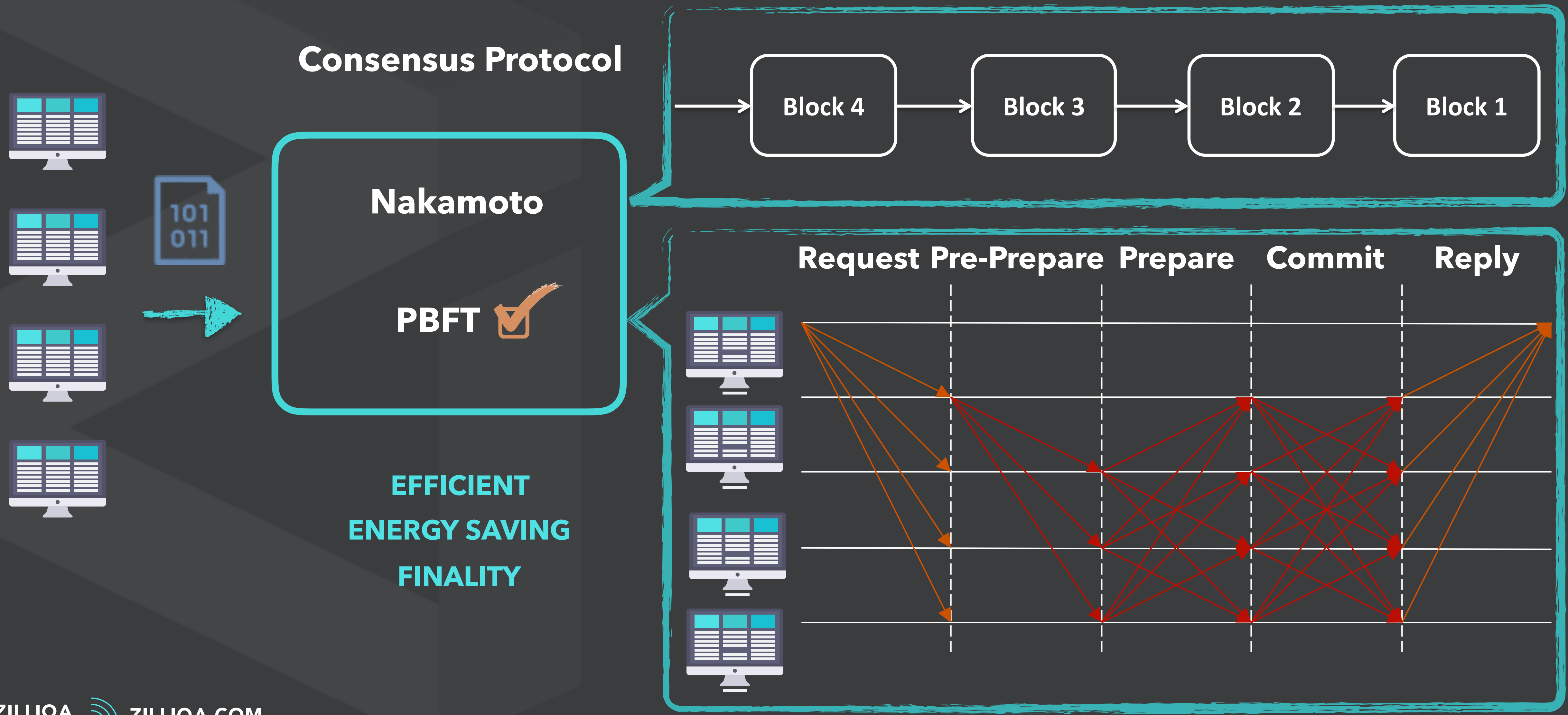


BASED ON THE
SENDER’S ADDRESS

“CONSENSUS ON TRANSACTIONS ”



“CONSENSUS PROTOCOL”



Consensus Protocol

Nakamoto

PBFT ✓

EFFICIENT

ENERGY SAVING

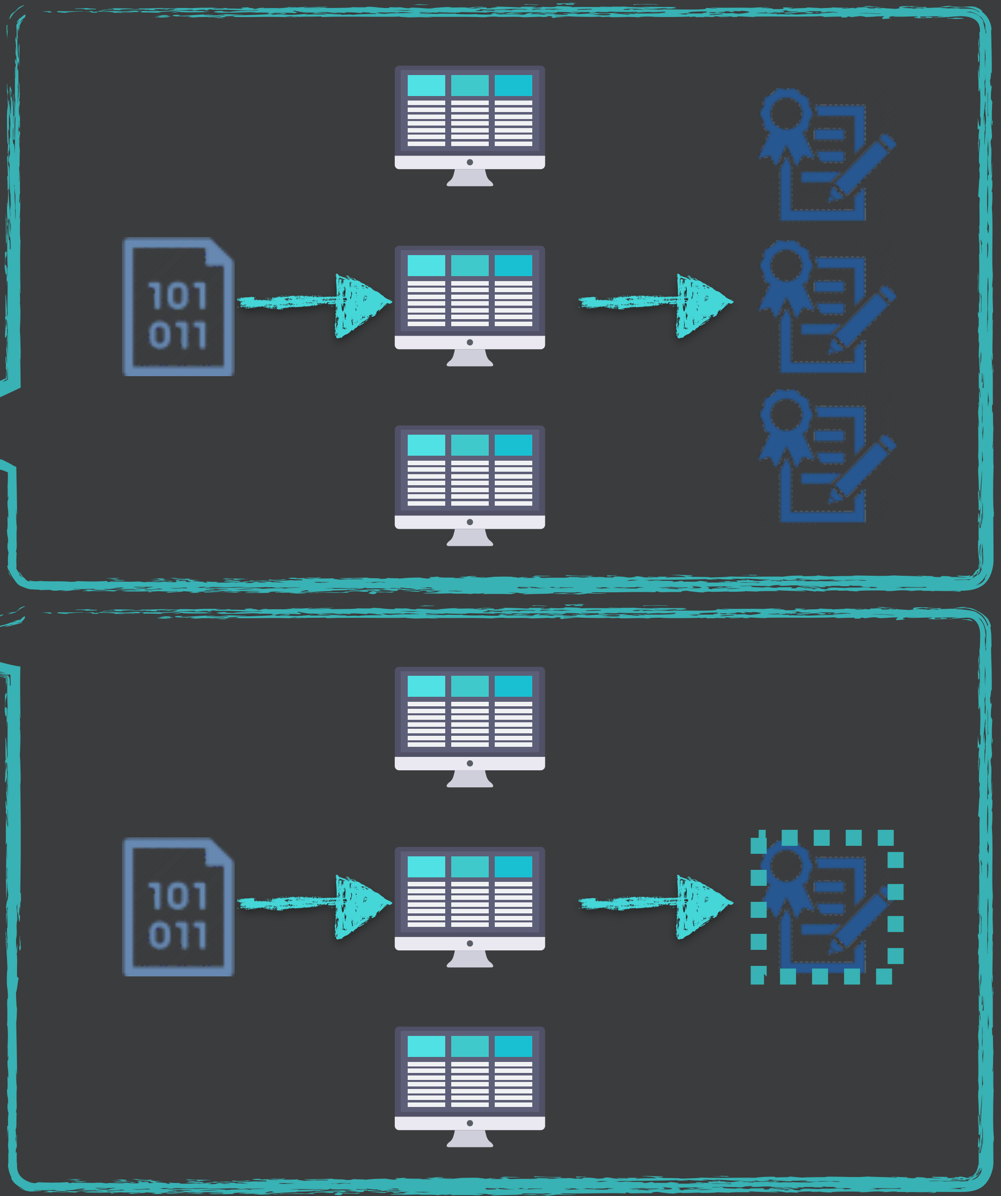
FINALITY

“SIGNATURE AGGREGATION”

Signature Scheme

Digital Signature

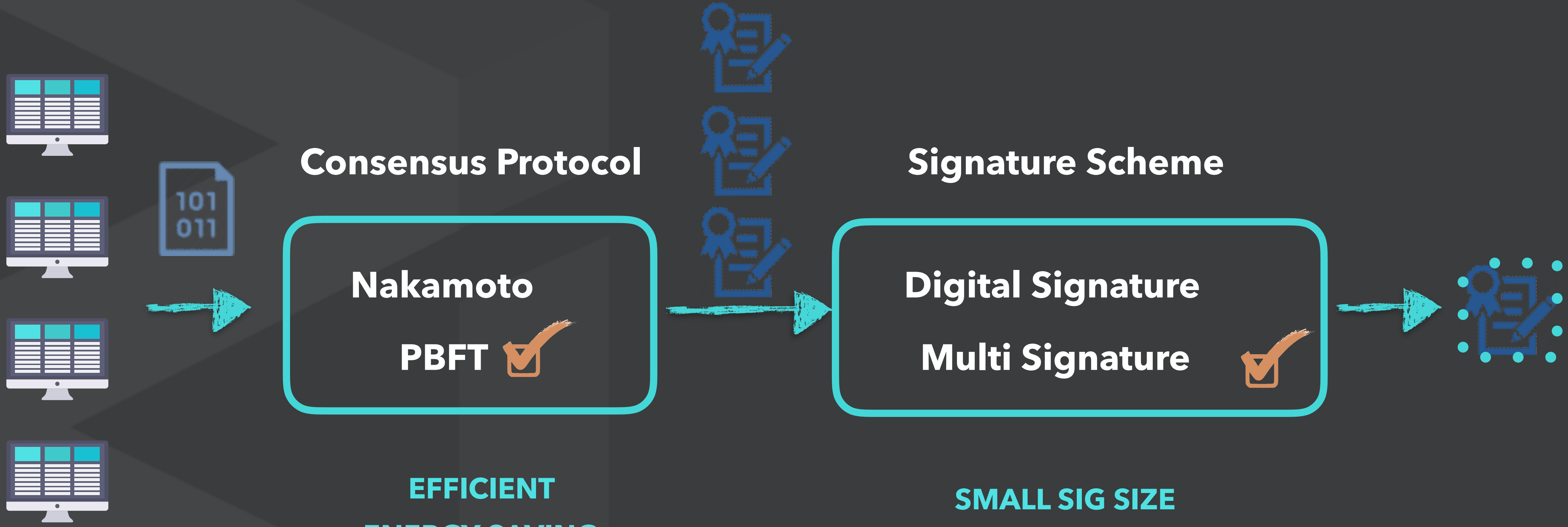
Multi Signature ✓



SMALL SIG SIZE

LOW COMM OVERHEAD

“ CONSENSUS AND SIGNATURE AGGREGATION ”



Consensus Protocol

Nakamoto

PBFT ✓

Signature Scheme

Digital Signature

Multi Signature ✓

EFFICIENT

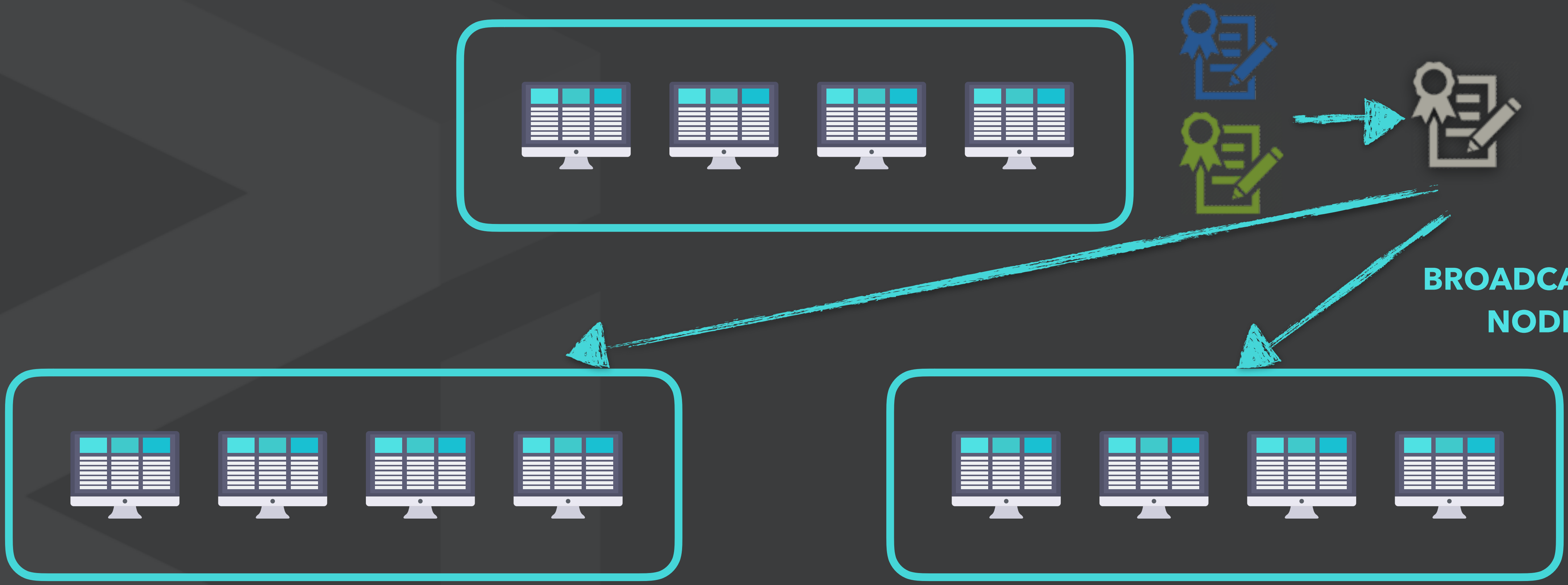
ENERGY SAVING

FINALITY

SMALL SIG SIZE

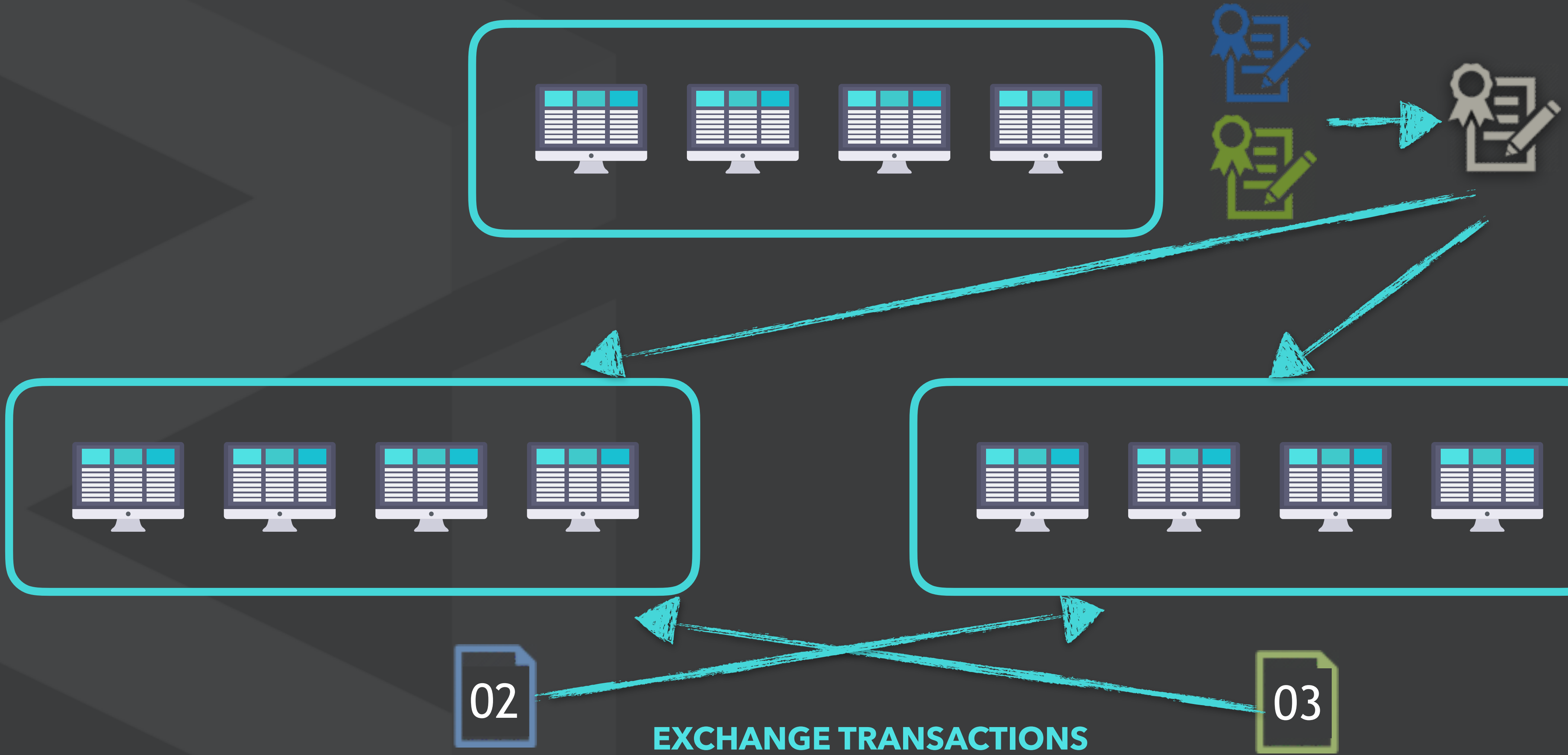
LOW COMM OVERHEAD

“CONSTRUCT & BROADCAST FINAL BLOCK”



BROADCAST TO NODES

“EXCHANGE VALID TRANSACTIONS„



EXCHANGE TRANSACTIONS
ACROSS SHARDS

“ PROFITABLE MINING & LOW-COST USAGE ”

LOWER ENERGY COST

PoW only used for sybil defense; not consensus

STABLE REWARDS

More even payout with lower variance

LOWER TX FEE

Users no longer need to compete for the few Tx/s

“SMART CONTRACTS”

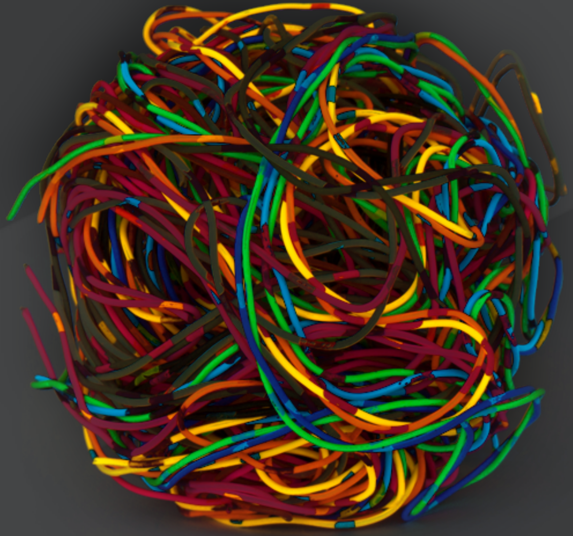
“INCIDENTS WITH SMART CONTRACTS”

$60 MIL
STOLEN

$300 MIL
FROZEN

?

“CAUSES„



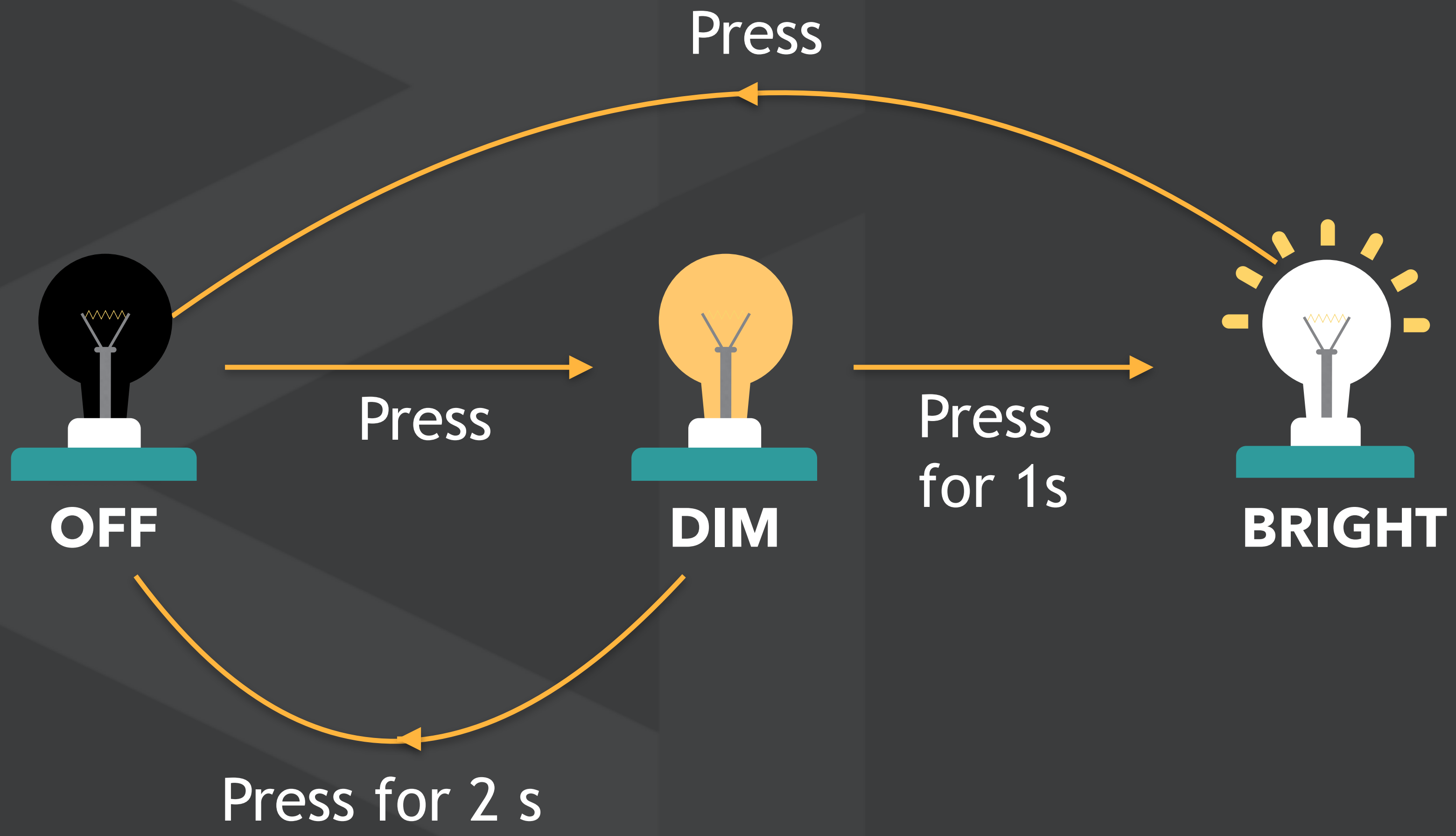
COMPLEXITY

EXPECTED VS UNEXPECTED BEHAVIOR

NO FORMAL VERIFICATION

“ SCILLA ”

AUTOMATA-BASED LANGUAGE



NON-TURING COMPLETE

DECIDABLE CONTRACTS

AMENABLE TO FORMAL VERIFICATION

CLEAN SEPARATION: COMMUNICATION VS COMPUTATION

“KICKSTARTER IN SCILLA”

IMMUTABLE PARAMS

```
contract Crowdfunding
          (owner    : address,
           deadline : uint,
           goal     : unit)
```

MUTABLE STATE

```
backers : address ⇒ uint = [];

success : boolean = false
```

STATE TRANSITIONS

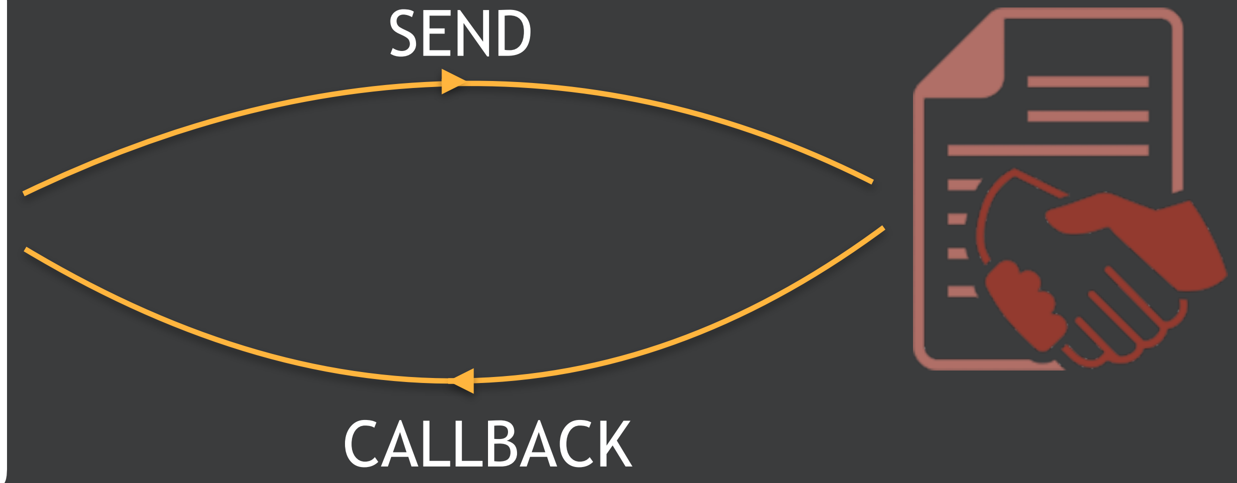
```
transition Donate
             (sender : address,
              value  : uint,
              tag    : string)
```

```
transition Reclaim
             (sender : address,
              value  : uint,
              tag    : string)
```

“DAO INCIDENT”

SOLIDITY

```
function reclaim
{
	uint amount = backers[msg.sender]
	if(msg.sender.call.value(amount) == false)
		throw
	// reset the amount for sender
	backers[msg.sender] = 0;
}
```



INSTRUCTION NEVER EXECUTED

“PREVENTING DAO INCIDENT”

SECURITY RECOMMENDATION

```
// THIS CONTRACT HAS A BUG, DO NOT USE
function reclaim
{
    uint amount = backers[msg.sender];
    if(msg.sender.call.value(amount) == false)
        throw
    // reset the amount for sender
    backers[msg.sender] = 0;
}
```

```
// SAFE TO USE

function reclaim
{
    uint amount = backers[msg.sender];
    backers[msg.sender] = 0;
    msg.sender.transfer(amount);
}
```

CHECKS-EFFECTS-INTERACTIONS

“ PREVENTING DAO INCIDENT

AT THE LANGUAGE LEVEL ”

SOLIDITY

```
// SAFE TO USE

function reclaim
{
      uint amount = backers[msg.sender];
      backers[msg.sender] = 0;
      msg.sender.transfer(amount);
}
```

SCILLA

```
transition Reclaim
            // Check if the sender is eligible to reclaim
      if ( … )
         send (<to → sender, amount → 0,
                tag  → “main", msg → "failure">, MT)
      else
            // remove sender from the list
            let v = get(backers, sender) in
            backers := remove(backers, sender);
            send (<to → sender, amount → v,
                    tag → “main", msg → "refunded">, MT)
```

EXTERNAL CALLS ALWAYS HAPPEN AT THE END

REENTRANCY FREE

“FORMAL VERIFICATION

USING COQ ”

SCILLA

+

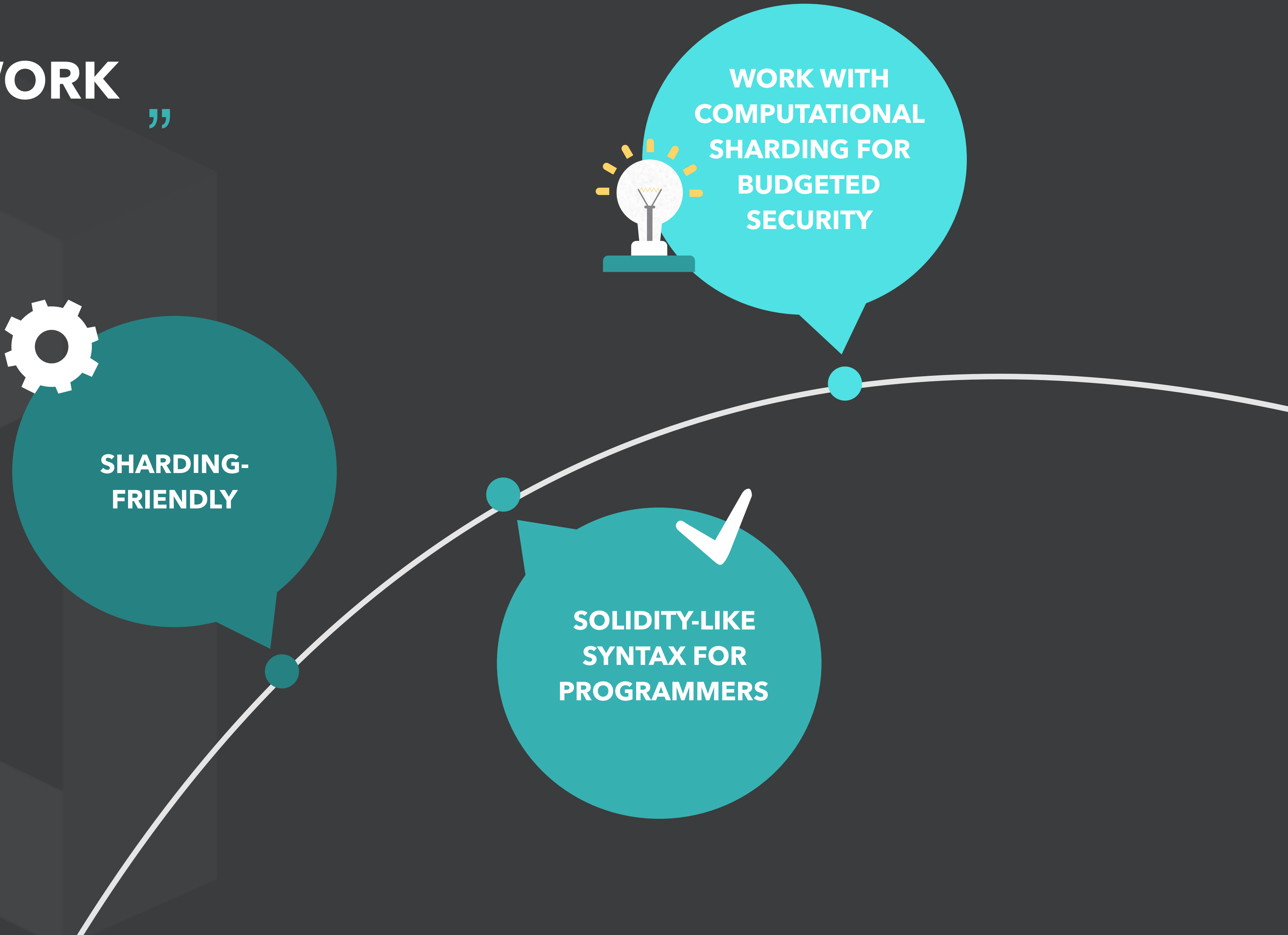
COQ

Lemma 1: Contract will have enough funds to refund.

Lemma 2: Contract will not alter its contribution records.

Lemma 3: Each contributor is refunded the right amount.

“ ONGOING WORK ”



SHARDING-FRIENDLY

SOLIDITY-LIKE SYNTAX FOR PROGRAMMERS

WORK WITH COMPUTATIONAL SHARDING FOR BUDGETED SECURITY

“ NEXT STEPS ”

“WHERE ARE WE NOW?

WORKING PROTOTYPE TESTED ON AWS EC2”

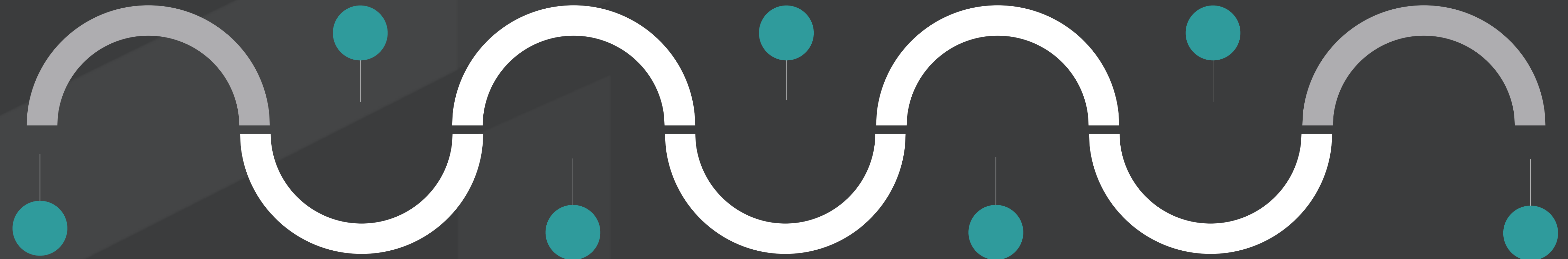
2,488 TX/S
FOR 3,600
NODES

MORE
FEATURES
UNDERWAY

INTENSIVE
TESTING &
OPTIMISATION

SMART
CONTRACT
SPECS

“ NEAR TERM ROADMAP ”



SOURCE CODE RELEASE
Q1 2018

RELEASING TESTNET V1.0
Q1 2018

SMART CONTRACT ALPHA
Q2 2018

RELEASING TESTNET V2.0
Q2 2018

SMART CONTRACT BETA
Q3 2018

MAIN NET LAUNCH
Q3 2018

ANCHOR APP RELEASE
Q4 2018

“ FUTURE PLANS ”

CONTINUAL RESEARCH & DEVELOPMENT

EXPLORE WAYS TO SUPPORT DAPPS FROM OTHER CHAINS

RESEARCH COLLABORATION WITH COMMUNITIES

ZILLIQA /'ZILIKƏ/

NEXT GEN HIGH-THROUGHPUT
BLOCKCHAIN PLATFORM

Q&A

Join our team

careers@zilliqa.com

Join our Slack & Telegram

Slack: https://invite.zilliqa.com

Telegram: @zilliqachat

@ZILLIQA ZILLIQA.COM ENQUIRY@ZILLIQA.COM