

BLOCKCHAIN: A NOVEL APPROACH FOR THE CONSENSUS ALGORITHM USING CONDORCET VOTING PROCEDURE

David Vangulick, PHD candidate University of Liège

Pr Bertrand Cornélusse & Pr Damien Ernst University of Liège

IEEE DAPPCON



AGENDA

- Introduction
- Problem statement
- Concepts of Condorcet miner selection
- Pseudo algorithm
- Conclusion

INTRODUCTION

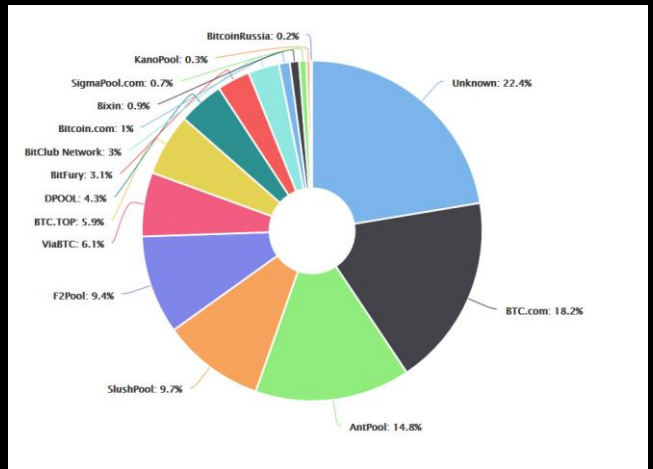
- Blockchain technology allows interested parties to access a common register, the update, and integrity of which are collectively managed in a decentralized manner by a network of actors.
- The consensus protocol ensures a common and unambiguous update of transactions by creating blocks of transactions for which integrity, veracity, and consistency are guaranteed through geographically distributed nodes.

PROBLEMS STATEMENT








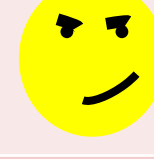
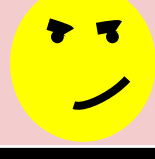

- Let's imagine that you want to have an **open public blockchain** to secure transactions into a block but **on a timely regular basis** examples of use cases:
 - Energy decentralized exchange like “collective self consumption”
 - Auctioning
 - Sport Bet platform
 - ...
- This blockchain needs to be
 - able to reach consensus
 - resistance against Sybill attacks: the system is subverted by forging false identities
 - sustainable = energy consumption of the whole system
 - synchronized : strong guarantee on the time when a block is created

PROBLEMS STATEMENT

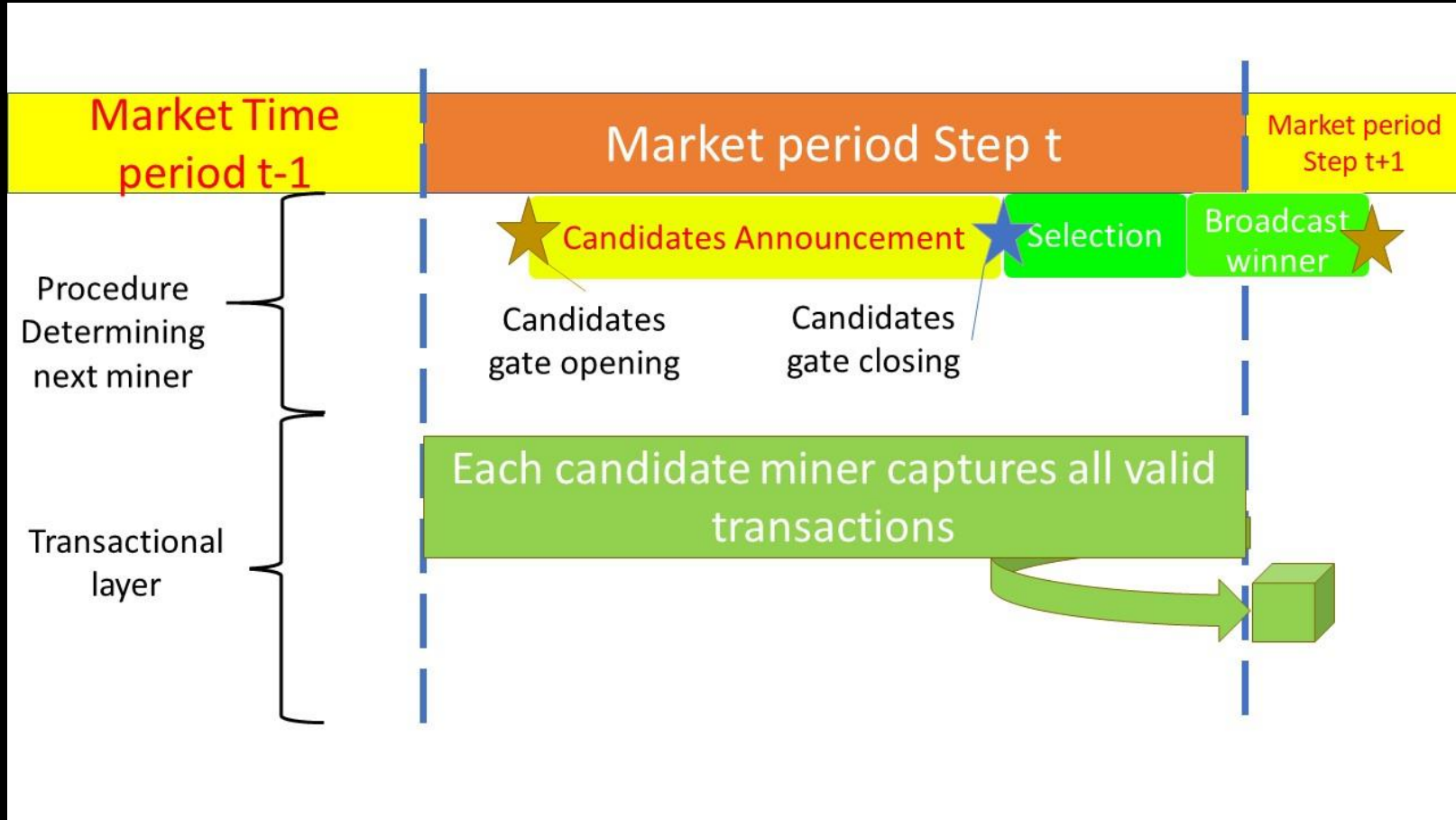
- To those requirements, we add a new one: Resistant to Dominance aka Concentration of decision-making power
- The core concept of blockchain technology is decentralization.
- In blockchain, there is no "chief of the staff", but the consensus protocol ensures a good balance between different parties with different interests such as
 - miners,
 - transaction makers,
 - smart contract promoters,
 - etc.

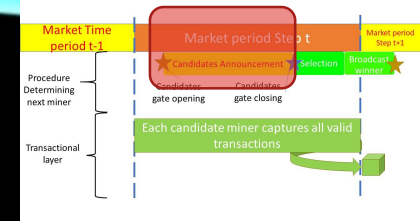


PROBLEMS STATEMENT

	Proof of Work	Proof of Stake
reach consensus		
Sybill attacks resistance		
Sustainable		
Synchronization		
Resistant to Dominance		

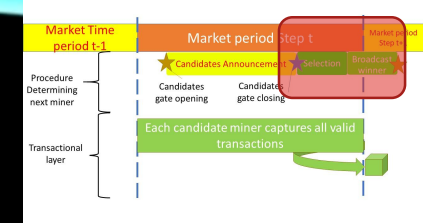
CONCEPT OF CONDORCET MINER SELECTION





CONCEPT OF CONDORCET MINER SELECTION

- Candidate announcement is a sort of auction
 - Candidate miners place their service offers in the form of voting tokens sent to the previously selected miner (this miner cannot be a candidate for this block anymore). He/she becomes the voting authority
 - They may do this for a period of time between two instances called "candidates gate opening" for the launch of the selection and "candidates gate closure" for the end.
- To publish the result, previous miner as voting authority sends a few of all voting tokens he received from candidate to the winner
- There are several possible ways to create a voting token e.g.
 - Created during the Initial Coin Offering (ICO)
 - Created as a reward for a node for its supporting activities or for having use the blockchain for a transaction ...

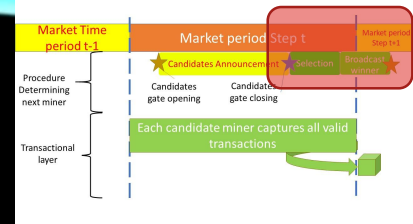


CONCEPT OF CONDORCET MINER SELECTION

- A Condorcet method : an election method that
 - elected = winner all of the head-to-head elections against each of the other candidates.
 - A candidate with this property is called the Condorcet winner.
- One well know draw back: The Condorcet paradox when collective preferences are cyclic

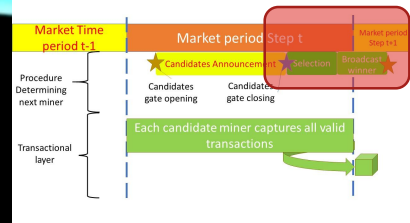


Marie Jean Antoine
Nicolas de Caritat
(by Jean-Baptise
Greuze)



CONCEPT OF CONDORCET MINER SELECTION

- After the candidate gate closure, the candidates are known
- There is no real physical voters committee by a set of criteria used as “voter”
 - Voter E voting token = number of voting token send by the candidate
 - Voter A for age = age of the last block created by the candidate
 - Voter R for reputation = number of block created by the candidate
 - Voter U with votes for the criterion random
- Specific for the random number creation
 - transparent in order that all nodes can redo the computation and come to the same conclusion and thus avoid manipulation
 - e.g. the ratio between the hash value of their public address divided by the sum of the hashes of the public address of all the candidates.



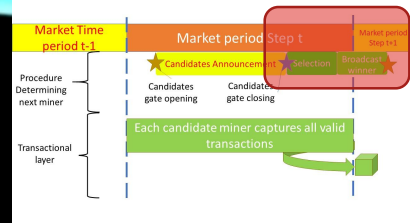
CONCEPT OF CONDORCET MINER SELECTION

- To illustrate this, let's say that we have 5 candidates

	George	Henry	John	Richard	Edward
A	45	3	0	1	2
R	0	2	10	27	42
E	16	5	8	997	59
U	0.78	0.82	0.56	0.67	0.05

Note:

- The values for A – R and E are transparent and can be determined by the voting authority
- Here “U” is purely random

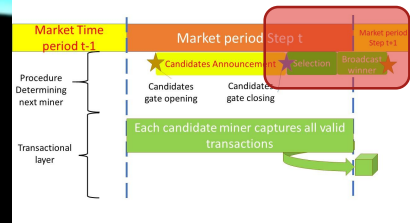


CONCEPT OF CONDORCET MINER SELECTION

Step 1:Tally: We create a pair to pair matrix for each voters (criteria), for instance for "A": (= setting preference)

	George	Henry	John	Richard	Edward
A	45	3	0	1	2

M^A	George	Henry	John	Richard	Edward
George	0	1	1	1	1
Henry	-1	0	1	1	1
John	-1	-1	0	-1	-1
Richard	-1	-1	1	0	-1
Edward	-1	-1	1	1	0



CONCEPT OF CONDORCET MINER SELECTION

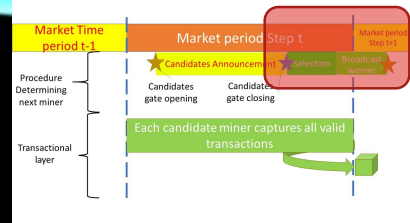
- We do the same for each voters/criteria

M^E	George	Henry	John	Richard	Edward
George	0	1	1	-1	-1
Henry	-1	0	-1	-1	-1
John	-1	1	0	-1	-1
Richard	1	1	1	0	1
Edward	1	1	1	-1	0

M^A	George	Henry	John	Richard	Edward
George	0	1	1	1	1
Henry	-1	0	1	1	1
John	-1	-1	0	-1	-1
Richard	-1	-1	1	0	-1
Edward	-1	-1	1	1	0

M^R	George	Henry	John	Richard	Edward
George	0	-1	-1	-1	-1
Henry	1	0	-1	-1	-1
John	1	1	0	-1	-1
Richard	1	1	1	0	-1
Edward	1	1	1	1	0

M^U	George	Henry	John	Richard	Edward
George	0	-1	1	1	1
Henry	1	0	1	1	1
John	-1	-1	0	-1	1
Richard	-1	-1	1	0	1
Edward	-1	-1	-1	-1	0



CONCEPT OF CONDORCET MINER SELECTION

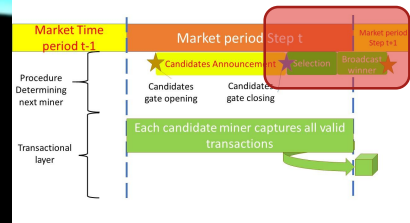
- From these 4 matrix, we build a total vote Matrix

$$M^{tot} = \alpha M^E + \beta M^A + \gamma M^R + \eta M^U$$

Let's pose for the illustration that
 $\alpha = \gamma = \eta = 1 \quad \beta = 2$

M^A	George	Henry	John	Richard	Edward
George			3		
Henry					
John					
Richard					
Edward					

$= 1 * 1 + 1 * 2 + 1 * (-1) + 1 * 1$



CONCEPT OF CONDORCET MINER SELECTION

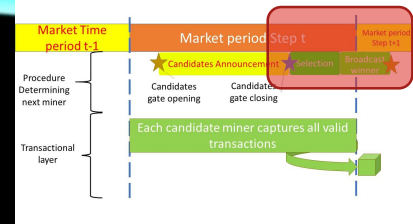
- From these 4 matrix, we build a total vote Matrix

$$M^{tot} = \alpha M^E + \beta M^A + \gamma M^R + \eta M^U$$

Let's pose for the illustration that
 $\alpha = \gamma = \eta = 1 \quad \beta = 2$



M^A	George	Henry	John	Richard	Edward
George	0	1	3	1	1
Henry	-1	0	1	1	1
John	-3	-1	0	-5	-3
Richard	-1	-1	5	0	-1
Edward	-1	-1	3	1	0



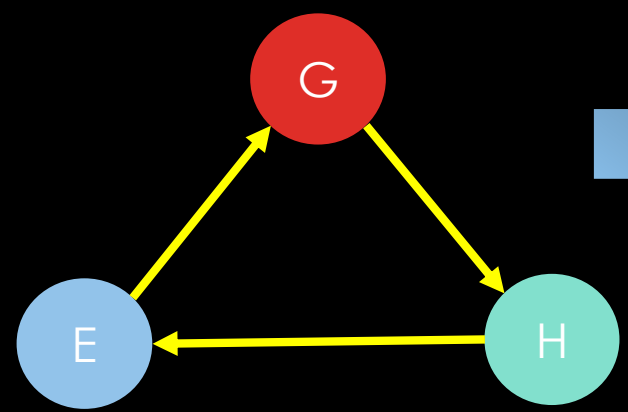
CONCEPT OF CONDORCET MINER SELECTION

- Step 2; if there is no immediate Condorcet winner
 - Situation 1 = there are more than 1 row with only positive or zero values => Dictatorial choice
 - Is there a absolute winner regarding reputation between tied candidates?
 - Yes, he is the winner
 - No, looking sequentially for absolute winner between tied candidate for A, E and U
 - Situation 2 = there is no row with only positive or zero values => Tideman procedure (also called ranked pair)
 - This method has been selected because of its characteristics regarding independence to irrelevant alternative and clones (important for Sybill attack resistance)

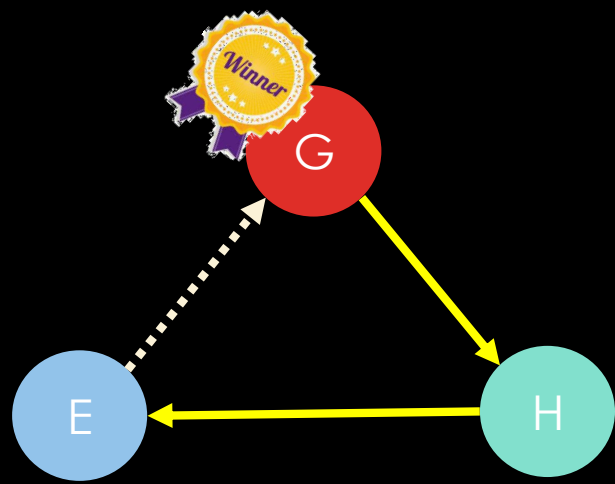
CONCEPT OF CONDORCET MINER SELECTION

- The Tideman procedure
 - it occurs when there are creation of cycle
 - A directed graph is build based on ranked relationship
 - If the relationship create a cycle, it is skipped (called skip or lock in the procedure)

M^{tot}	George	Henry	Edward
George	0	7	-5
Henry	-7	0	6
Edward	5	-6	0



Duel	Ranked relationship
George - Henry	7
Henry - Edward	6
Edward - George	5



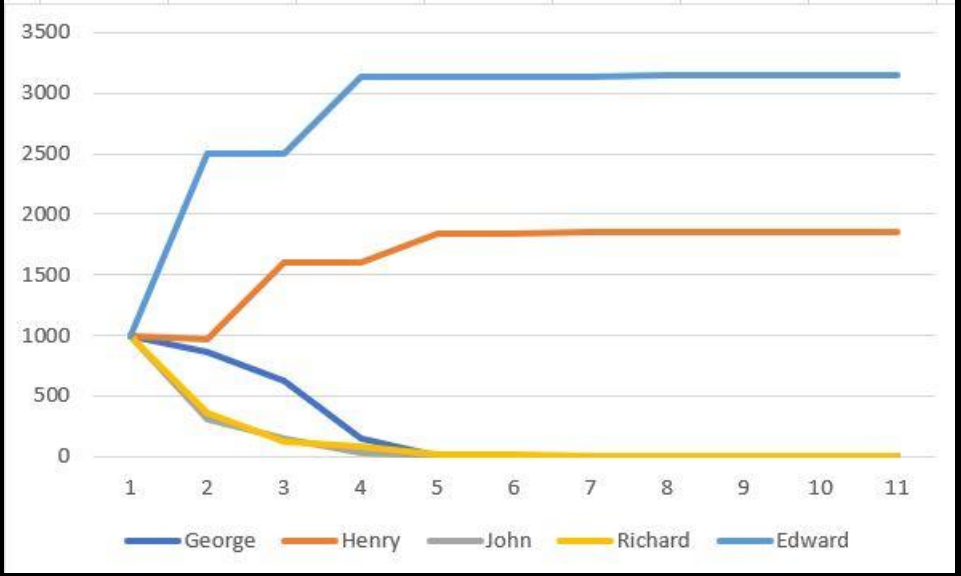
Note:

• This matrix is illustrative. Obviously the values of α ; γ ; η and β are not the same as the previous illustration

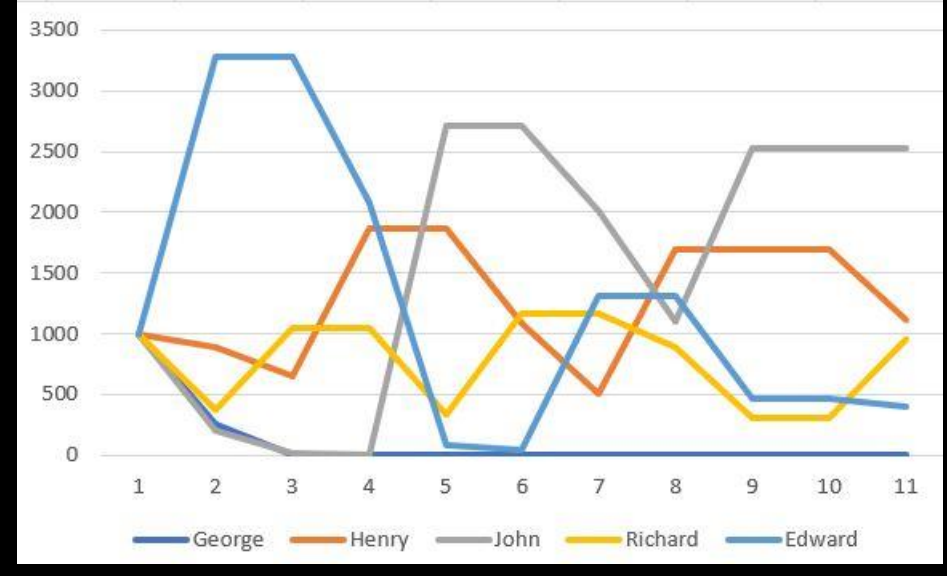
CONCEPT OF CONDORCET MINER SELECTION

- The selection of the weight for each voter is crucial to avoid Concentration of decision-making power

$$\alpha = \gamma = \eta = \beta = 1$$


















$$\alpha = \gamma = \eta = 1 \quad \beta = 2$$



PSEUDO ALGORITHM

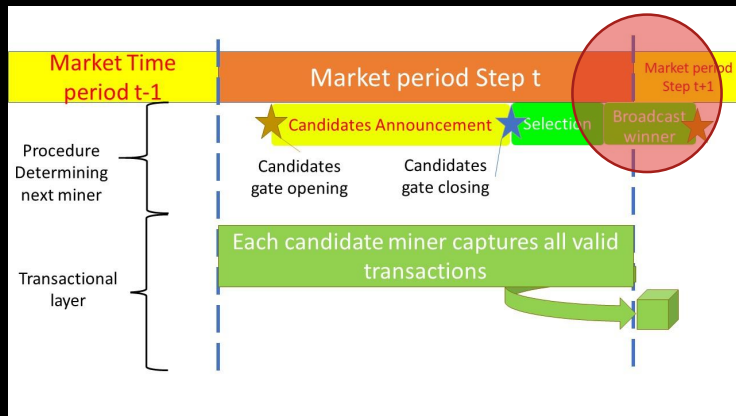
1. Create the different matrix and compute the total voting matrix
2. Check if there is an immediate Condorcet winner
 - ⇒ if yes, next miner is found
 - ⇒ Else continue
3. Check situation 1 (multiple rows with value ≥ 0)
 - ⇒ if yes, apply dictatorial choice = next miner is found
 - ⇒ Else continue
4. Apply Tideman procedure
 - ⇒ Next miner is found

CONCLUSION

	Proof of Work	Proof of Stake	Condorcet
reach consensus			
Sybill attacks resistance			
Sustainable			
Synchronization			
Resistant to Dominance			

CONCLUSION

- Further works
 - Issue 1



- There is a risk that information about the winner comes too late to some candidate
- In order to prevent information loss, these nodes will broadcast their own block.

➔ Fork management

- Issue 2: The procedure relies on the previous miner. That's a possible threat.

➔ Multiple voting authorities = others nodes or other previous miner