Block Fairness and Byzantine Generals

Ashish Goel
Algorithms for Decentralized Finance

Maximum Extractable Value

MEV: The value extracted by nodes in the blockchain ecosystem which goes beyond the regular gas fees and transaction fees

— Example (Front-running): A centrally located node on a blockchain network observes an order before others in the network, and manages to extract additional value by front-running an order ahead of it

— Example (block assembly:) A node that has some say in how blocks are assembled sandwiches a legitimate pair of buy and sell orders with its own orders to extract the bid-ask spread

— Momentum trading: A node or set of nodes created demand for an asset by trading it and making it look attractive, and then capitalize on the created demand

This class: focus on front running

Ideal property

Order consistency — Transactions on a blockchain should be arranged in arrival order

Problem: Even in the absence of dishonest nodes, network latency and jitter imply that transactions may arrive in arbitrary order

— And in the presence of malicious adversaries, misreporting the order in which transactions were received, it is unreasonable to expect that the orders at different nodes are the same

— There is no consistent way to resolve this. Eg. If three nodes receive transactions A, B, C in the order (A, B,C), (B, C, A), (C, A, B), then A beats B, B beats C, and C beats A in the majority order.

Social Choice Perspective

N voters, M alternatives. Each voter submits a full ranking of the alternatives, and a Social Choice Function f (SCF) chooses a single ranking

Pareto optimality: If every voter prefers a to b, then a is strictly above b in the output of the SCF

IIA, Independence of Irrelevant Alternatives: The relative order of a and b in the output of the SCF should only depend on the relative order of a and b in each ranking

Arrow's Impossibility Theorem: Any SCF that is weakly Pareto Optimal, and satisfies IIA, must be dictatorial.

And the impossibility results get even stronger when voters are being strategic, let alone adversarial

Order-Fairness vs Block-Fairness

Order-Fairness is hopeless in the absence of a central timestamping server (and perhaps even then)

Block-Fairness: If Transaction A is received before Transaction B by a substantial majority of honest nodes, then B can not be placed in an earlier block than A (no guarantee on their order within the block)

Block-Fairness can generally be achieved

Today

— An outline of Byzantine Fault Tolerance, https://lamport.azurewebsites.net/pubs/byz.pdf

— A sketch of Block-Fairness: https://eprint.iacr.org/2020/269

Note: Block-fairness dovetails well with Arrow-Debreu exchanges

Byzantine Generals

N generals, f of which are adversarial/dishonest/traitorous/malicious

Need to agree on a strategy to attack or retreat (binary); each has a private opinion

Problem: there may be dishonest generals

Goal: (a) All honest generals should agree on the outcome, and (b) If all honest generals agree on the private opinion, then all honest generals agree on this shared private opinion as the outcome

Equivalent goal: There is a single commander who issues an order, and (a) All honest generals obey the same order (attack or stay), and (b) if the commander is honest, then all honest generals agree on the order given by the commander (The Byzantine Consensus Problem)

The latter implies the former

A counter-example: f = 1, N = 3

(sketched interactively in class)

Impossibility Result

If N <= 3f, then the Byzantine Consensus conditions can not be satisfied.

Sketch: Assume yes. Set N =3f. Think of a 3 generals problem where each general simulates f generals, and obtain a contradiction

Possibility Result: Oral Messages

A1. Every message that is sent is delivered correctly.

A2. The receiver of a message knows who sent it.

A3. The absence of a message can be detected.

Algorithm OM(f) works if $N > 3f$

OM(0):

(1) The commander sends his value to every lieutenant.

(2) Each general uses the value he receives from the commander, or uses the value RETREAT if he receives no value.

OM(f) for f > 0

v_i: The private value received by general i from the commander (who is assumed to be general N)

(1) The commander sends his value to every other general.

(2) For each i, let v_i be the value General i receives from the commander, or else be RETREAT no value is received. General i acts as the commander in Algorithm OM(f - 1) to send the value v_i to each of the N - 2 other generals.

(3) For each i, and each j ~ i, let v_j be the value General i received from General j in step (2) (using Algorithm OM(f - 1)), or else RETREAT if no value received. General i uses the value *majority* (v_1 ..... v_{N-1})

Proof sketch

Inductive, illustrated for N = 4, f = 1

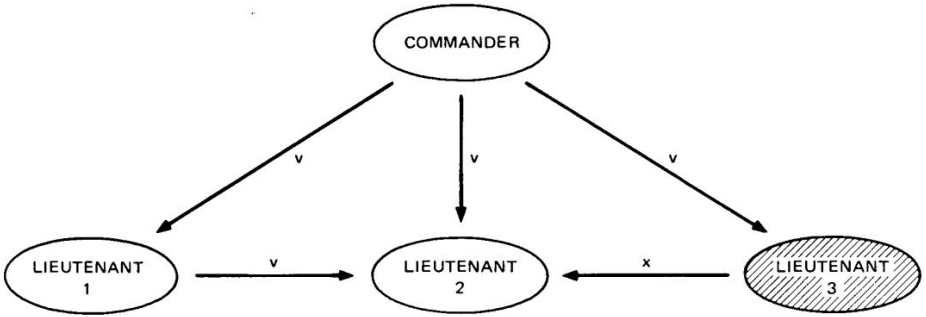

Fig. 3. Algorithm OM(1); Lieutenant 3 a traitor.

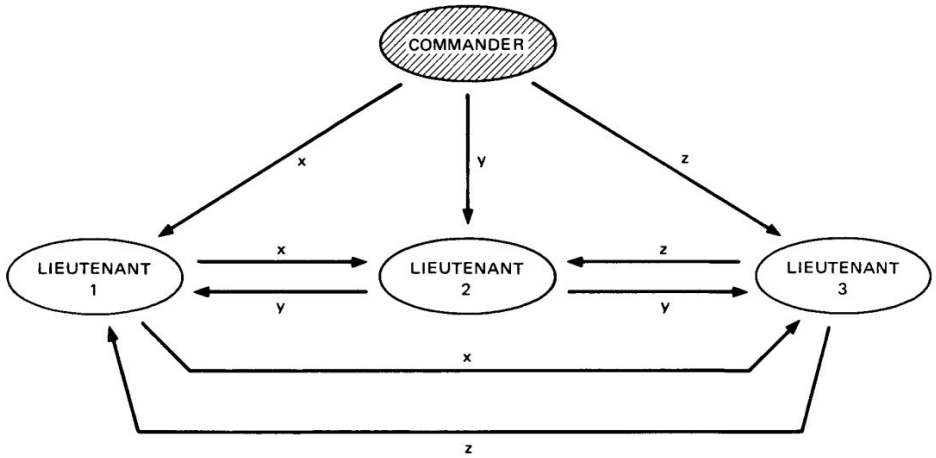

Fig. 4. Algorithm OM(1); the commander a traitor.

Back to Block Fairness

Three Steps

(a) Gossip Stage. In this stage, nodes gossip transactions in the order that they were received. That is, each node gossips its local transaction ordering.
(b) Agreement Stage. In this stage, nodes agree on the set of nodes whose local orderings should be considered for deciding on the global ordering of a particular transaction.
(c) Finalization Stage. In this stage, nodes finalize the global ordering of a transaction tx using the set of local orderings decided on in the agreement stage.

Each step can be implemented using Byzantine consensus; details in the posted paper

Take away: Batch auctions like SPEEDEX can provide better protection against frontrunning