Blockchain, Kryptowährungen und Disruption

Prof. Dr. Tim Weingärtner

Hochschule Luzern
Facts & Figures 2016

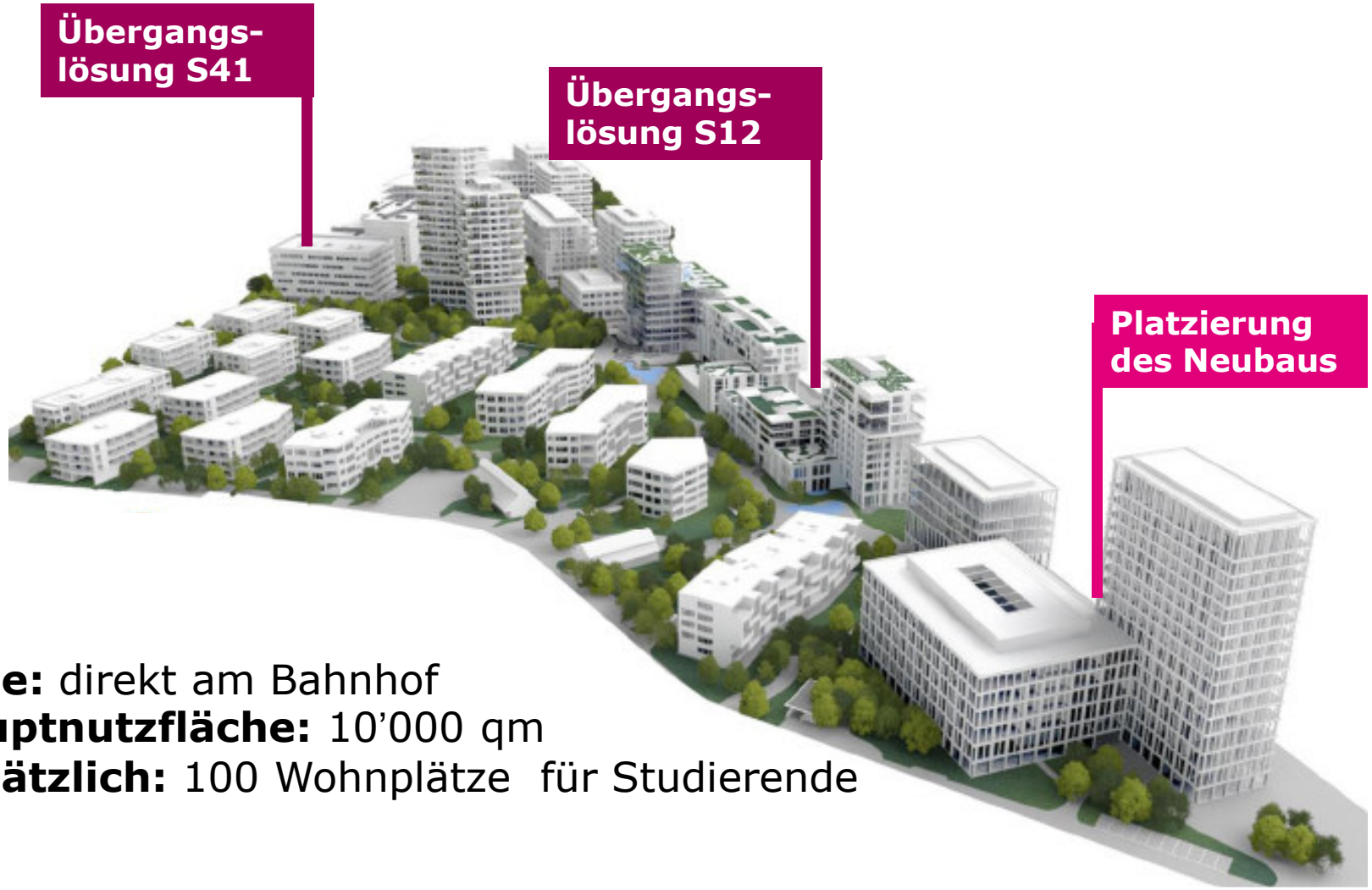
6‘209 Bachelor- und Master-Studierende (Ausbildung)

416 Forschungsprojekte

8‘334 Weiterbildungsstudierende

1‘645 Mitarbeiterinnen & Mitarbeiter

Campus Zug-Rotkreuz:
Hochschule Luzern auf dem Suurstoffi-Areal



Lage: direkt am Bahnhof
Hauptnutzfläche: 10’000 qm
Zusätzlich: 100 Wohnplätze für Studierende

Quelle:
ZugEstates

Historie von Blockchain und Bitcoin

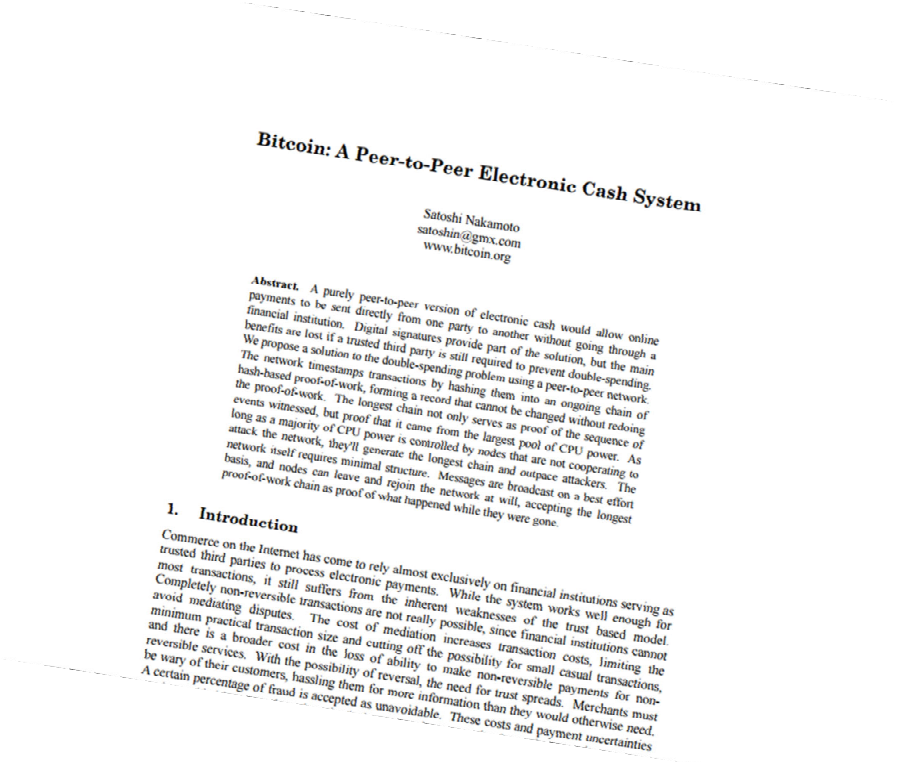
- Oktober 2008:

  Paper von Satoshi Nakamoto

- Nakamoto ist ein Pseudonym

- Blockchain = Technologie

  Bitcoin = Währung



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

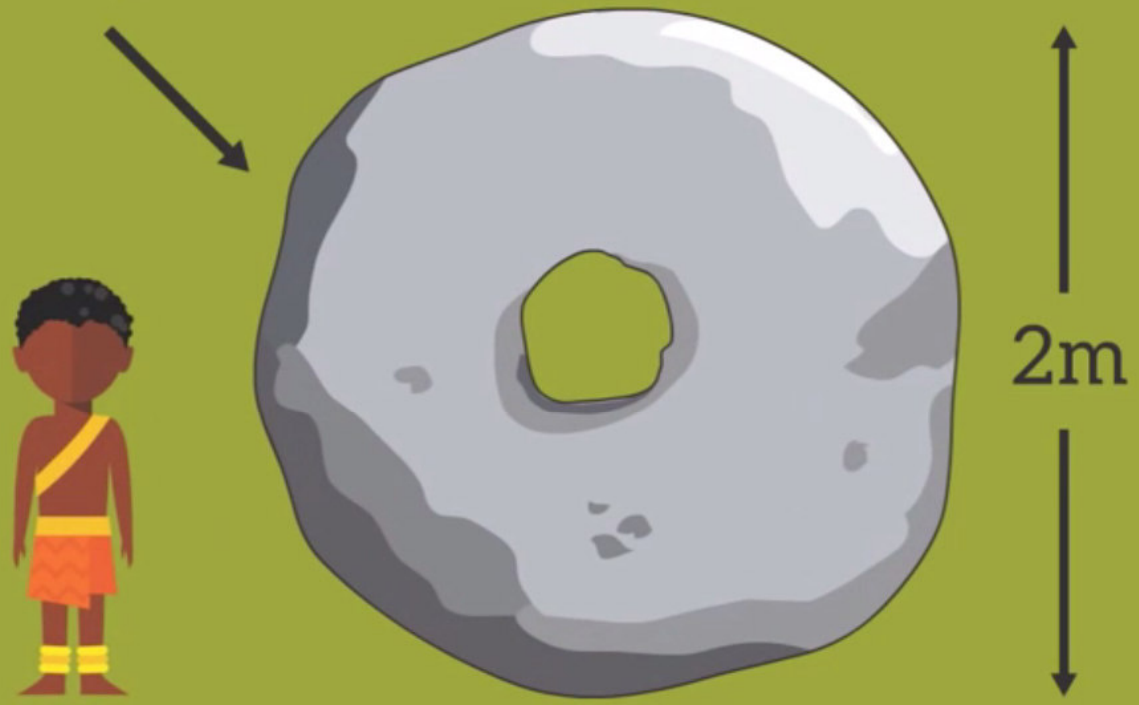
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties

http://www.finanzen.ch/devisen/chart/bitcoin-franken-kurs

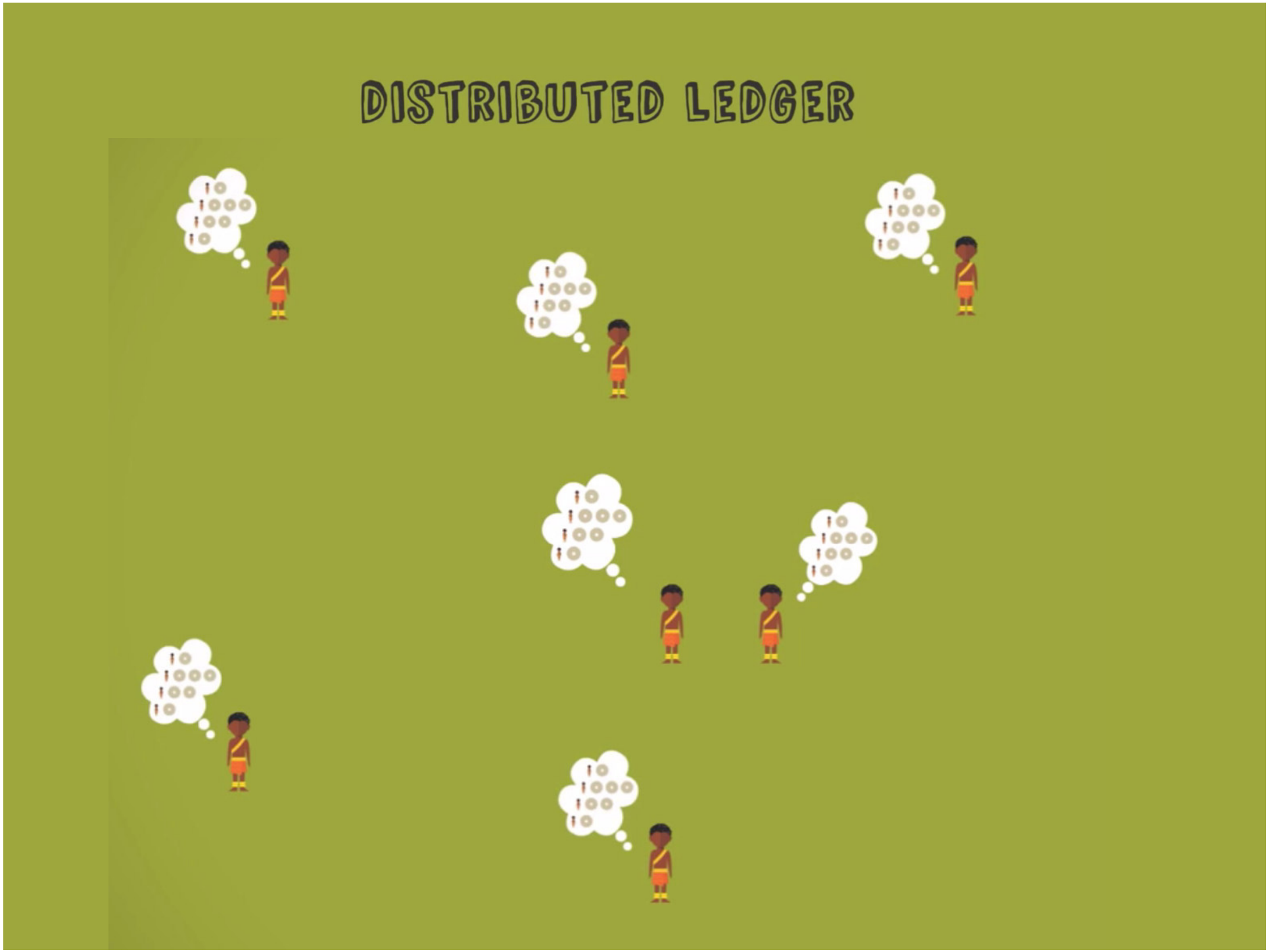
Quelle: https://www.youtube.com/watch?v=Fy8BfVrj4dk

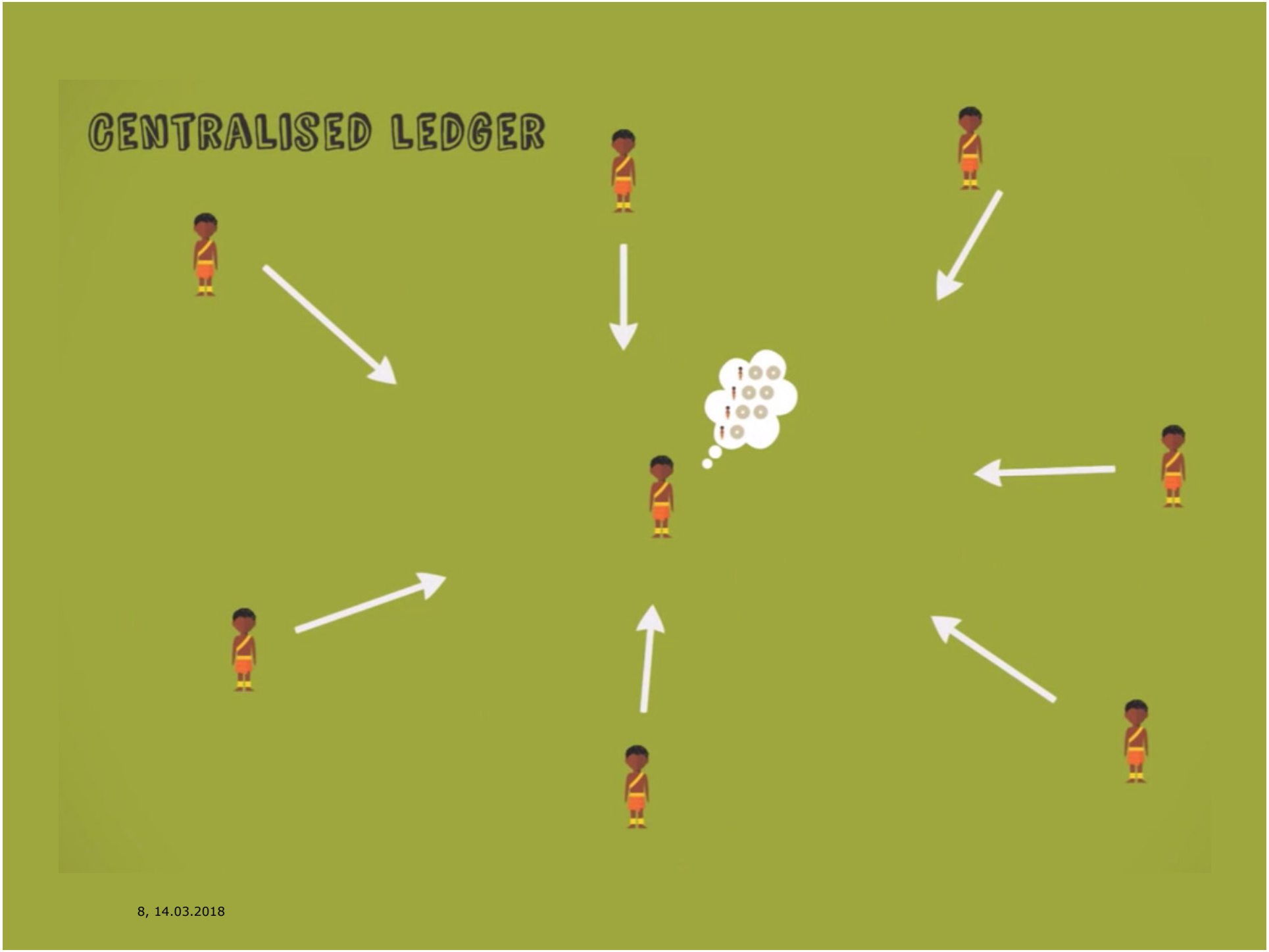
RAI STONE

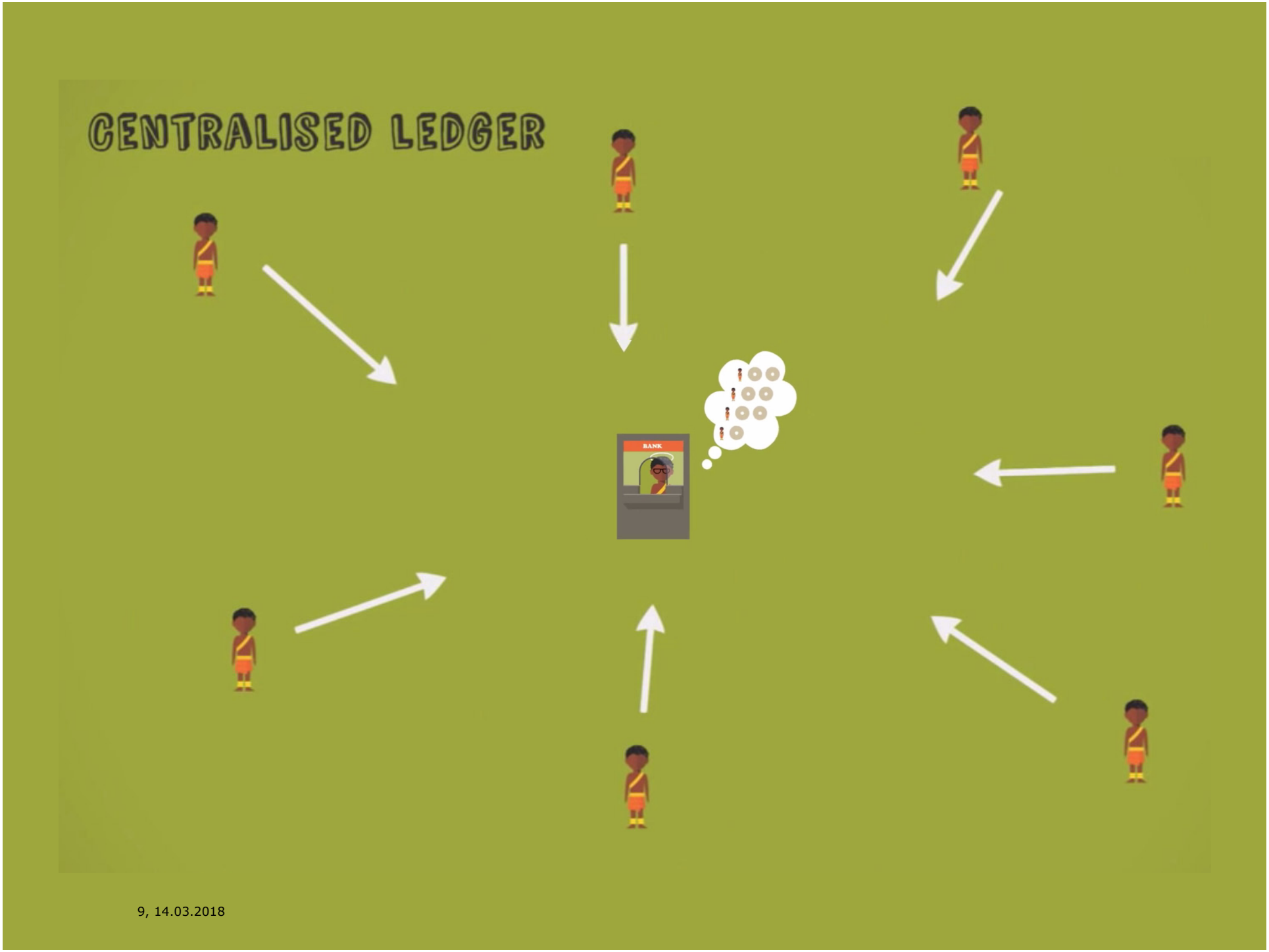


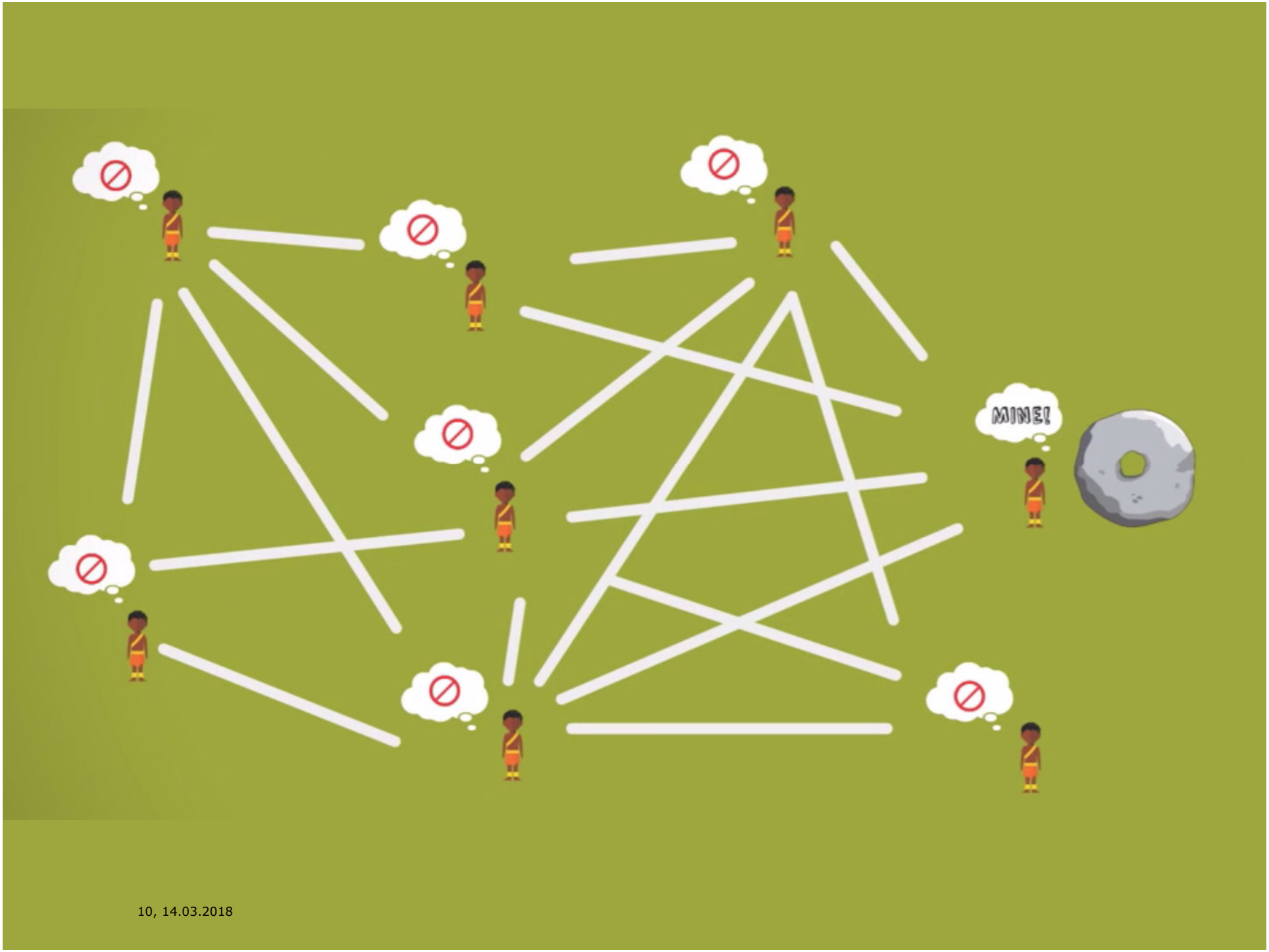
Composition: Limestone

Weight: 200kg


DISTRIBUTED LEDGER


CENTRALISED LEDGER

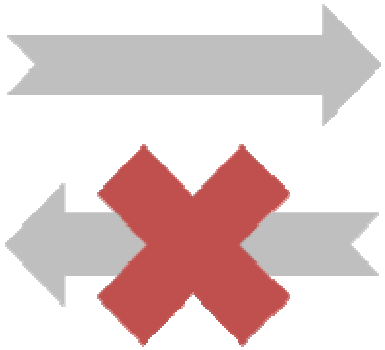

CENTRALISED LEDGER
BANK


MINE!

Hash Code - «Spiegelei-Prinzip»

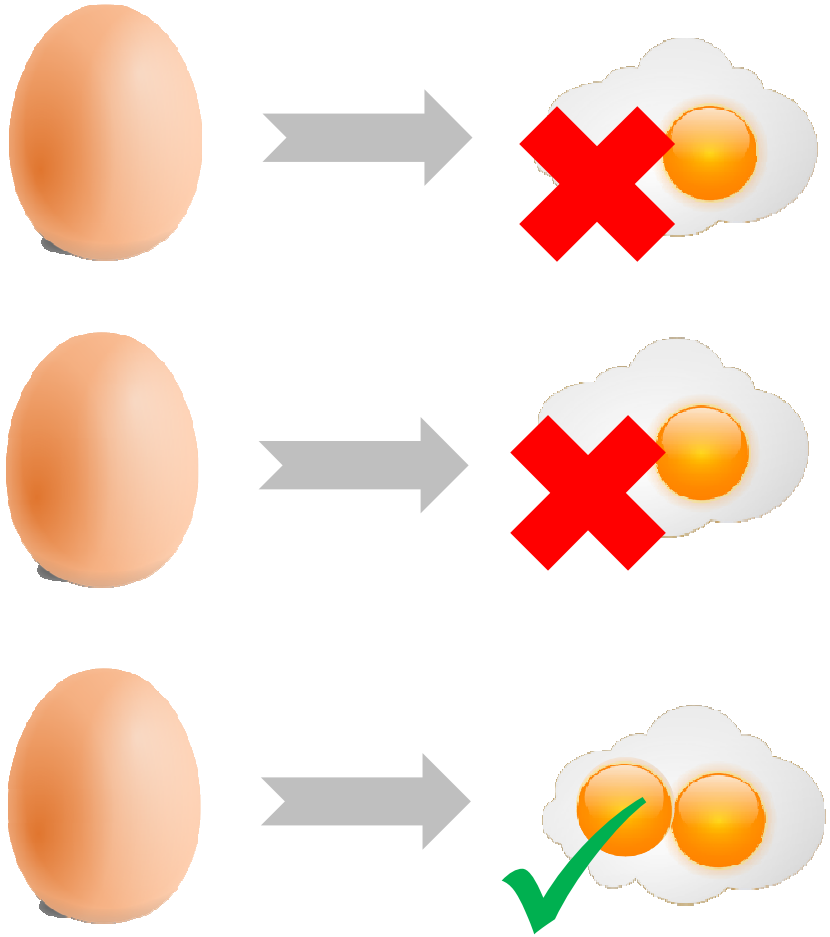
Hash Code

PASSWORD!

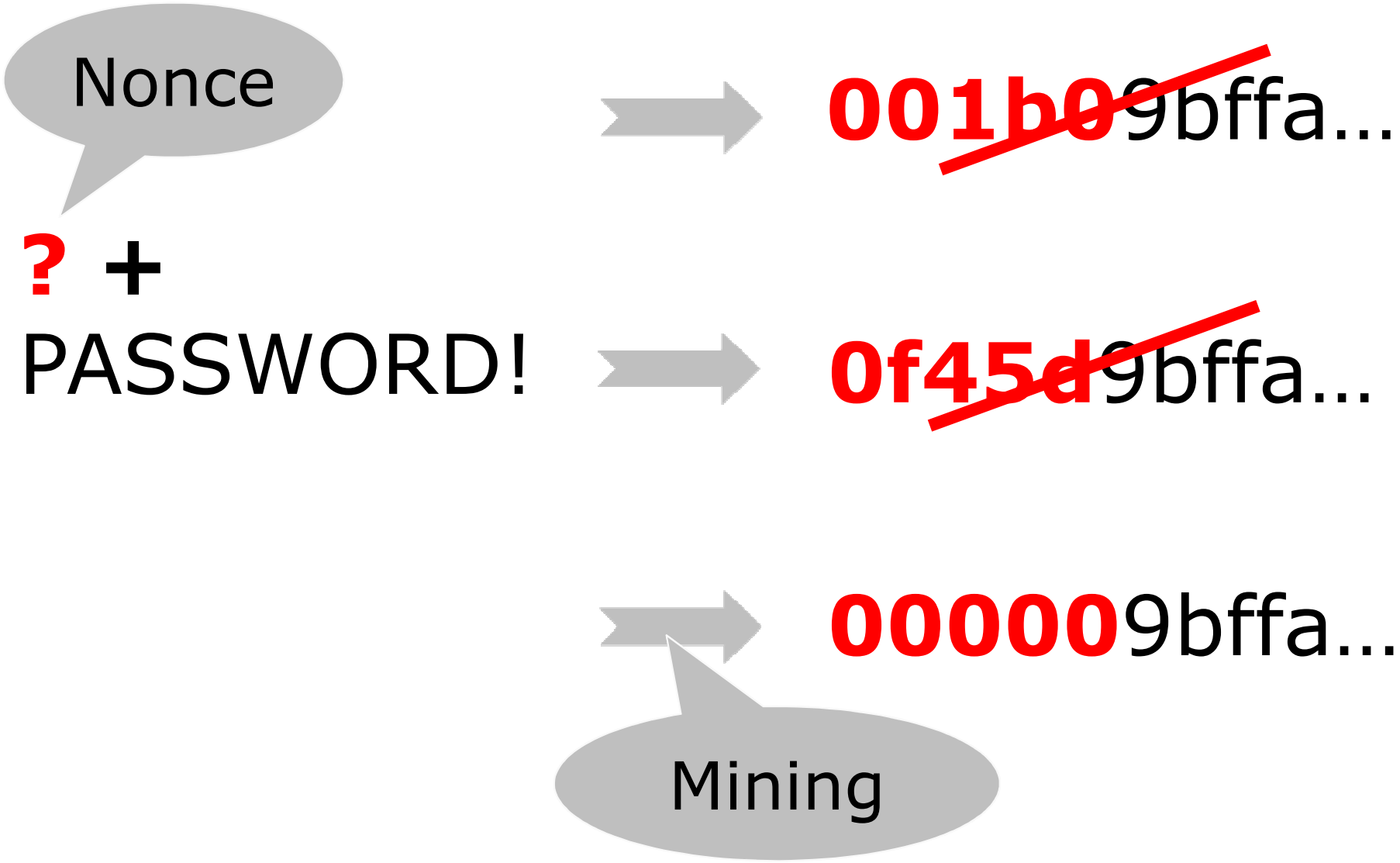


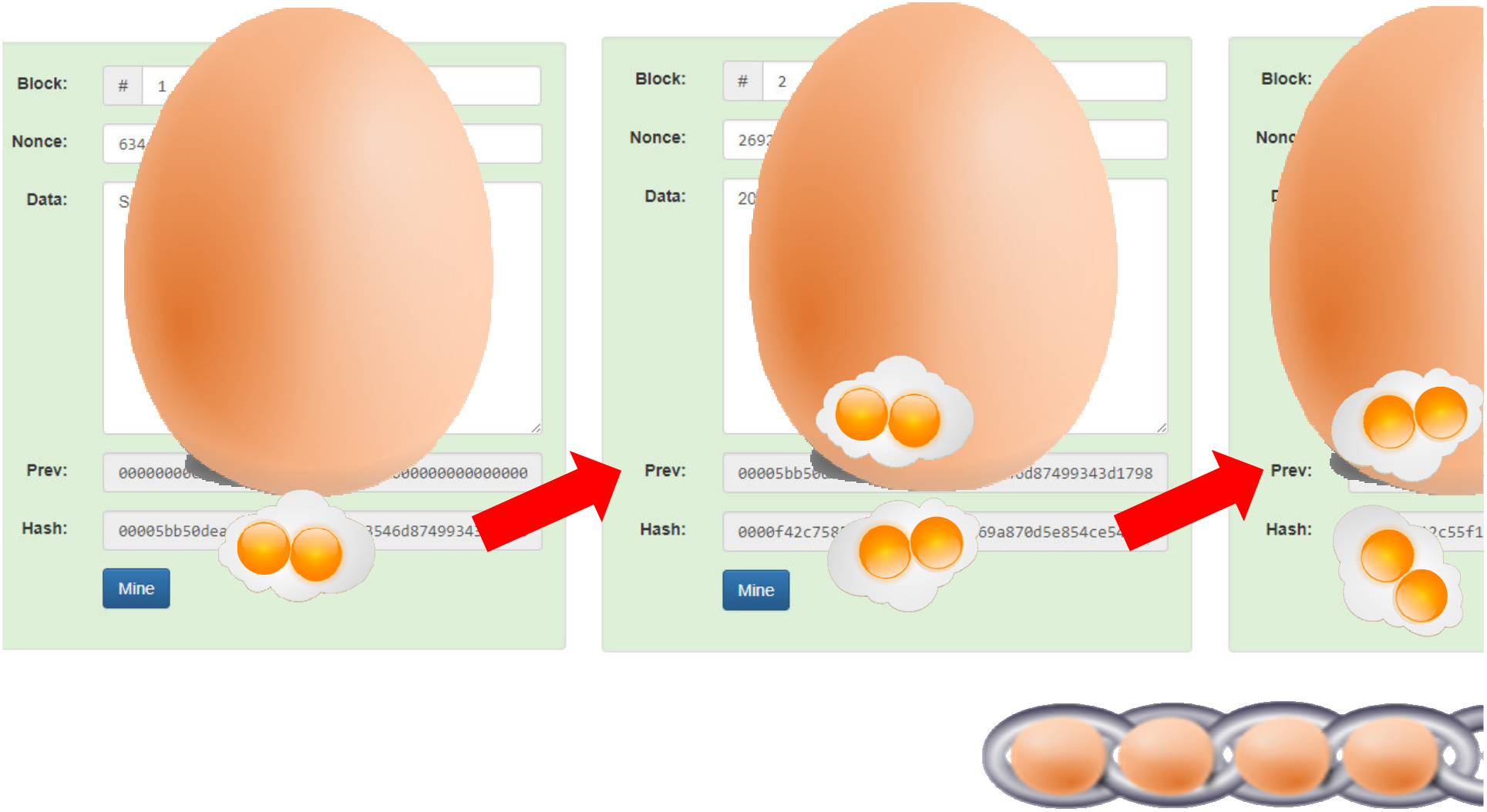
09bffa954fe
f56de82867
1a2b64da71
009bae89de
f060eb355a
7d

Proof of Work – «ausprobieren»

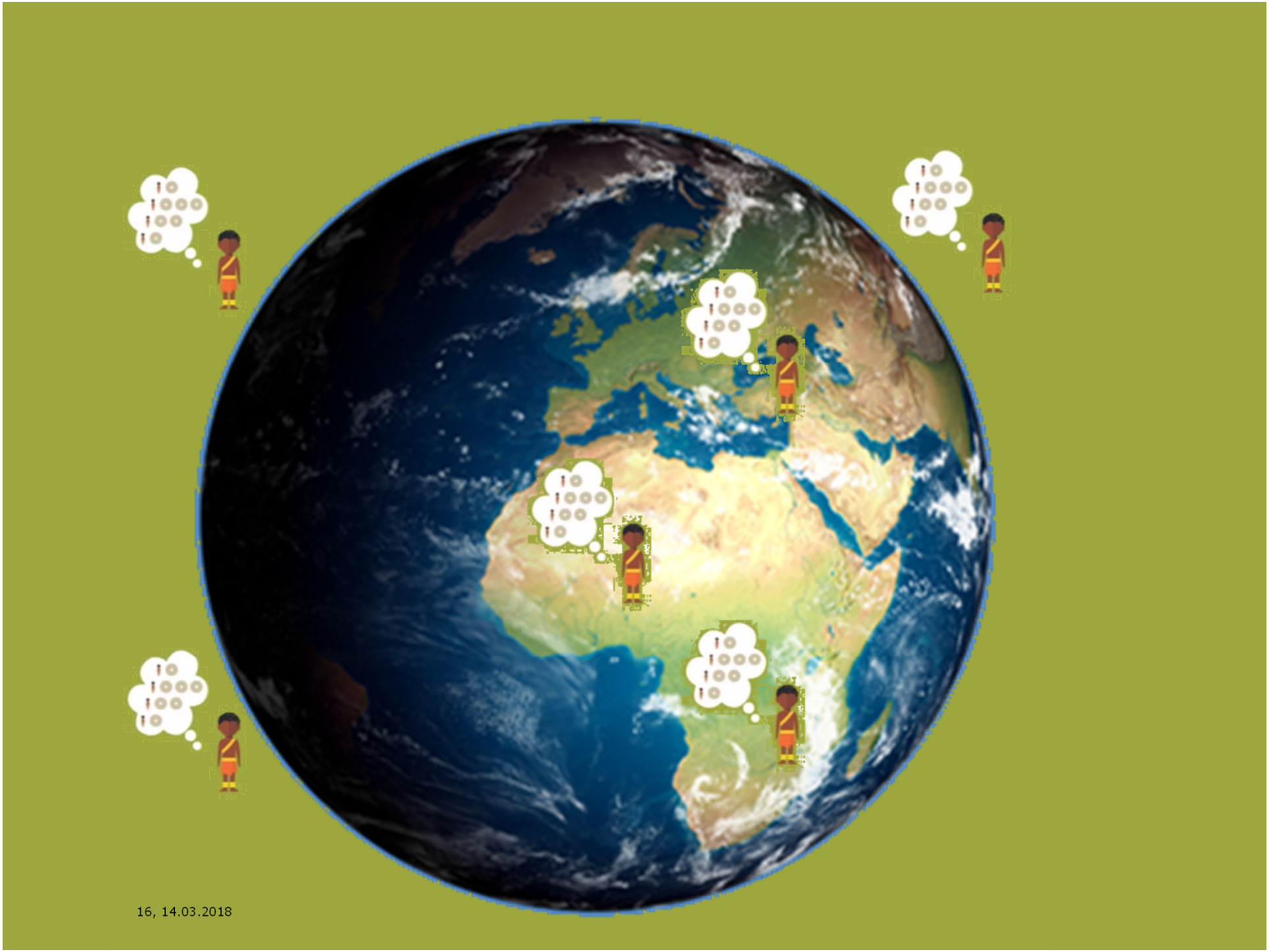


Proof of Work

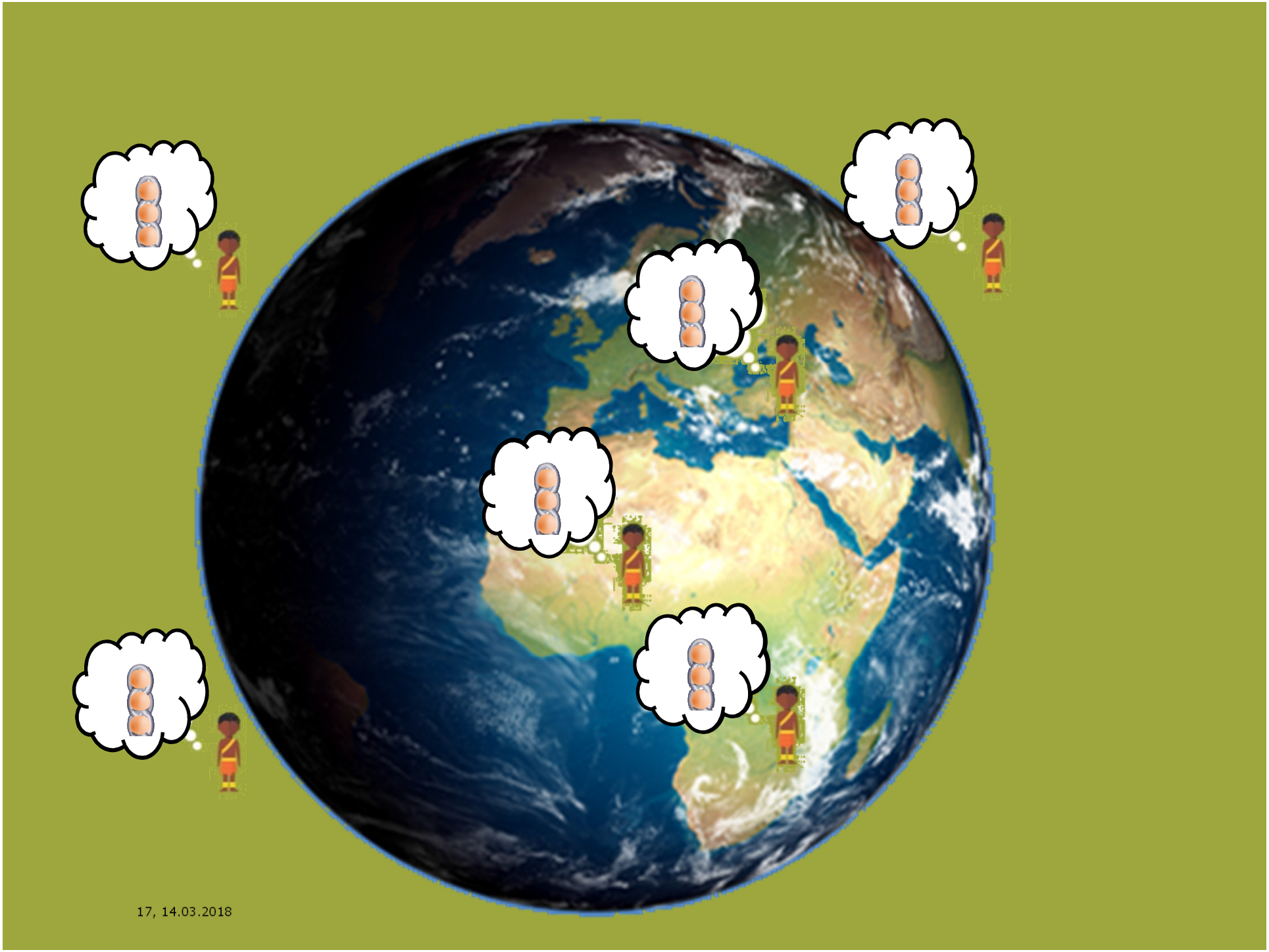




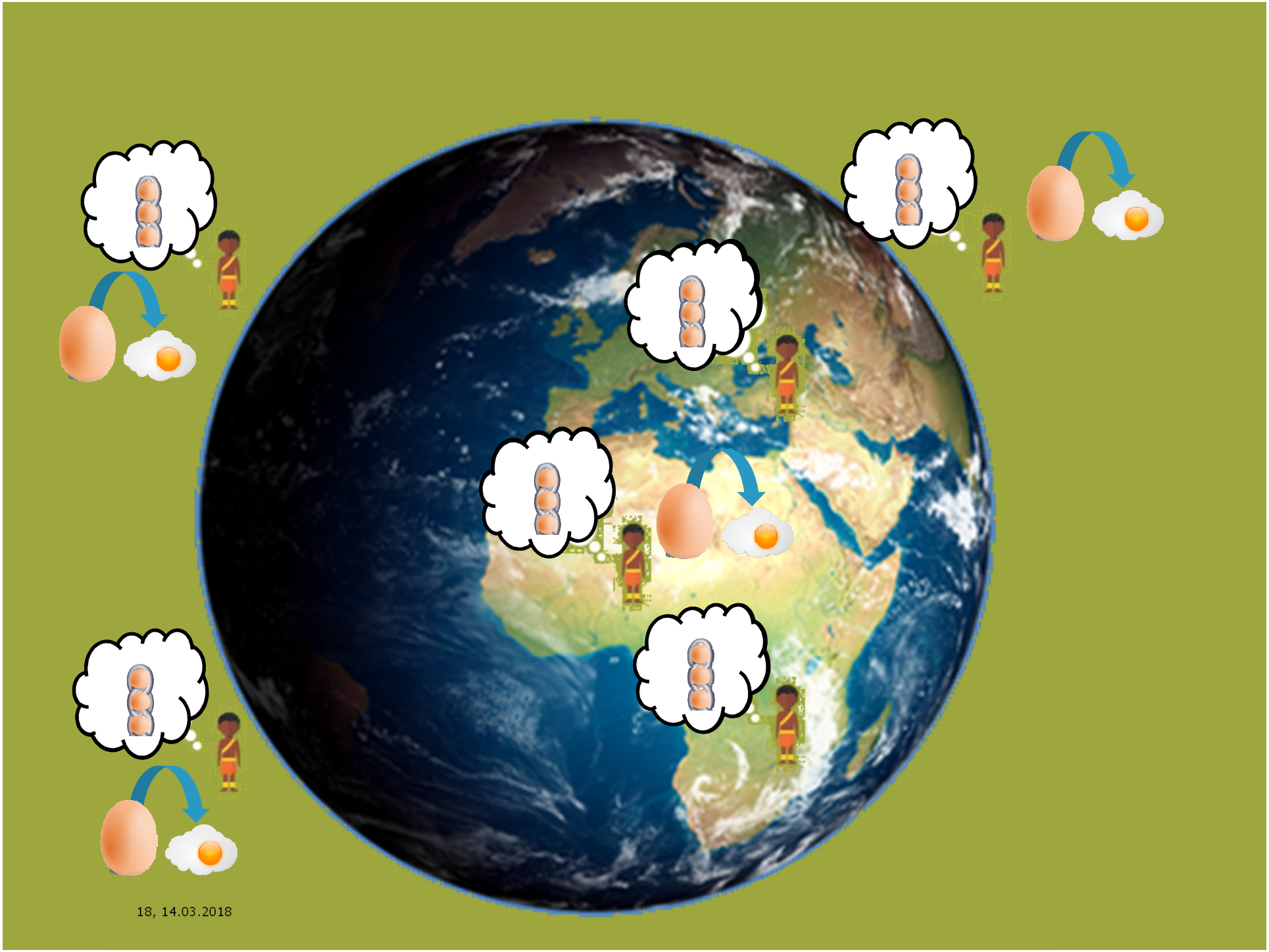
Quelle: https://anders.com/blockchain/



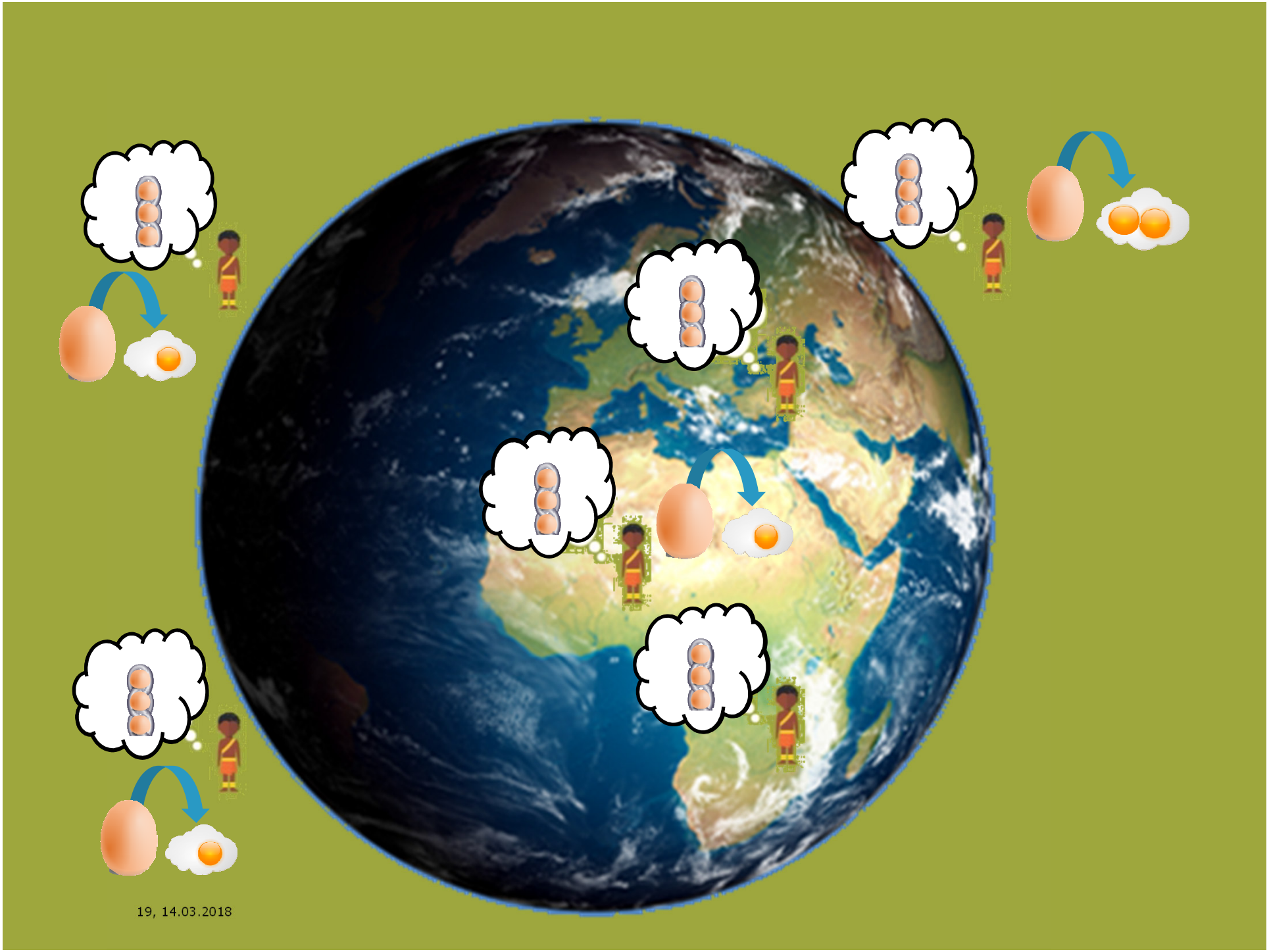
16, 14.03.2018



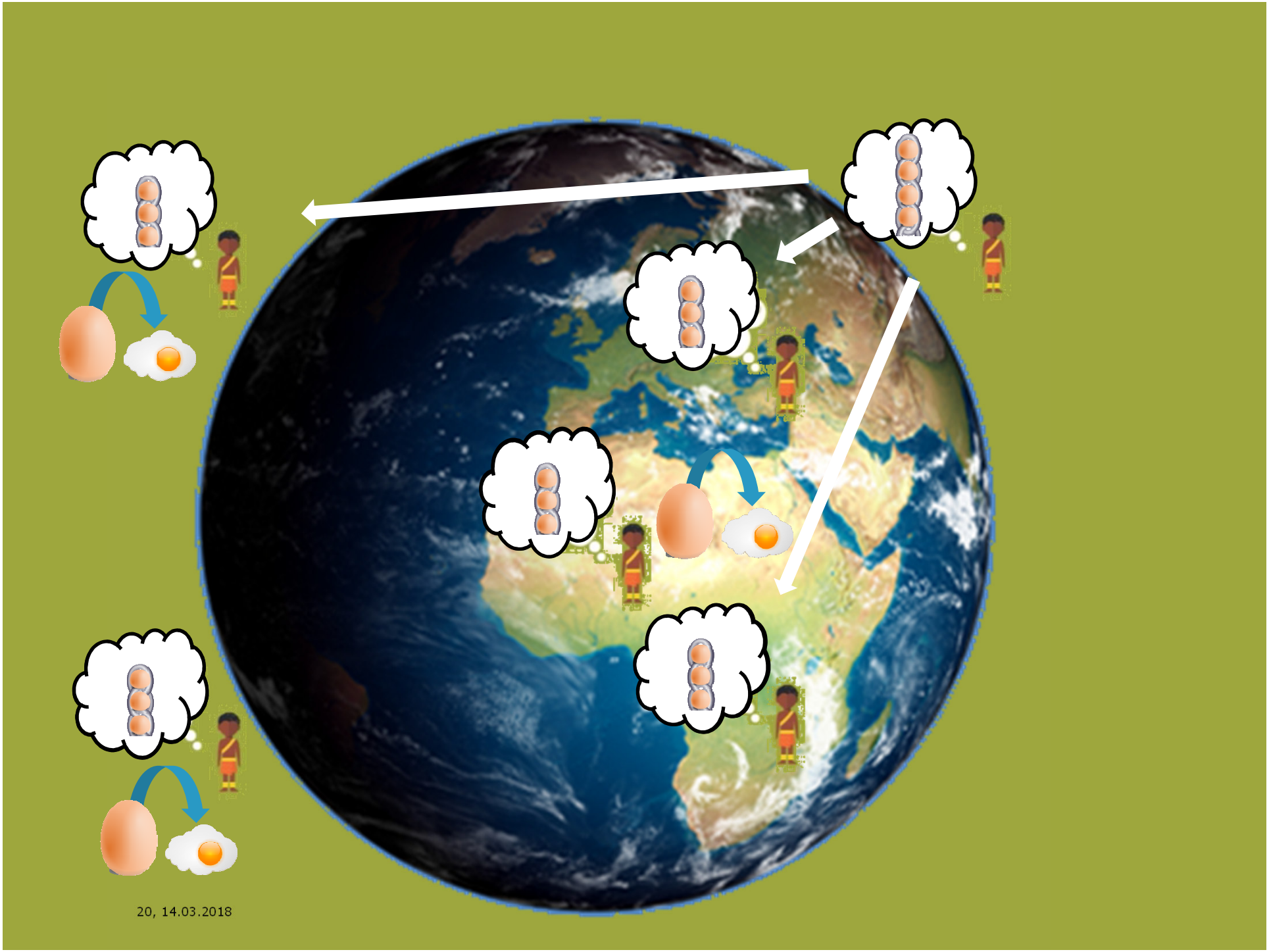
17, 14.03.2018



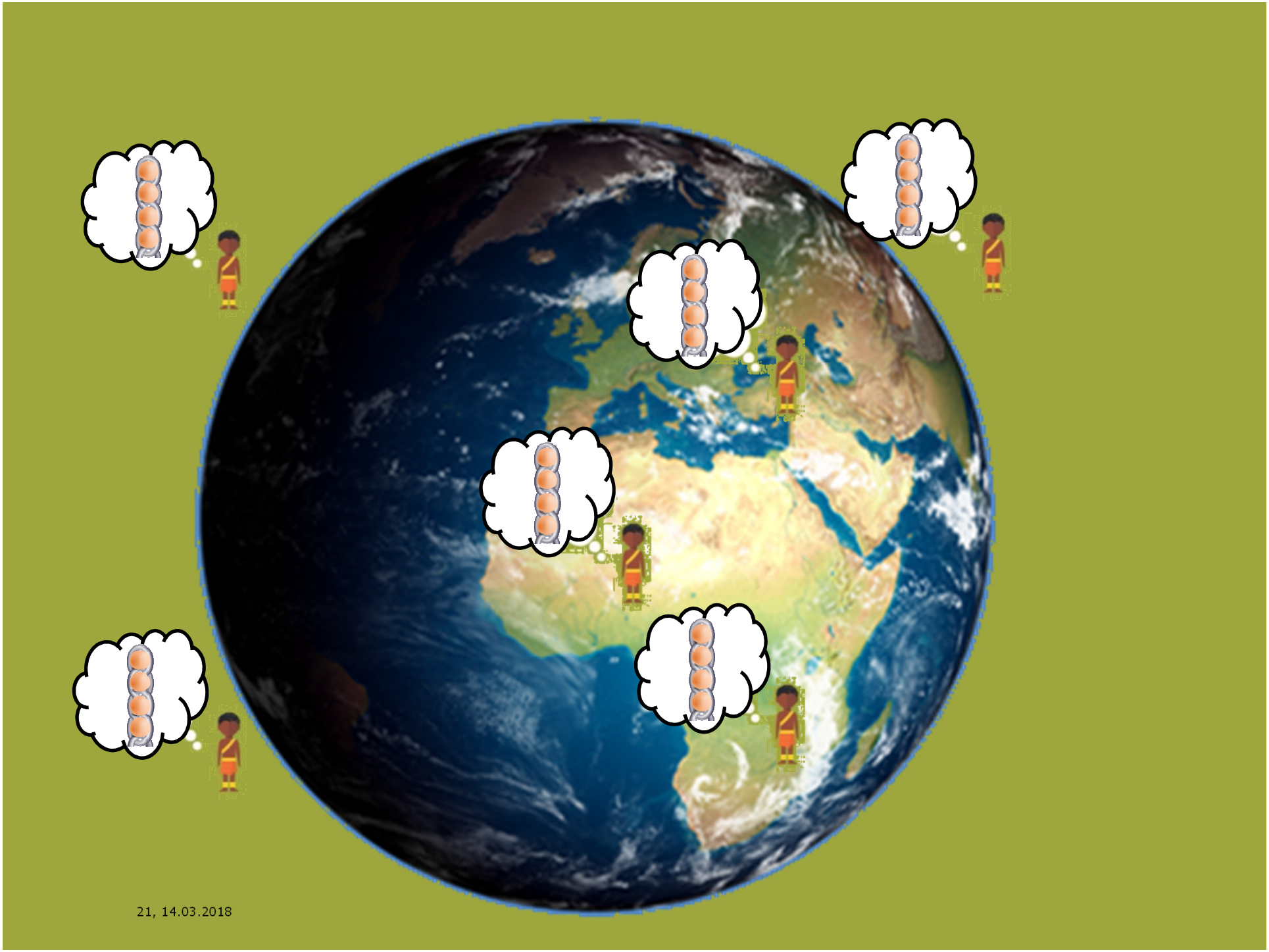
18, 14.03.2018



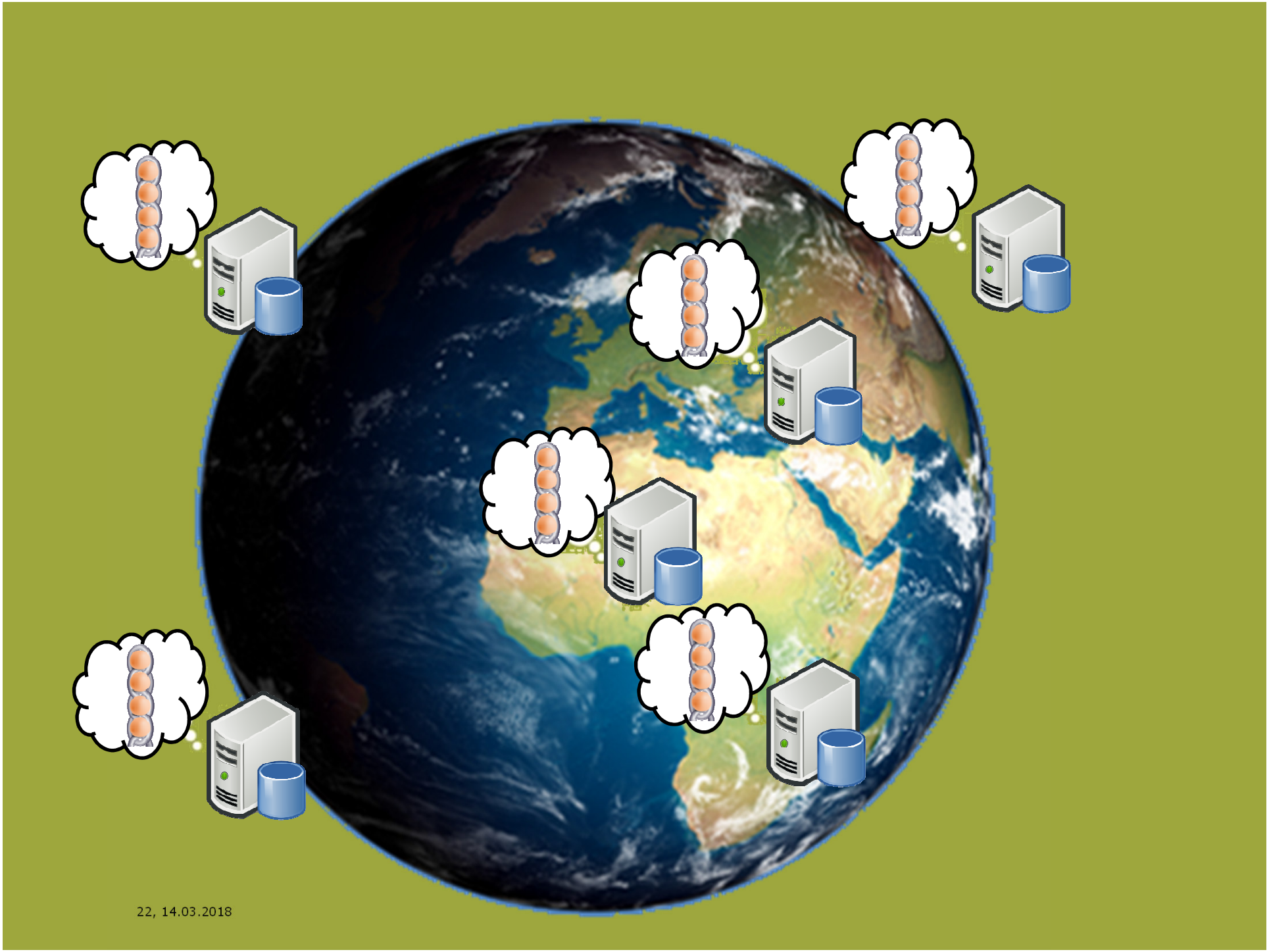
19, 14.03.2018

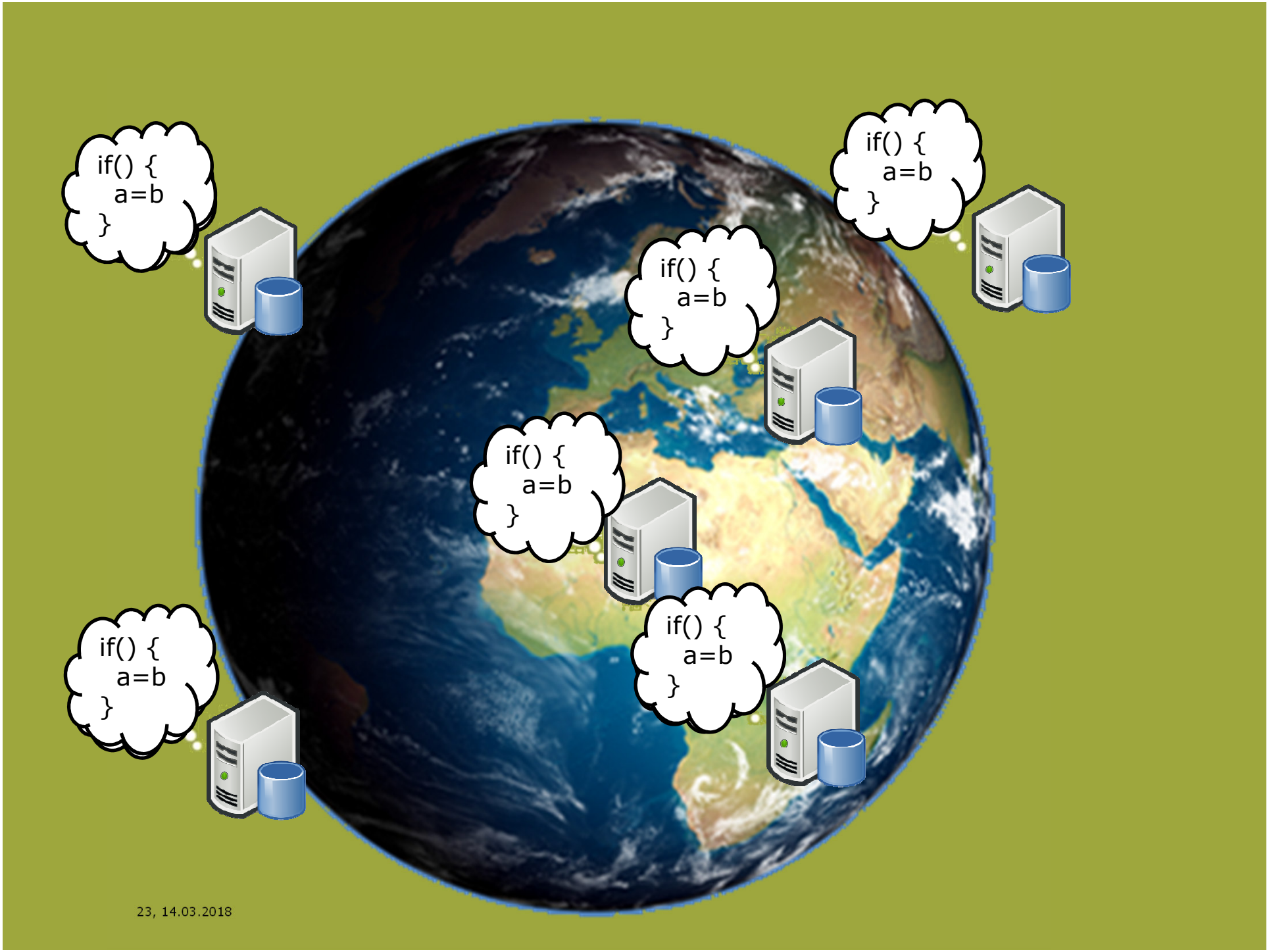


20, 14.03.2018



21, 14.03.2018




if() {
a=b
}
if() {
a=b
}
if() {
a=b
}
if() {
a=b
}
if() {
a=b
}
if() {
a=b
}

Wo ist die Disruption?