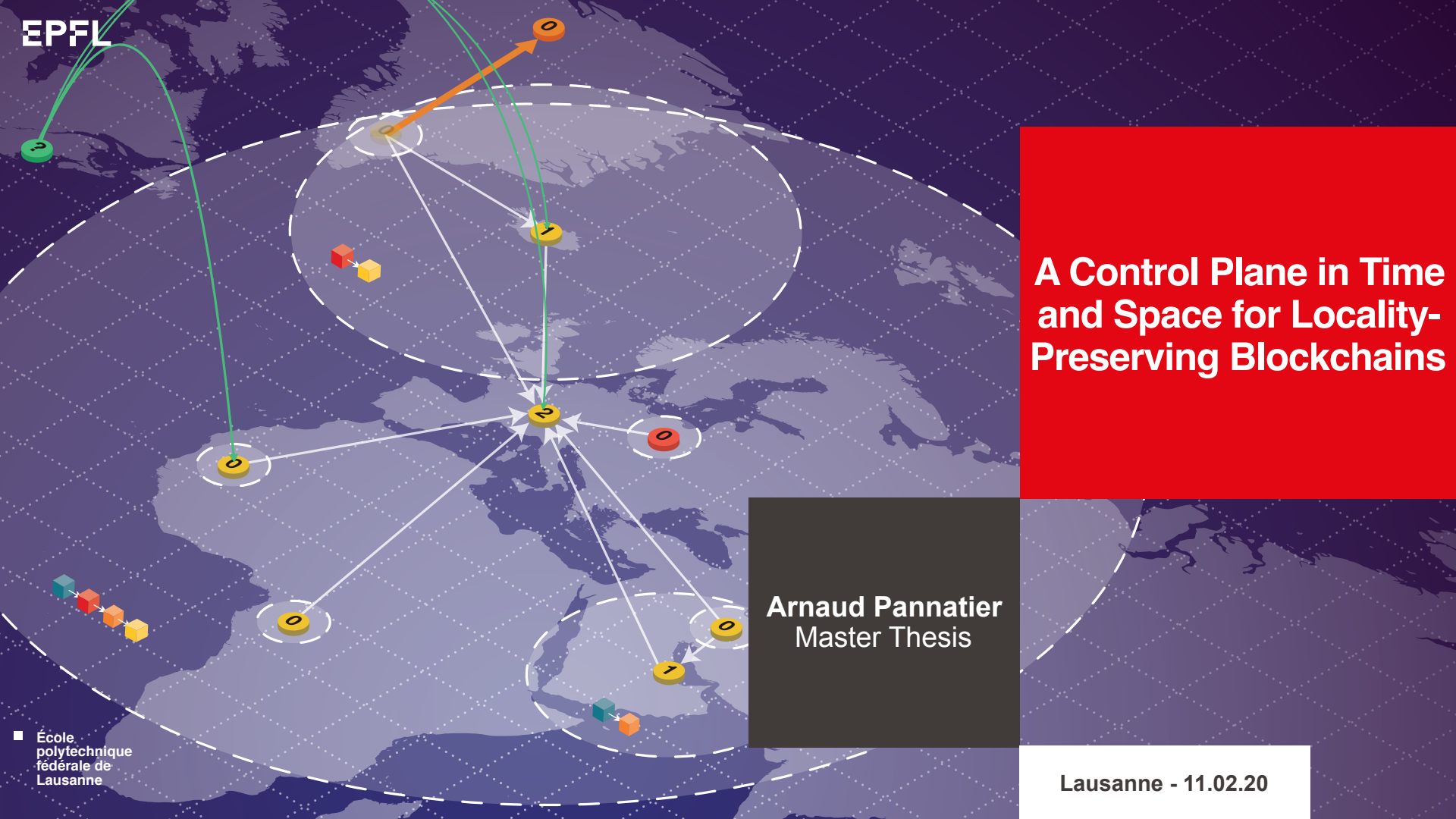


A Control Plane in Time and Space for Locality-Preserving Blockchains

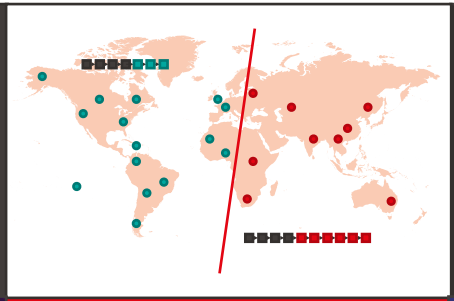
Arnaud Pannatier
Master Thesis

École polytechnique fédérale de Lausanne

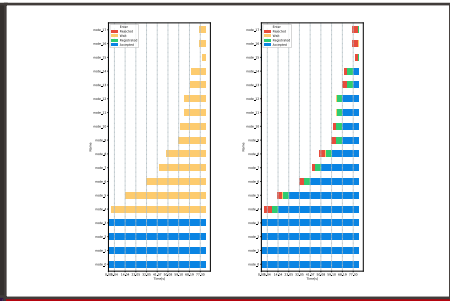
Lausanne - 11.02.20

Outline

1. Some problems of traditional blockchains
WWIII Scenarios
Time for validation



4. Results

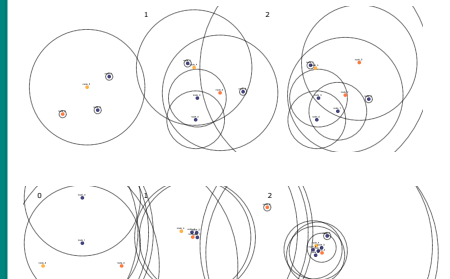


2. A solution : Nyle
Using regions replication to defeat the problems

5. Improvements

3. My work
Adapt the regions to nodes modifications

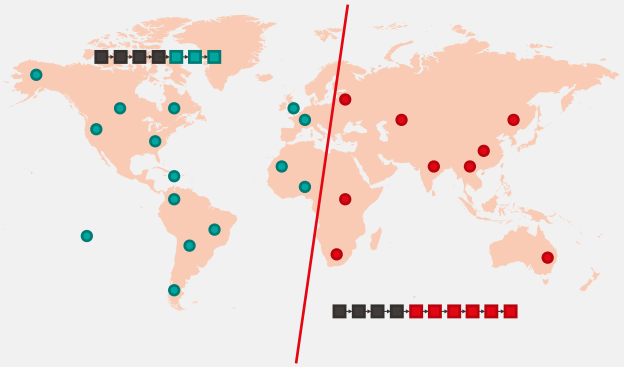
6. Conclusion



Problems of traditional blockchains

World War III Scenarios

Time for validation



A Solution : Nyle

Replicates the system in regions, from local to global

Arnaud Pannatier

A Solution : Nyle

Replicates the system in regions, from local to global

- **World War III Scenarios**

  If a global partition occurs, the systems still works in regions that are not split

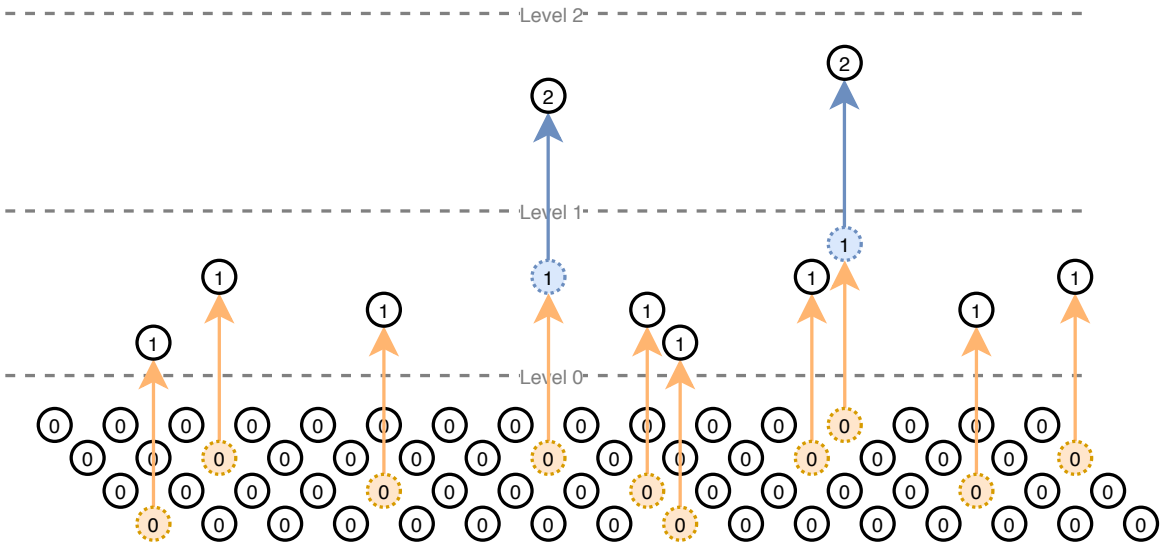
- **Time for validation**

  Transactions can be validated in regions

Arnaud Pannatier

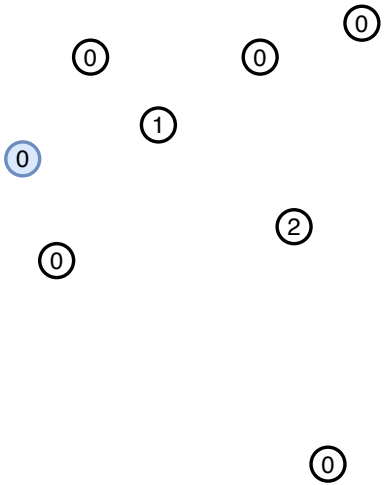
Nyle : Tools

Lottery



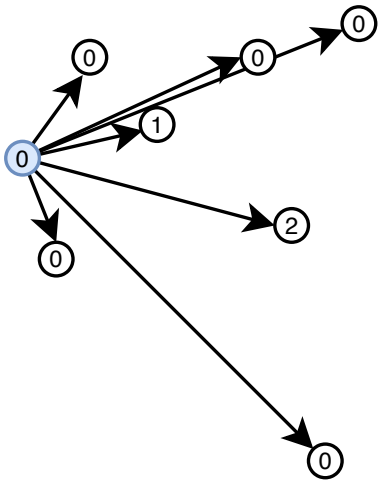
Nyle : Tools

Bunch



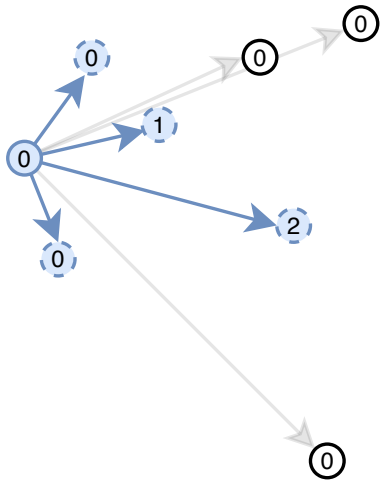
Nyle : Tools

Bunch



Nyle : Tools

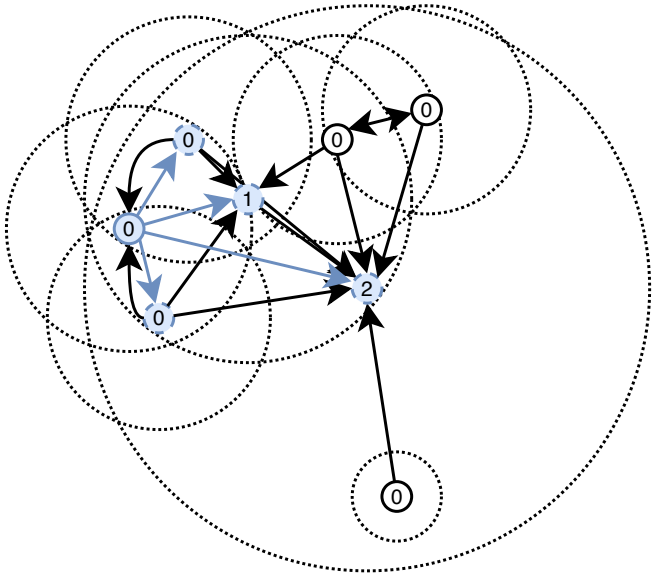
Bunch

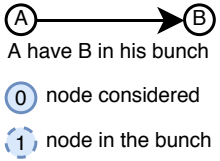


Arnaud Pannatier

Nyle : Tools

Bunch

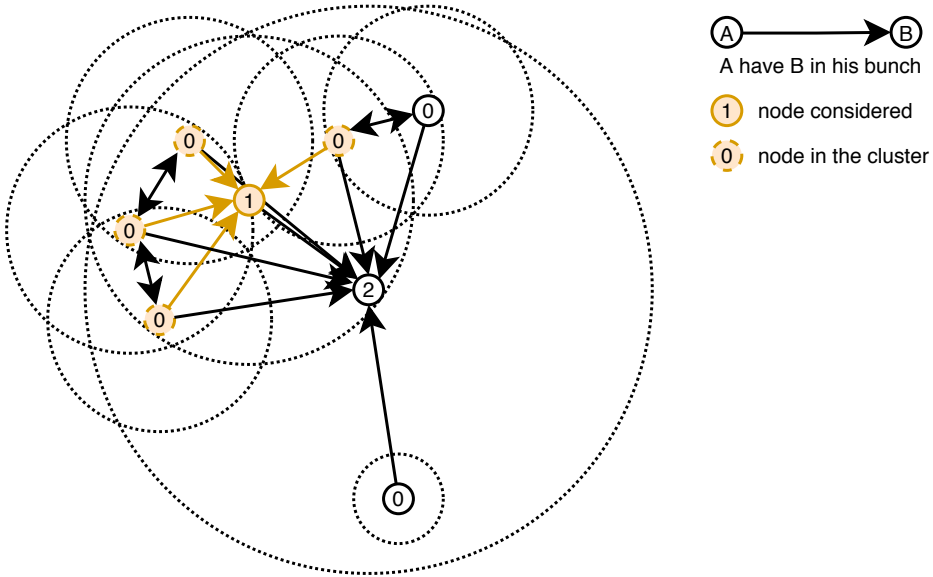




Nyle : Tools

Arnaud Pannatier

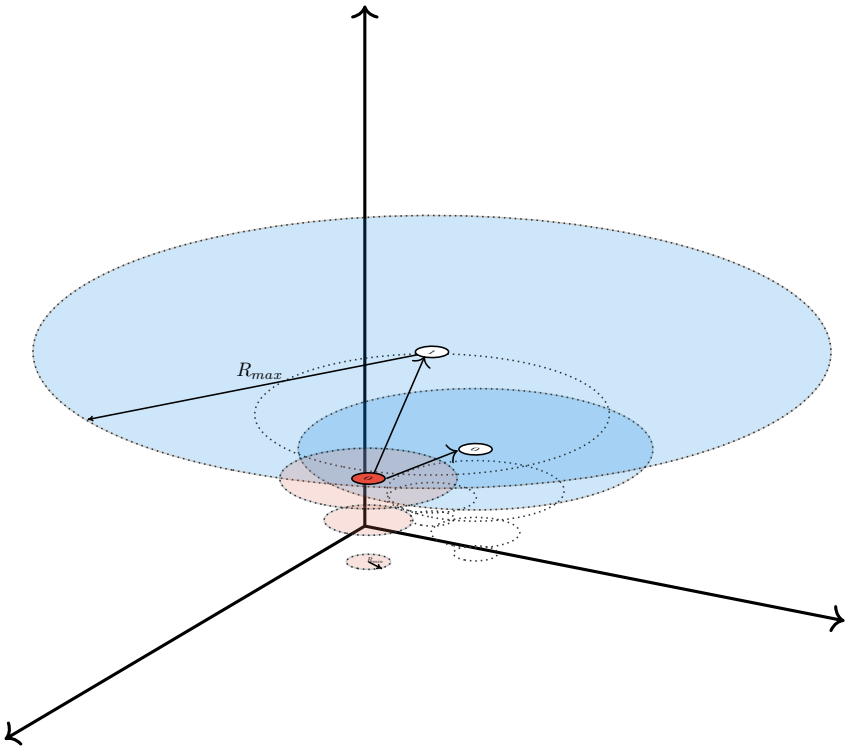
Cluster



Arnaud Pannatier

Nyle : Tools

Regions



A Solution : Nyle

Arnaud Pannatier

Property

By design : Any two nodes in the system participate within a region with a radius of a small multiple of their *RTT (Round-trip-time)*

Master Thesis : Movement & Churn

Arnaud Pannatier

What if nodes move, join or leave ?

We know how to create region for a **static system**, but we need to find a way to **adapt** the region as the system **evolves**

Master Thesis : A Control Plane for Locality Preserving Blockchains

Arnaud Pannatier

Need a Control Plane !

We need a **Control Plane for Locality Preserving Blockchains** : a protocol that can adapt the regions through time

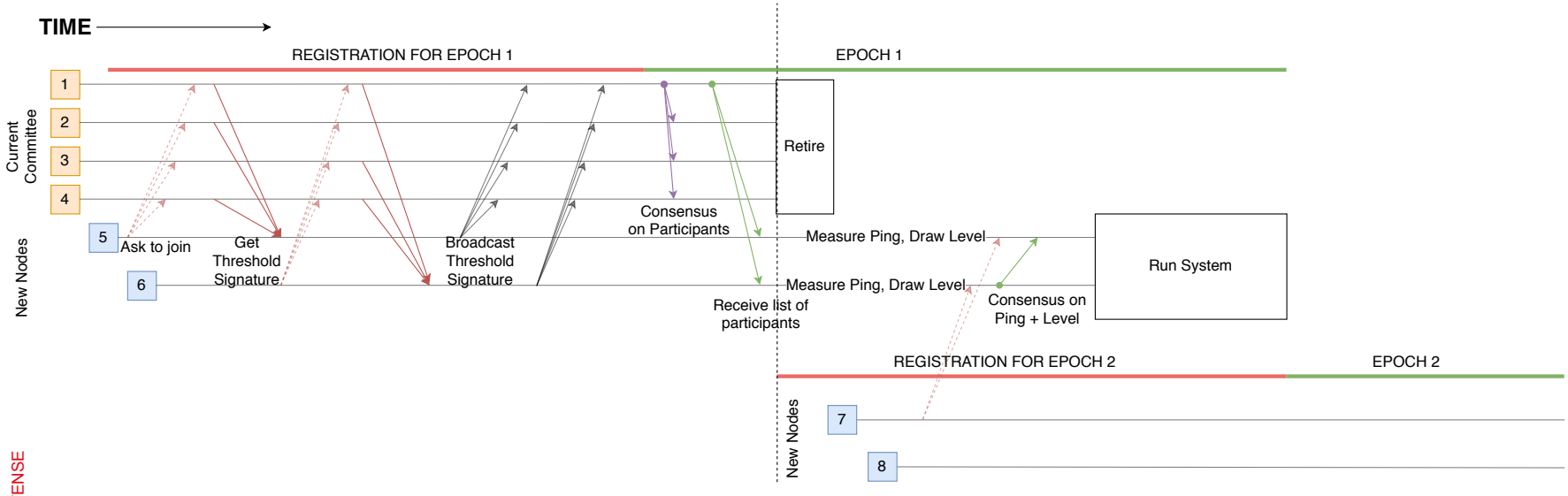
Control Plane : Hypotheses

- Internet-like network
  (one to one communication)

- Round Trip Time is correlated with distance

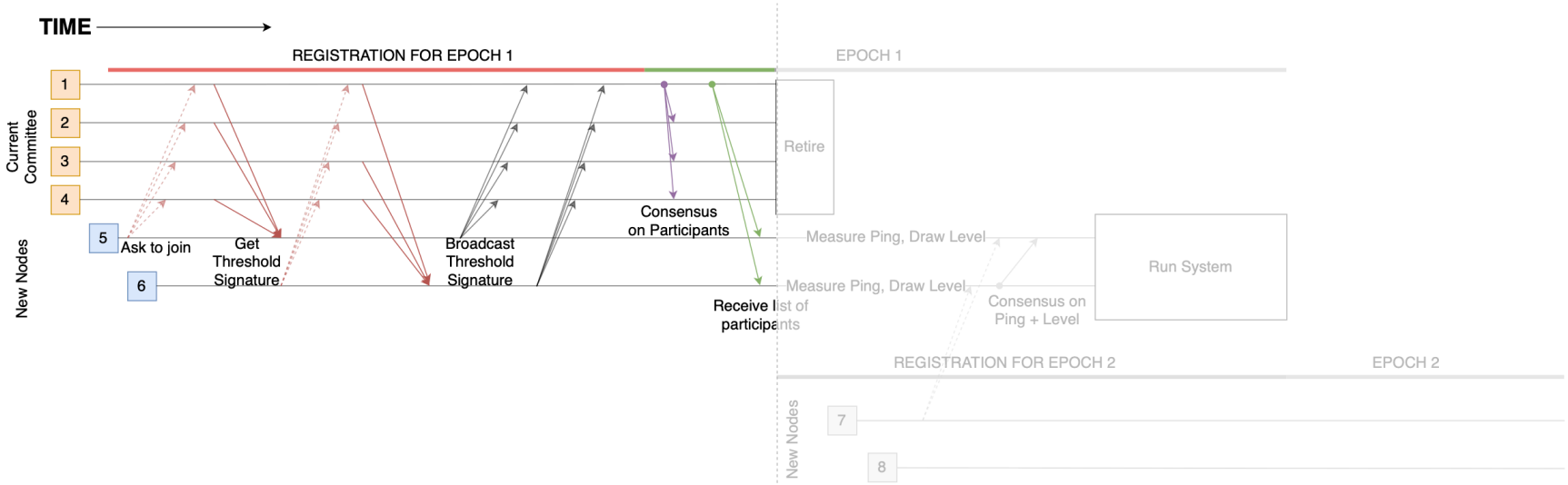
Control Plane: Protocol

Arnaud Pannatier



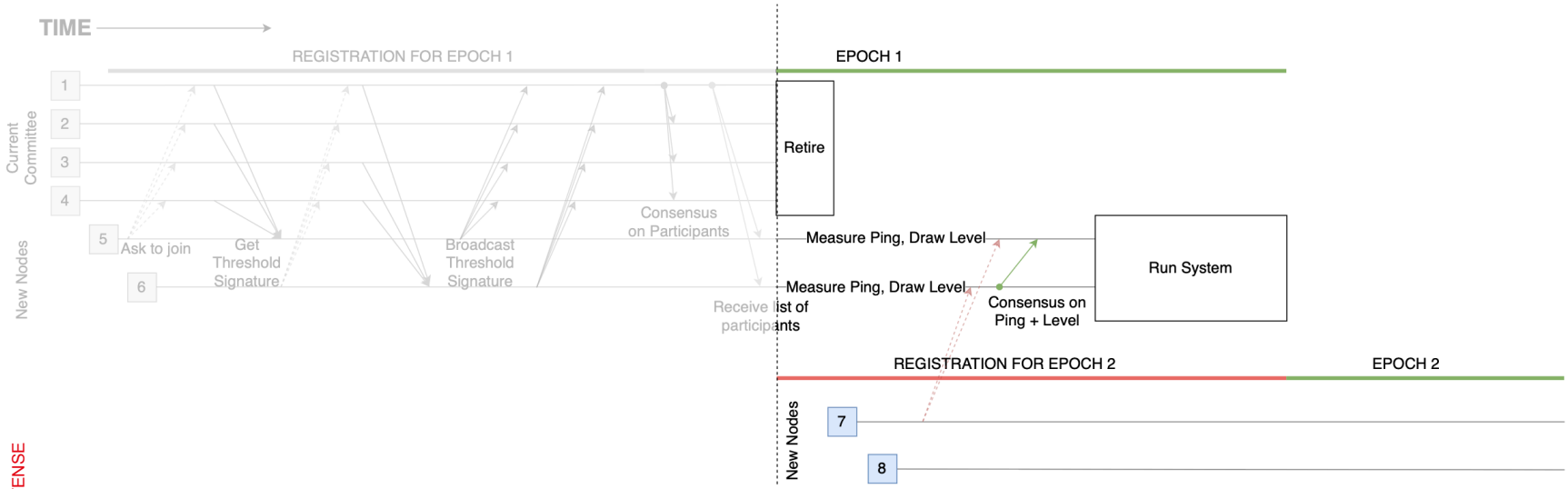
Control Plane: Protocol

Arnaud Pannatier

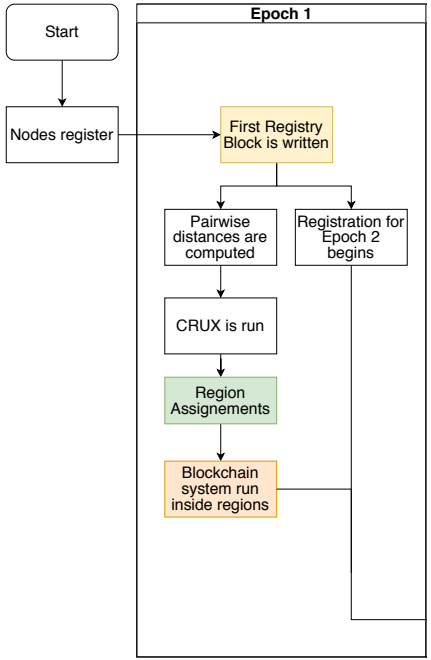


Control Plane: Protocol

Arnaud Pannatier

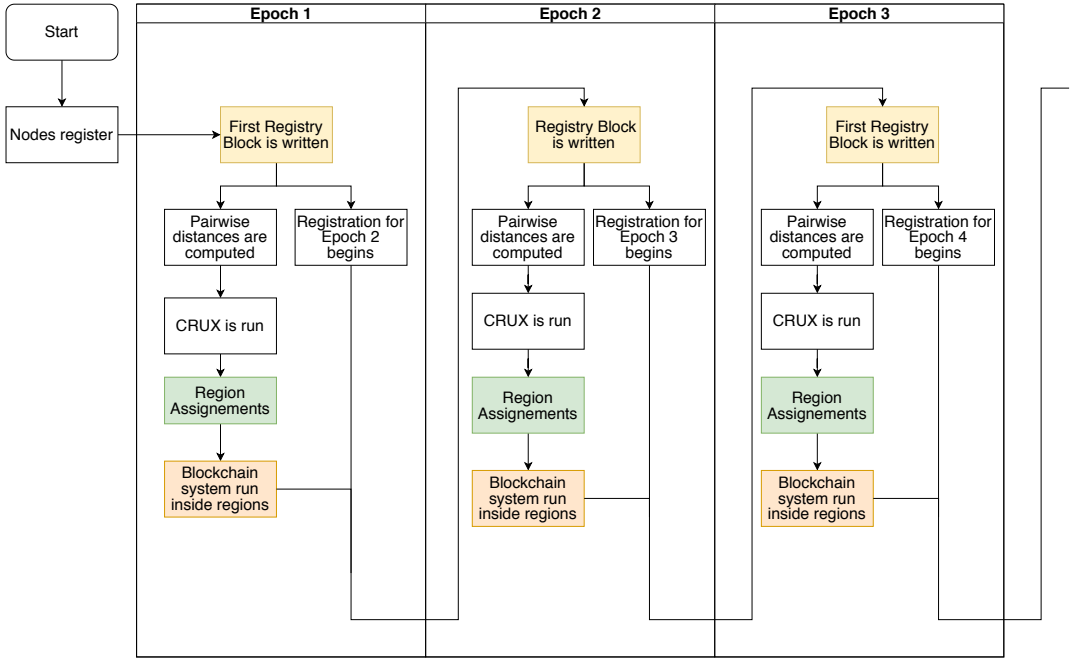


Control Plane: Design



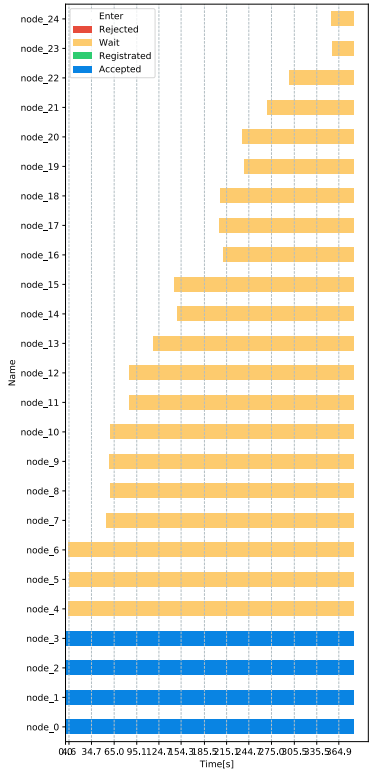
Control Plane: Design

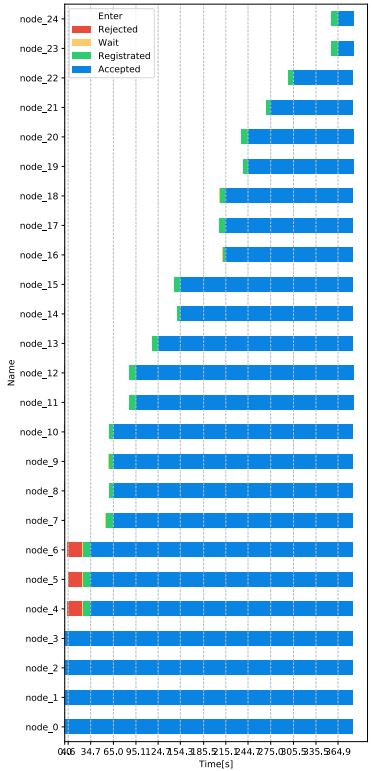
Arnaud Pannatier



Control Plane: Results

Without Control Plane

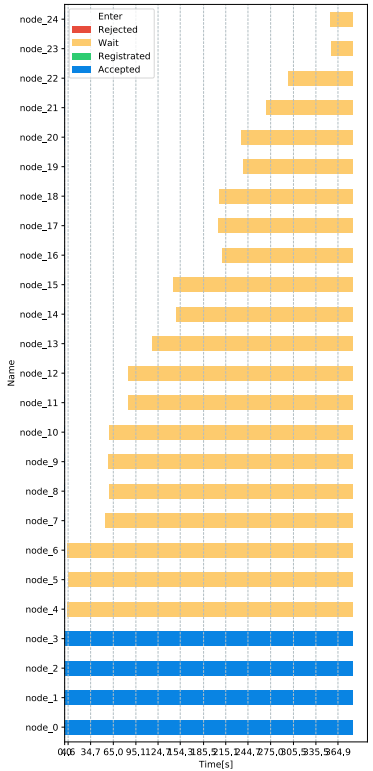




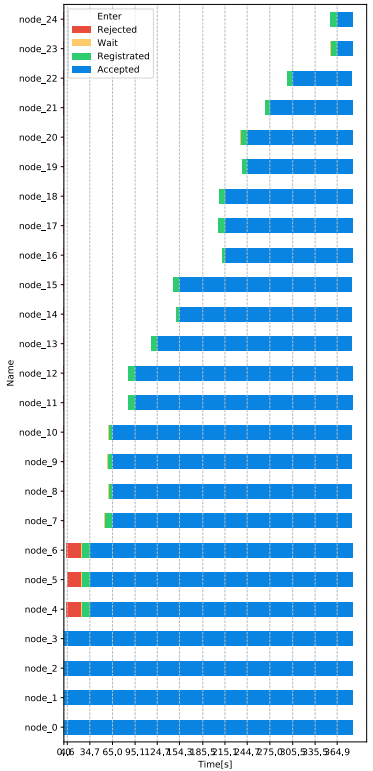
With Control Plane

Control Plane: Results

Arnaud Pannatier



Without Control Plane

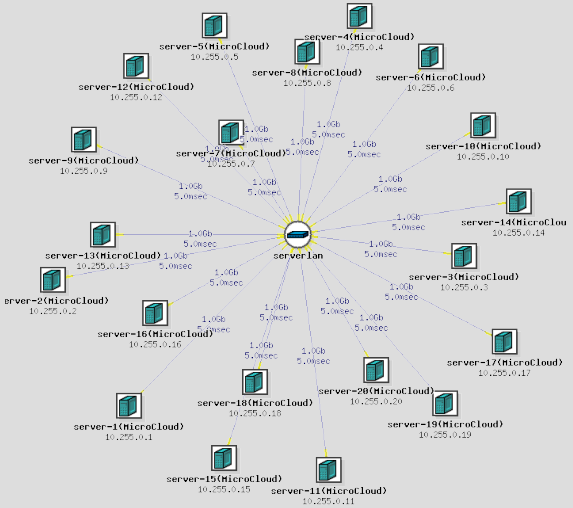


With Control Plane

Parameters of the experiment

Hardware
20 MicroCloud nodes
Linked to a central LAN
Delay of links : 5ms
Throughput of link 1.0Go
Total of 30 processes

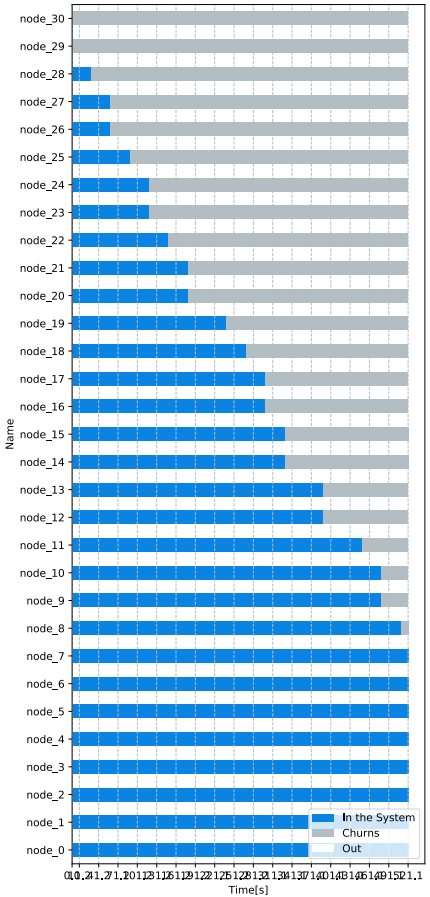
Experiment
Registration period : 10sec
Epoch duration : 20 sec
A committee of 4 nodes is set at genesis
A random number (between 0-7) of nodes joins at each epoch.
Each node waits a random amount of time (between 0 and 7.5 sec) before asking for admission.
If a node failed to join at the first attempt it will ask again for the next epoch.

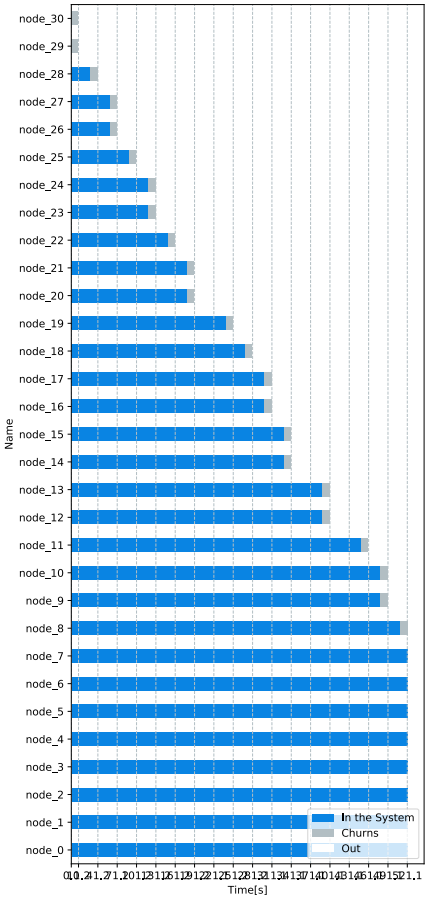


Control Plane: Results

Arnaud Pannatier

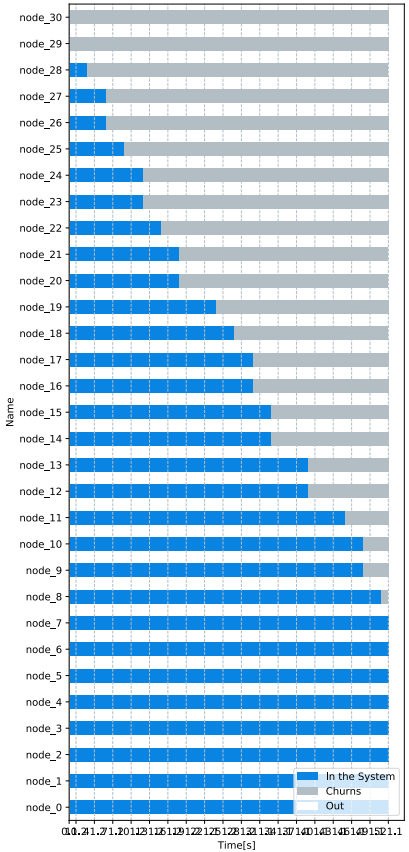
Without Control Plane



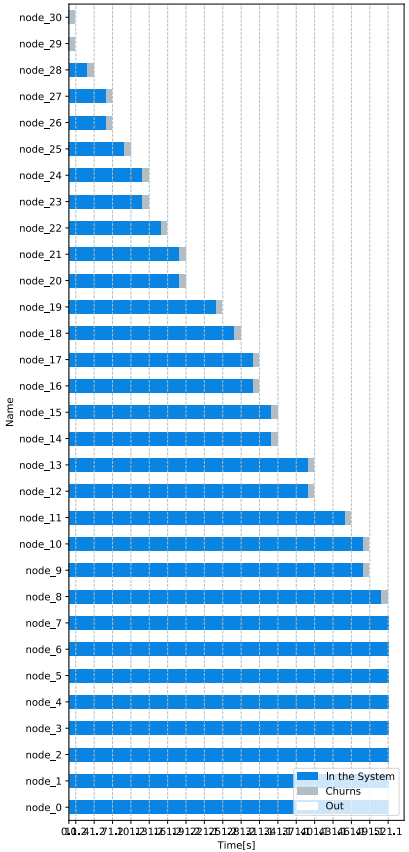


With Control Plane

Control Plane: Results



Without Control Plane

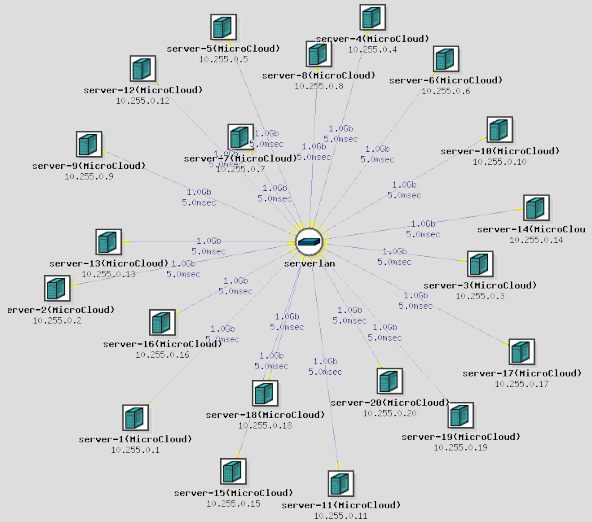


With Control Plane

Parameters of the experiment

Hardware
20 MicroCloud nodes
Linked to a central LAN
Delay of links : 5ms
Throughput of link 1.0Go
Total of 30 processes

Experiment
Registration period : 10sec
Epoch duration : 20 sec
A committee of 30 nodes is set at genesis
A random number (between 0-3) of Nodes fail at each epoch.
Each node waits a random amount of time (between 0 and 7.5 sec) before failing.



Security Analysis

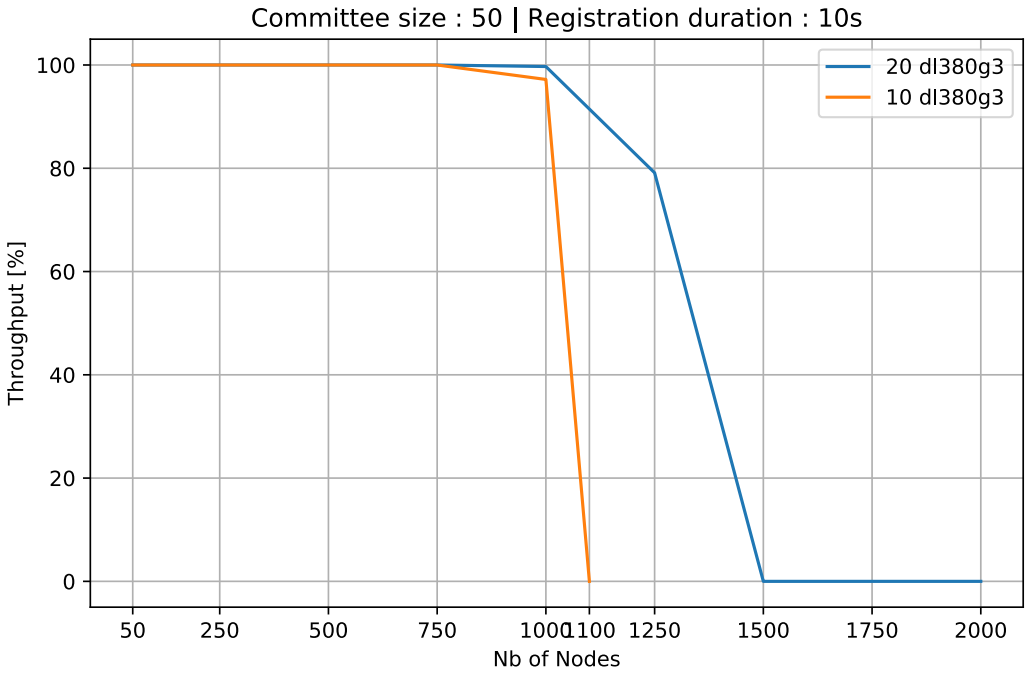
- Delay Attacks
- Man-in-the-middle
- Malicious nodes
- Adversary have limited computational power

	Message	Signature	Effects of a Sufficient Delay
1.	Join request	Requesting node	Request refused
2.	Threshold signature of the request	Threshold number of the current committee	Request refused
3.	Broadcasting of the Threshold signature	Threshold number of the current committee	Request refused
4.	Messages for the consensus on the participants, list of the participants	Leader of the current committee	View Change
5.	List of pings and levels	Leader of the current committee	View Change

Table 4.1 – List of the messages exchanged during the protocol. The signature of the message and the effects of a delay are given.

Control Plane: Experiment - Throughput

If the load on one machine becomes too large, the registration rate drops as nodes cannot complete the protocol in time



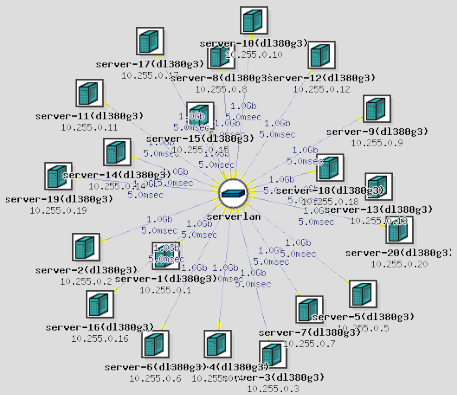
Control Plane: Experiment - Throughput

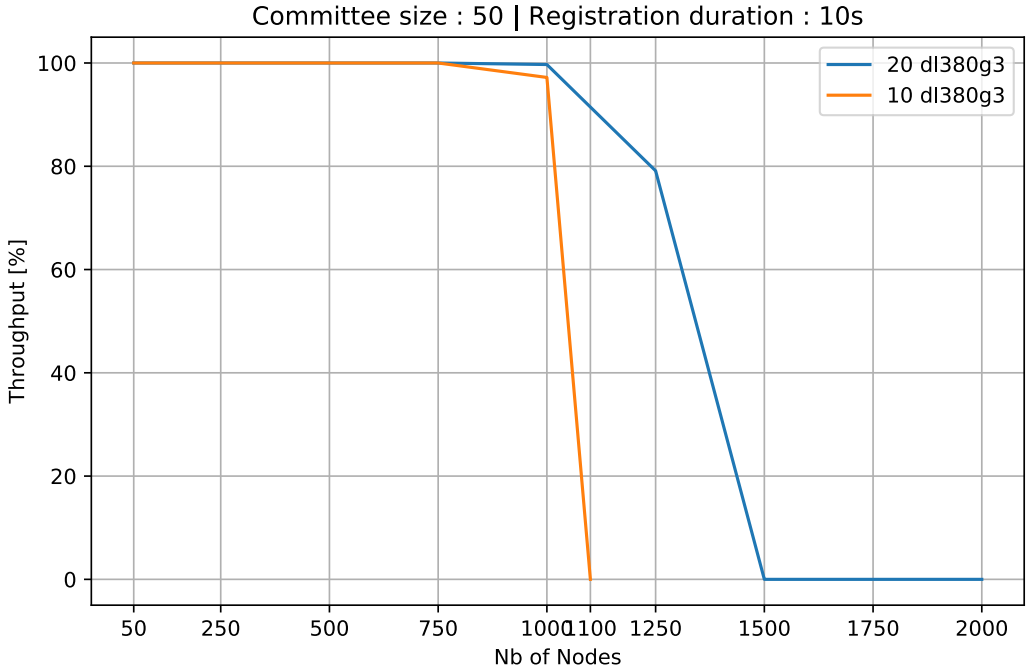
Arnaud Pannatier

Parameters of the experiment

Hardware
20 - 10 dl380g3 nodes
Linked to a central LAN
Delay of links : 5ms
Throughput of link 1.0Go
Total of 2000 - 1100 processes

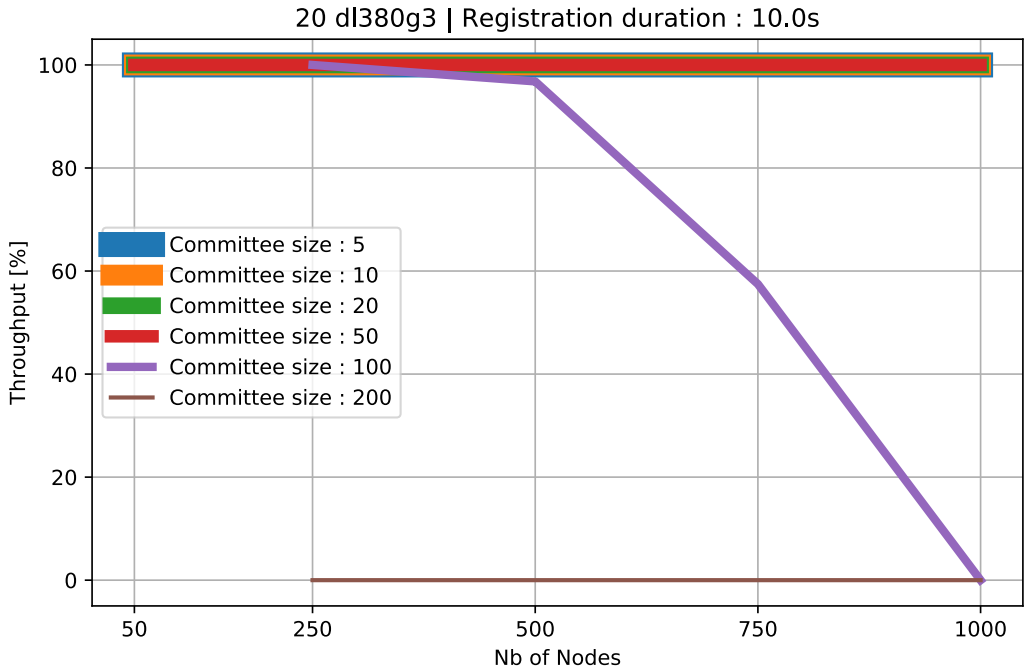
Experiment
Registration period : 10sec
Epoch duration : 20 sec
A committee of 50 nodes is set at genesis
A certain number of nodes (depicted on x axis) try to get accepted for the next epoch





Experiment - Committee Size

As the committee size increases, the throughput drop as the load on nodes increases



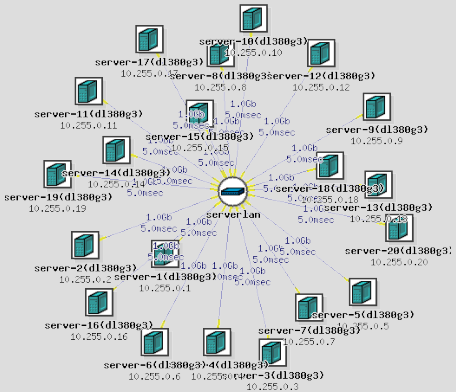
Experiment - Committee Size

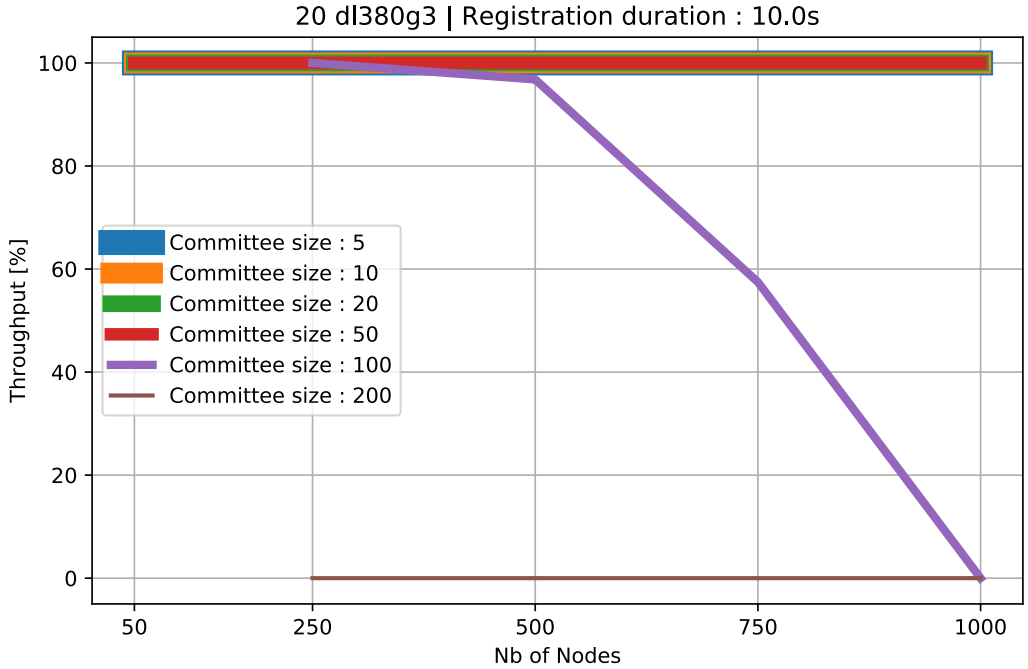
Arnaud Pannatier

Parameters of the experiment

Hardware
20 dl380g3 nodes
Linked to a central LAN
Delay of links : 5ms
Throughput of link 1.0Go
Total of 1000 processes

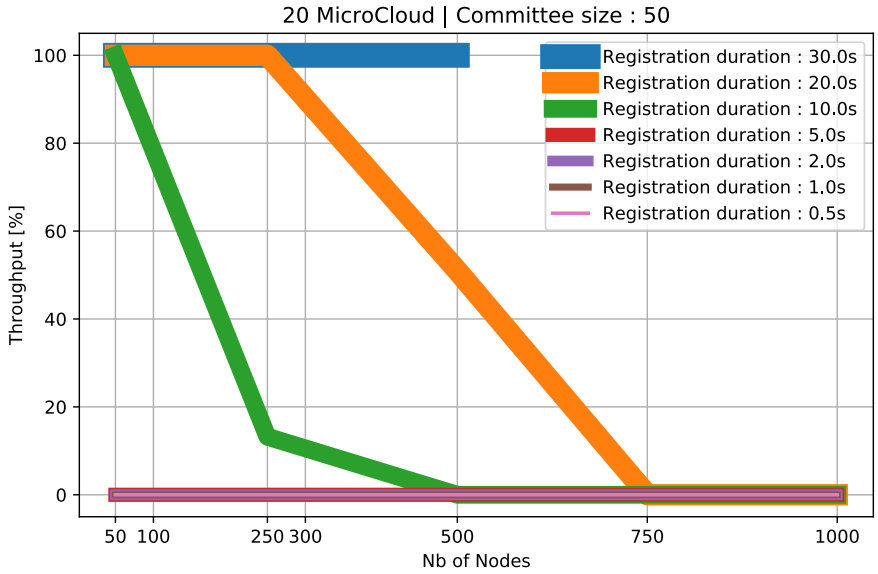
Experiment
Registration period : 10sec
Epoch duration : 20 sec
Committee Size : variable (legend)
A certain number of nodes (depicted on x axis) try to get accepted for the next epoch





Experiment - Change Duration

As the duration increases, the protocol starts to work again !

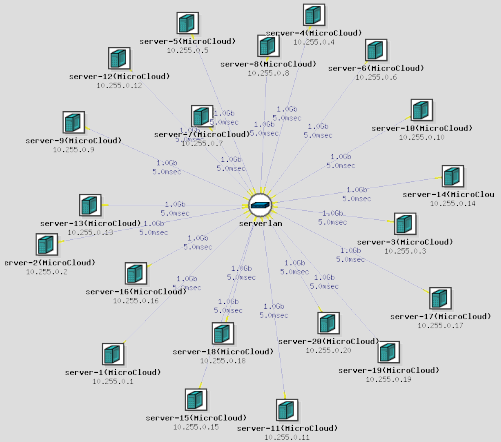


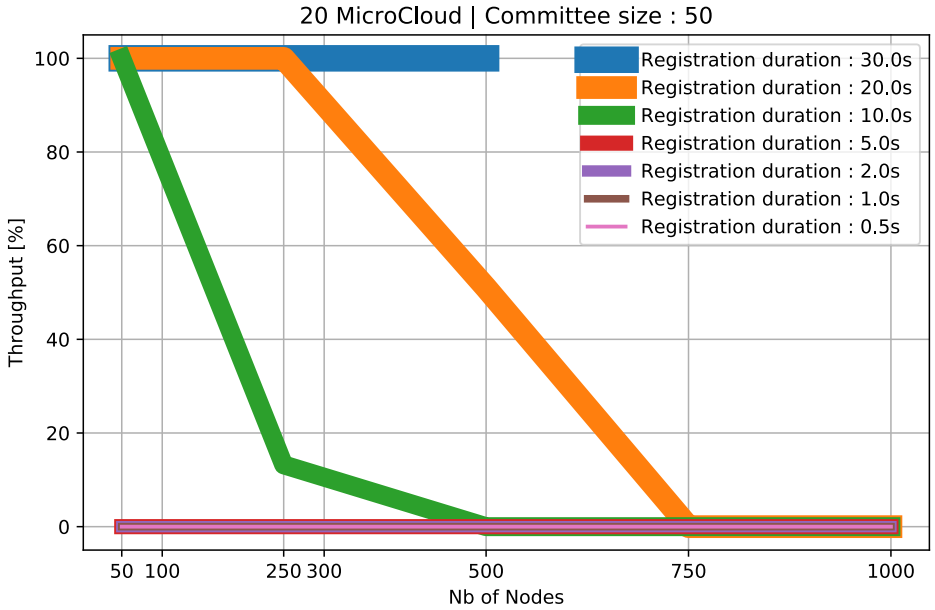
Experiment - Change Duration

Parameters of the experiment

Hardware
20 MicroCloud nodes
Linked to a central LAN
Delay of links : 5ms
Throughput of link 1.0Go
Total 500 - 1000 processes

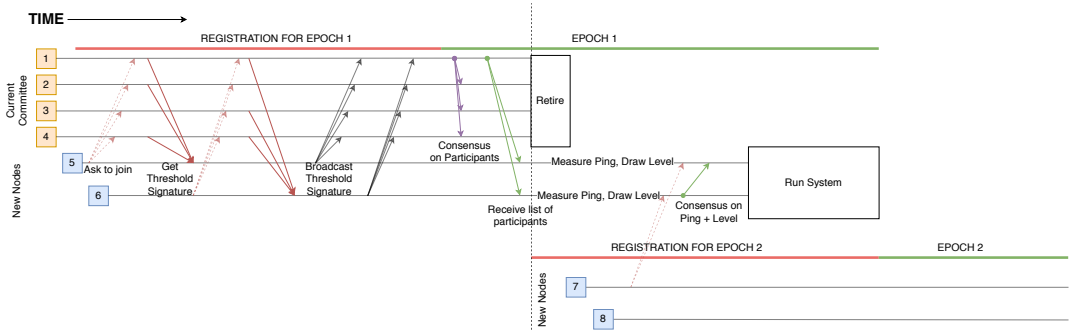
Experiment
Registration period : variable (legend)
Epoch duration : 20 sec
Committee size : 50
A certain number of nodes (depicted on x axis) try to get accepted for the next epoch





Control Plane: Drawbacks

- Control Plane is global
- Epoch transition requires ressources
- Communications



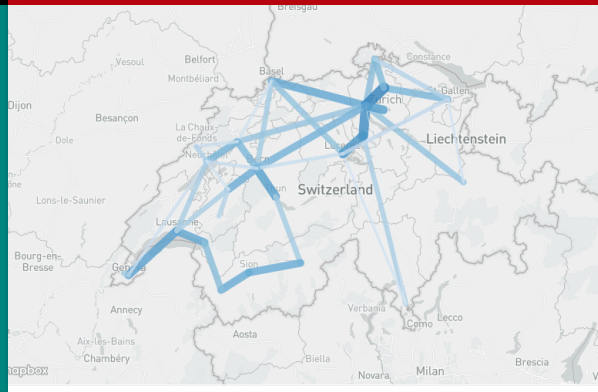
Control Plane: Improvements

Arnaud Pannatier

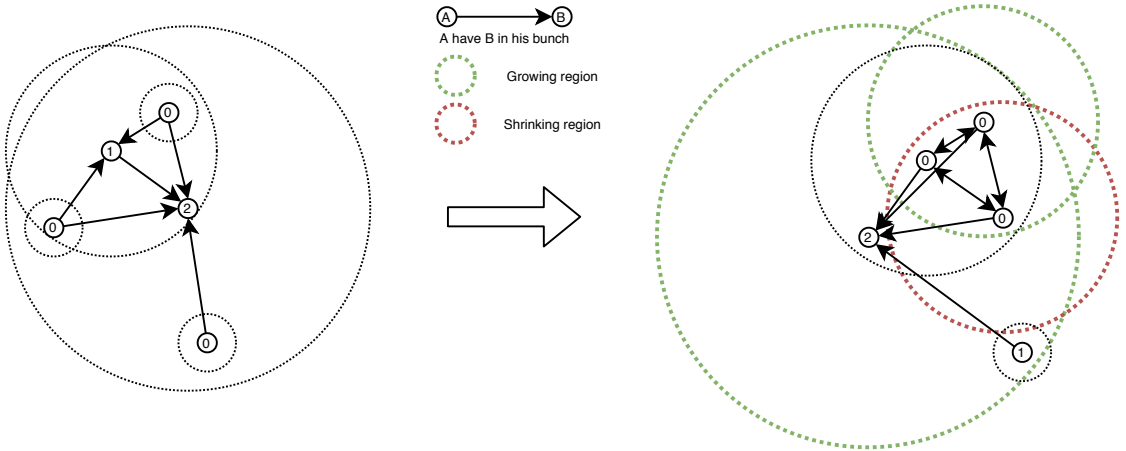
Locarno Treaties
reduces the differences from one epoch to the next

Space Time Interaction distance

Fog of the war
reduces the amount of informations one node needs to know



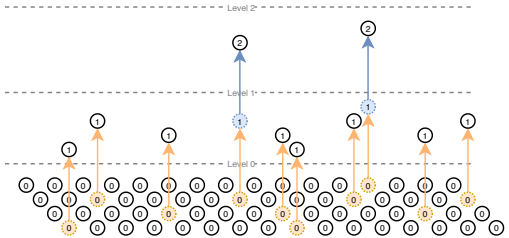
Locarno Treaties : Purpose



Random Lottery implies a lot of changes in region

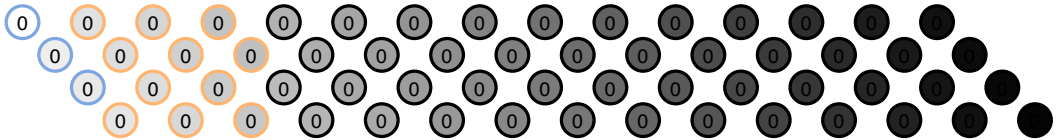
Locarno Treaties : Idea

Random Lottery



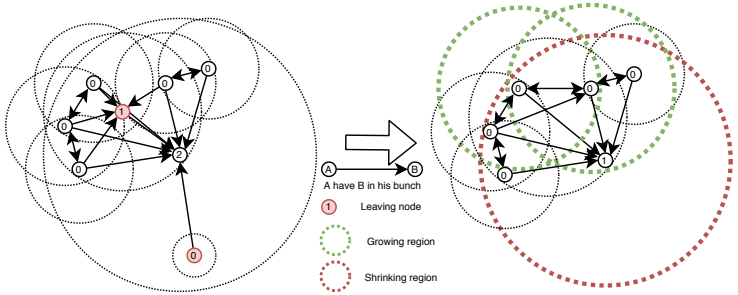
Locarno Lottery

Total : 60	Level 2 **3**	Level 1 **11**	Level 0 **46**

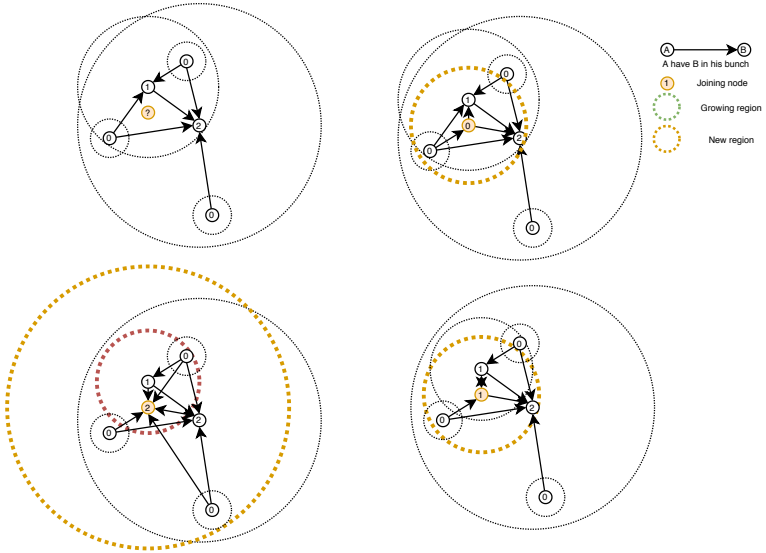


Change the lottery to allow nodes to keep their levels

Locarno Treaties : Example



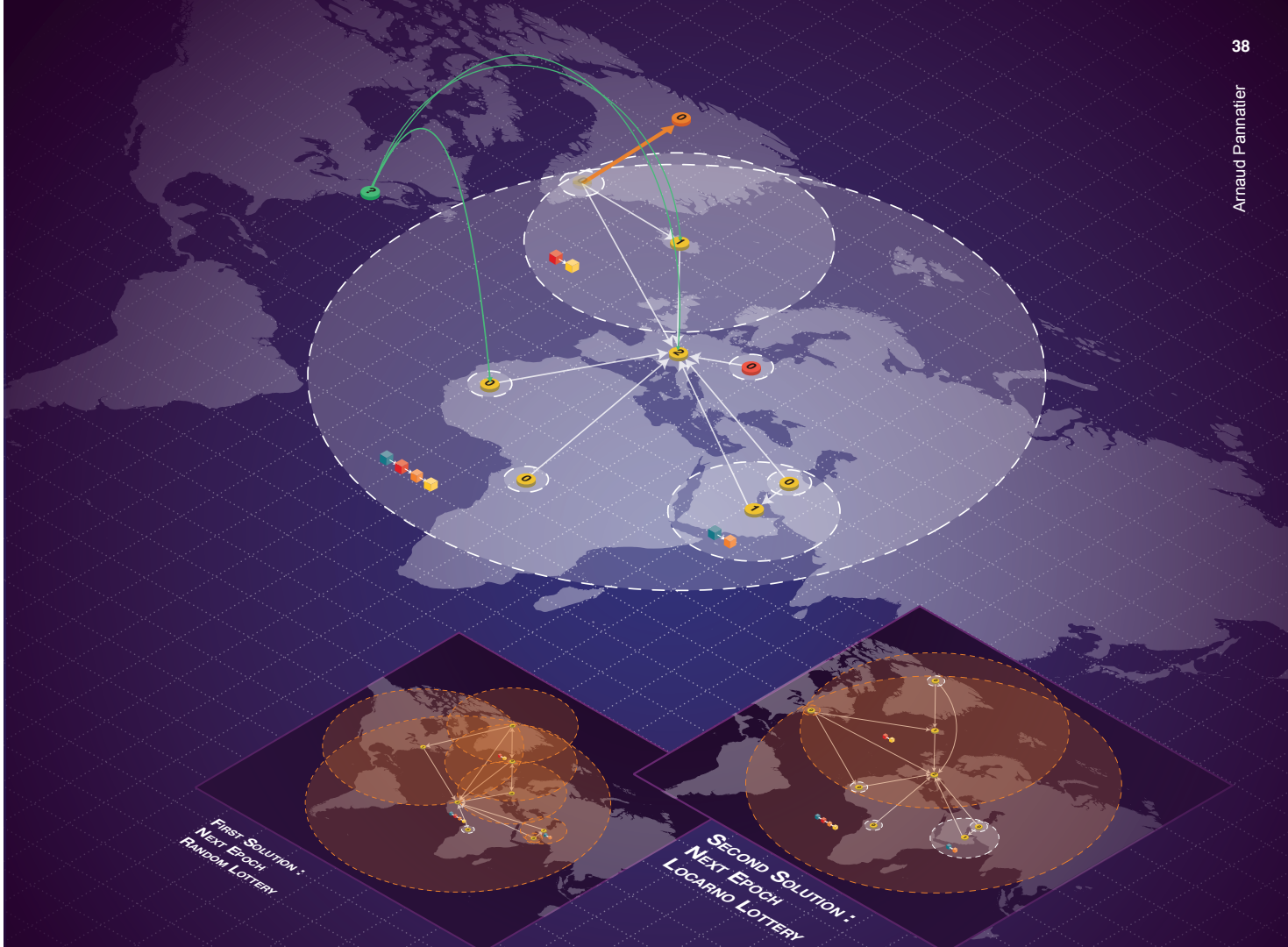
Example : node leaving



Example : node joining

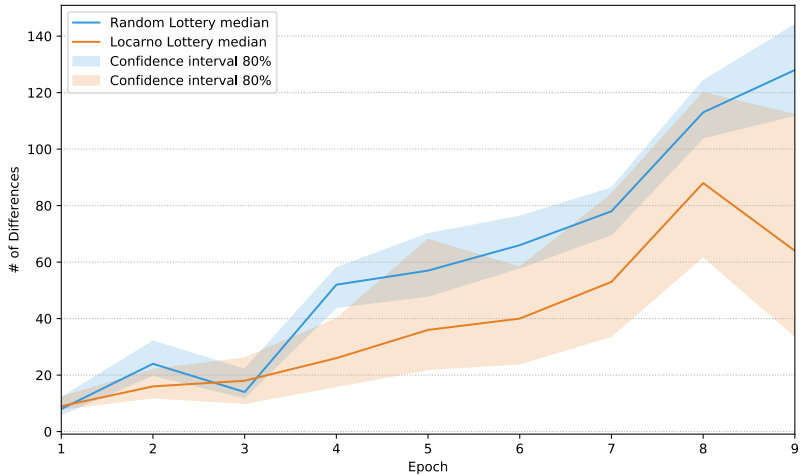
If nodes keep their level, regions does not need to be changed that much

Comparison


First Solution :
Next Epoch
Random Lottery
Second Solution :
Next Epoch
Locarno Lottery

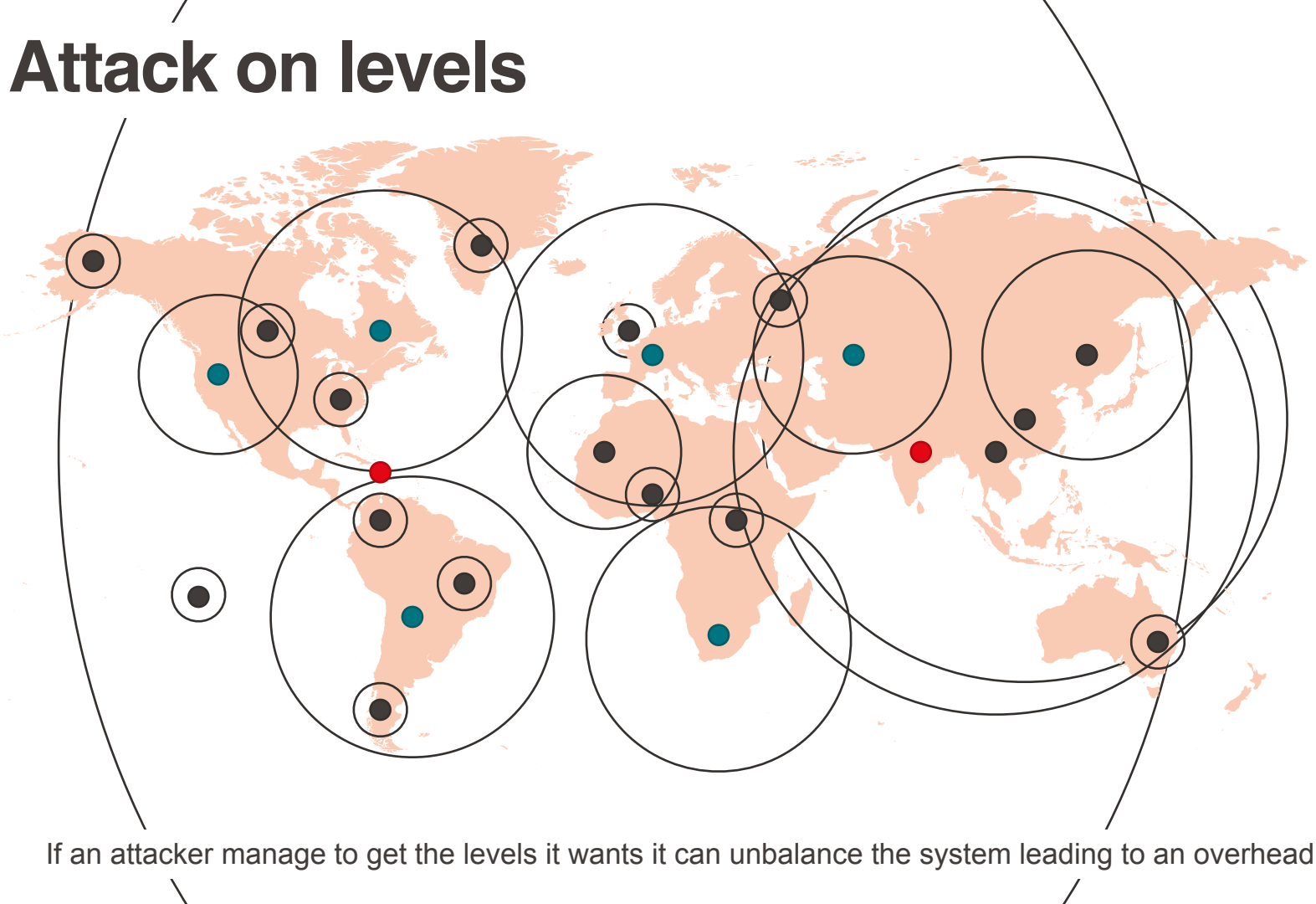
Locarno Treaties : Evaluation

- 100 different experiment using both lotteries
- System starts with 4 nodes, 2 are added at each epochs
- Same evolution for both lotteries
- Locarno Lottery reduces the number of differences
- Variance comes from teleportation



Arnaud Pannatier

Attack on levels



If an attacker manage to get the levels it wants it can unbalance the system leading to an overhead

Fog of the war : Purpose

Arnaud Pannatier

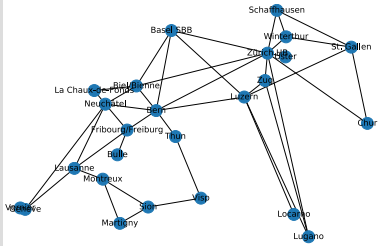
Nodes do not need to know everything

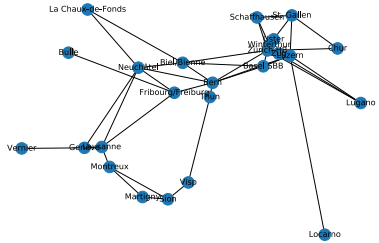
Arnaud Pannatier

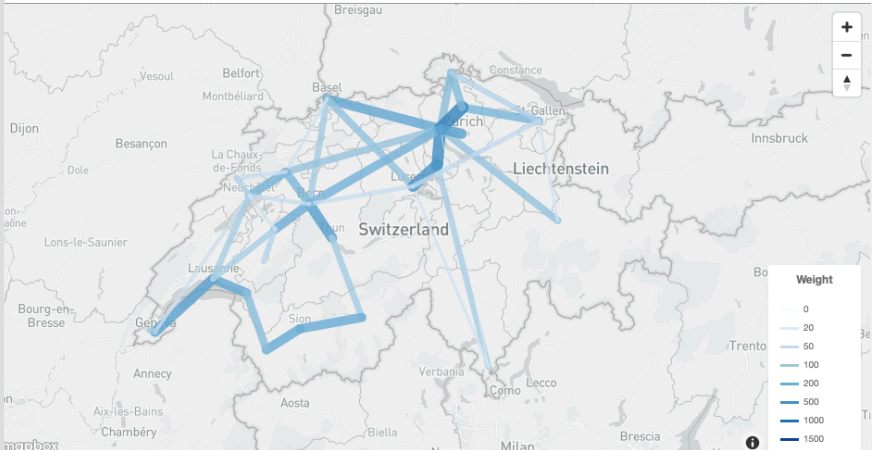
Space Time interaction metric

- Maybe what we want to conserve might not be latencies or availability but *interactions* between nodes

- If there is random partitions, one might want to protect nodes that interacts a lot from failing







Possible improvements

- Replace synchronized clocks by *Timestamp Logical Clocks (TLC)*
- Allow the creation of region with special meaning (for example Switzerland, Europe, …)

- Protect against attack on level by checking at the beginning of one epoch the density of a levels are constant across the whole system

Conclusion

- I designed a protocol for a **control plane in time and space for locality-preserving blockchains**
- I did a security analysis for the control plane, did some experiments and outlined it's drawbacks

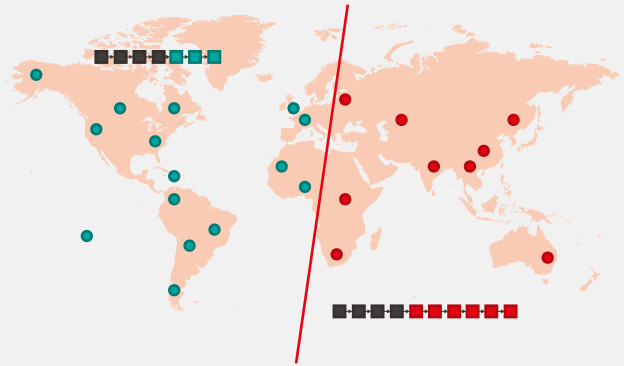
- I proposed a solution for each drawbacks and I implemented some of them

References

- *Maps of the world came from Free Vector Maps*
- *The video game depicted in Fog of the War is Microsoft. Age of Empires II : The Age of Kings. [CD-ROM]. 1999.*
- *Maps used to display Swiss Federal Railway connection info : MapBox. https:// www.mapbox.com. Accessed: 2020-01-15.*
- *The data for Swiss Federal Railway are accessible at : opendata.swiss. https:// opendata.swiss/en/dataset/fahrplanentwurf-2019-hrdf/ resource/ 32dfd2e1-86a6-4680-9935-b76226dddee1. Accessed: 2020-01-07.*
- ***This works has found inspiration in the following papers :***
- ***Cristina Basescu, Michael F. Nowlan, Kirill Nikitin, Jose M. Faleiro, and Bryan Ford. "Crux: Locality-Preserving Distributed Services". In: (June 2014). arXiv: 1405.0637. U R L : http: /arxiv.org/abs/1405.0637.***
- *Dan Boneh, Manu Drijvers, and Gregory Neven. "Compact Multi-signatures for Smaller Blockchains". In: Advances in Cryptology – ASIACRYPT 2018. Ed. by Thomas Peyrin and Steven Galbraith. Cham: Springer International Publishing, 2018, pp. 435–464. I S B N : 978- 3-030-03329-3.*
- *Miguel Castro and Barbara Liskov. "Practical Byzantine Fault Tolerance". In: February (1999), pp. 1–14.*
- *D. Greenhoe. "Properties of distance spaces with power triangle inequalities". In: Carpathian Mathematical Publications 8.1 (2016). I S S N : 2075-9827. D O I : 10 . 15330 / cmp.8.1.51-82.*
- *Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, Bryan Ford, Eleftherios Kokoris-Kogias, and Bryan Ford Epfl. "Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing". In: Proceedings of the 25th USENIX Security Symposium (2016). arXiv: 1602.06997. U R L : https://www.usenix. org/conference/usenixsecurity16/technical-sessions/presentation/kogias.*
- *Leslie Lamport. "The Part-Time Parliament". In: 2.May 1998 (2000*
- *Marta Lokhava, Giuliano Losa, David Mazières, Graydon Hoare, Nicolas Barry, Eli Gafni, Jonathan Jove, Rafał Malinowsky, and Jed McCaleb. "Fast and secure global payments with Stellar". In: (2019), pp. 80–96. D O I : 10.1145/3341301.3359636.*
- *Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: (Mar. 2009). U R L : https://bitcoin.org/bitcoin.pdf.*
- *Maxime Sierro, Bryan Ford, Cristina Basescu, and Kelong Cong. "Locality-Preserving Blockchain Implementation". In: (2019). URL: https://github.com/dedis/student% 7B%5C_%7D19%7B%5C_%7Dnylechain/blob/master/report/report.pdf.*
- *Ewa Syta, Philipp Jovanovic, Eleftherios Kokoris Kogias, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Michael J. Fischer, and Bryan Ford. "Scalable Bias-Resistant Distributed Random- ness". In: (2016). https://eprint.iacr.org/2016/1067.*
- *Jiaping Wang and Hao Wang. "Monoxide: Scale out Blockchains with Asynchronous Con- sensus Zones". In: Proceedings of the 16th USENIX Symposium on Networked Systems De- sign and Implementation (NSDI '19) (2019). U R L : https://www.usenix.org/conference/ nsdi19/ presentation/wang-jiaping.*
- *Gavin Wood et al. "Ethereum: A secure decentralised generalised transaction ledger". In: Ethereum project yellow paper 151.2014 (2014), pp. 1–32.*
- *Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan Gueta, and Ittai Abraham. "Hot- Stuff: BFT Consensus in the Lens of Blockchain". In: (2018), pp. 1–23. arXiv: 1803.05069. U R L : http://arxiv.org/abs/1803.05069.*

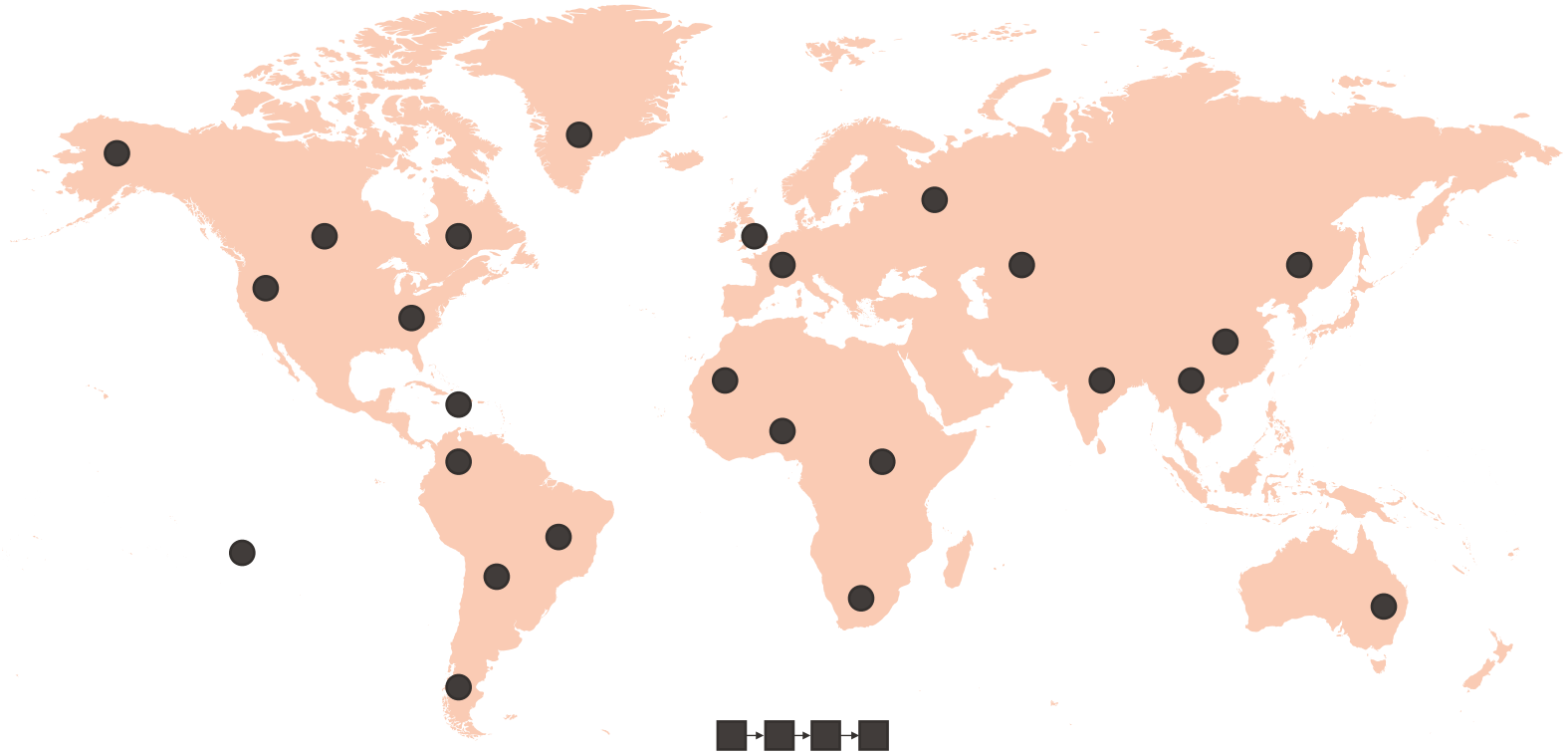
Problems of traditional blockchains

World War III Scenarios

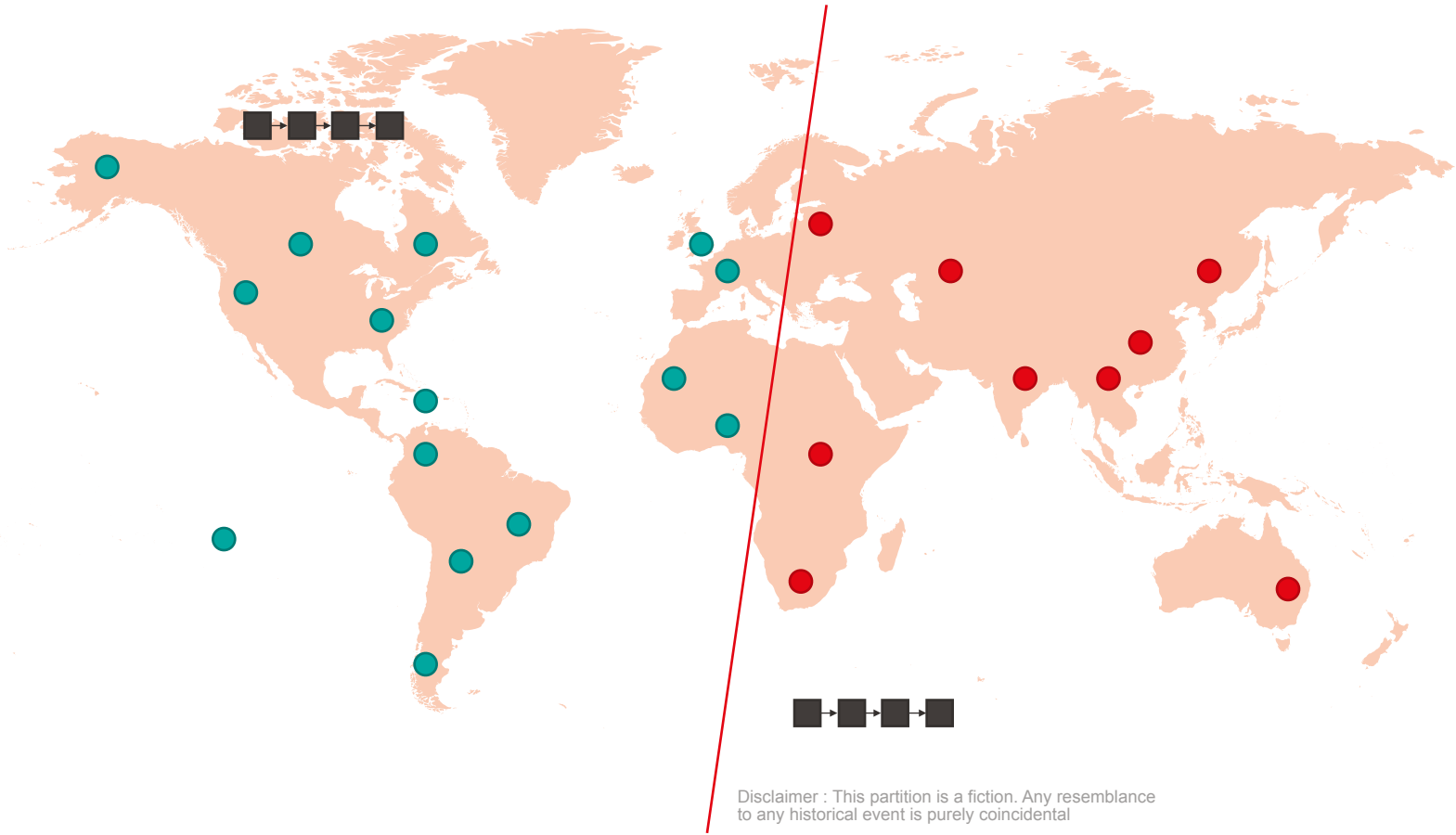


Time for validation

World War III Scenarios

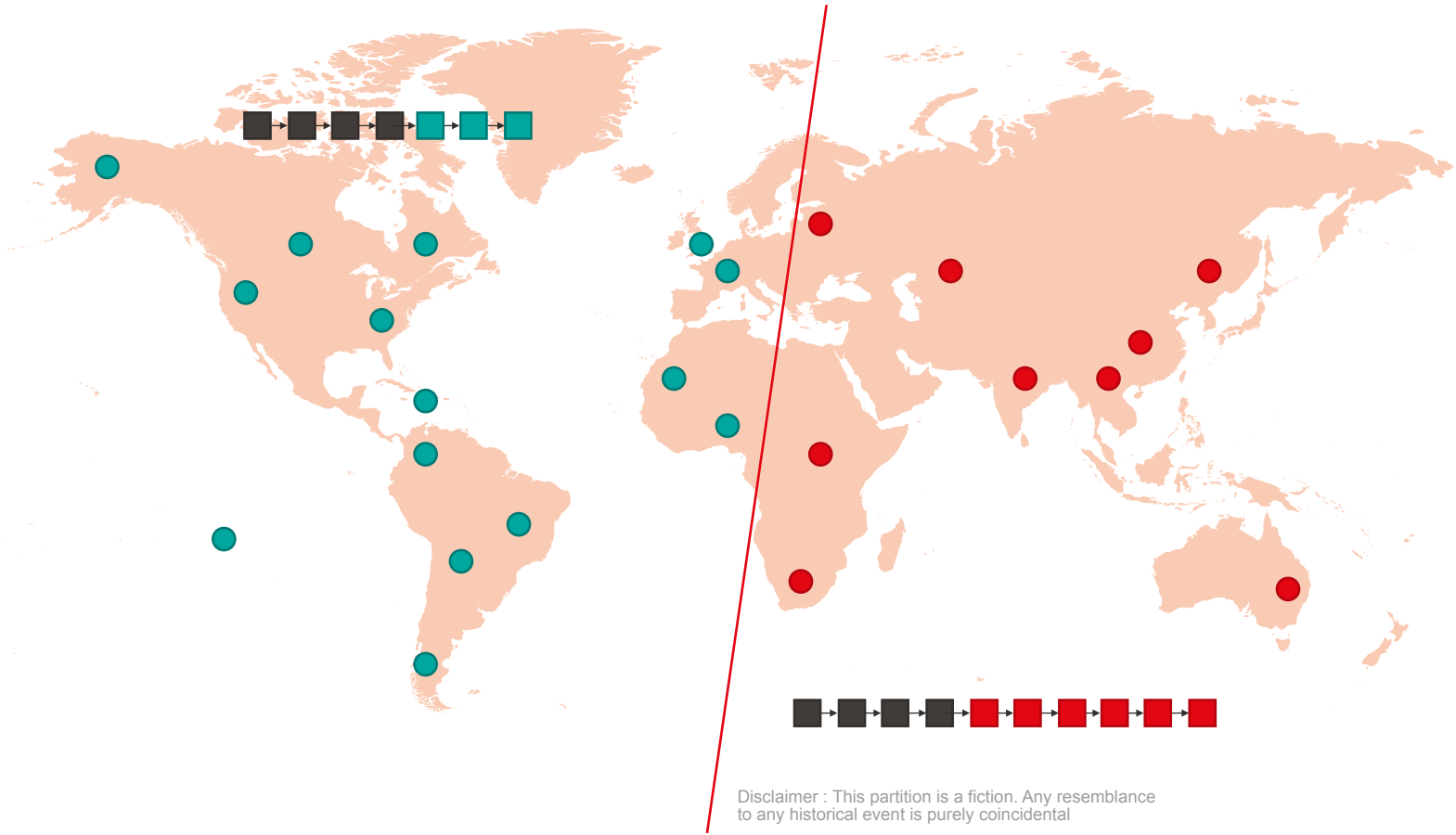


World War III Scenarios



Disclaimer : This partition is a fiction. Any resemblance to any historical event is purely coincidental

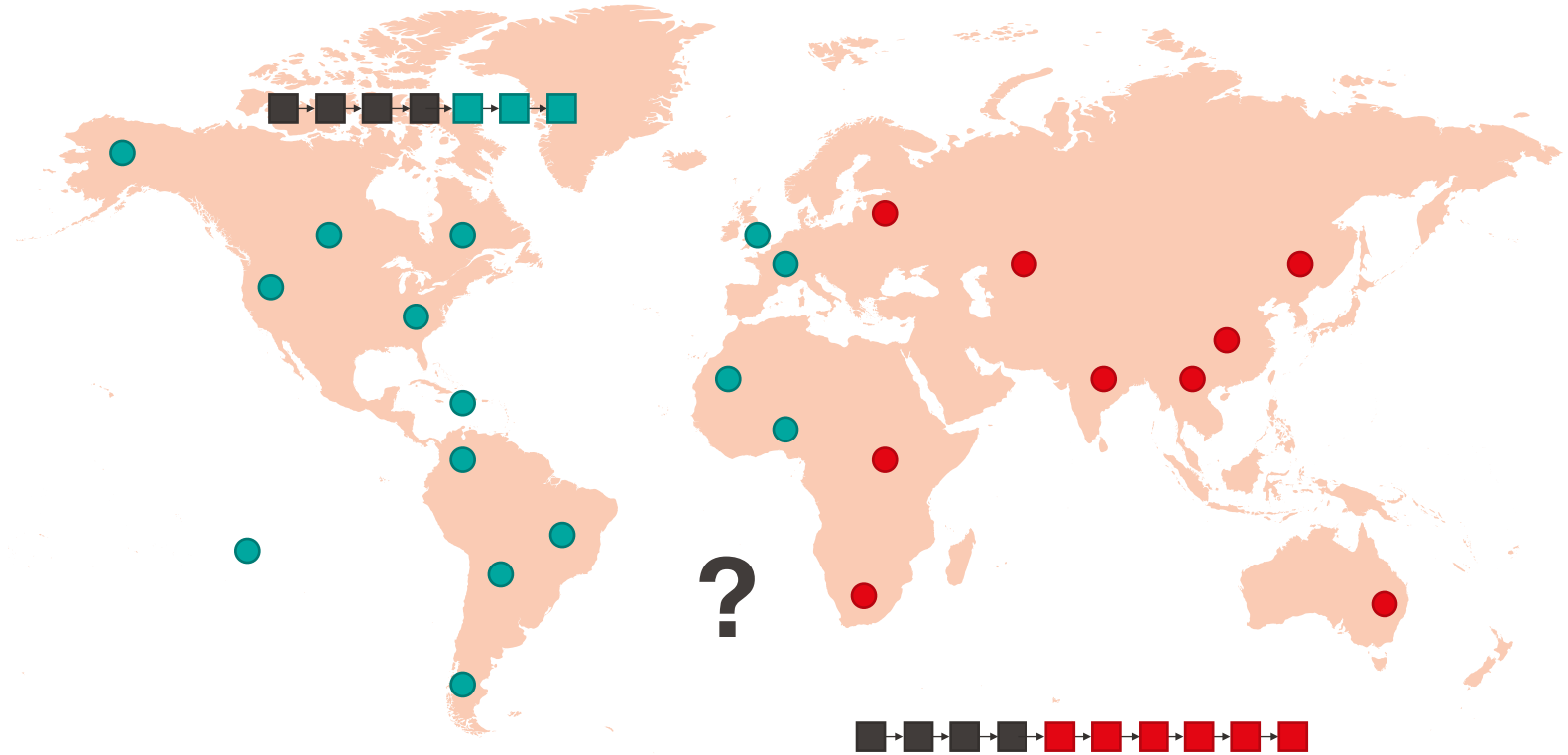
World War III Scenarios



Disclaimer : This partition is a fiction. Any resemblance to any historical event is purely coincidental

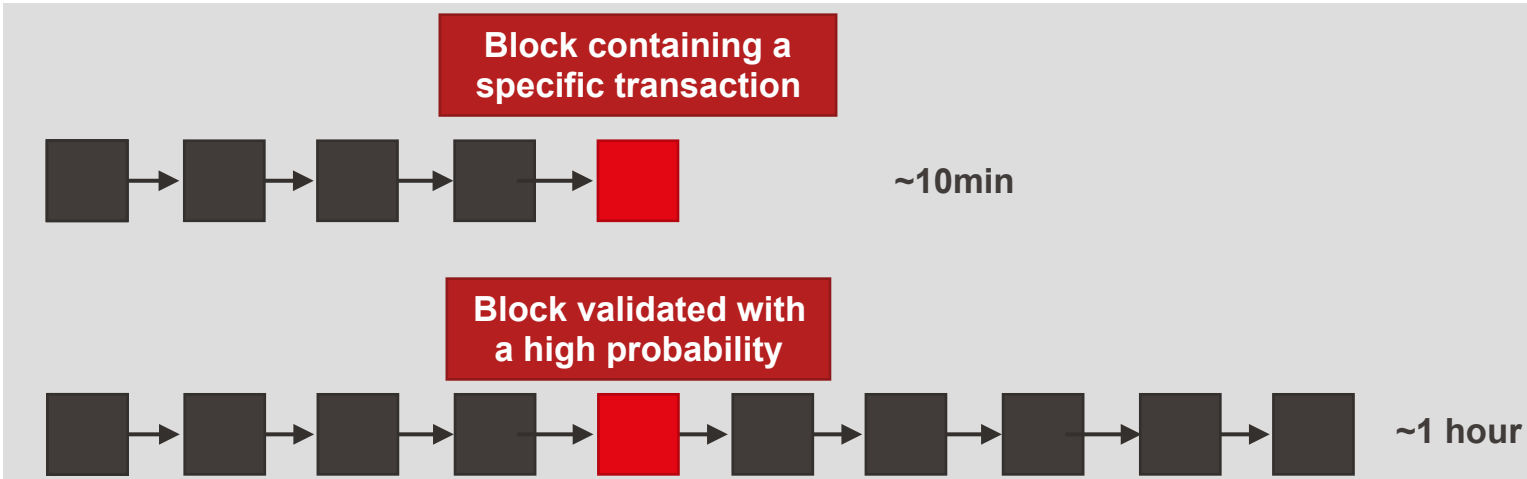
Arnaud Pannatier

World War III Scenarios

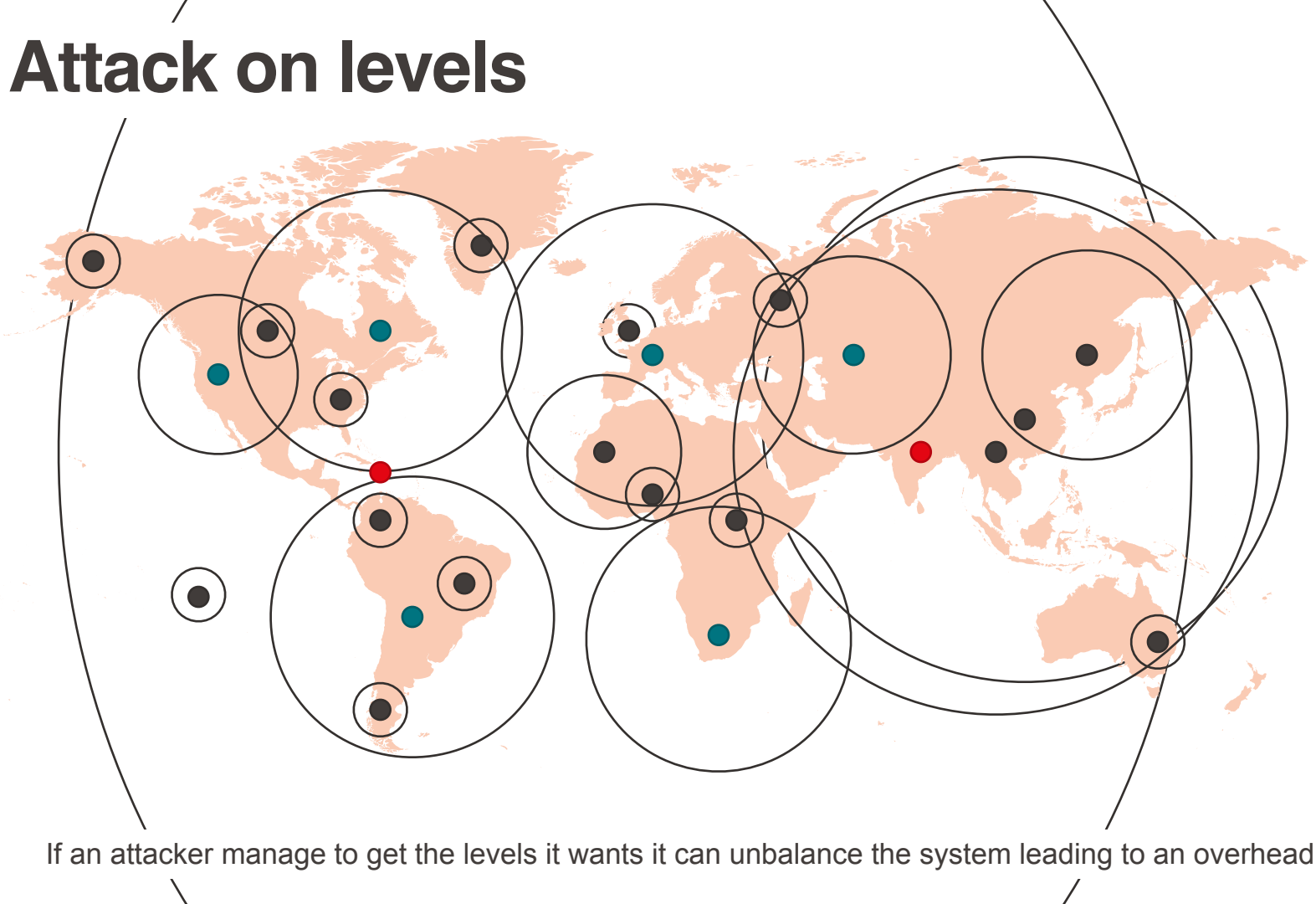


Time for validation

Adding a block takes around 10minutes

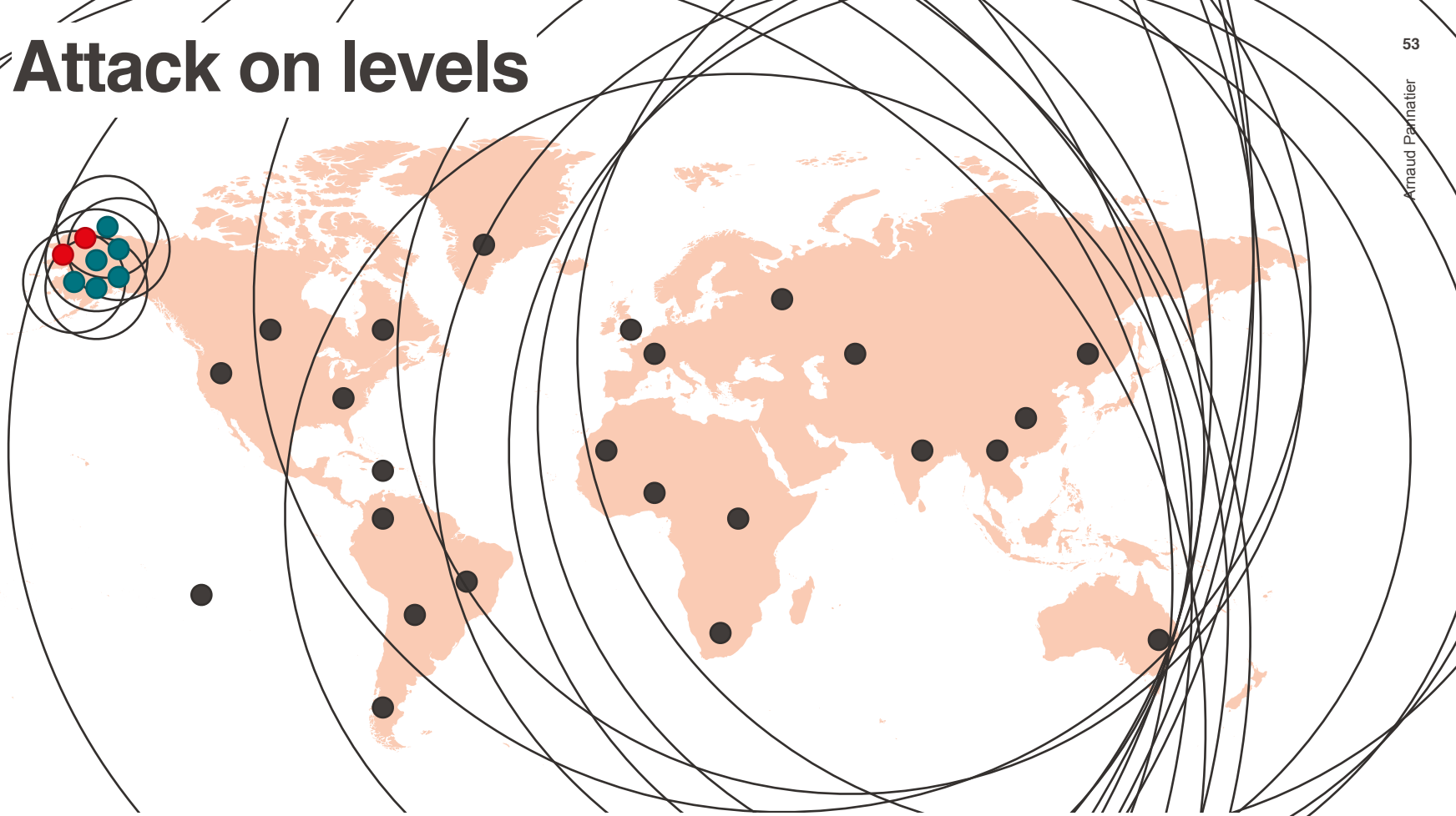


Attack on levels



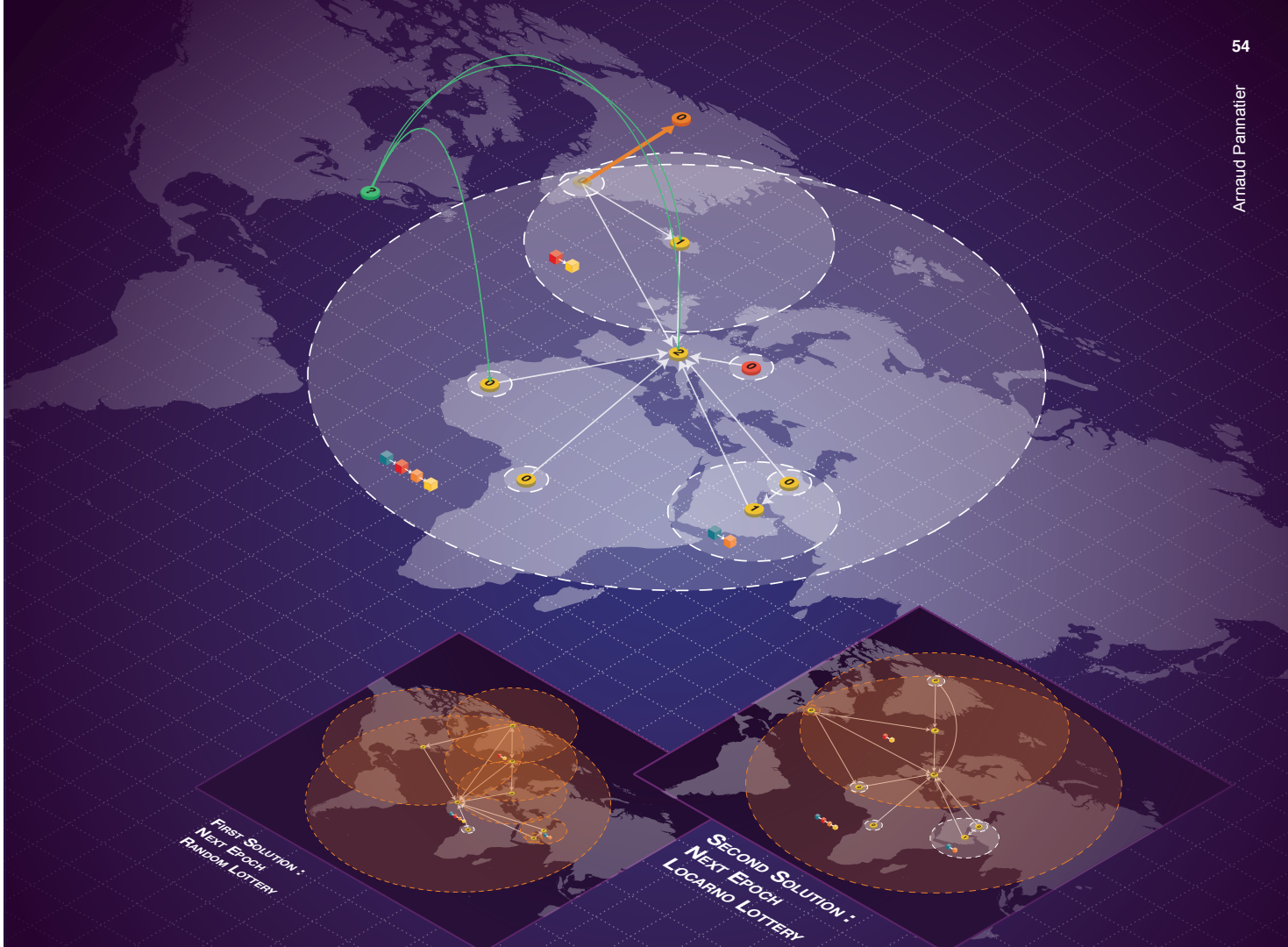
If an attacker manage to get the levels it wants it can unbalance the system leading to an overhead

Attack on levels



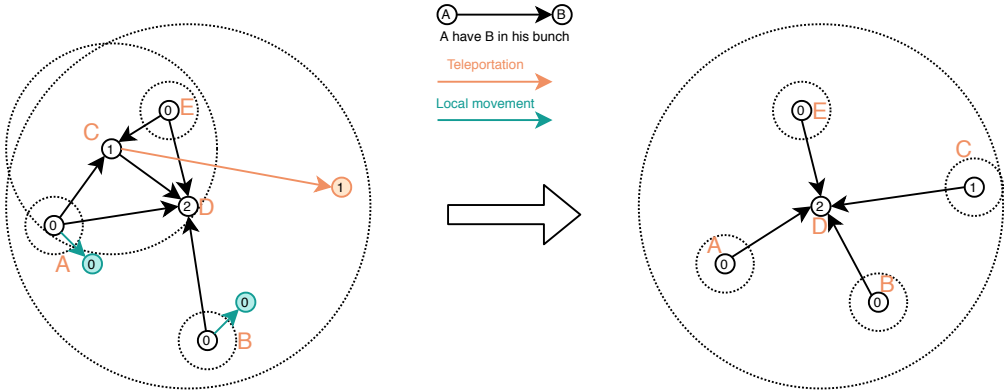
Level 0 nodes (in black) create regions that covers their cluster, but as high level nodes are far away, they have a lot of nodes in their cluster

Comparison


First Solution :
Next Epoch
Random Lottery
Second Solution :
Next Epoch
Locarno Lottery

Locarno Treaties : Evaluation - Model

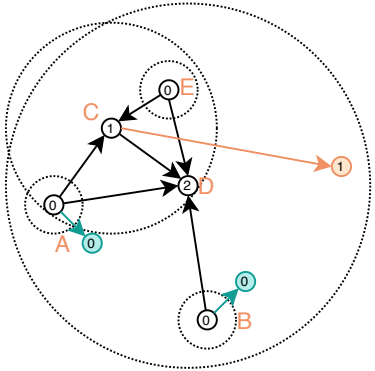
- Nodes are distributed randomly across space
- 10% chance of teleportation at the next epoch
- 20% chance of local movement at the next epoch
- Differences are counted



Arnaud Pannatier

Locarno Treaties : Evaluation - Model

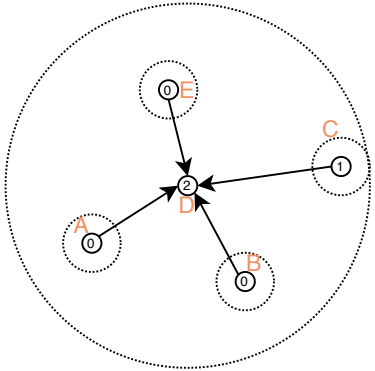
- Nodes are distributed randomly across space
- 10% chance of teleportation at the next epoch
- 20% chance of local movement at the next epoch
- Differences are counted



A have B in his bunch

Teleportation

Local movement



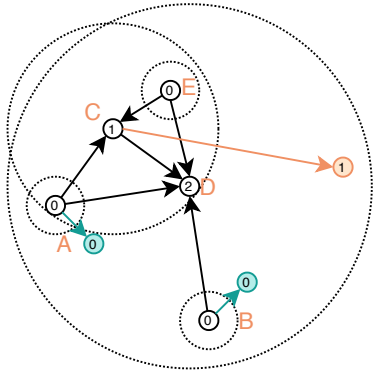
	Bunch	Cluster
A	C, D	-
B	D	-
C	D	A, E
D	-	A, B, C, D
E	C, D	-

4 differences

	Bunch	Cluster
A	~~C~~, D	-
B	D	-
C	D	~~A, E~~
D	-	A, B, C, D
E	~~C~~, D	-

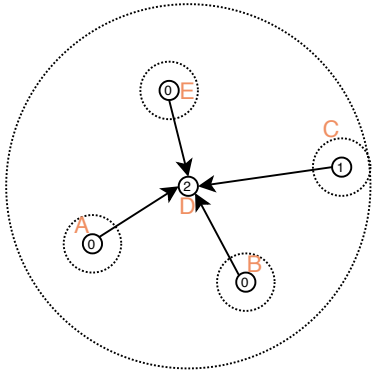
Locarno Treaties : Evaluation - Model

- Nodes are distributed randomly across space
- 10% chance of teleportation at the next epoch
- 20% chance of local movement at the next epoch
- Differences are counted



Teleportation

Local movement



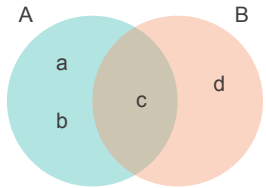
	Bunch	Cluster
A	C, D	-
B	D	-
C	D	A, E
D	-	A, B, C, D
E	C, D	-

4 differences

	Bunch	Cluster
A	~~C~~, D	-
B	D	-
C	D	~~A, E~~
D	-	A, B, C, D
E	~~C~~, D	-

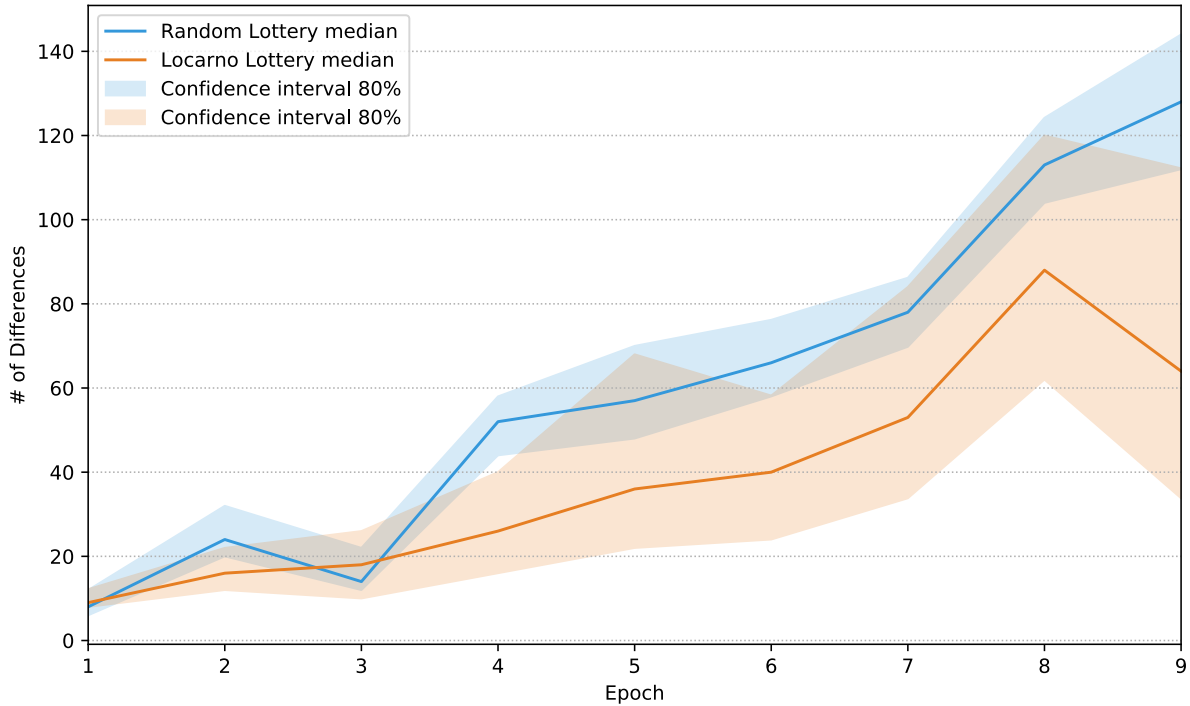
$$\#\text{Diff}(A, B) = \#(A \cup B - A \cap B)$$

A = {a,b,c}



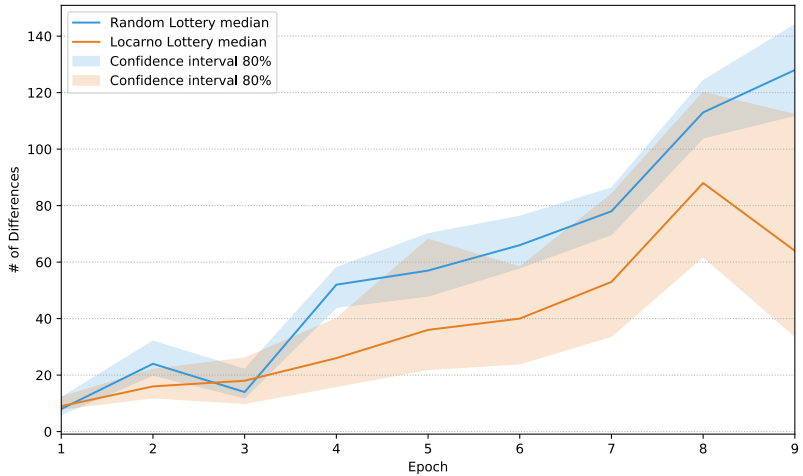
B = {c, d}

Locarno Treaties : Evaluation



Locarno Treaties : Evaluation

- 100 different experiment using both lotteries
- System starts with 4 nodes, 2 are added at each epochs
- Same evolution for both lotteries
- Locarno Lottery reduces the number of differences
- Variance comes from teleportation

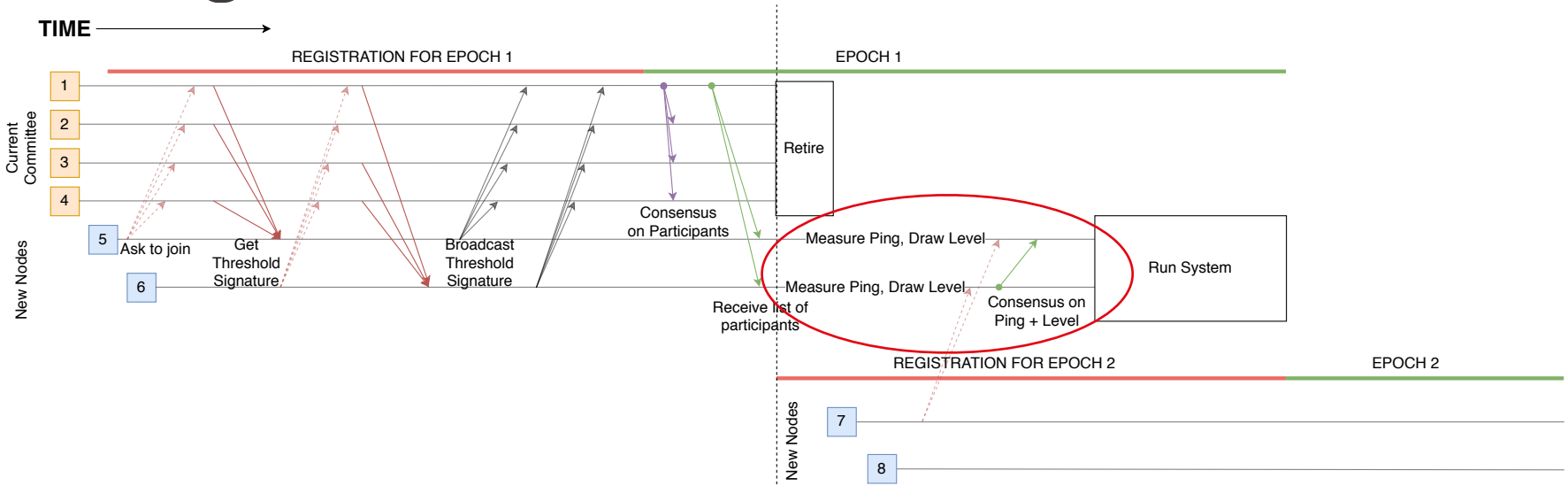


Fog of the war : Purpose

Arnaud Pannatier

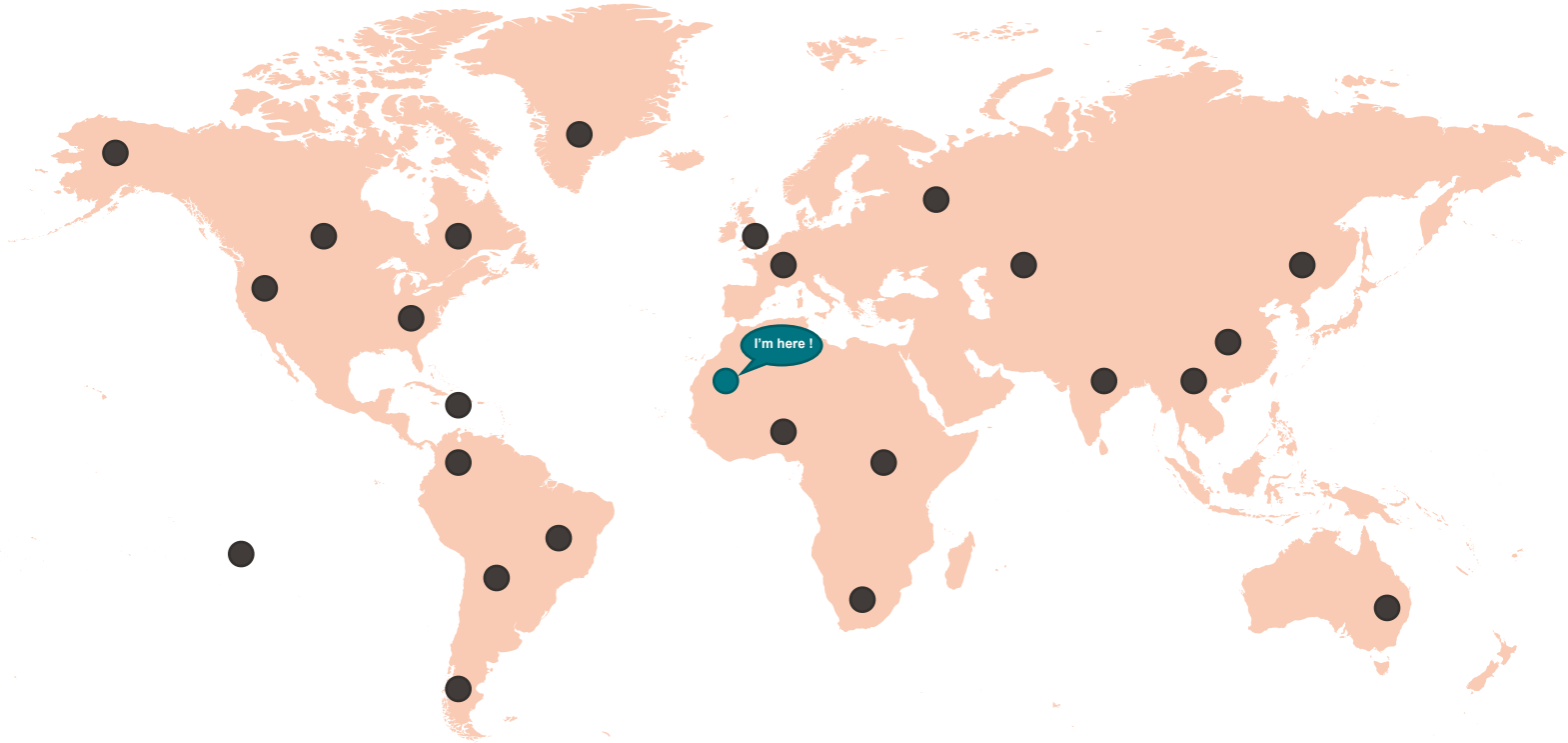
Nodes does not need to know every thing

Fog of the war : Idea

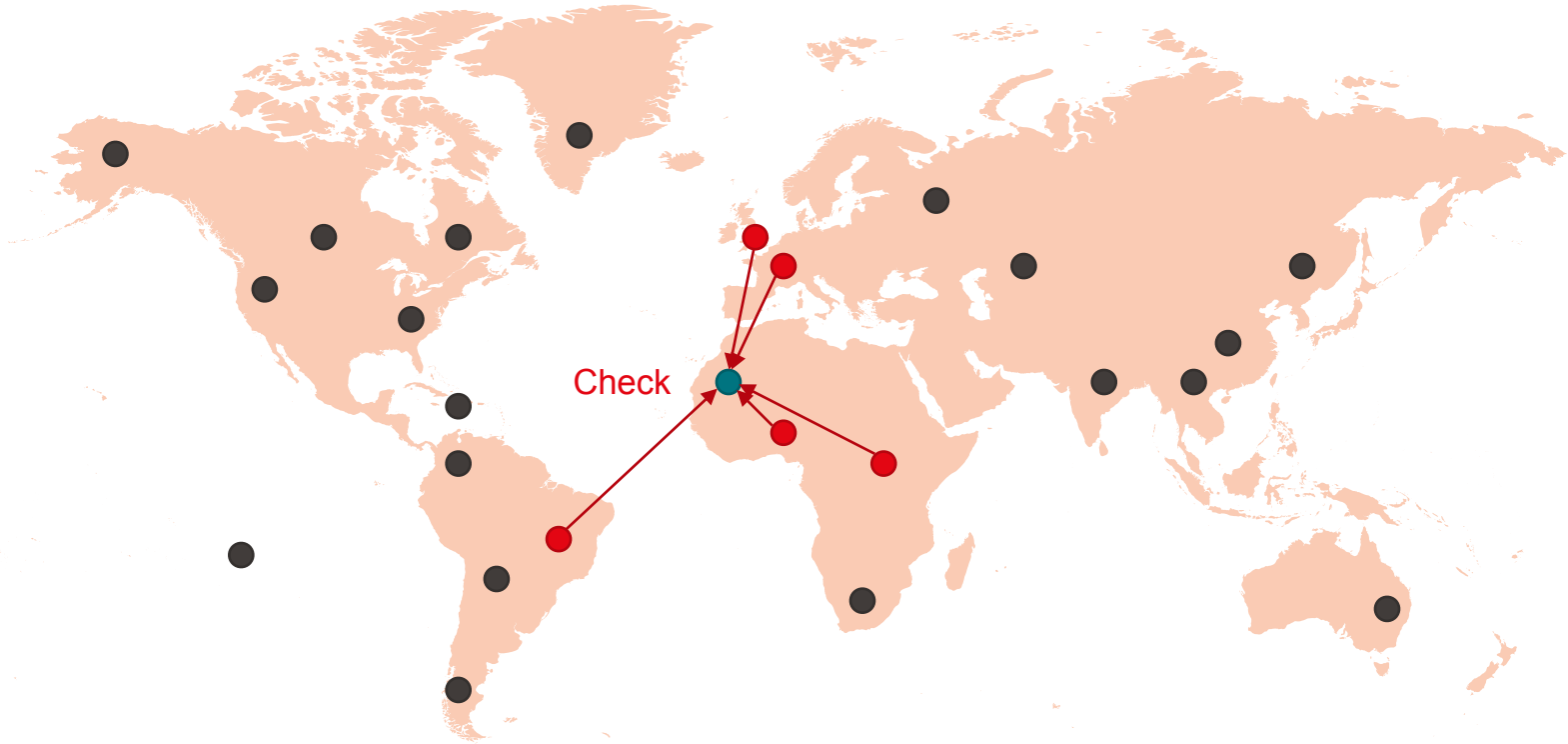


Change measure and consensus on pings with a declared position and a series of checks

Fog of the war : Idea

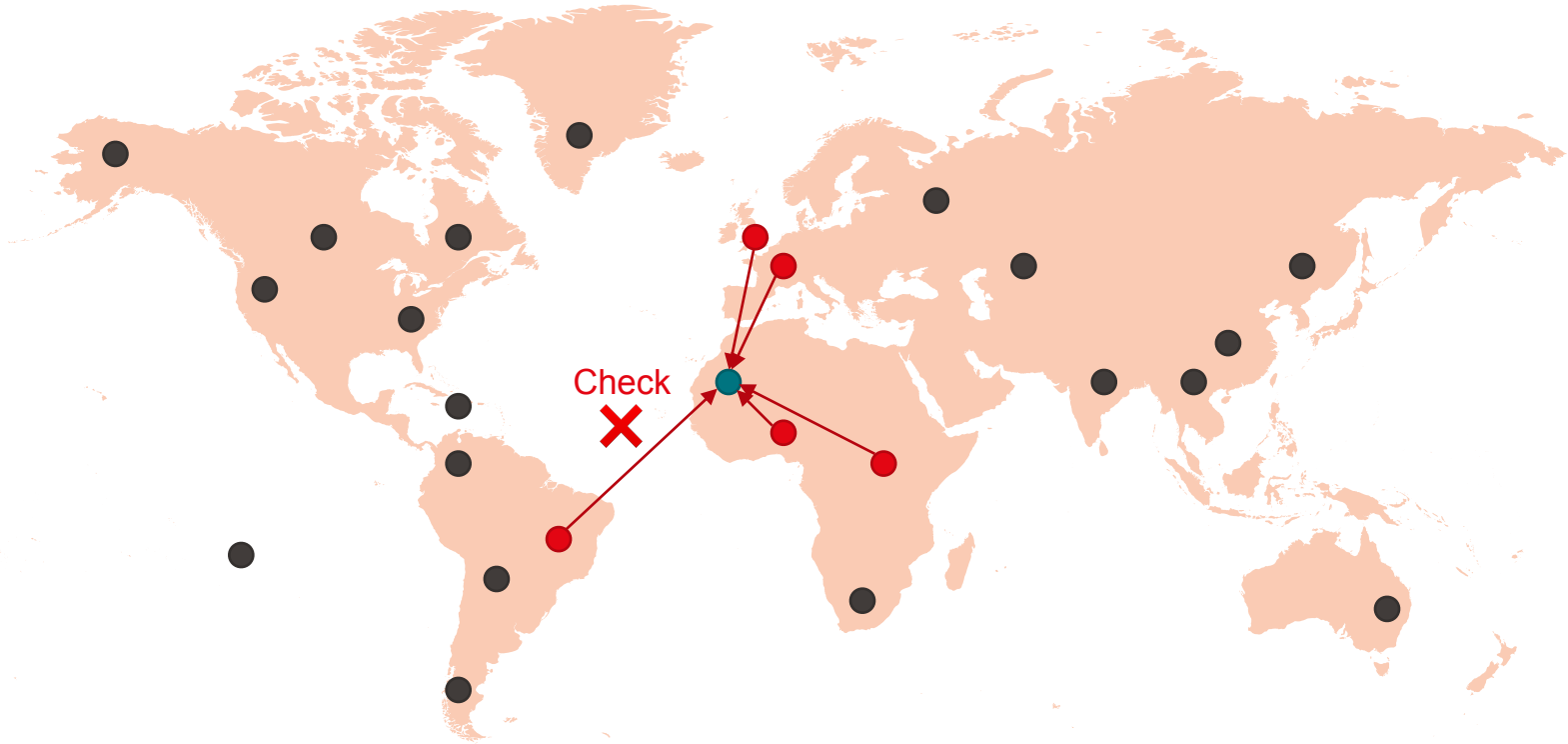


Fog of the war : Idea

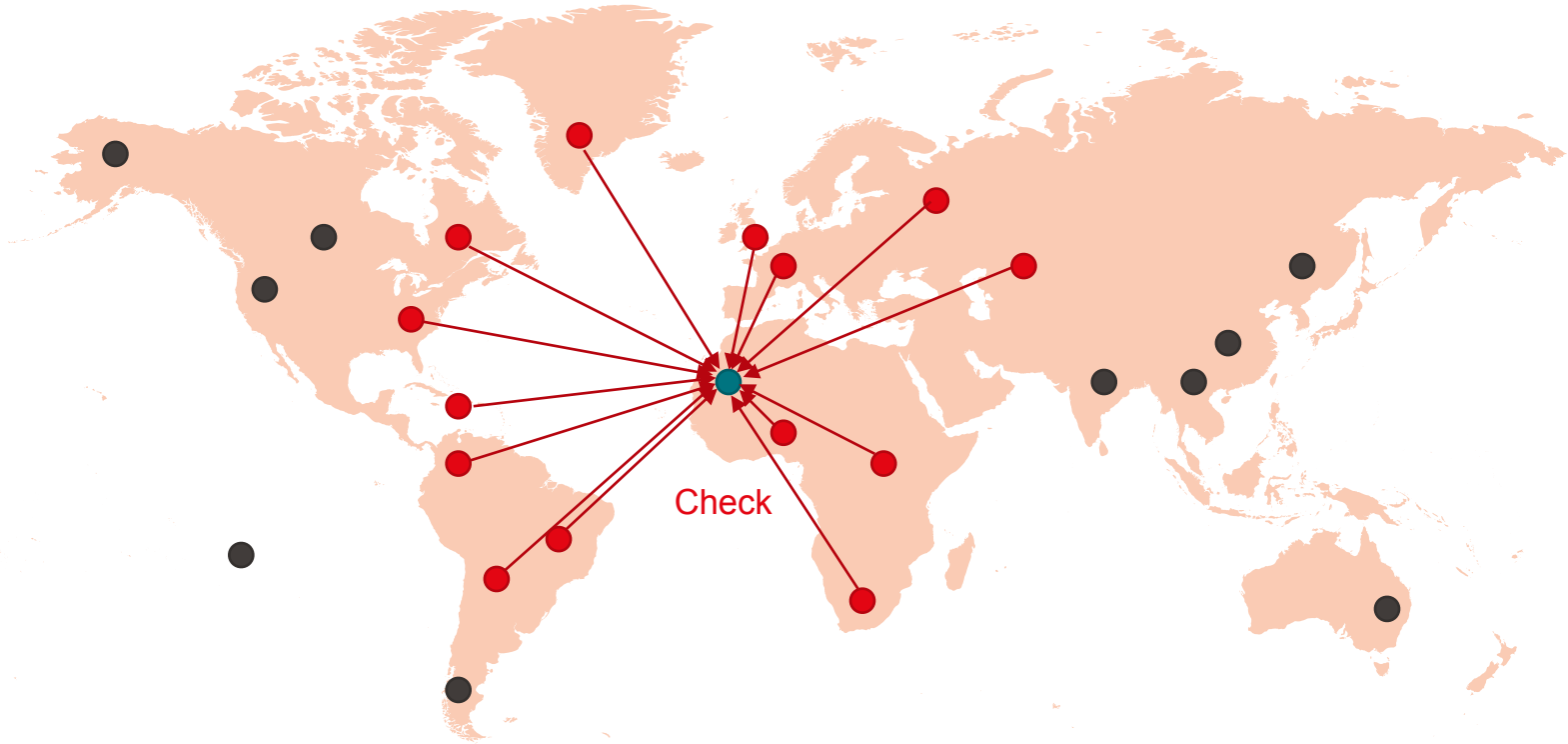


Fog of the war : Idea

Arnaud Pannatier



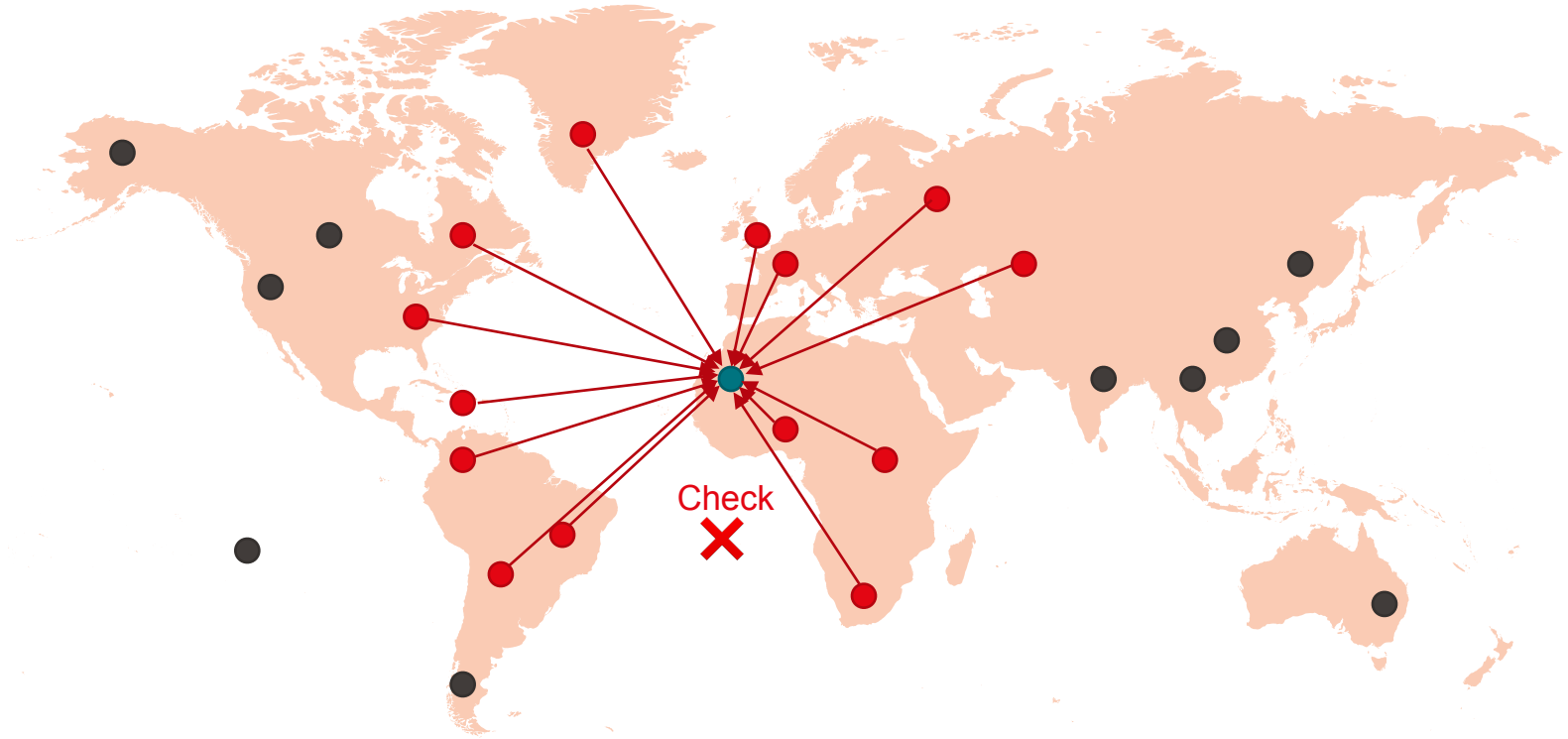
Fog of the war : Idea



Arnaud Pannatier

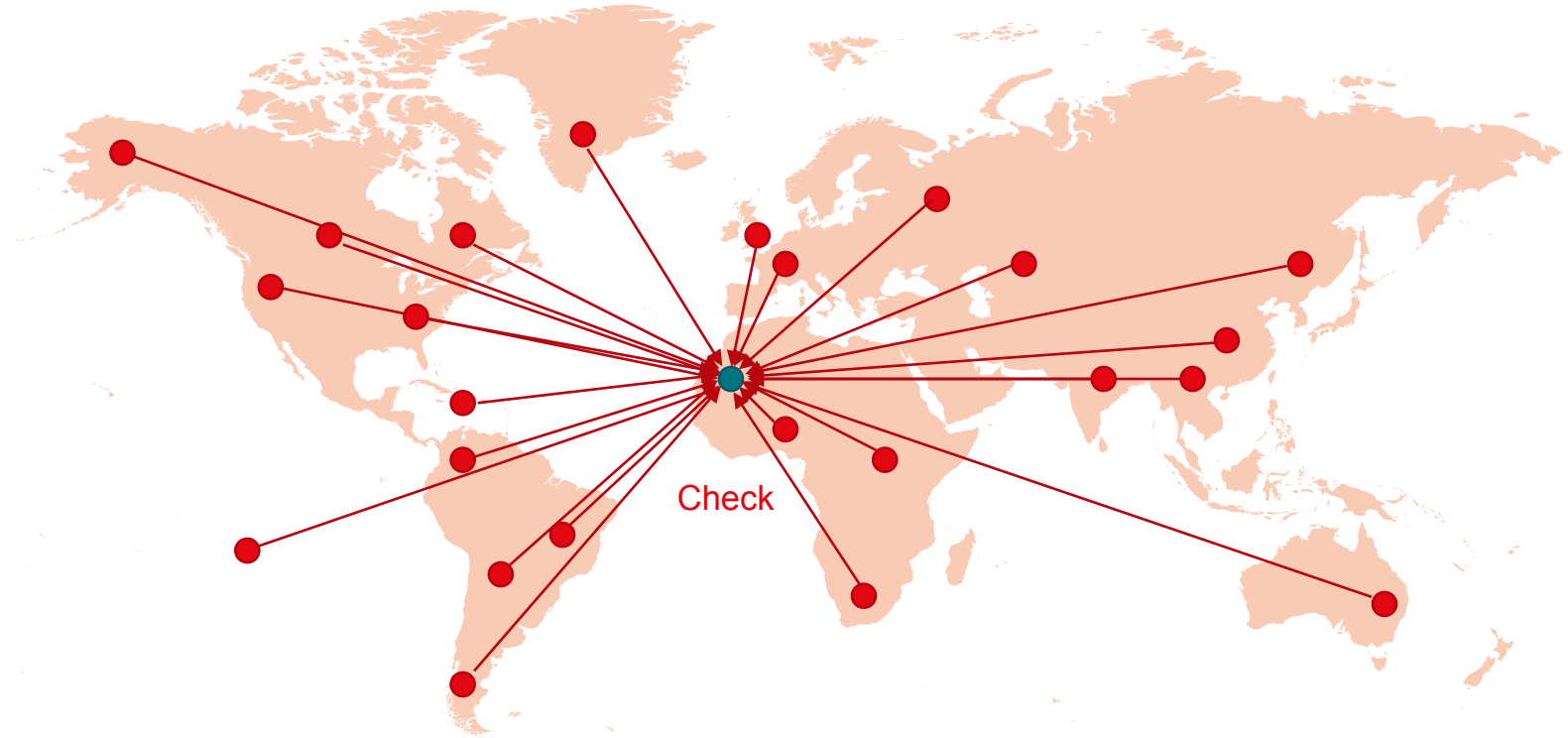
Fog of the war : Idea

Arnaud Pannatier



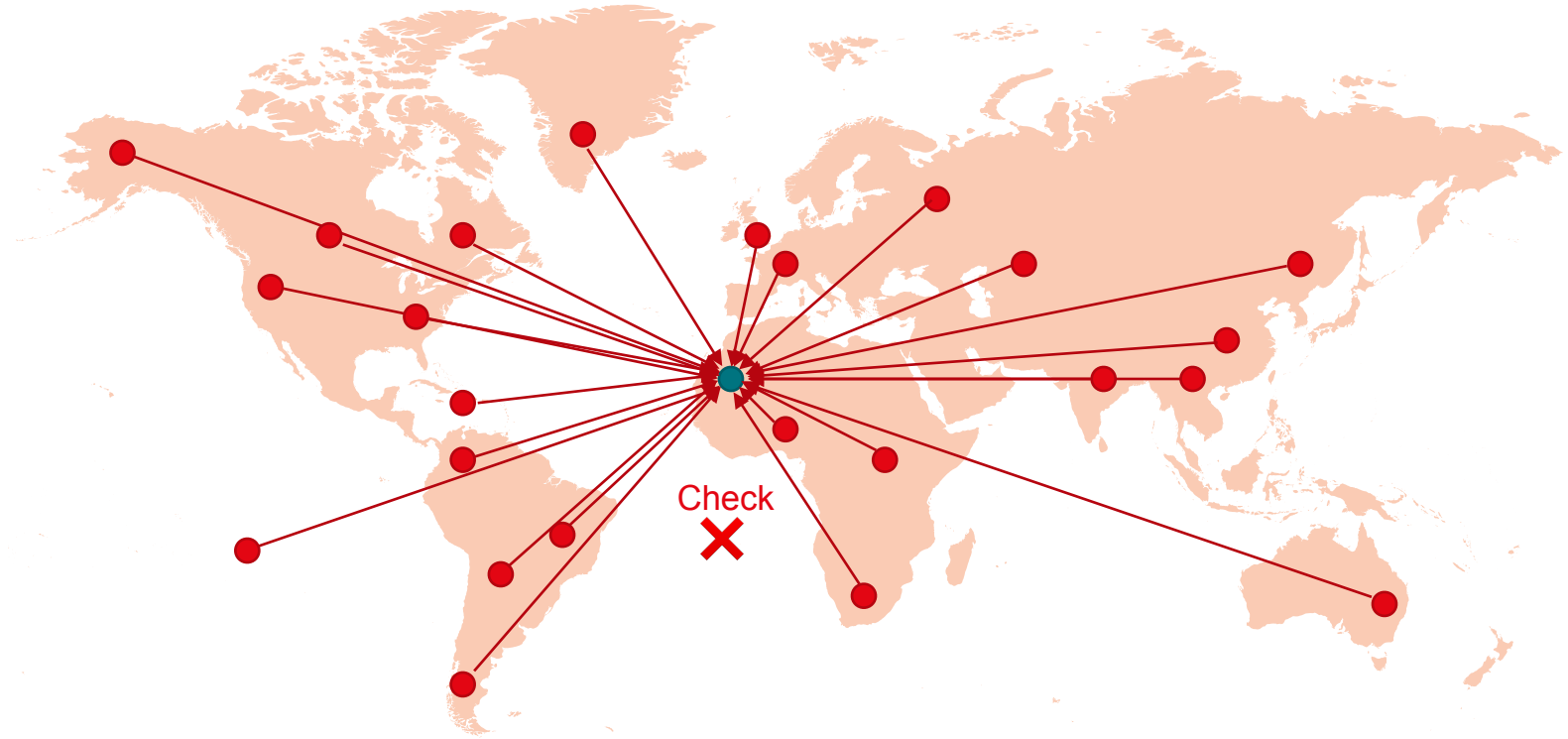
Fog of the war : Idea

Arnaud Pannatier



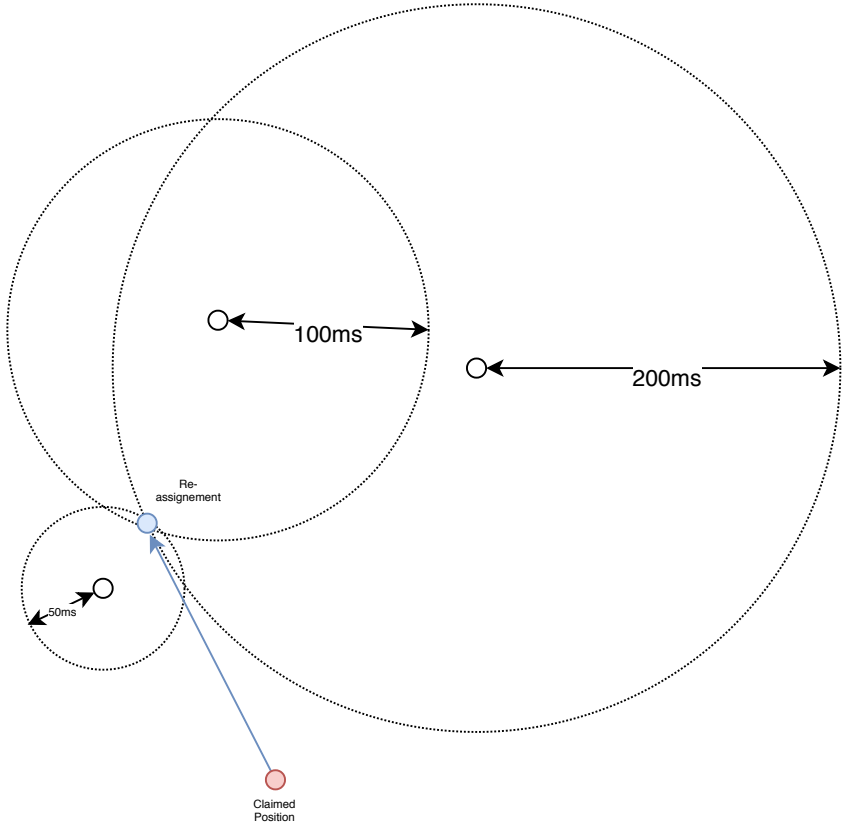
Fog of the war : Idea

Arnaud Pannatier



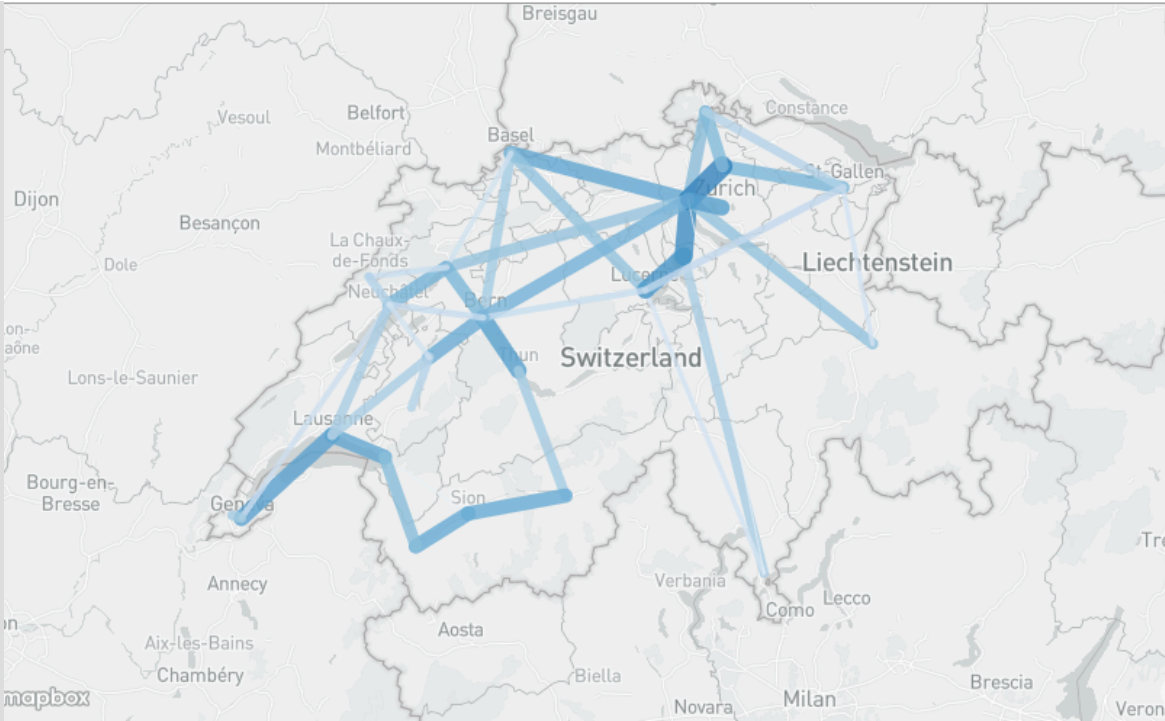
If no checks pass

- Assign a new position to the node based on the pings
- A kind of triangulation strategy can be used
- As in Internet-like networks there is triangle inequality violation, this might not be possible
- Could be replaced by the « best candidate » for the position
- Was not implemented

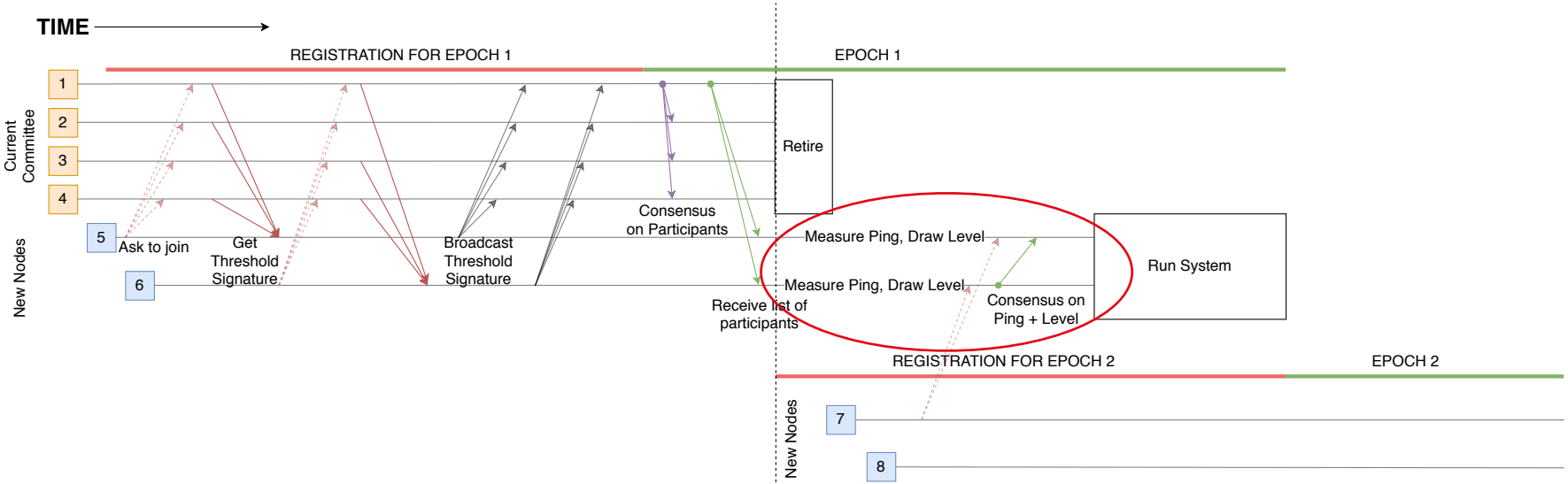


Space Time interaction metric

- Maybe what we want to conserve might not be latencies or availability but *interactions* between nodes
- Might be useful if cross-region interaction between nodes add overhead



Space Time interaction metric

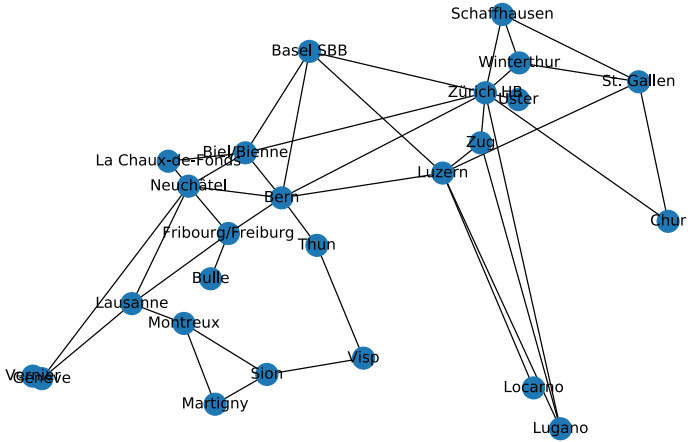


Change ping with a new measure of distance

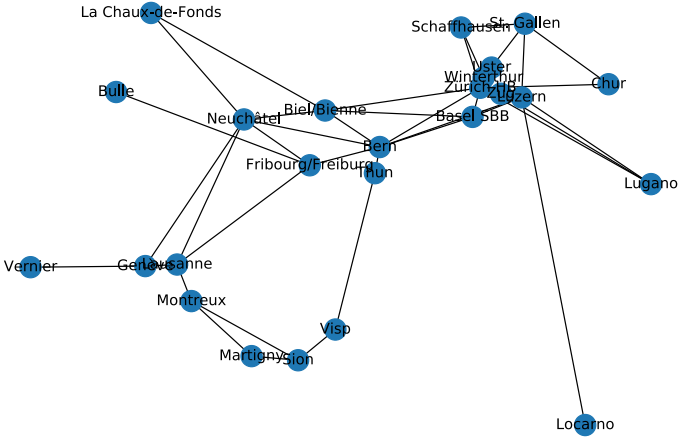
$$d(A, B) = \frac{1}{\#\text{ messages between A and B per unit of time}}$$

Each node count each time it interacts with another node during one epoch and publish it at the beginning of the next

Space Time interaction metric explanation



Map using regular distance



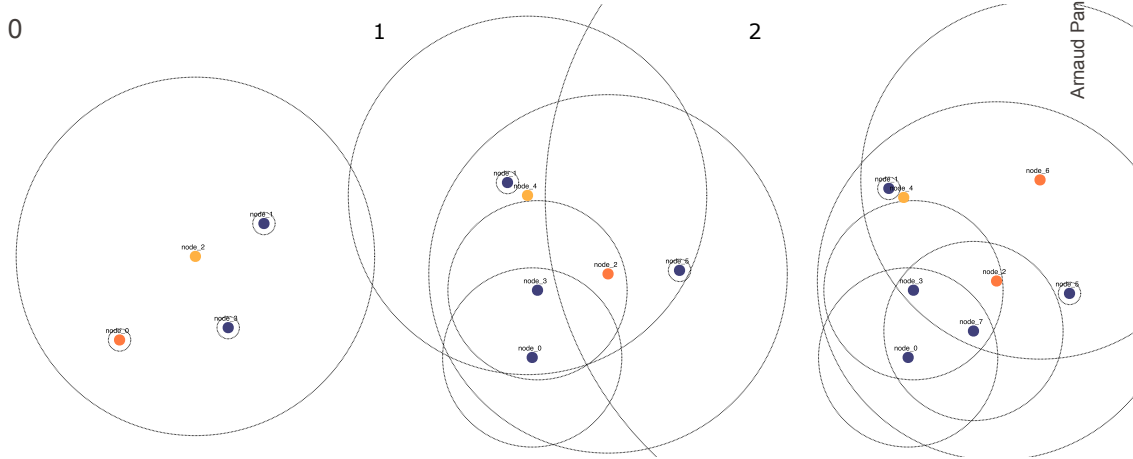
Map using interaction distance

Points are close if there is a lot of connections between them

Space Time interaction metric Drawbacks

- Interactions might change a lot from an epoch to the next
- Might be more complex to conceptualize for user
- Preserving Interactions over availability and latencies might be discutable

3 Epochs - Locarno Lottery - Regular distances



3 Epochs - Locarno Lottery - Space Time interaction distances