This would be a perfect application for blockchain.

I'm in marketing. Can you explain that in terms I can understand?

I kinda doubt it. Because you're a bad explainer, right?
WHERE BLOCKCHAINS FAIL
(AND WHY HPC IS OF NO HELP)

MAARTEN VAN STEEN
ALICE CREATES A TRANSACTION

ALICE SIGNS THE TRANSACTION

SIGNED TRANSACTION NEEDS TO BE FINALIZED: VALIDATED AND IMMUTABLE
THE NETWORK
VALIDATION AND STORAGE
OF TRANSACTIONS?
VALIDATOR COLLECTS & VALIDATES TRANSACTIONS

THE NETWORK
VALIDATION AND STORAGE OF TRANSACTIONS?

UNIVERSITY OF TWENTE | DIGITAL SOCIETY INSTITUTE
ATTEMPTS TO LINK TO CURRENT BLOCK CHAIN

PUBLICLY ACCESSIBLE & DISTRIBUTED BLOCKS OF VALIDATED TRANSACTIONS
THE NETWORK

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
THE NETWORK

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

REQUEST

REQUEST

REQUEST

REQUEST

REQUEST

REQUEST

REQUEST

REQUEST

GO FOR IT!
REQUIREMENTS THAT HAVE BECOME PROMISES

1. HIGHLY SCALABLE
   • TRANSACTIONS / TIME UNIT
   • PARTICIPATING VALIDATORS

2. FULLY DECENTRALIZED

3. COMPLETE CONSENSUS AMONG CORRECTLY BEHAVING PARTICIPANTS
FULLY DECENTRALIZED?

1. Run a decentralized leader-election algorithm for each new block to be added.
2. Allow the elected leader to validate the transactions.
3. Make sure that you can trust the elected leader.
PROTOCOLS BASED ON RACING
COMPUTATIONALLY EASY

INPUT → HASHING → HASH

COMPUTATIONALLY HARD
(BRUTE FORCE NEEDED)
HASH WITH K LEADING ZEROES

FIND N

0000000000D6A8.....
• LIMIT THE NUMBER OF BLOCKS / TIMEUNIT SO THAT VALIDATORS CAN FIND OUT IF SOMEONE ELSE WON
• VERY SMALL TIMEOUT: YOU’LL FIND OUT TOO LATE AND HAVE WASTED EFFORTS (LONGEST CHAIN WINS)
VARIATIONS ON A THEME

• SEPARATE LEADER ELECTION FROM TRANSACTION VALIDATION (BUT STILL REQUIRES RACING)

• VALIDATORS SHOULD ALREADY HAVE A PROVEN STAKE IN THE SYSTEM (BUT STILL REQUIRES SOME LEADER ELECTION; VULNERABLE TO ATTACKS)
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 THROUGHPUT/SCALABILITY PROBLEMS
PROTOCOLS BASED ON TALKING
FLOODING CONSENSUS
FLOODING CONSENSUS
• NODES NEED TO BE TRUSTED
• CLOSED GROUP
• (FAILURES CAN BE HANDLED)
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)

NODES NEED TO BE TRUSTED?
CLOSED GROUP?

• NEEDED IF CONSENSUS IS TO BE REACHED BEFORE APPENDING A BLOCK TO THE BLOCKCHAIN (PESSIMISTIC APPROACH)

• MAY BE LEFT OUT IF UNRIGHTFUL APPEND OPERATIONS CAN BE MITIGATED (OPTIMISTIC APPROACH)
PRACTICAL BYZANTINE FAULT TOLERANCE
PRACTICAL BYZANTINE FAULT TOLERANCE

- CLOSED GROUP
- SCALES IN THROUGHPUT
- DOES NOT SCALE IN PARTICIPANTS
- HIGHLY FAULT-TOLERANT SOLUTION

CONSENSUS-AS-A-SERVICE
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
THE STORY SO FAR
1. HIGHLY SCALABLE
2. FULLY DECENTRALIZED
3. FULL CONSENSUS
CONSENSUS-AS-A-SERVICE:

- SERVICE IS CENTRALIZED
- # PARTICIPANTS RESTRICTED
- SERVICE NEEDS TO BE TRUSTED

COMPUTATIONAL RACES:

- WASTE ENERGY DUE TO RACING
- THROUGHPUT IS LIMITED

1. SCALABLE
2. DECENTRALIZED
A PROTOCOL THAT MAY GET US SOMEWHERE
FEDERATED BYZANTINE AGREEMENT

- EACH NODE N DEFINES A SET OF NODES WHO SHOULD AGREE BEFORE IT WILL ALSO AGREE: **A QUORUM SLICE**
- A NODE MAY HAVE MULTIPLE SLICES
- IF Q IS IN A **QUORUM**, THEN SO MUST ONE OF ITS SLICES BE IN THAT QUORUM
- IF ALL NODES HAVE THE SAME QUORUM SLICE(S), WE HAVE BFT
FEDERATED BYZANTINE AGREEMENT

• TO REACH AGREEMENT AMONG A SET OF NODES, THEIR RESPECTIVE QUORUM SLICES NEED TO PAIRWISE HAVE A (NONFAULTY) NODE IN COMMON

• YOU DISCOVER THE NODES NEEDED TO REACH CONSENSUS

• THE PROTOCOL GOES THROUGH 3 PHASES:
  • NOMINATE < some value >
  • PREPARE < that value >
  • CONFIRM < that value >
FEDERATED BYZANTINE AGREEMENT

- **IMPORTANT PROPERTIES:**
  - OPEN MEMBERSHIP
  - DECENTRALIZED

- **KEY OBSERVATIONS:**
  - CLAIMS A TRANSACTION CAN BE HANDLED IN 3 SECONDS
  - STELLAR CLAIMS IT CAN HANDLE 1000 TRANSACTIONS PER SECOND
  - NO SCIENTIFIC PUBLICATION OF THE PROTOCOL EXISTS
FROM HYPE TO RESEARCH
• **BLOCKCHAIN IS SURPRISINGLY POPULAR**
  • COOL APPLICATIONS
  • SOME PEOPLE GOT VERY RICH
  • EVERYONE IGNORES THE TOUGH STUFF

• **BLOCKCHAIN IS SURPRISINGLY POPULAR**
  • VERY FEW PEOPLE UNDERSTAND WHAT’S REALLY GOING ON (AND THE CORE *IS* VERY DIFFICULT)
  • THERE ARE MANY FUNDAMENTAL PROBLEMS THAT WILL HINDER DEPLOYMENT