Tecnologies disruptives

IGD Tech & Drinks - Setembre 2019

Dario Castañé

- Enginyer informàtic: Engisoft Cloud Services
- Pirates de Catalunya
- Blockchain Catalunya
- Fundació Inceptum
- Divulgador

Xerrades

- **2014:** Techno Politics
- **2014-...:** Tallers de defensa digital personal
- **2016:** Municipi i tecnologia: On som i futurs possibles
- **2018-...:** IGD Tech & Drinks: Blockchain, contenidors, etc.
- **2019:** Espiadas y vendidas
- **2019:** Estònia estat digital. Realitat o ficció?
- Més a dario.im

</falca>

Què entenem per disruptiu?

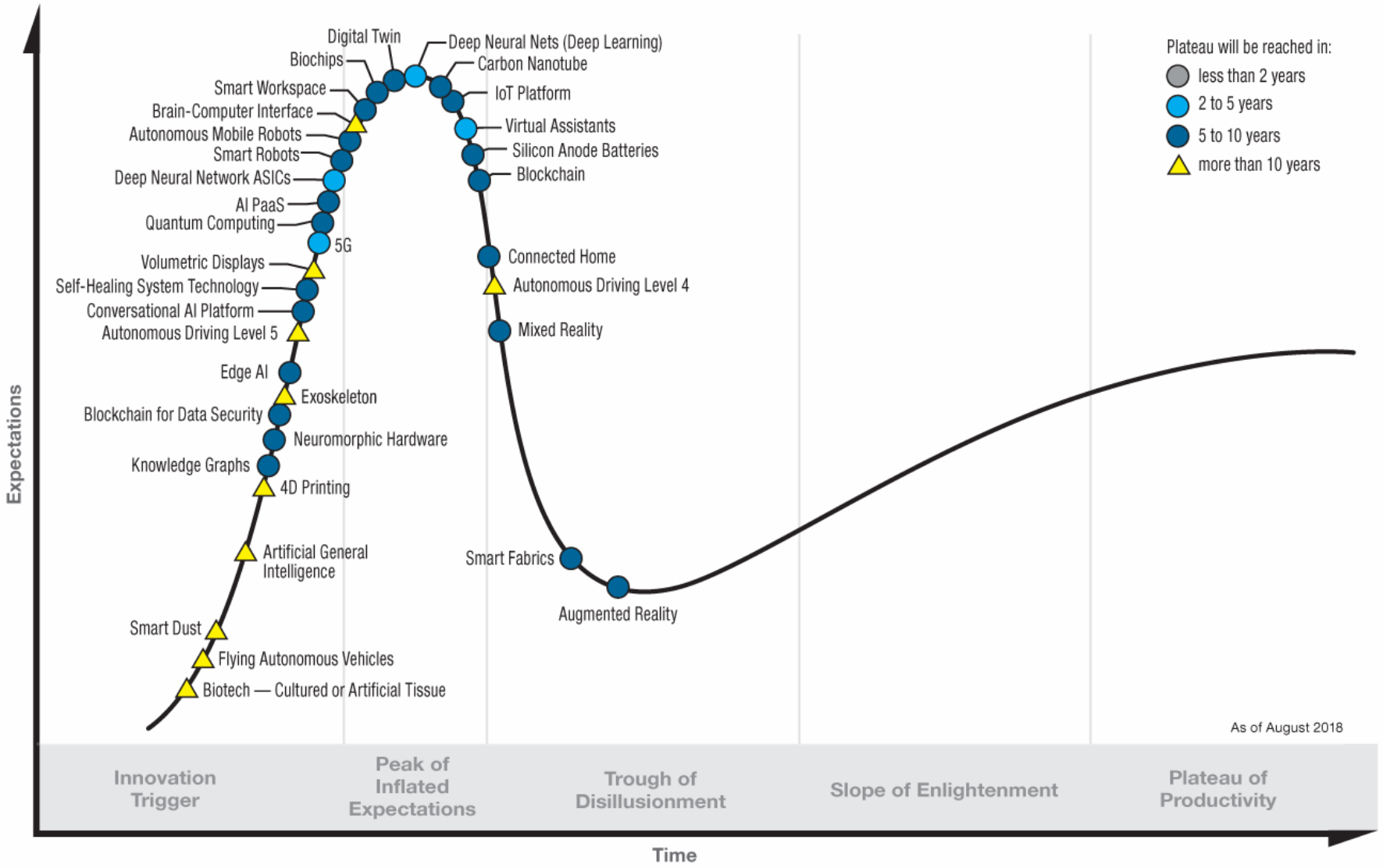
- Innovació que genera nous mercats
- Que irromp en els ja establerts
- No necessàriament és radicalment nova: evolució

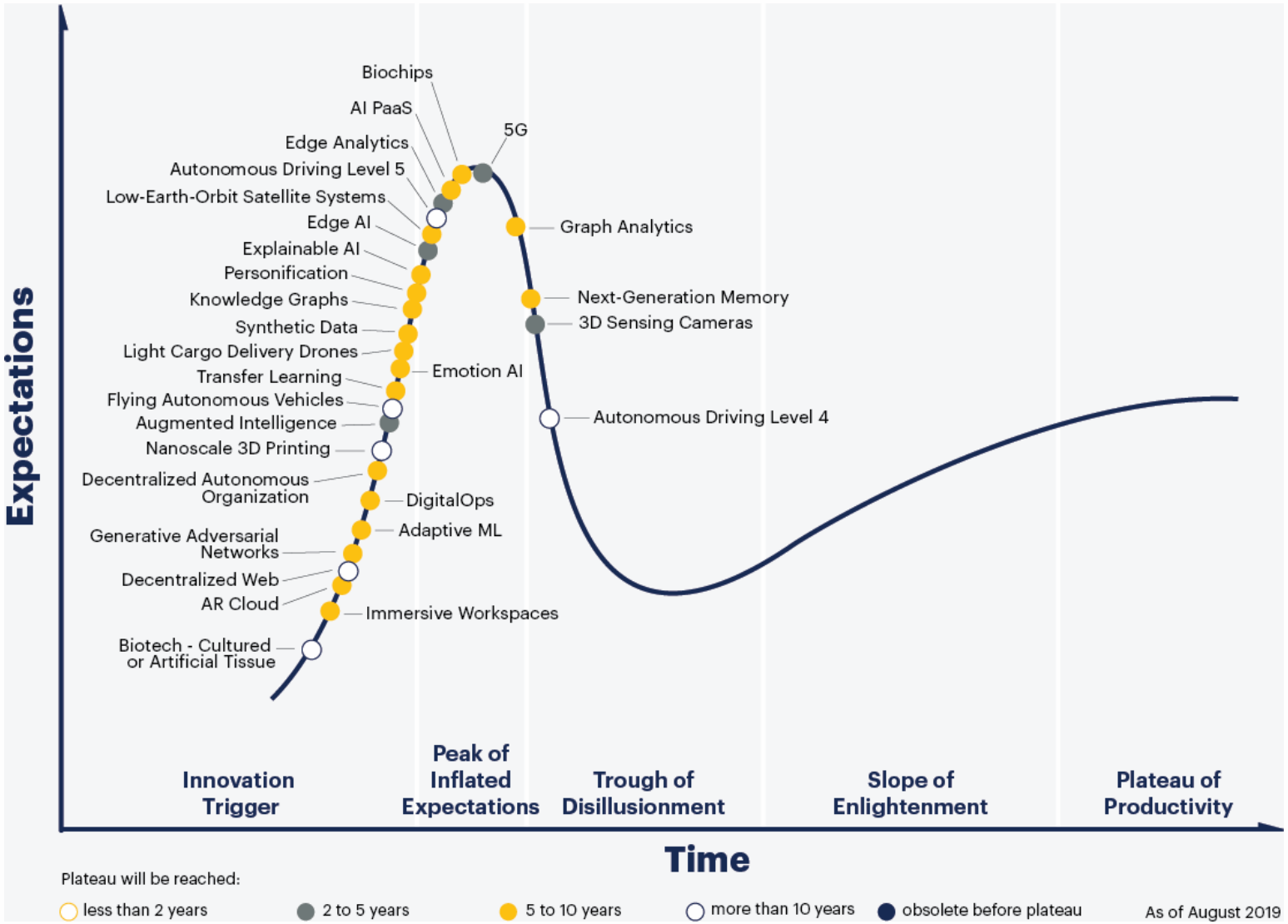
Exemples

- **Cotxe:** carruatges de tracció animal
- **PC:** màquina d'escriure i formes de comunicació
- **Smartphone:** PDAs, càmares, reproductors, etc.

Hype cycle

O cicle de sobreexpectació


Digital Twin
Deep Neural Nets (Deep Learning)
Biochips
Carbon Nanotube
Smart Workspace
IoT Platform
Brain-Computer Interface
Virtual Assistants
Autonomous Mobile Robots
Silicon Anode Batteries
Smart Robots
Blockchain
Deep Neural Network ASICs
AI PaaS
Quantum Computing
5G
Connected Home
Volumetric Displays
Autonomous Driving Level 4
Self-Healing System Technology
Conversational AI Platform
Mixed Reality
Autonomous Driving Level 5
Edge AI
Exoskeleton
Blockchain for Data Security
Neuromorphic Hardware
Knowledge Graphs
4D Printing
Artificial General Intelligence
Smart Fabrics
Augmented Reality
Smart Dust
Flying Autonomous Vehicles
Biotech — Cultured or Artificial Tissue
Plateau will be reached in:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
As of August 2018
Expectations
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
Time


Expectations
Biochips
AI PaaS
Edge Analytics
Autonomous Driving Level 5
Low-Earth-Orbit Satellite Systems
Edge AI
Explainable AI
Personification
Knowledge Graphs
Synthetic Data
Light Cargo Delivery Drones
Transfer Learning
Flying Autonomous Vehicles
Augmented Intelligence
Nanoscale 3D Printing
Decentralized Autonomous Organization
Generative Adversarial Networks
Decentralized Web
AR Cloud
Biotech - Cultured or Artificial Tissue
5G
Graph Analytics
Next-Generation Memory
3D Sensing Cameras
Emotion AI
Autonomous Driving Level 4
DigitalOps
Adaptive ML
Immersive Workspaces
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
Time
Plateau will be reached:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau
As of August 2019

zk-SNARKs

Què són?

- Tècnica criptogràfica
- Proves de coneixement zero (Zero Knowledge)
- Permet que algú demostri a altri que quelcom és cert, sense revelar informació

representation of $x_i \in \mathbb{F}_p$ is the i-th block of $\lceil \log p \rceil$ bits in s (padded with 0's if needed). We extend the notation $[\![s]\!]_p^m$ to binary strings $s \in \{0,1\}^n$ with $n < m$ bits via padding: $[\![s]\!]_p^m := [\![s0^{m-n}]\!]_p^m$.

2.3 Quadratic arithmetic programs

Our zk-SNARK leverages *quadratic arithmetic programs* (QAPs), introduced by Gennaro et al. [GGPR13].

Definition 2.2. *A* **quadratic arithmetic program** *of size m and degree d over $\mathbb{F}$ is a tuple $(\vec{A}, \vec{B}, \vec{C}, Z)$, where $\vec{A}, \vec{B}, \vec{C}$ are three vectors, each of $m+1$ polynomials in $\mathbb{F}^{\leq d-1}[z]$, and $Z \in \mathbb{F}[z]$ has degree exactly d.*

Like a circuit, a QAP induces a satisfaction problem:

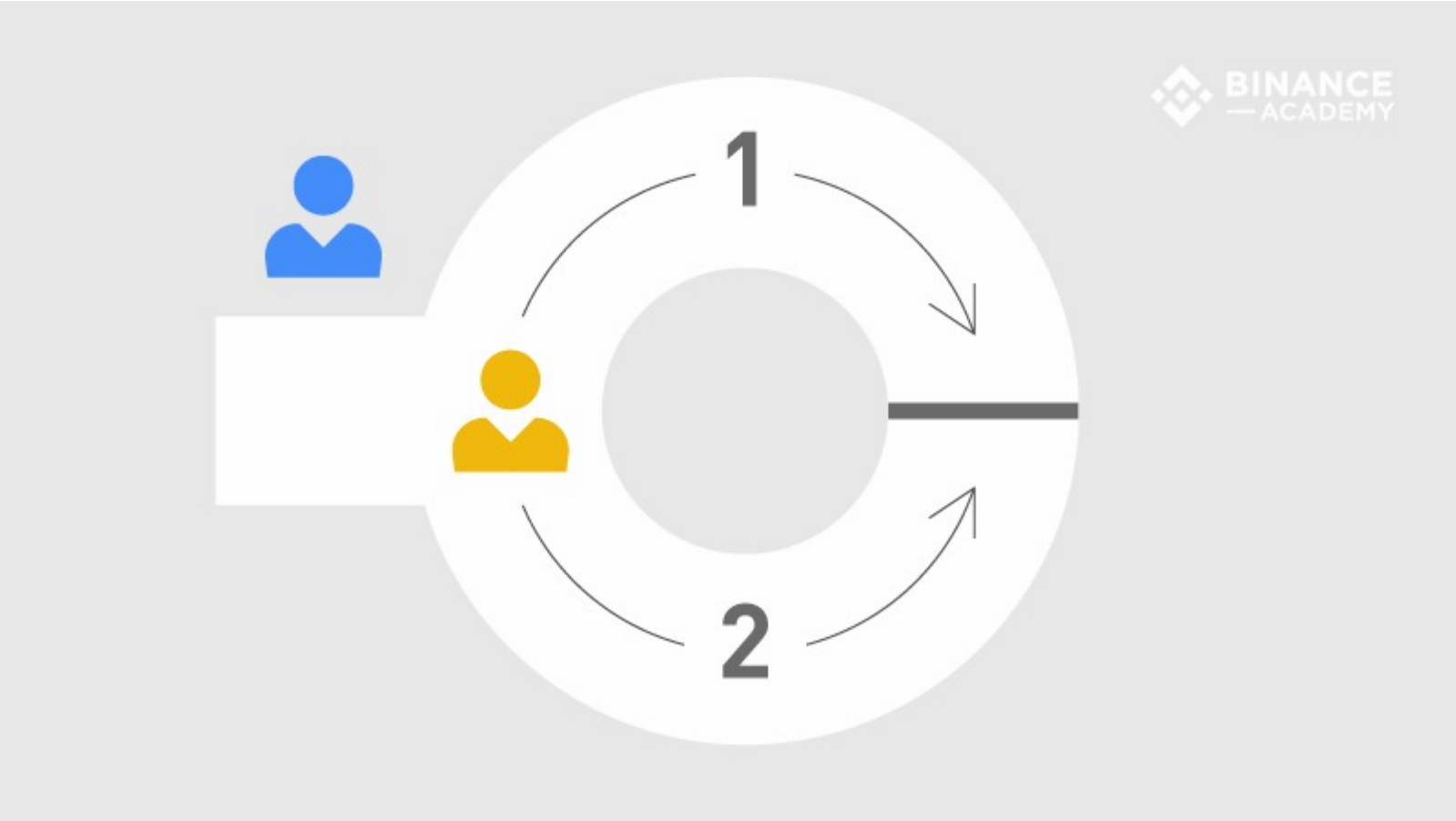
Definition 2.3. *The* **satisfaction problem** *of a size-m QAP $(\vec{A}, \vec{B}, \vec{C}, Z)$ is the relation $\mathcal{R}_{(\vec{A},\vec{B},\vec{C},Z)}$ of pairs $(\vec{x}, \vec{s})$ such that (i) $\vec{x} \in \mathbb{F}^n$, $\vec{s} \in \mathbb{F}^m$, and $n \leq m$; (ii) $x_i = s_i$ for $i \in [n]$ (i.e., $\vec{s}$ extends $\vec{x}$); and (iii) the polynomial $Z(z)$ divides the following one:*

$$(A_0(z) + \sum_{i=1}^m s_i A_i(z)) \cdot (B_0(z) + \sum_{i=1}^m s_i B_i(z)) - (C_0(z) + \sum_{i=1}^m s_i C_i(z)) \,.$$

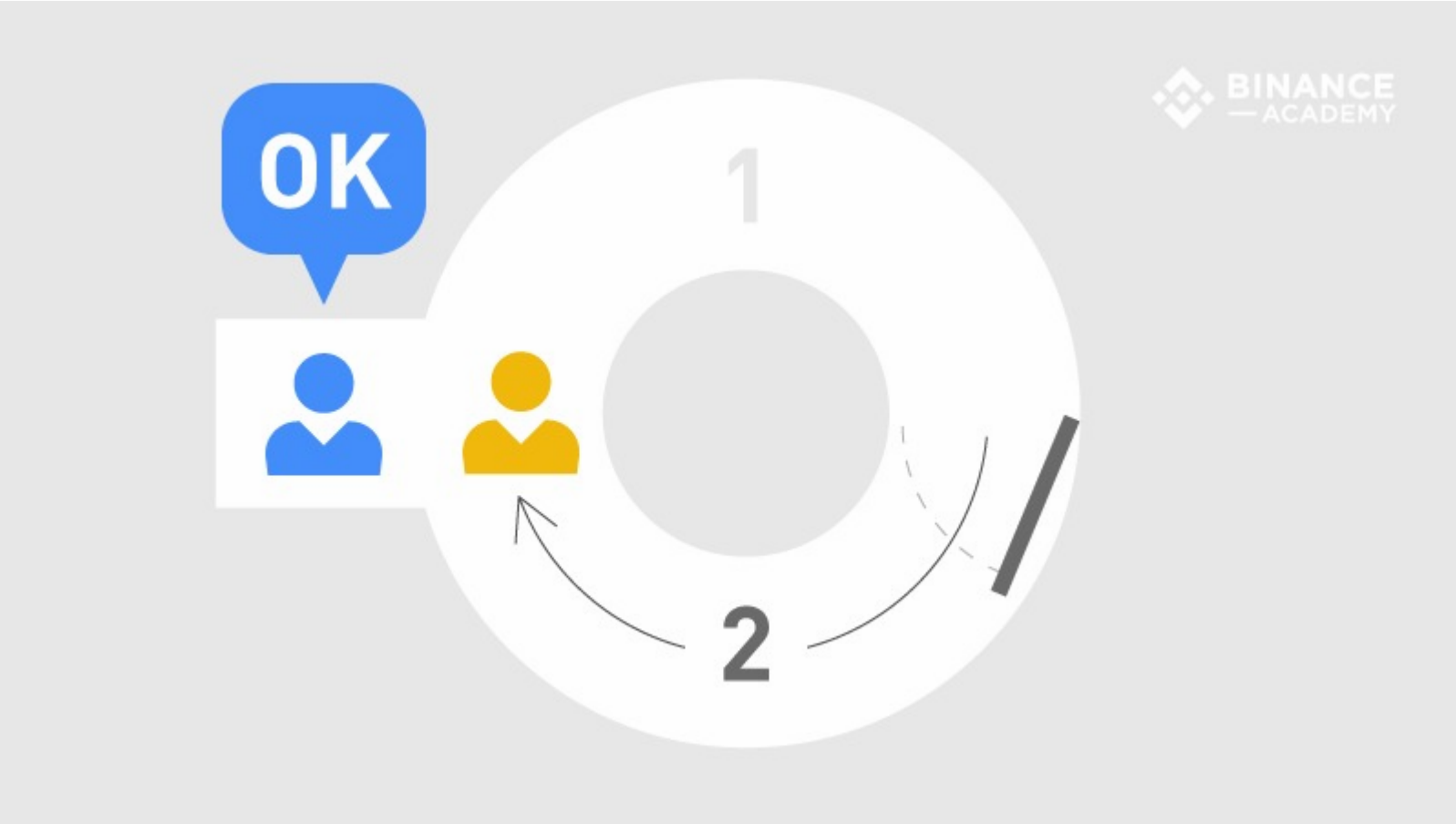
We denote by $\mathcal{L}_{(\vec{A},\vec{B},\vec{C},Z)}$ the language of $\mathcal{R}_{(\vec{A},\vec{B},\vec{C},Z)}$.

Gennaro et al. [GGPR13] showed that circuit satisfiability can be efficiently reduced to QAP satisfiability (which can then be proved and verified using zk-SNARKs):

Lemma 2.4. *There exist two polynomial-time algorithms* QAPinst, QAPwit *that work as follows. For any*


BINANCE
ACADEMY
1
2


BINANCE
ACADEMY
2!
1
2


BINANCE
ACADEMY
OK
1
2

Quina utilitat tenen?

- Identitats sobiranes: IdentiCAT
- Votació electrònica: Vocdoni
- Transaccions econòmiques: Zcash

Per què és disruptiva?

- Desintermediació
- Sobirania de dades personals

Deep fakes

Què són?

- Aplicació pràctica del deep learning


Bill Hader channels Tom Cruise [DeepFake]
Ver más tarde
Compartir

Per què és disruptiva?

- Impacte social: fake news
- Industria cinematogràfica

APM?

Gràcies!

- i@dario.im
- @im_dario
- github.com/imdario
- @dario@mastodon.social
- keybase.io/dario