The Nexus Between Blockchain and Telephony

Michael Iedema - iedemam.com

Range Networks

Principal Engineer, RangeSDMN

ITNS Decentralized VPN

Core Developer, Blockchain Team

kapsulate.com

IoT

VoIP

RESTful

Blockchain

Mobile Apps

Embedded Linux

Complete Products

blockchain

“Blockchain” sounds so much cooler than
“slowest distributed database known to man”.

- random Twitter snark (2018)

VoIP

"Truth be told, the debate about VoIP versus TDM-based services ranks with discussions of the relative merits of PVC versus copper for plumbing conduit, it is an item of interest to plumbers."

- Dan Miller in Opus Research (2004)

the internet

Then there's cyberbusiness. We're promised instant catalog shopping —just point and click for great deals. We'll order airline tickets over the network, make restaurant reservations and negotiate sales contracts.

Stores will become obsolete. So how come my local mall does more business in an afternoon than the entire Internet handles in a month?

Even if there were a trustworthy way to send money over the Internet—which there isn't—the network is missing a most essential ingredient of capitalism: salespeople.

– Clifford Stoll in Newsweek (1995)

telephone / telegraph / printing press

Blockchain vs Bitcoin

Blockchain is a technology.
Bitcoin is an application.

invented concurrently

Blockchain was invented in 2008 for use in Bitcoin.

a breakthrough application

Bitcoin solved an unsolved problem to create a new product.

decentralized electronic cash

Bitcoin creates trust among users using blockchain.

true peer-to-peer payments

Bitcoin invented blockchain to solve the “double-spend” problem.

a breakthrough technology

Blockchain can record transactions accurately without a central authority.

decentralized consensus

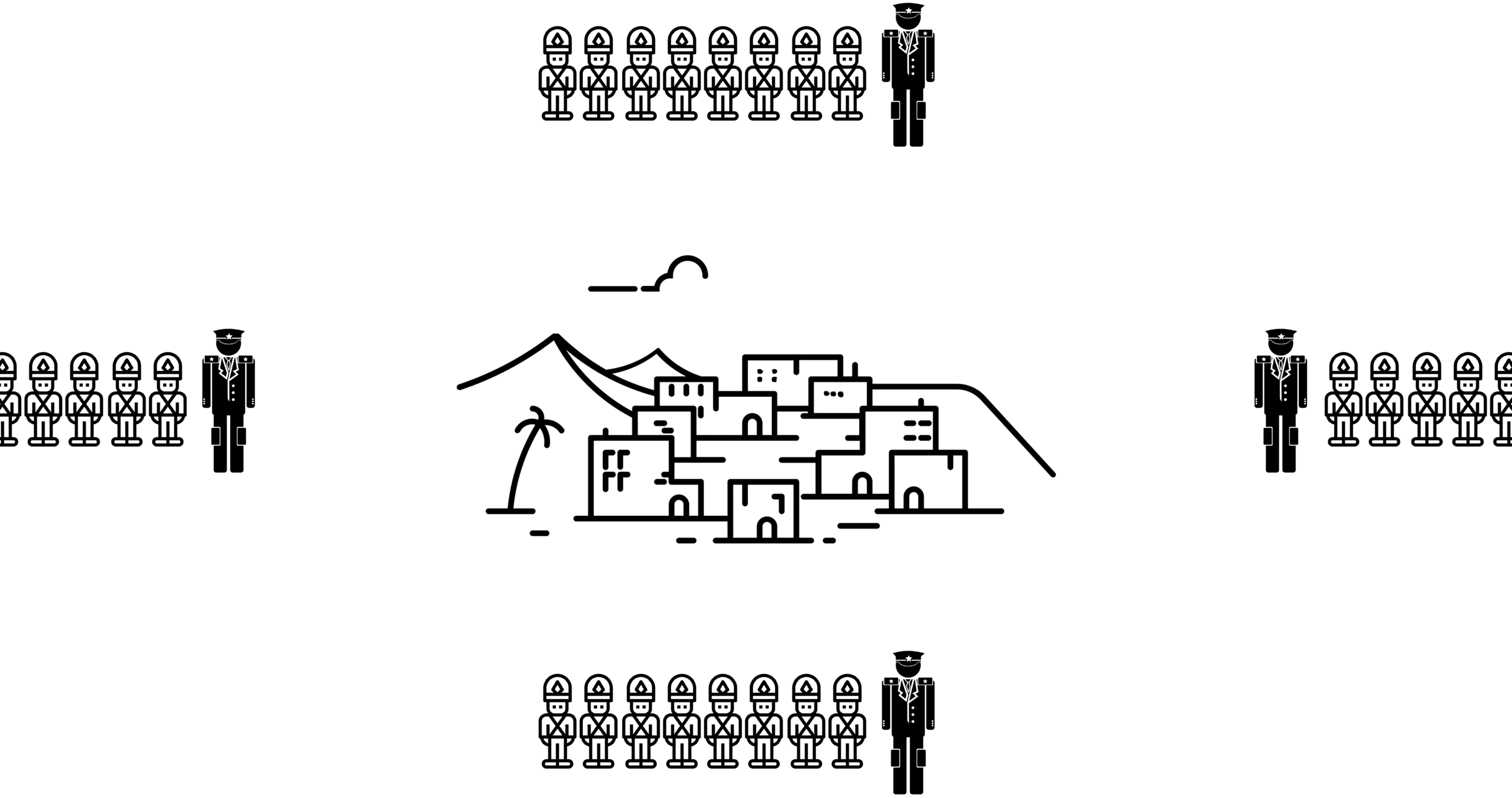
This opens up an entirely new way to think about network applications.

decentralized consensus

It’s kind of like inventing e-mail and creating the internet as a by-product.

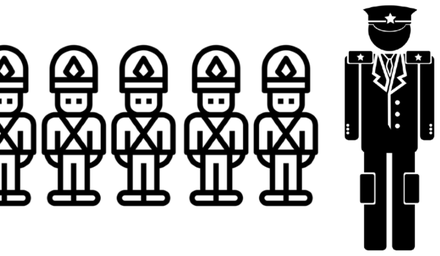
Byzantine Generals Problem

How do entities, separated by distance, reach full consensus?

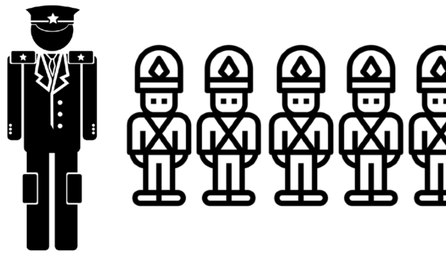


"Attack at 09:00!"

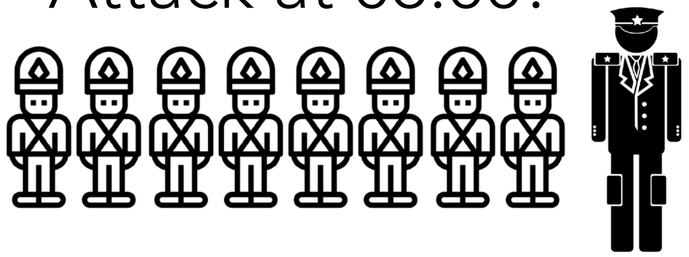
"Attack at 10:00!"



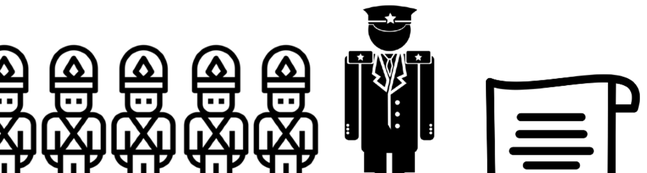
"Attack at 07:00!"

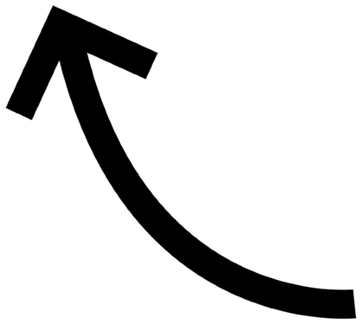


"Attack at 08:00!"

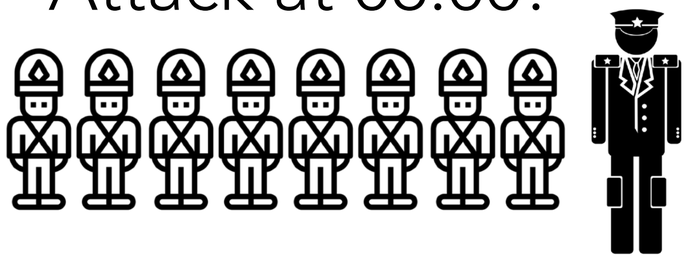


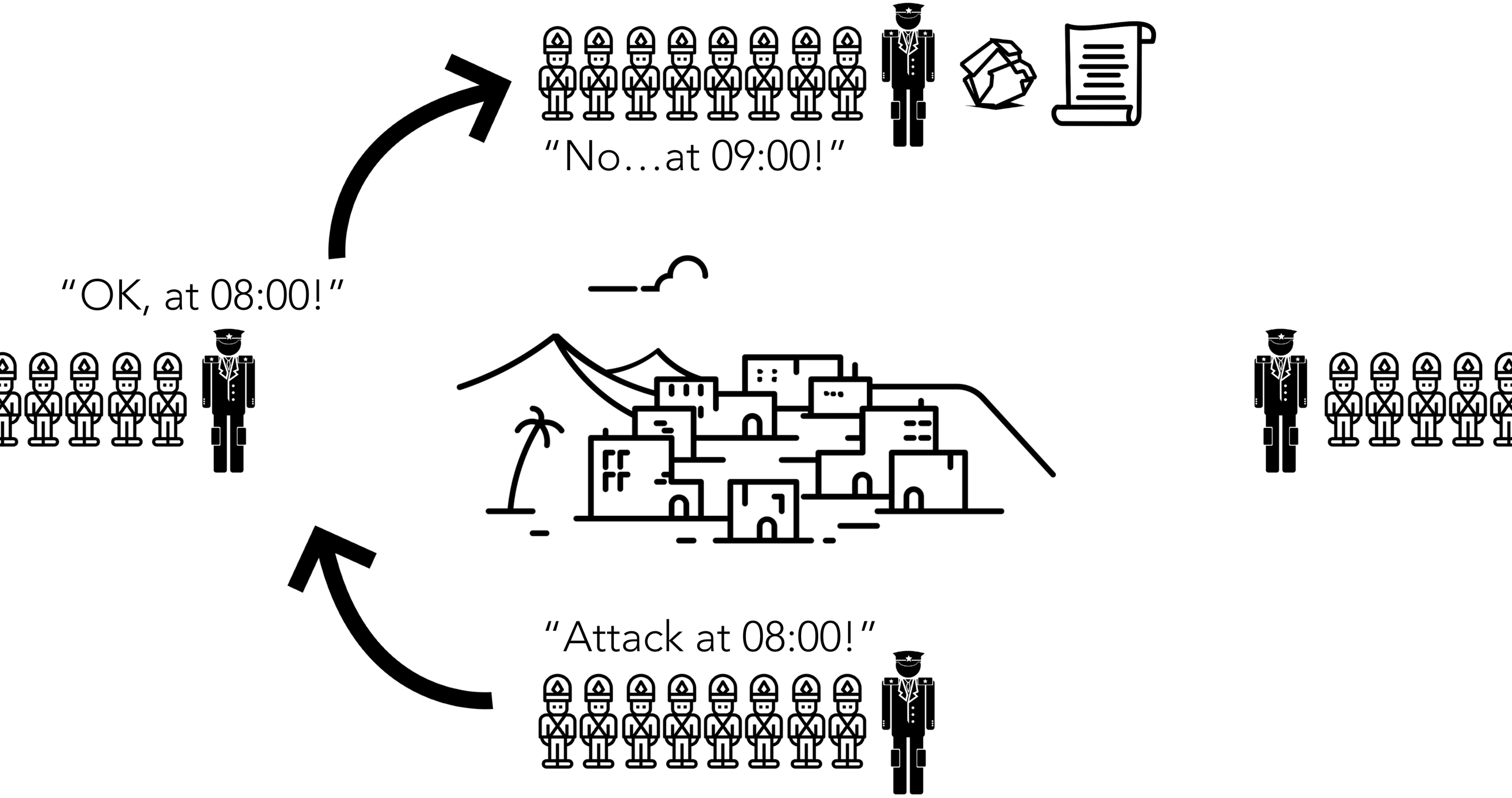
“OK, at 08:00!”

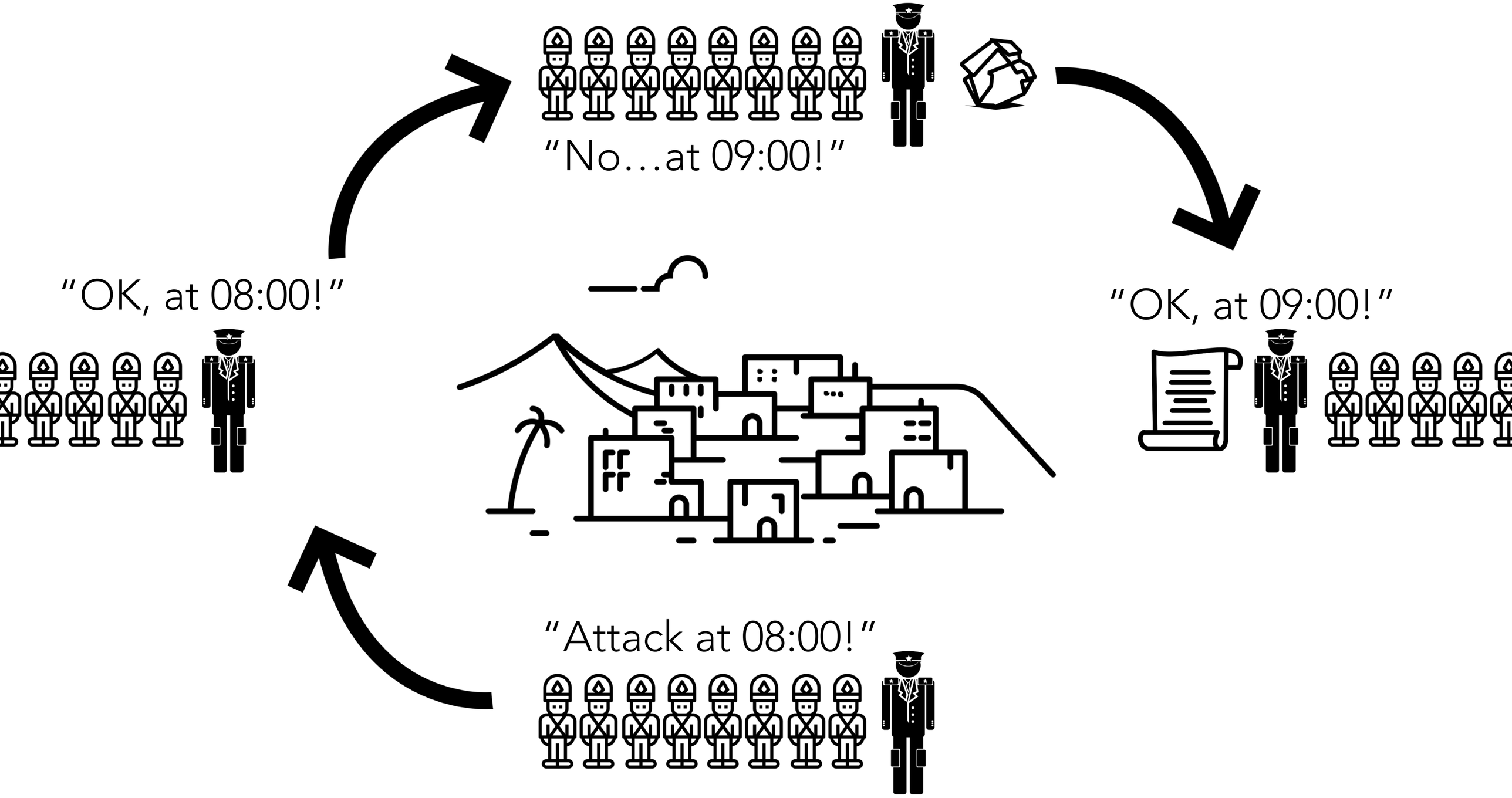


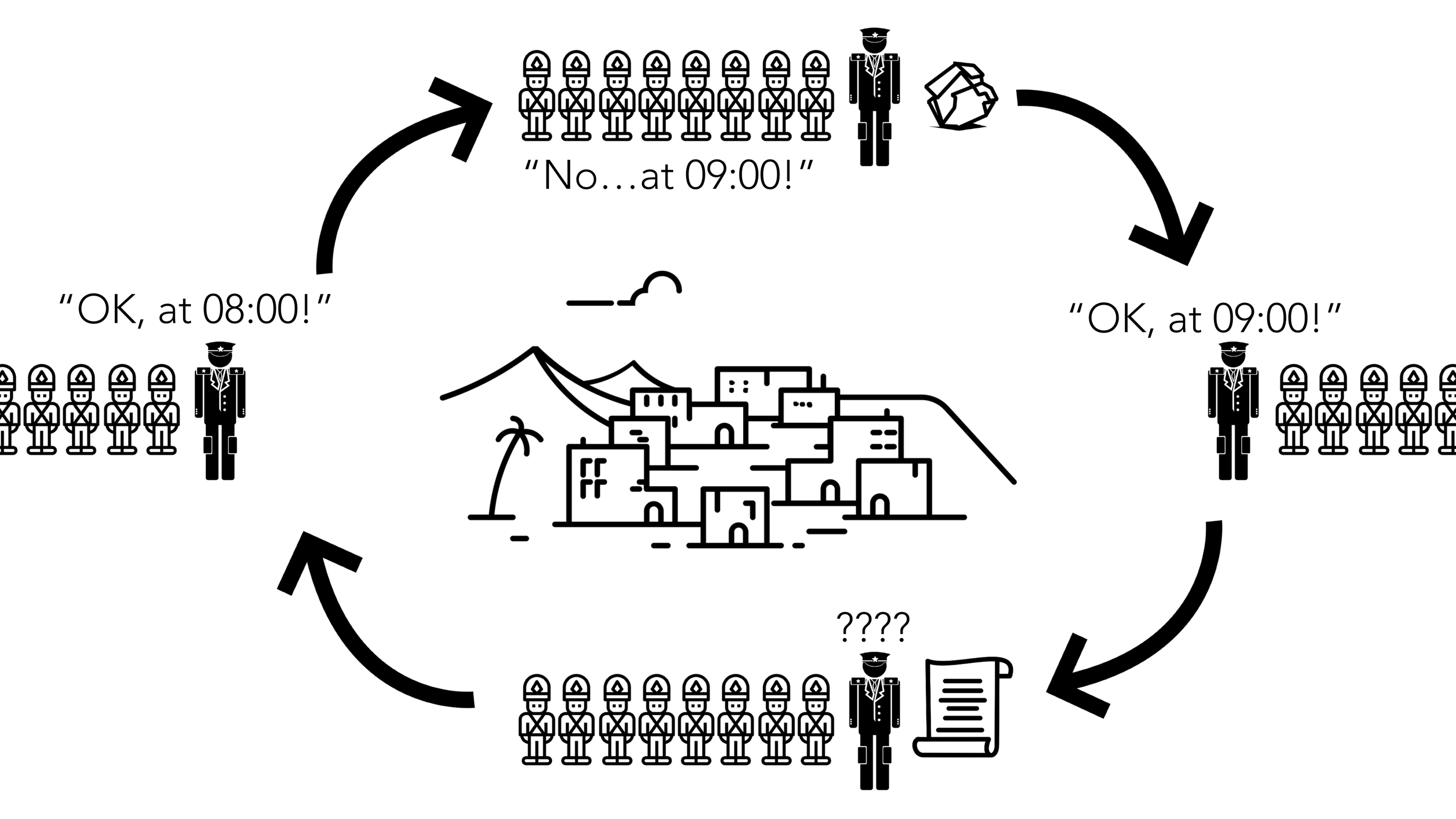


“Attack at 08:00!”

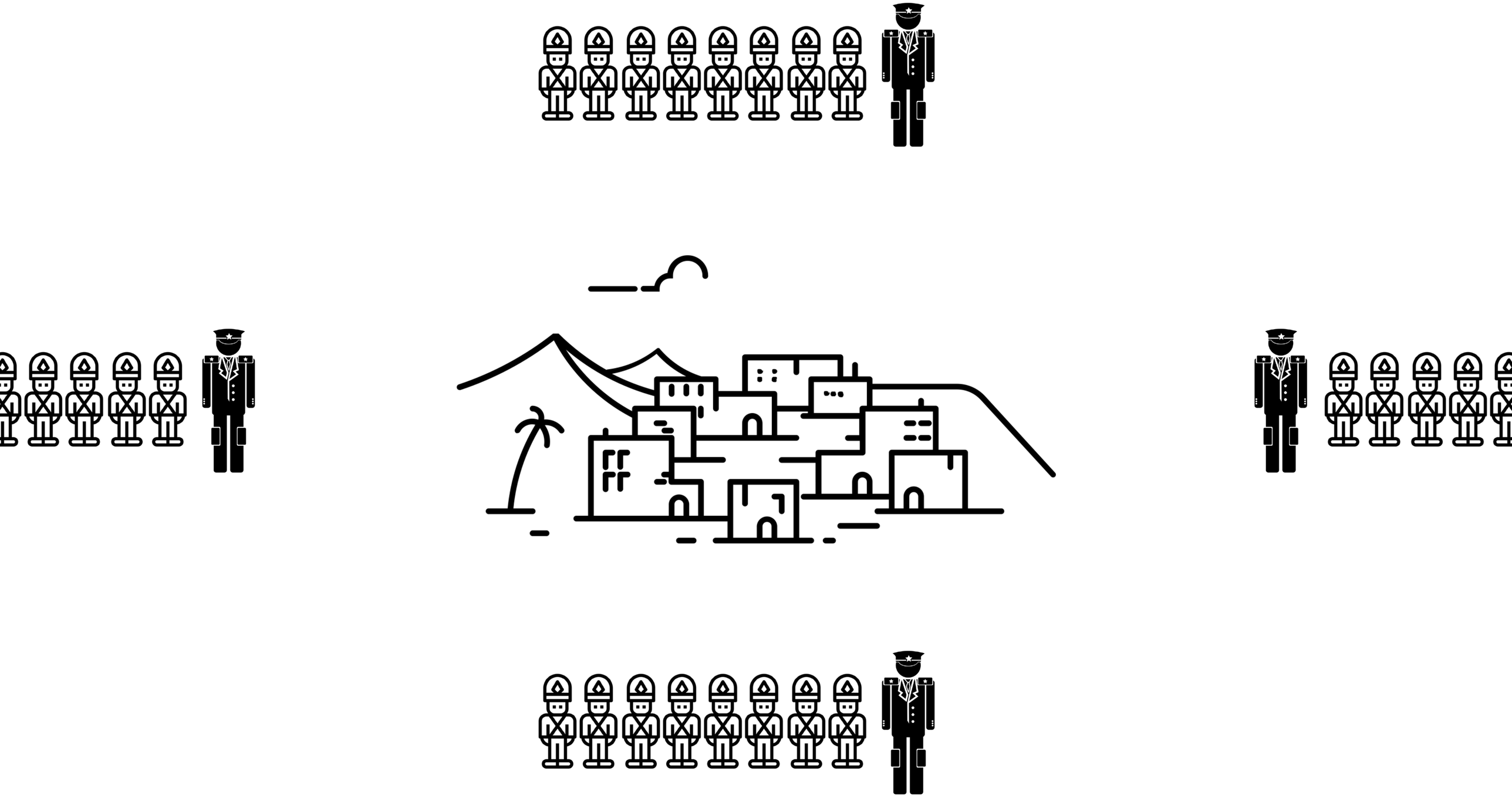



"No…at 09:00!"
"OK, at 08:00!"
"Attack at 08:00!"


"No…at 09:00!"
"OK, at 09:00!"
"Attack at 09:00!"
"OK, at 08:00!"

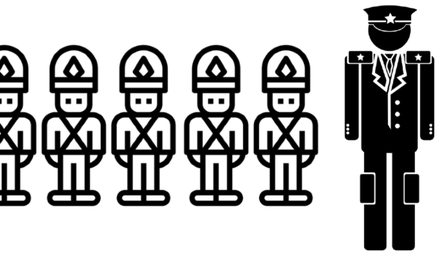

"No…at 09:00!"
"OK, at 09:00!"
????
"OK, at 08:00!"

How does blockchain help the generals?

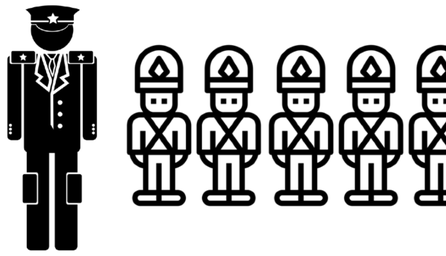


"Attack at 09:00!"

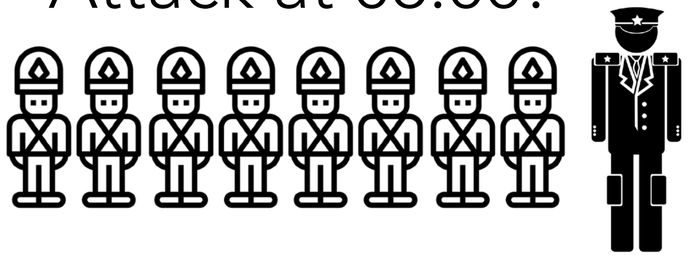
"Attack at 10:00!"

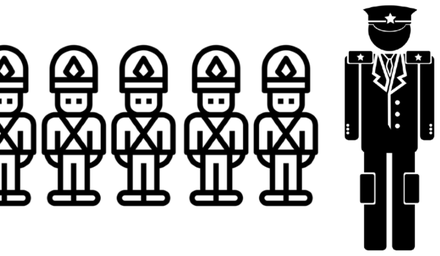


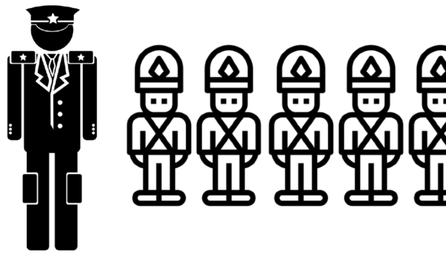
"Attack at 07:00!"



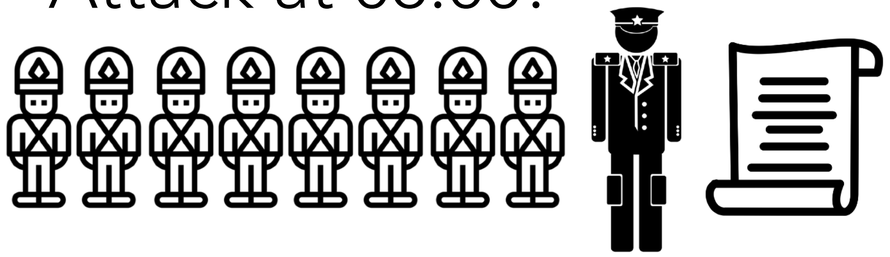
"Attack at 08:00!"







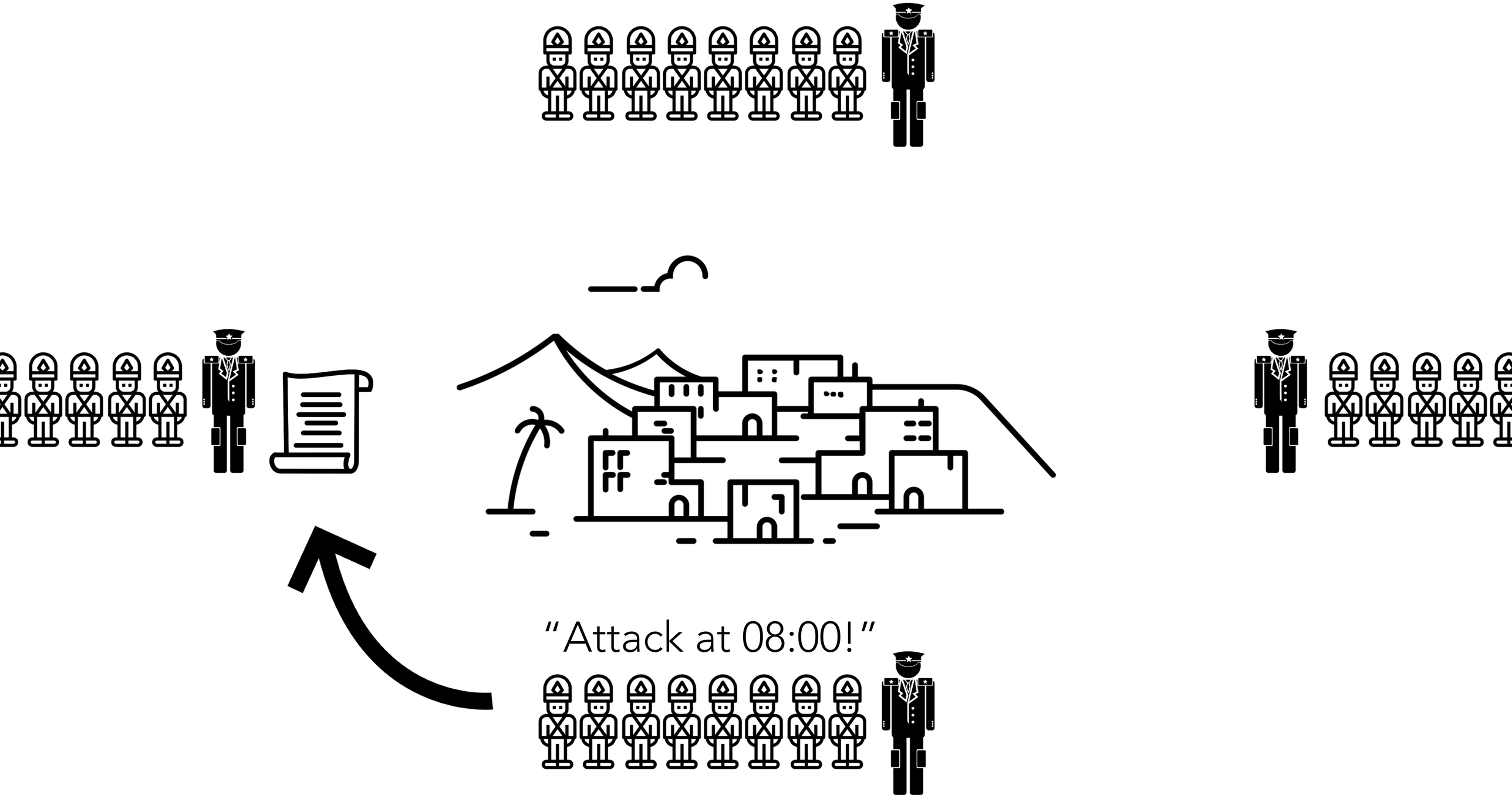
"Attack at 08:00!"



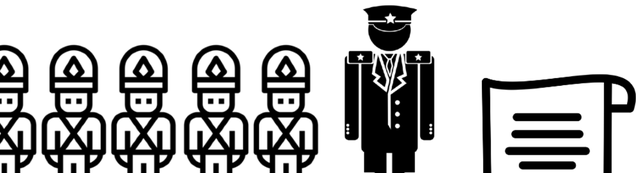
Messages Creation

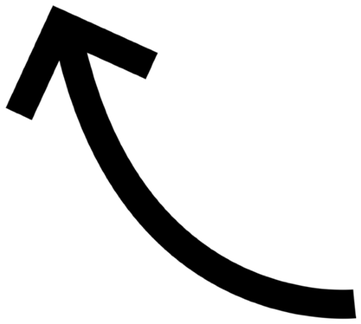
Creating a message always takes a fixed amount of time.

IT IS WITH GREAT HONOR AND RESPECT THAT I, SIR GENERAL NUMBER ONE WRITE TO YOU, MY DEAREST COLLEAGUE, SIR GENERAL NUMBER TWO OF MY PLANS FOR THE MORROW. WE SHALL ATTACK AT THE HOUR OF EIGHT AND THE HOUR OF EIGHT SHALL BE THE HOUR OF THE ATTACK.

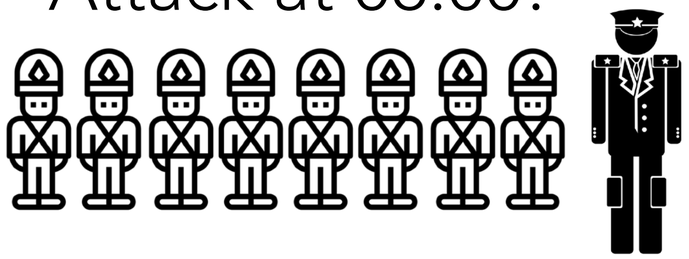

"Attack at 08:00!"

“OK, at 08:00!”





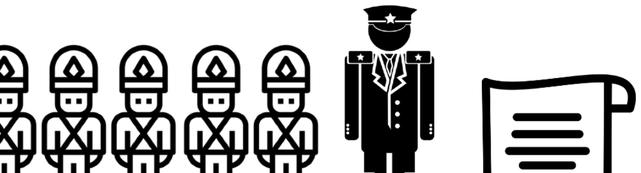
“Attack at 08:00!”

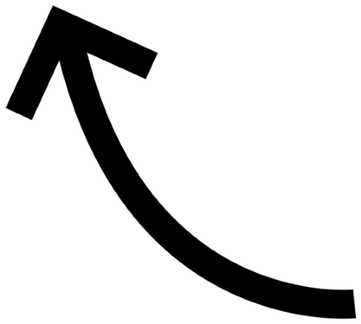


Message Uniqueness

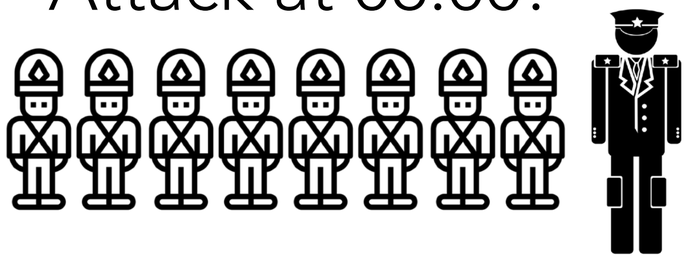
Messages are not reused, altered or deleted. Messages can only be created.

“OK, at 08:00!”

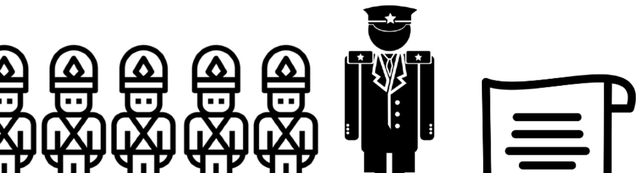


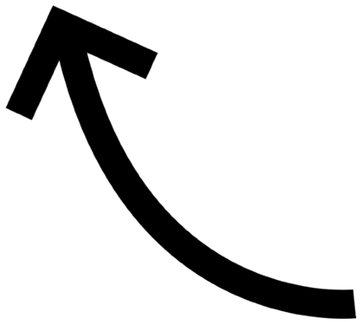


“Attack at 08:00!”

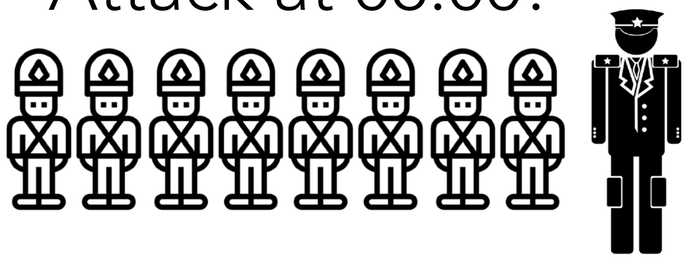


"OK, at 08:00!"

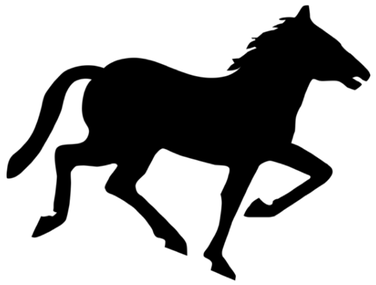




"Attack at 08:00!"

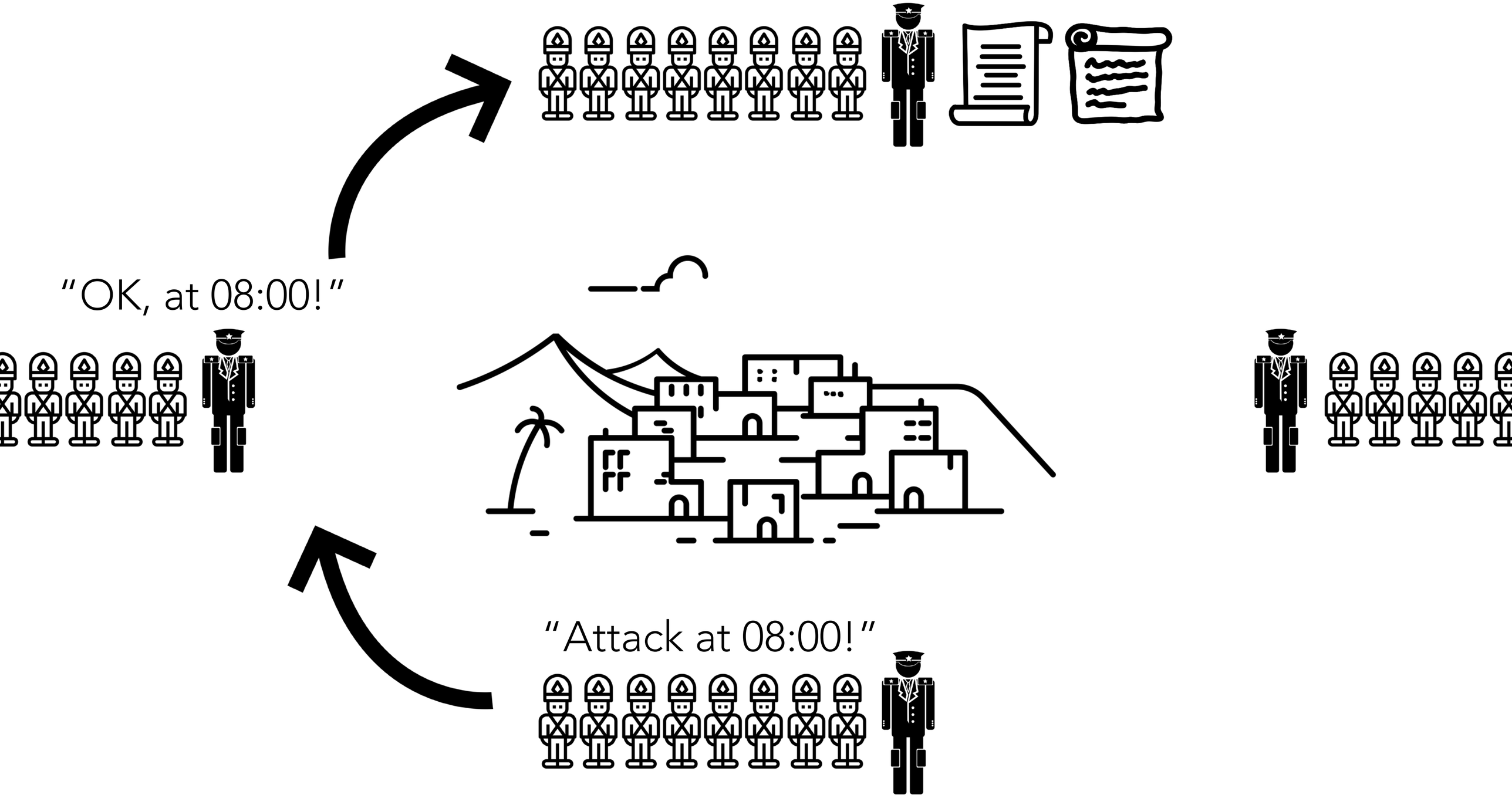


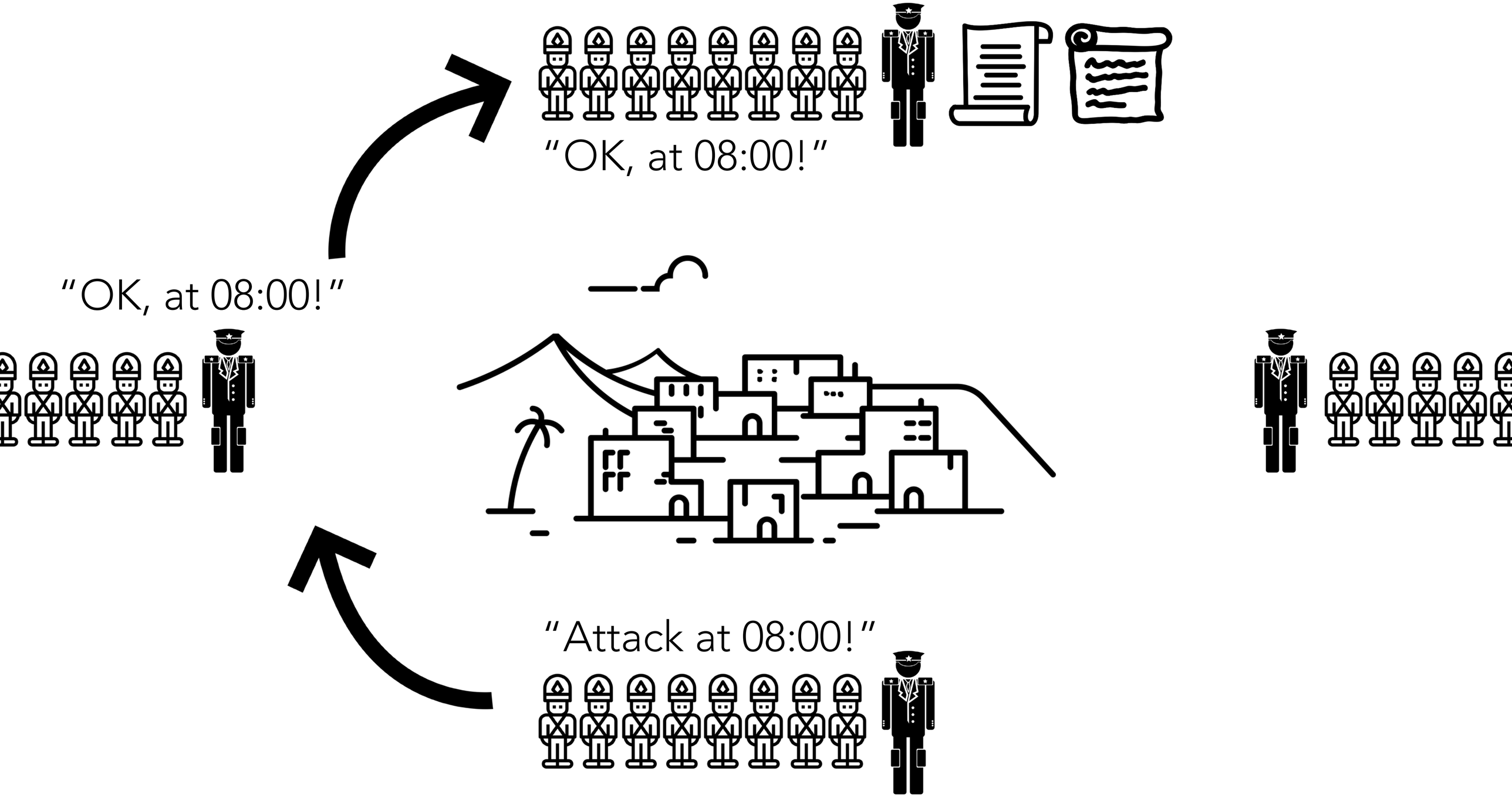
IT IS WITH GREAT HONOR AND RESPECT THAT I, SIR GENERAL NUMBER TWO WRITE TO YOU, MY DEAREST COLLEAGUE, SIR GENERAL NUMBER THREE OF MY PLANS FOR THE MORROW. WE SHALL ATTACK AT THE HOUR OF EIGHT AND THE HOUR OF EIGHT SHALL BE THE HOUR OF THE ATTACK.

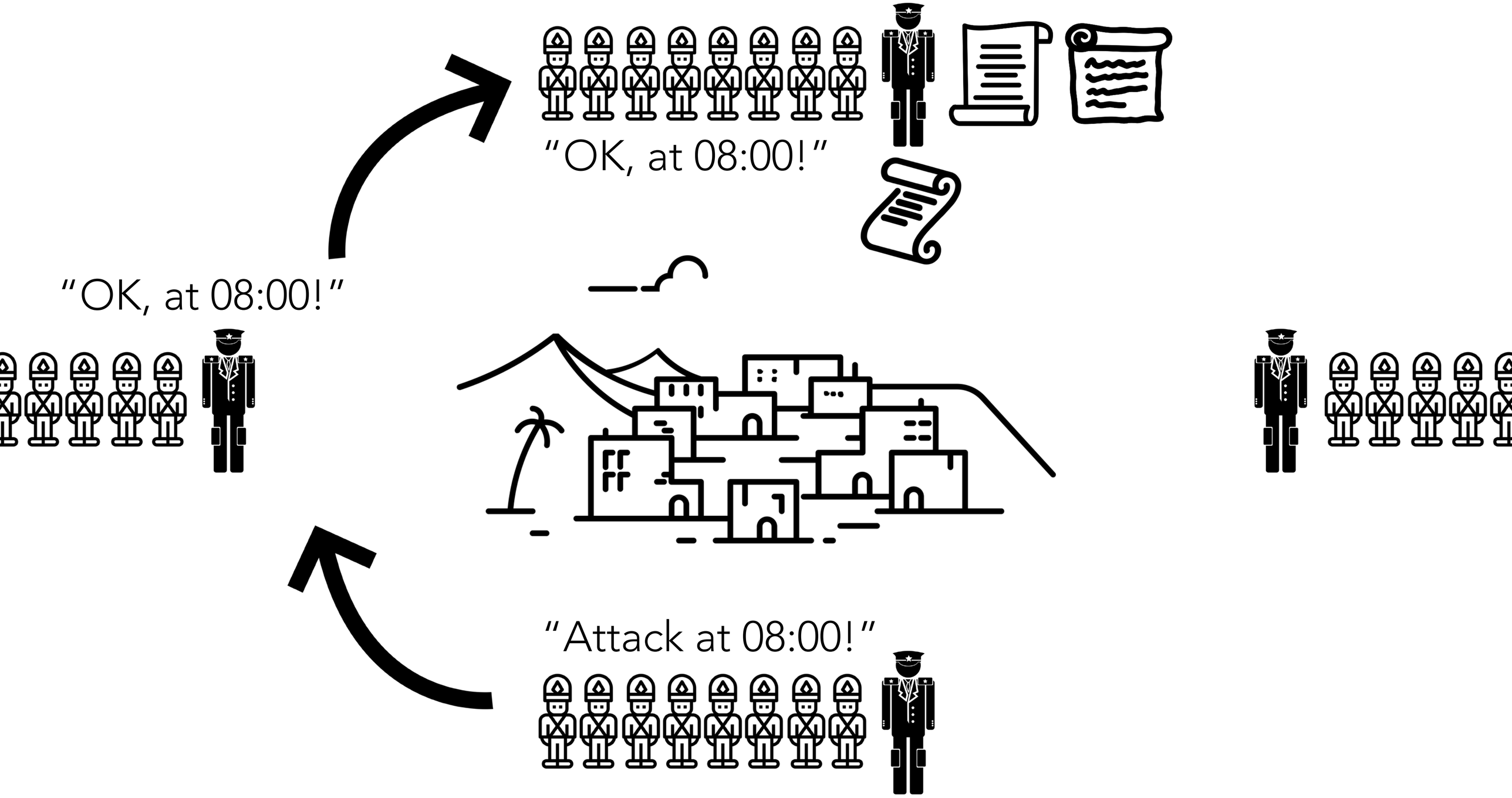


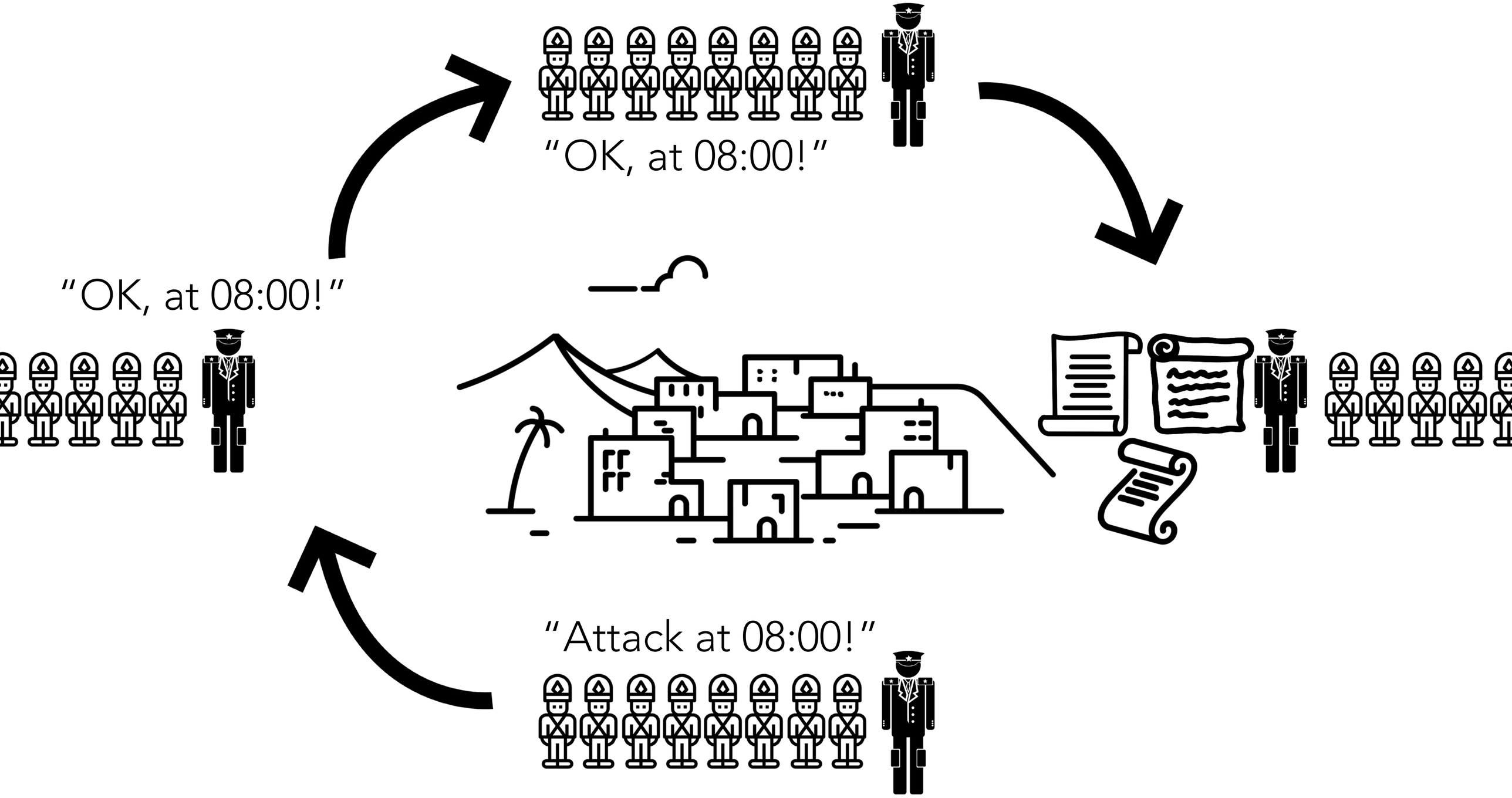
Message Distribution

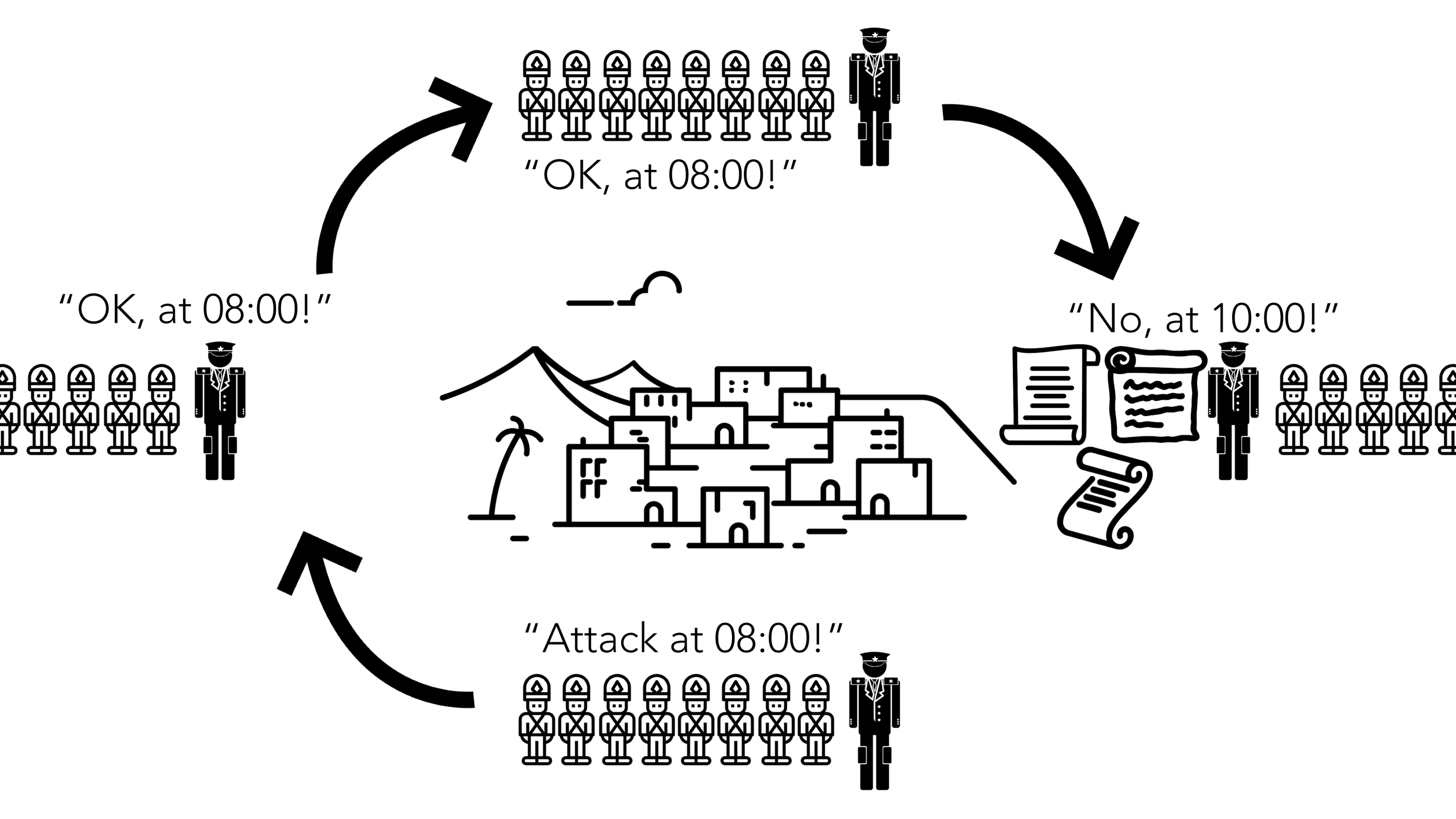
New messages are appended to all previous messages.

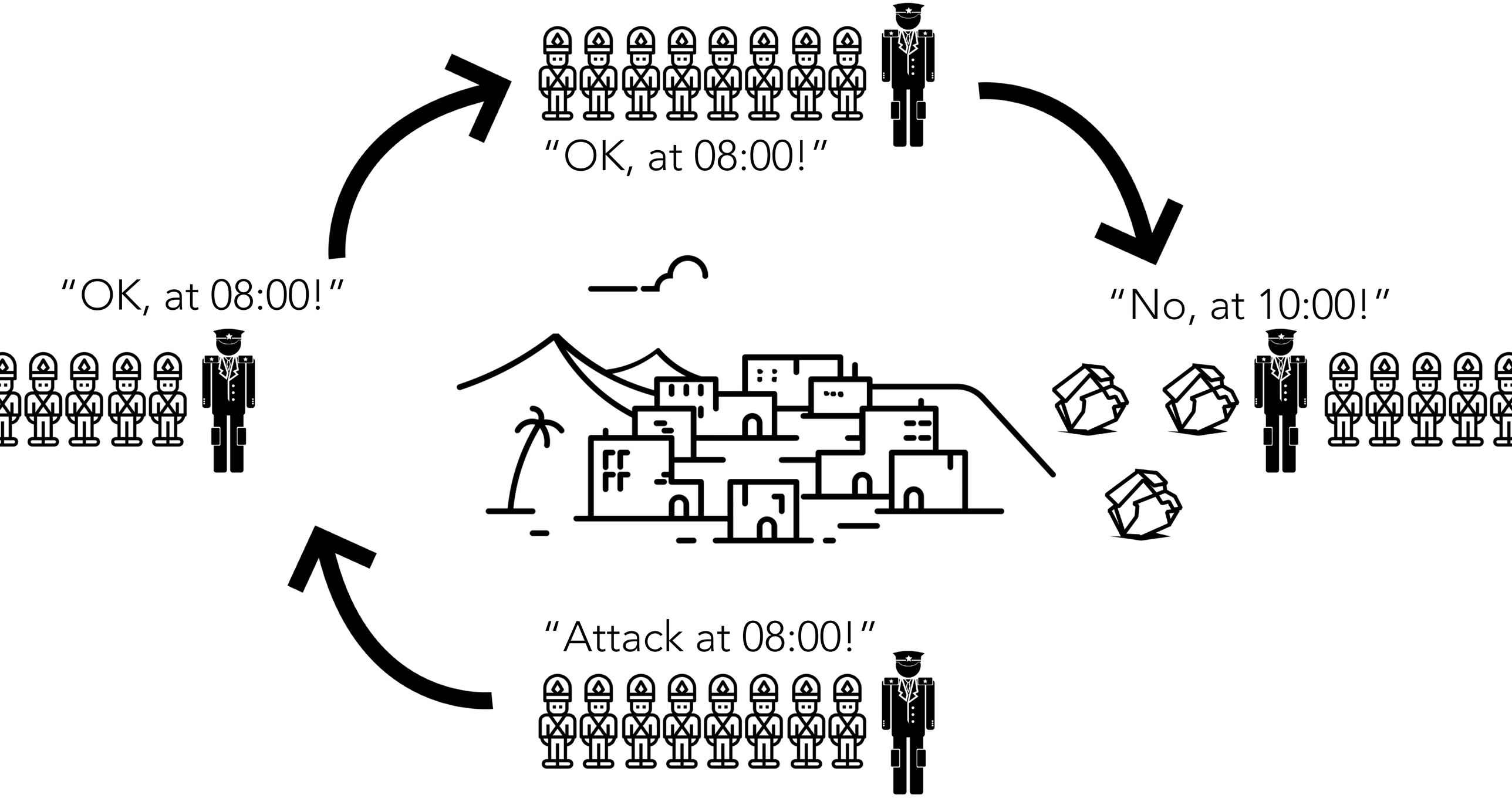

"OK, at 08:00!"
"Attack at 08:00!"

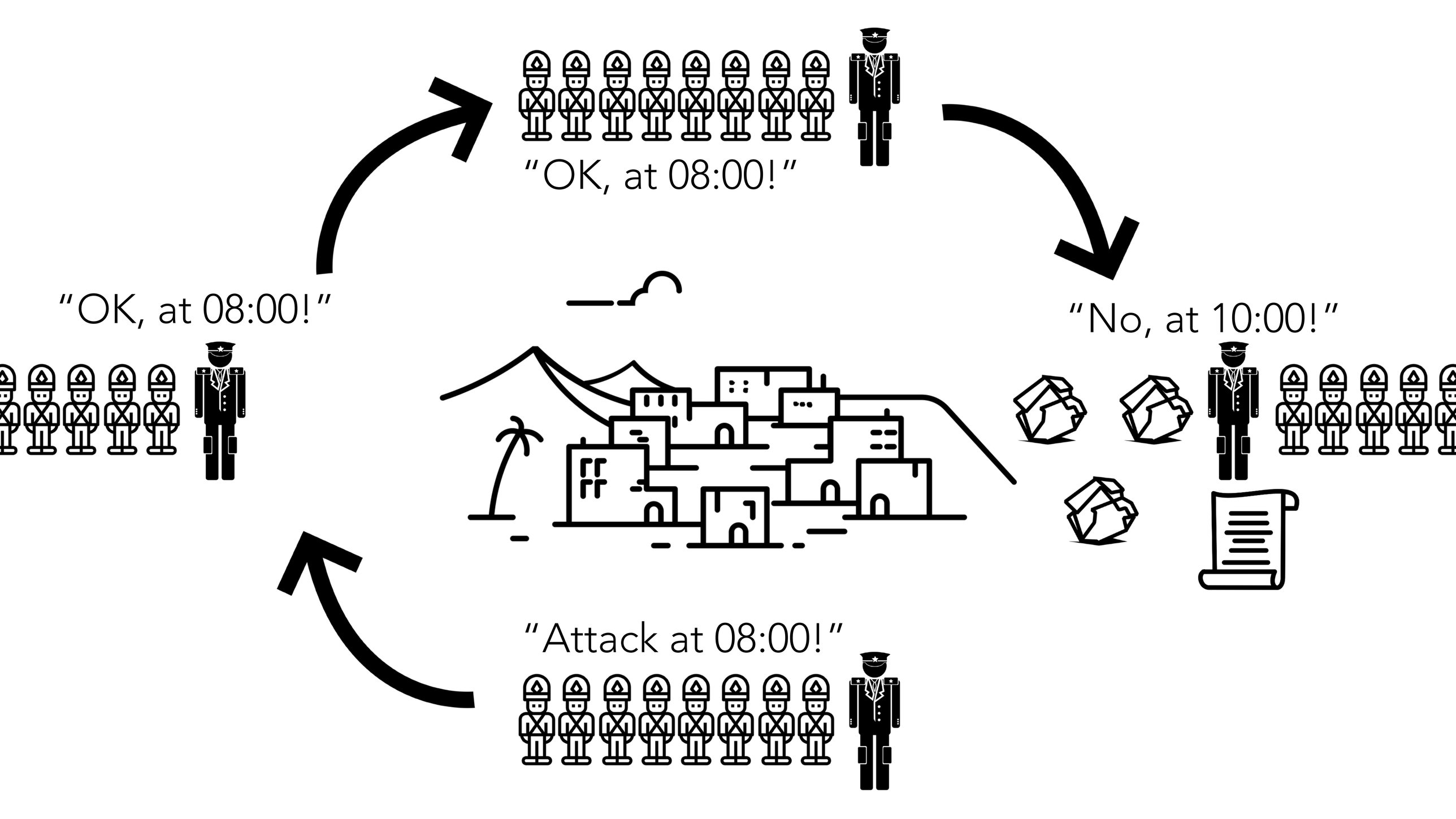

"OK, at 08:00!"
"OK, at 08:00!"
"Attack at 08:00!"

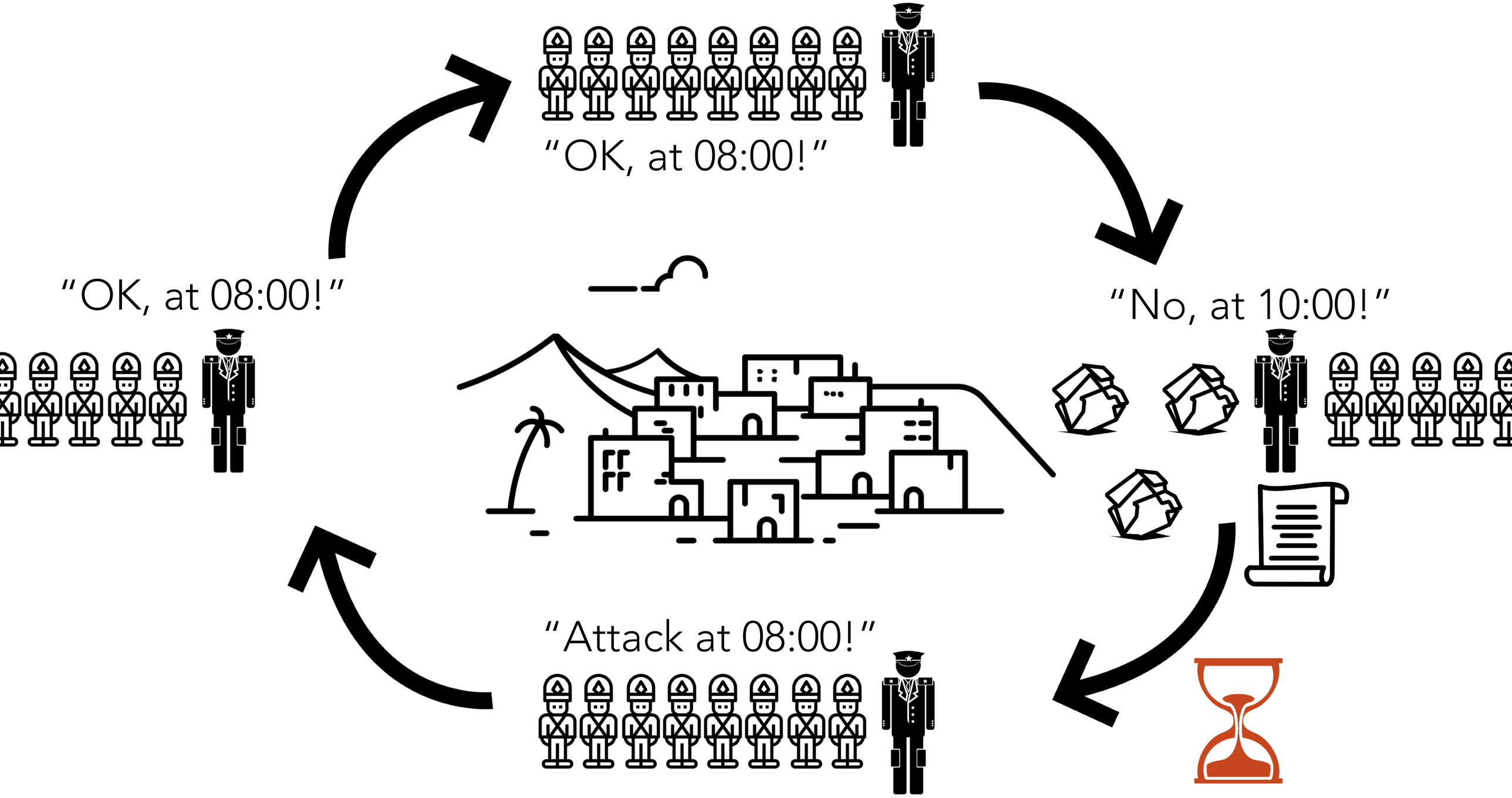

"OK, at 08:00!"
"OK, at 08:00!"
"Attack at 08:00!"

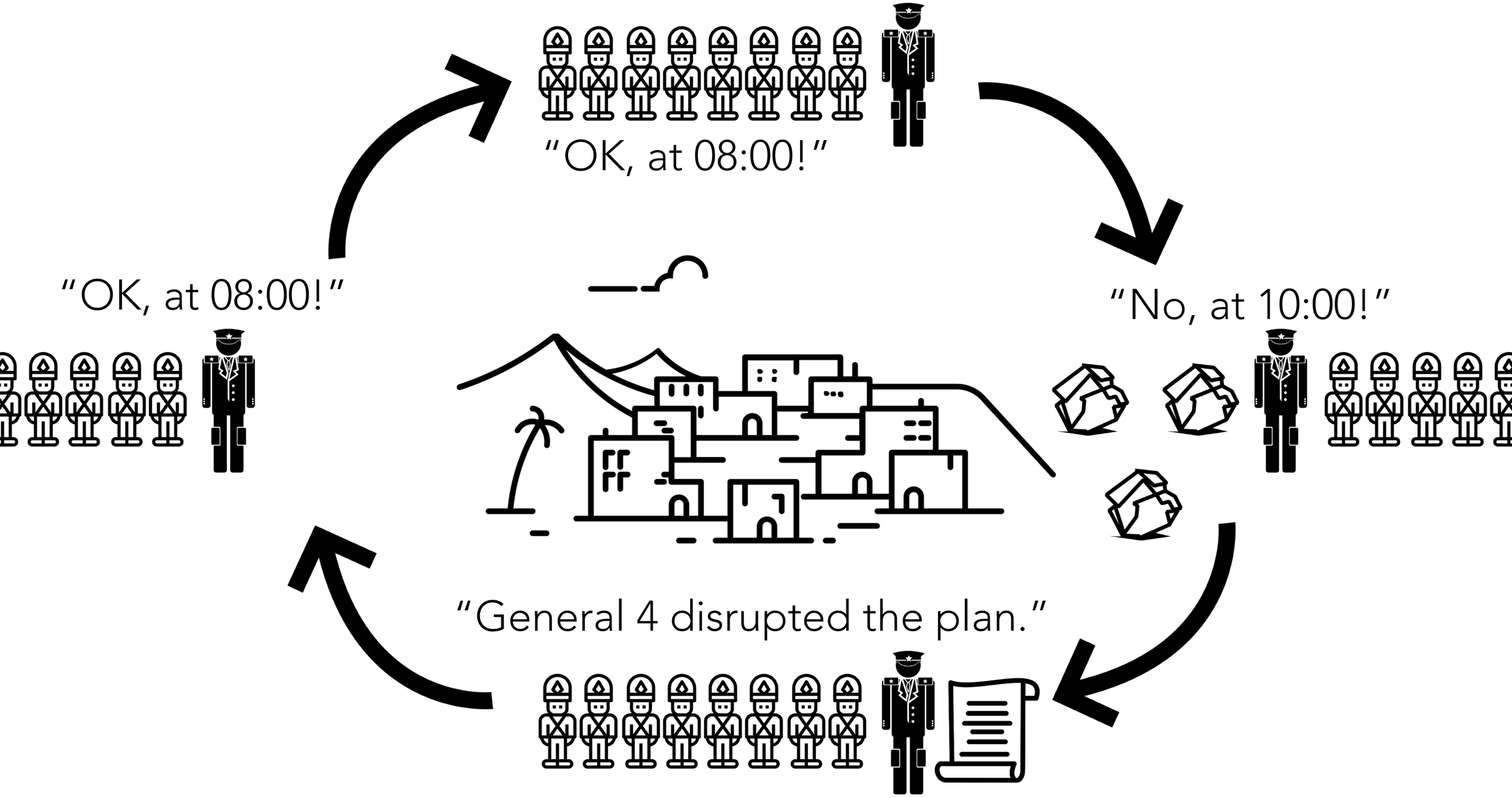

"OK, at 08:00!"
"OK, at 08:00!"
"Attack at 08:00!"


"OK, at 08:00!"
"No, at 10:00!"
"Attack at 08:00!"
"OK, at 08:00!"


"OK, at 08:00!"
"No, at 10:00!"
"Attack at 08:00!"
"OK, at 08:00!"


"OK, at 08:00!"
"No, at 10:00!"
"Attack at 08:00!"
"OK, at 08:00!"


"OK, at 08:00!"
"No, at 10:00!"
"Attack at 08:00!"
"OK, at 08:00!"


"OK, at 08:00!"
"No, at 10:00!"
"General 4 disrupted the plan."
"OK, at 08:00!"

Blockchain Terminology

node

Each general represents an instance of a decentralized application.

network

Each rider represents a network traffic flow.

transaction

Each message represents a transaction.

block

Multiple transactions are bundled into a block.

block time

Each block of transactions must be created in a fixed amount of time.

proof-of-work

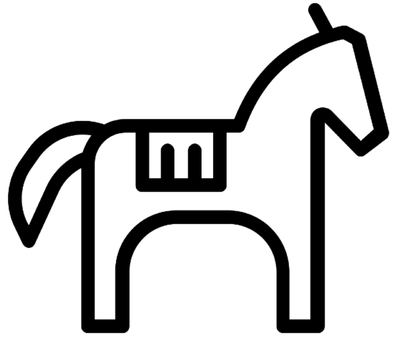
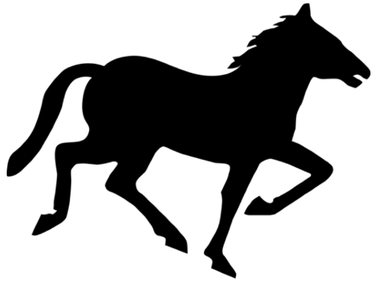
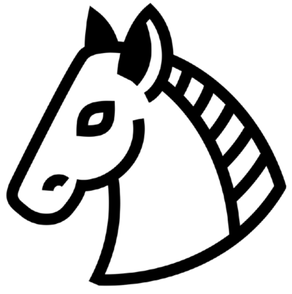
Each block requires significant effort to be created.

difficulty

To achieve a fixed block time, the difficulty is adjusted.

IT IS WITH GREAT HONOR AND RESPECT THAT I, SIR GENERAL NUMBER ONE WRITE TO YOU, MY DEAREST COLLEAGUE, SIR GENERAL NUMBER TWO OF MY PLANS FOR THE MORROW. WE SHALL ATTACK AT THE HOUR OF EIGHT AND THE HOUR OF EIGHT SHALL BE THE HOUR OF THE ATTACK.

IT IS WITH GREAT HONOR AND RESPECT THAT I, SIR GENERAL NUMBER ONE WRITE TO YOU, MY DEAREST COLLEAGUE, SIR GENERAL NUMBER TWO OF MY PLANS FOR THE MORROW. WE SHALL ATTACK AT THE HOUR OF EIGHT AND THE HOUR OF EIGHT SHALL BE THE HOUR OF THE ATTACK.


mining

Not every general wants to draw a bunch of horses.

mining

The network stops if no one is drawing horses.

mining

“Drawing horses” creates valid blocks and is rewarded by the network.

blockchain

A sequence of blocks.

public ledger

Every node has a copy of the blockchain.

public ledger

The blockchain contains every transaction ever made.

Every node can know the truth.

Decentralized Users

How do I create an account?

You don’t.

“Accounts” are based entirely on public/private key pairs.

public key

Analogous to a username or address on the network.

private key

Analogous to a password on the network.

I sign messages to you with my private key.

I address messages to your public key.

Everyone validates my messages with my public key.

This confirms that only I could have sent them.

Your public key is used to deposit.

Your private key is used to withdraw.

wallet

To participate on the network, you need a “wallet.”

wallet

This is a misleading term.

It is just a pair of keys.

If anyone has your keys, they ARE you on the network.

When does blockchain make sense?

Do you need a data store?

Are there multiple writers?

Do the transactions’ order matter?

Are there untrusted participants?

Could a trusted third-party be used?

Blockchain ∩ Telephony

digital goods

digital goods

minutes, messages and megabytes

digital goods

intra-carrier is easy, inter-carrier is not

"I can send you something digitally
and prove that I don't have it anymore.”

– Jon Choi, Ethereum Foundation

digital goods

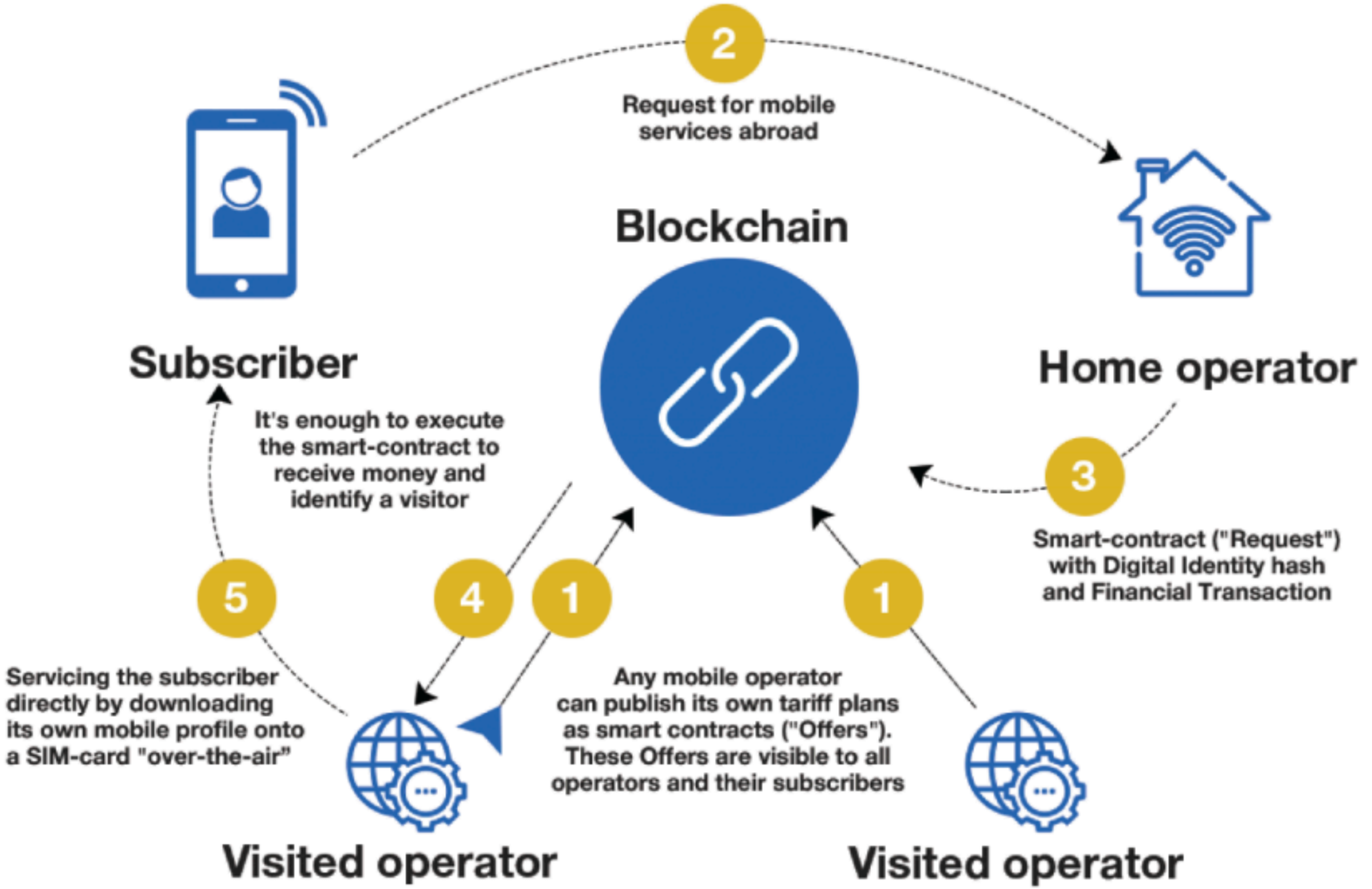
IP moves information, blockchain moves value

share or sell what is leftover on your mobile plan

~$95,000,000 market cap

BUBBLETONE

market making among mobile networks and users
currently at ICO stage


2
Request for mobile services abroad
Blockchain
Subscriber
Home operator
It's enough to execute the smart-contract to receive money and identify a visitor
3
Smart-contract ("Request") with Digital Identity hash and Financial Transaction
5
4
1
1
Servicing the subscriber directly by downloading its own mobile profile onto a SIM-card "over-the-air"
Any mobile operator can publish its own tariff plans as smart contracts ("Offers"). These Offers are visible to all operators and their subscribers
Visited operator
Visited operator

Blockchain ∩ Telephony

RFC 2916, 3761, 6116

ENUM

mapping E.164 to DNS

ENUM

room for improvement?

ENUM

always needed a “higher authority” to record mappings

ENUM

authority downtime leads to outage

EMERCOIN

“distributed blockchain services for business and personal use”

~$140,000,000 market cap

Conditonal transactions

Bitcoin merged mining

Bitcoin Core 14 (SegWit)

Internal

TECH and SOLUTIONS

T-network

Merkle vault

Advertisement
decentrized advertisement network solution

Access and security

Networking

DPO
Digital proof of ownership

DPA

TTS

Help services

Wallets and tools

ENUMER

EMCSSH — Done:basics TODO: «box solution»

EMCSSL — Done:basics TODO: «box solution»

EMCDNS — Done:basics, opennic TODO: Toolset

I2P

Magnet

Infocards

DPO main — Done:basics TODO: advanced docs and tutorials antifake toolset

Anti-fake

IPO — Securities and commodities toolkit

DPA — Done:basics TODO: «box solution» Mobile platform support

TTS — Done:basics TODO: «box solution»

Micropayment lib

Atom

Wallet

Business case

Underway technology or tool

echnology
tool

Existing technology or tool

ENUMER

register your own E.164 to DNS mapping

ENUMER

automatic verification performed via 3rd party service

ENUMER

mappings stored locally in each participant’s copy of the blockchain

Blockchain ∩ Telephony

infrastructure

QLINK

“The world’s first decentralized mobile network.”

~$40,000,000 market cap

QLINK

I've read it. I don't get it.

infrastructure

“Blockchain-Enabled Spectrum Access in Cognitive Radio Networks”

by Khashayar Kotobi and Sven G. Bilén

Blockchain ∩ Telephony

mobile payments

mobile payments

room for improvement?

mobile payments

blockchain was literally invented for payments

mobile payments

carriers and shops now have an open technology to deploy

mobile payments

users can move their assets between carriers and countries

~$30,000,000,000 market cap

12 of top 100 banks participating

Blockchain ∩ Telephony

stolen device database

stolen device database

new devices ship with token or can generate one on first use

stolen device database

transfer token to new owner when sold

stolen device database

“spend” token when stolen

stolen device database

shops, e-bay, police, carriers, etc can all read blockchain contents

Blockchain ∩ Telephony

number portability database

number portability database

fresh DID requires cash deposit, generates token

number portability database

transfer token and fee to smart contract to update DID and token

number portability database

“spend” token to return deposit

Blockchain ∩ Telephony

inter-carrier settlement

inter-carrier settlement

room for improvement?

inter-carrier settlement

untrusted parties

inter-carrier settlement

no trusted higher authority

inter-carrier settlement

enforced by fear of repercussions

inter-carrier settlement

pilot program already entering second year

Blockchain ∩ VPN

decentralized VPN

Intense Coin open source blockchain-backed VPN

market making for VPN connectivity

Intense Coin open source blockchain-backed VPN

faster than TOR

Intense Coin open source blockchain-backed VPN

reward for providing connectivity

Intense Coin open source blockchain-backed VPN

potentially safer than centralized providers

Intense Coin open source blockchain-backed VPN

egalitarian mining

Intense Coin open source blockchain-backed VPN

Current Limitations

transactions per second

Cryptocurrencies Transaction Speeds Compared to Visa & Paypal

Article & Sources:
https://howmuch.net/articles/crypto-transaction-speeds-compared
https://howmuch.net/sources/crypto-transaction-speeds-compared

howmuch.net

only implicit finality

interoperability

3rd party trust required for inter-blockchain transactions

usability

data visibility

centralized governance

Progress on all Fronts

sharding

transactions per second

side-chains

transactions per second

state channels

transactions per second

proof-of-stake

explicit finality

delegated proof-of-stake

explicit finality

atomic cross-chain swaps

interoperability

swapready.net

interoperability

	ABY	BTC	BCH	BLK	DASH	DCR	DOGE	ETH	GRS	LTC	XMR	PART	SYS	VIA	VTC	XZC	ZEC	ERC20
ABY		5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	4 / 8	5 / 8	5 / 8	5 / 8	2 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8
BTC	5 / 8		7 / 8	5 / 8	7 / 8	8 / 8	6 / 8	7 / 8	5 / 8	8 / 8	2 / 8	8 / 8	7 / 8	7 / 8	8 / 8	8 / 8	6 / 8	5 / 8
BCH	5 / 8	7 / 8		5 / 8	7 / 8	7 / 8	6 / 8	5 / 8	5 / 8	7 / 8	2 / 8	7 / 8	7 / 8	7 / 8	7 / 8	5 / 8	5 / 8	5 / 8
BLK	5 / 8	5 / 8	5 / 8		5 / 8	5 / 8	4 / 8	5 / 8	5 / 8	5 / 8	2 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8
DASH	5 / 8	7 / 8	7 / 8	5 / 8		7 / 8	6 / 8	5 / 8	5 / 8	7 / 8	2 / 8	7 / 8	7 / 8	7 / 8	7 / 8	5 / 8	5 / 8	5 / 8
DCR	5 / 8	8 / 8	7 / 8	5 / 8	7 / 8		6 / 8	7 / 8	5 / 8	8 / 8	2 / 8	8 / 8	7 / 8	7 / 8	8 / 8	8 / 8	5 / 8	5 / 8
DOGE	4 / 8	6 / 8	6 / 8	4 / 8	6 / 8	6 / 8		4 / 8	4 / 8	6 / 8	1 / 8	6 / 8	6 / 8	6 / 8	6 / 8	4 / 8	4 / 8	4 / 8
ETH	5 / 8	7 / 8	5 / 8	5 / 8	5 / 8	7 / 8	4 / 8		5 / 8	7 / 8	2 / 8	7 / 8	5 / 8	5 / 8	7 / 8	7 / 8	5 / 8	5 / 8
GRS	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	4 / 8	5 / 8		5 / 8	2 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8
LTC	5 / 8	8 / 8	7 / 8	5 / 8	7 / 8	8 / 8	6 / 8	7 / 8	5 / 8		2 / 8	8 / 8	7 / 8	7 / 8	8 / 8	8 / 8	5 / 8	5 / 8
XMR	2 / 8	2 / 8	2 / 8	2 / 8	2 / 8	2 / 8	1 / 8	2 / 8	2 / 8	2 / 8		2 / 8	2 / 8	2 / 8	2 / 8	2 / 8	2 / 8	2 / 8
PART	5 / 8	8 / 8	7 / 8	5 / 8	7 / 8	8 / 8	6 / 8	7 / 8	5 / 8	8 / 8	2 / 8		7 / 8	7 / 8	8 / 8	8 / 8	5 / 8	5 / 8
SYS	5 / 8	7 / 8	7 / 8	5 / 8	7 / 8	7 / 8	6 / 8	5 / 8	5 / 8	7 / 8	2 / 8	7 / 8		7 / 8	7 / 8	5 / 8	5 / 8	5 / 8
VIA	5 / 8	7 / 8	7 / 8	5 / 8	7 / 8	7 / 8	6 / 8	5 / 8	5 / 8	7 / 8	2 / 8	7 / 8	7 / 8		7 / 8	5 / 8	5 / 8	5 / 8
VTC	5 / 8	8 / 8	7 / 8	5 / 8	7 / 8	8 / 8	6 / 8	7 / 8	5 / 8	8 / 8	2 / 8	8 / 8	7 / 8	7 / 8		8 / 8	5 / 8	5 / 8
XZC	5 / 8	8 / 8	5 / 8	5 / 8	5 / 8	8 / 8	4 / 8	7 / 8	5 / 8	8 / 8	2 / 8	8 / 8	5 / 8	5 / 8	8 / 8		5 / 8	5 / 8
ZEC	5 / 8	6 / 8	5 / 8	5 / 8	5 / 8	5 / 8	4 / 8	5 / 8	5 / 8	5 / 8	2 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8		5 / 8
ERC20	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	4 / 8	5 / 8	5 / 8	5 / 8	2 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8	5 / 8

account recovery

usability

pull payments

usability

view keys

data visibility

Want to take a guess?

centralized governance

breadth first approach

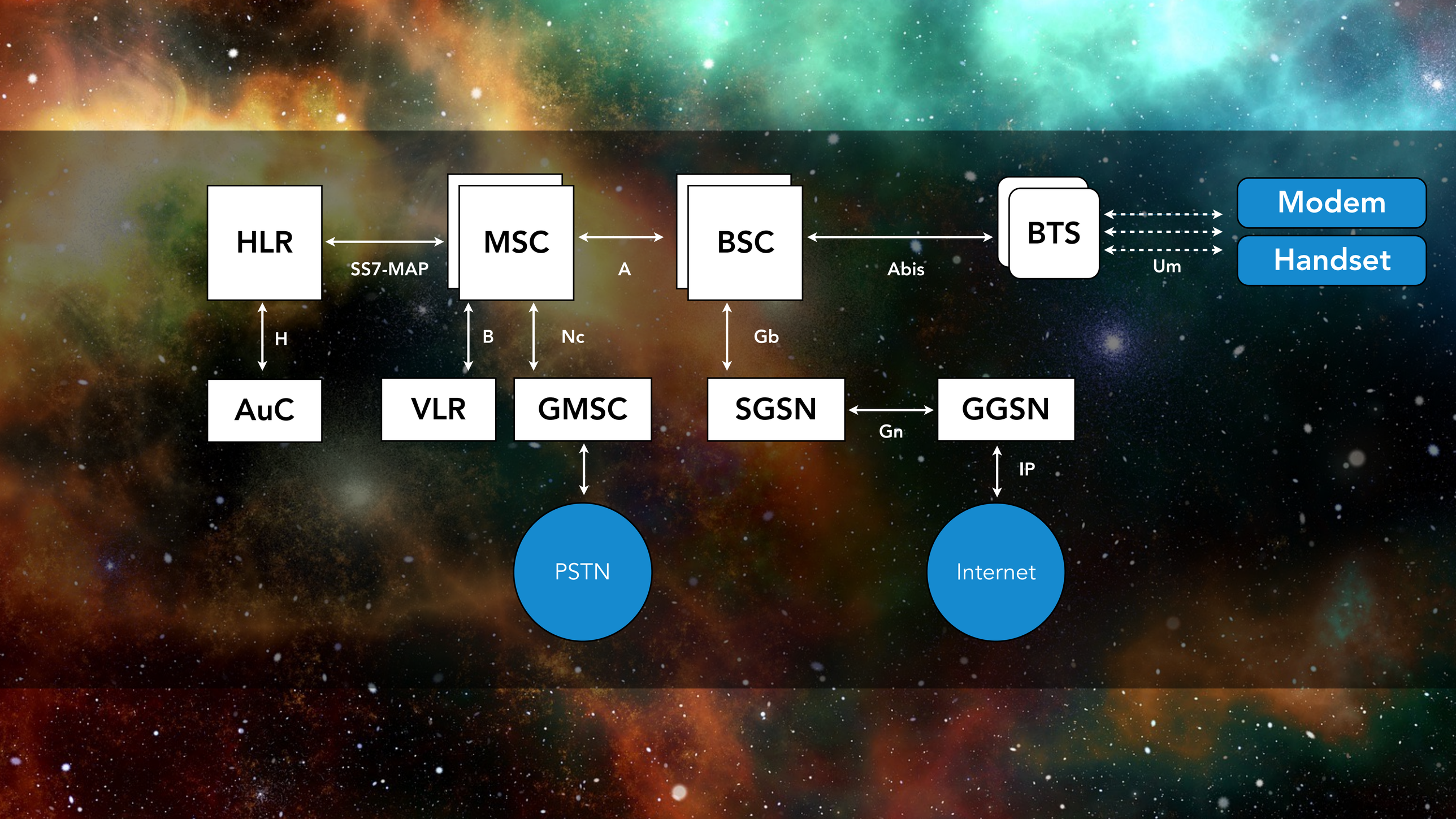
swaps help proof-of-stake

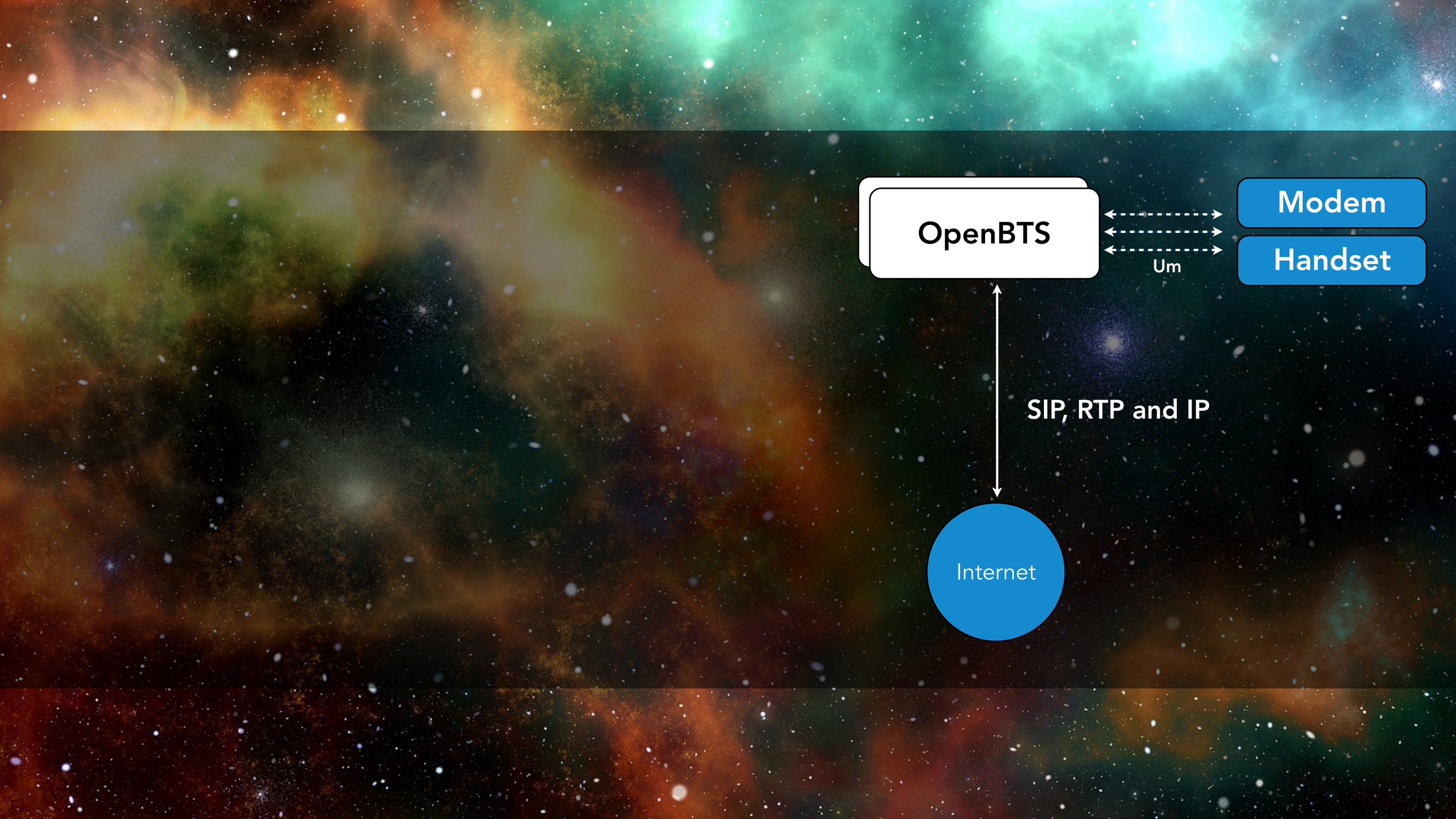
decentralized exchanges ∴ exchanges can’t hold stake power

proof-of-stake helps sharding

explicit finality ∴ multiple chains can be reliably maintained


it’s fun to think outside the box


HLR
SS7-MAP
MSC
A
BSC
Abis
BTS
Um
Modem
Handset
H
B
Nc
Gb
AuC
VLR
GMSC
SGSN
Gn
GGSN
IP
PSTN
Internet

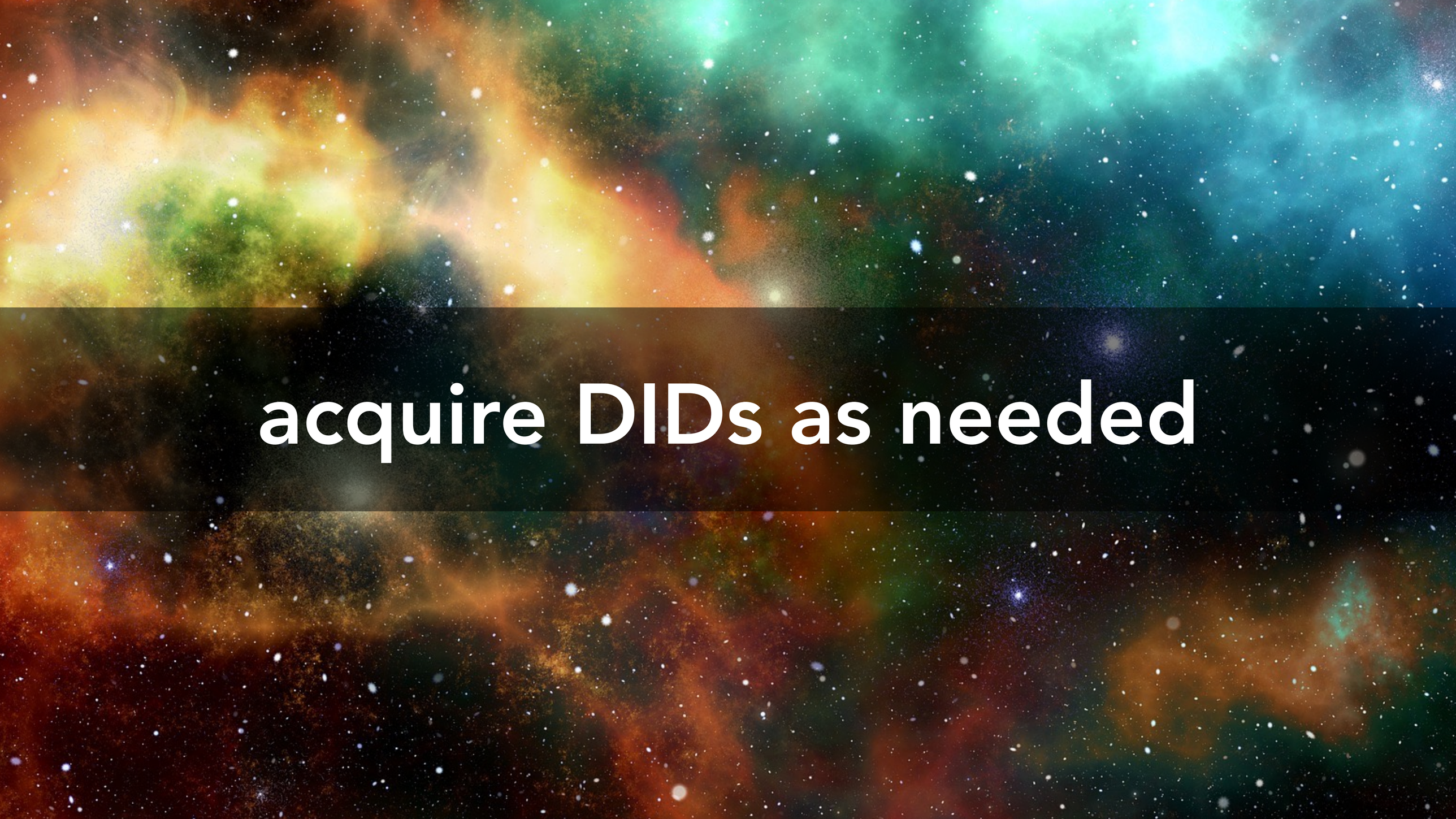

OpenBTS
Um
Modem
Handset
SIP, RTP and IP
Internet


Blockchain ∩ Telephony

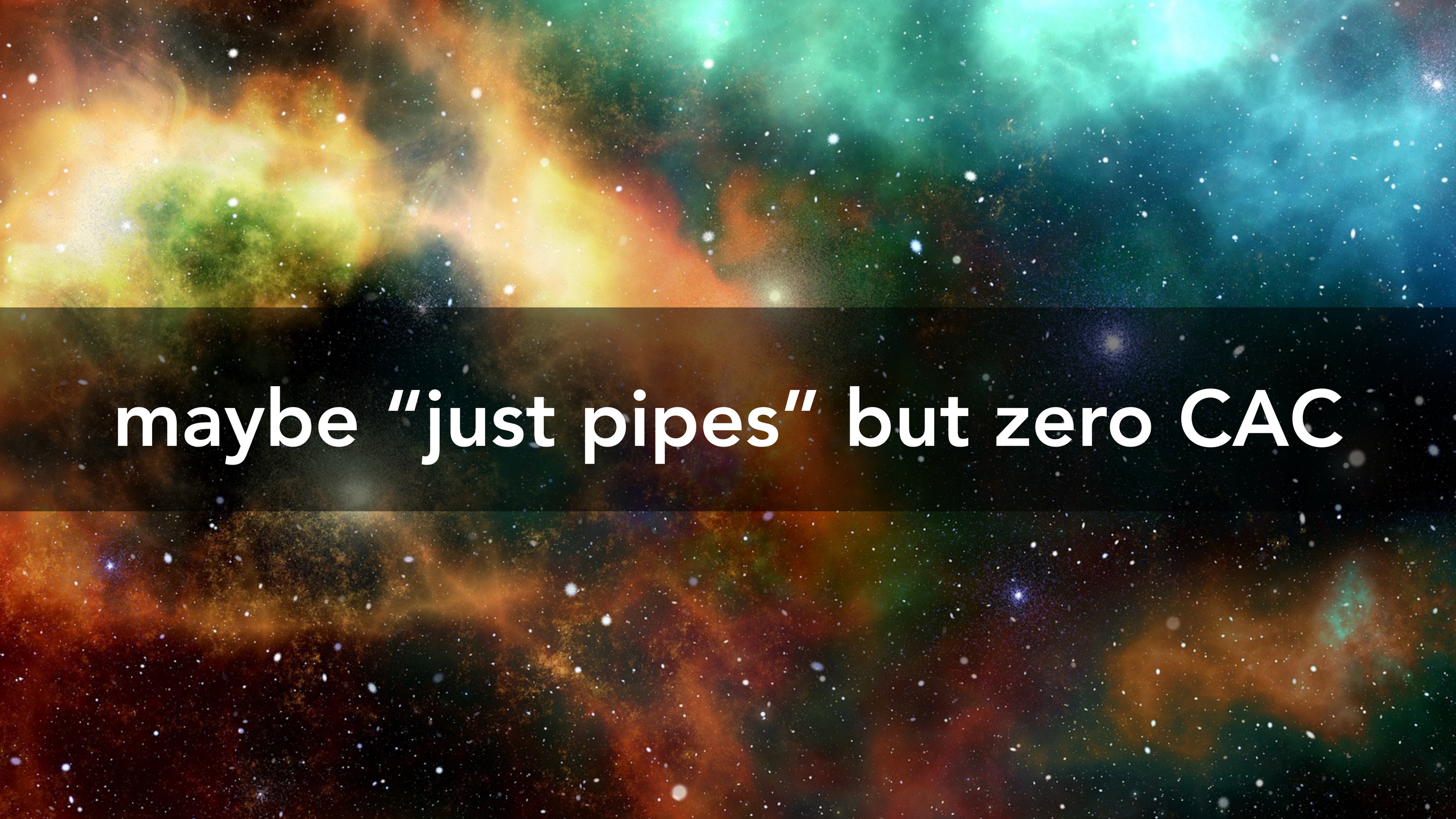

no centralized user accounts

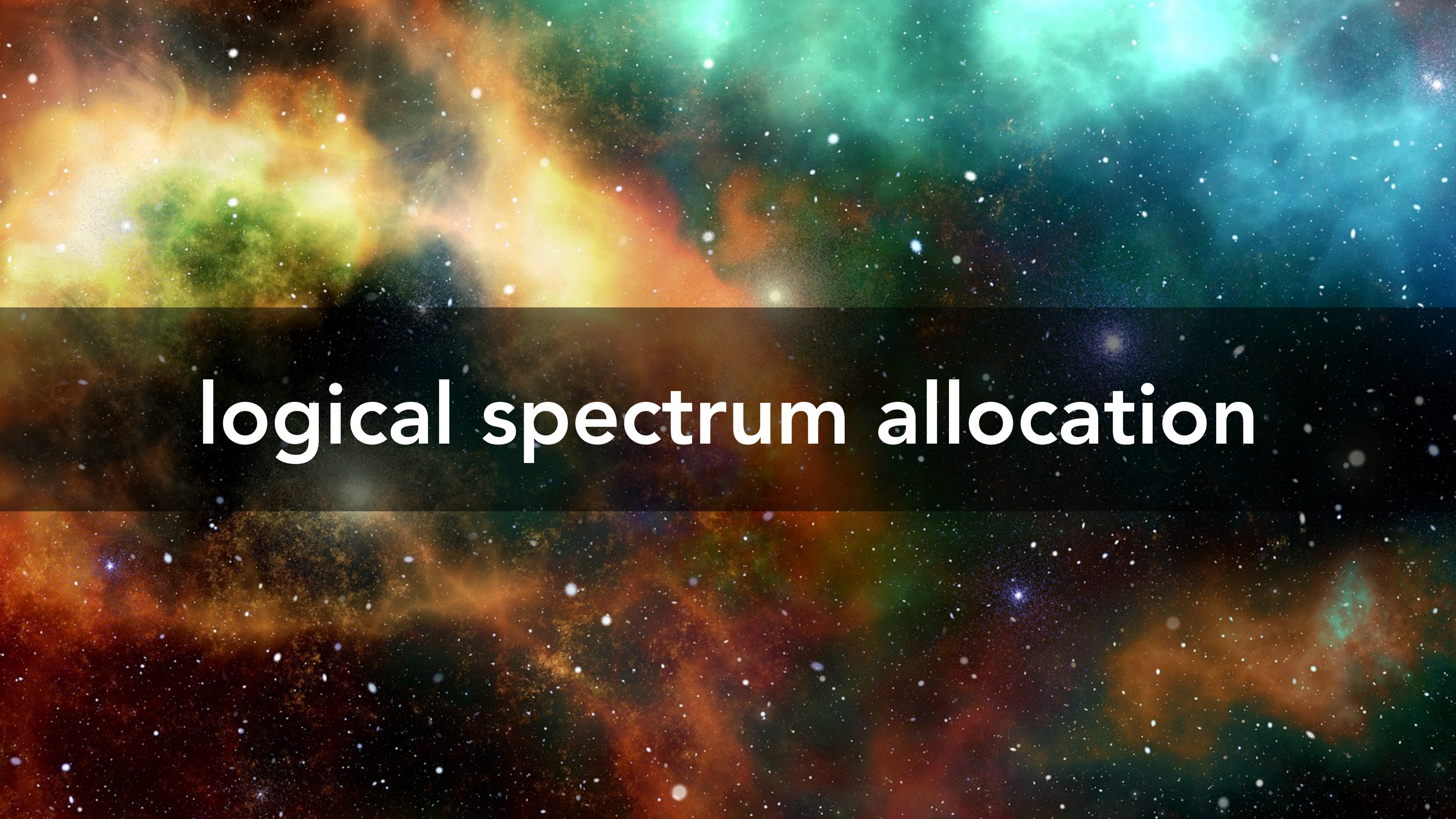

KYC via reputation service


market open to all carriers


acquire DIDs as needed


everyone is always roaming


maybe “just pipes” but zero CAC


logical spectrum allocation


sharing-economy for infra


“bare-metal OTT”

A fast moving target.

“Most people overestimate what they can do in one year and underestimate what they can do in ten years.”

– Bill Gates

Kapsulate R&D
michael@kapsulate.com

@iedemam
iedemam.com/presentations

?'s