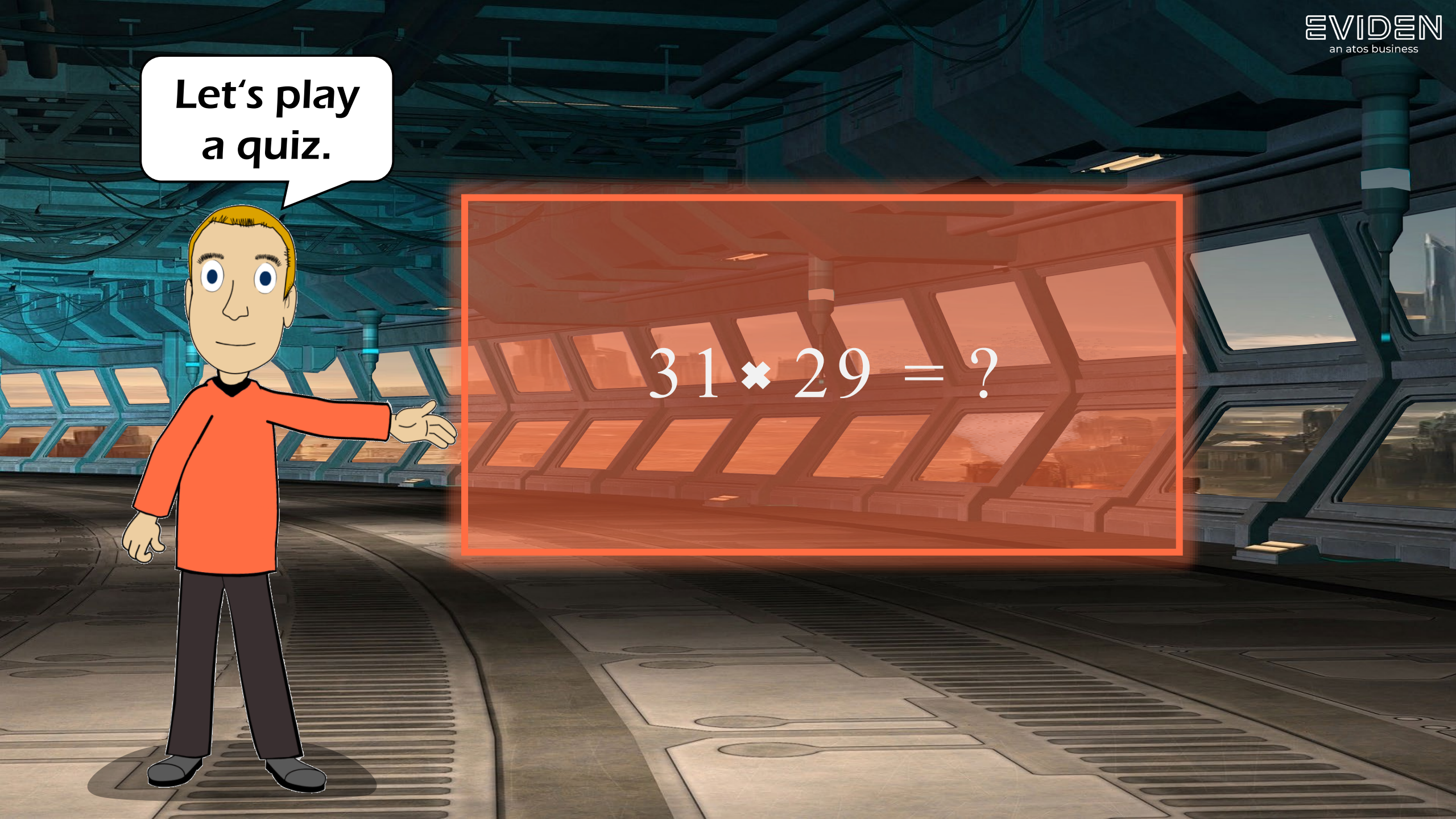
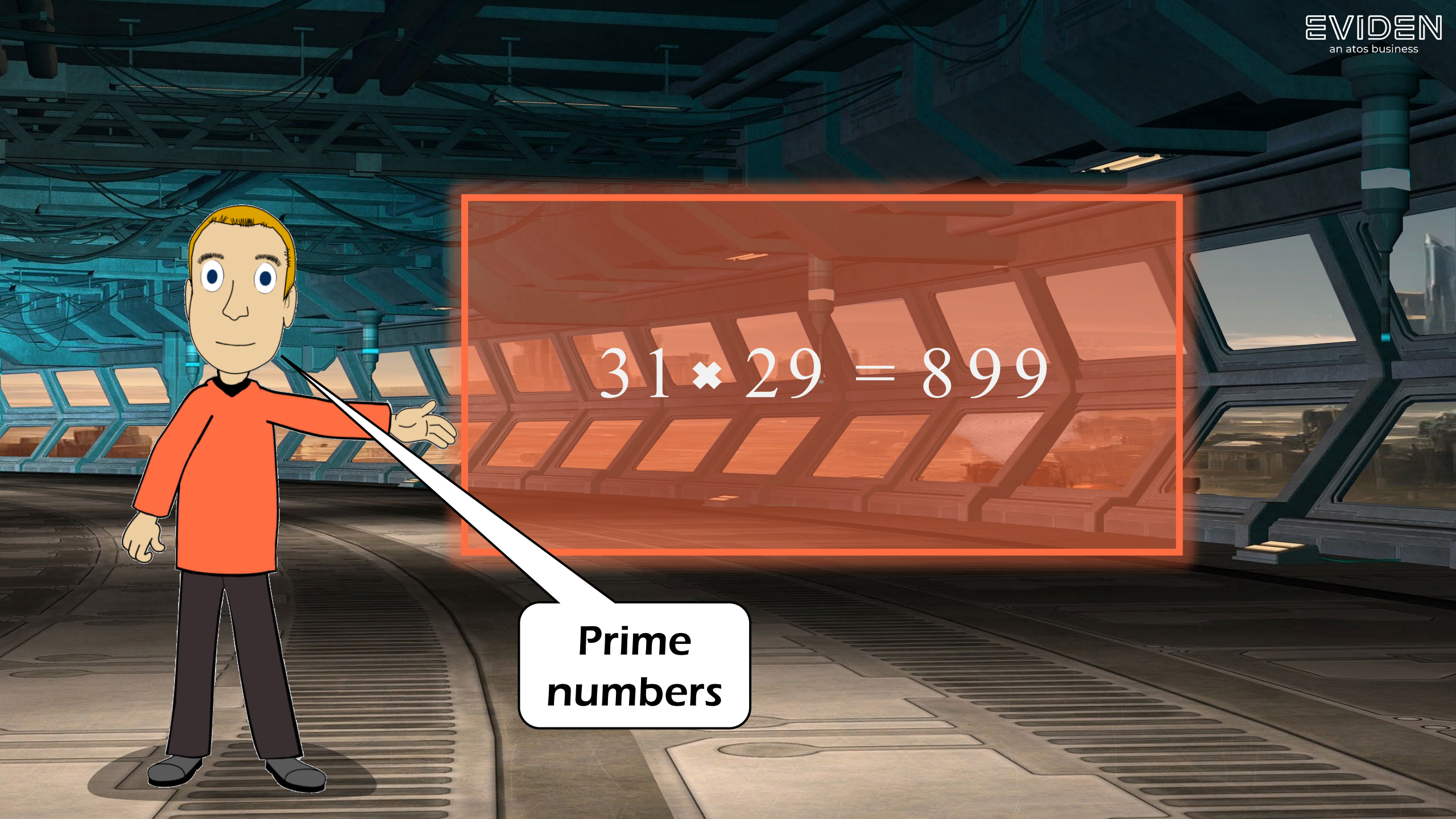
EVIDEN
an atos business

Post-Quantum Tutorial

Klaus Schmeh
Eviden


Let's play a quiz.
31 × 29 = ?


EVIDEN
an atos business
31 × 29 = 899
Prime numbers


Another quiz!
? ✖ ? = 851


37 × 23 = 851

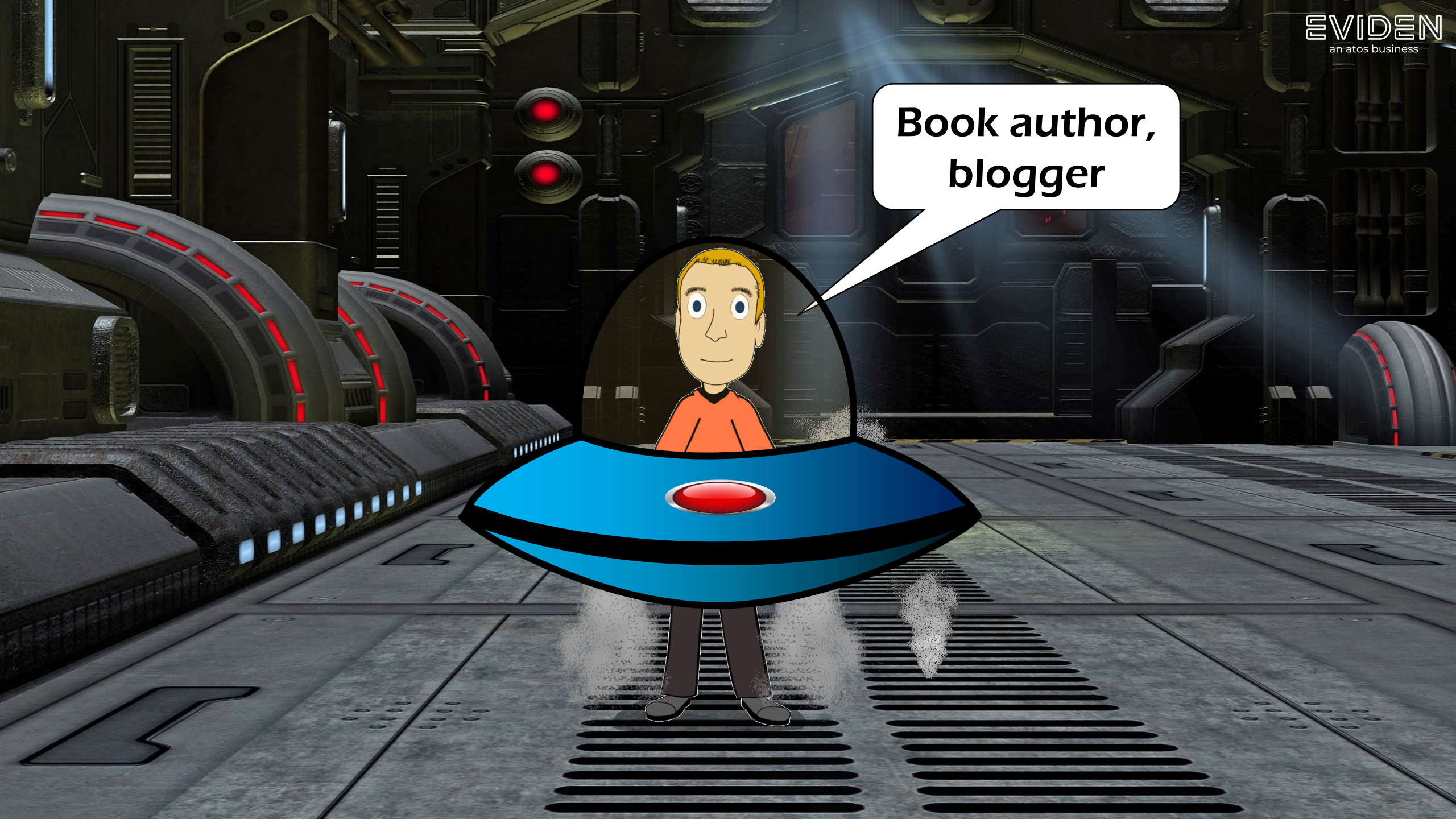

Multiplying two prime numbers is much easier than the reverse operation.


A third quiz!
? × ? = 1230186684530117755130 49
4958384962720772853569595334792
19732245215172640050726365751 87
4520219978646938995647494277406
384592519255732630345373154 8268
5079170261221429134616704292143
1160222124047927473779408066535
14 19597459856902143413
3347807169895689878604416984821269081 77
0479498371376856891243138898288379387 80
76147116525317430877378144679994 89
043666799590428244633799627952632 2
643430876426760322838157396665112 79
3734 17143396810270092798736308917
Current world record in factorizing: 232 digits or 768 bits

Multiplying prime numbers is easier than factorizing.

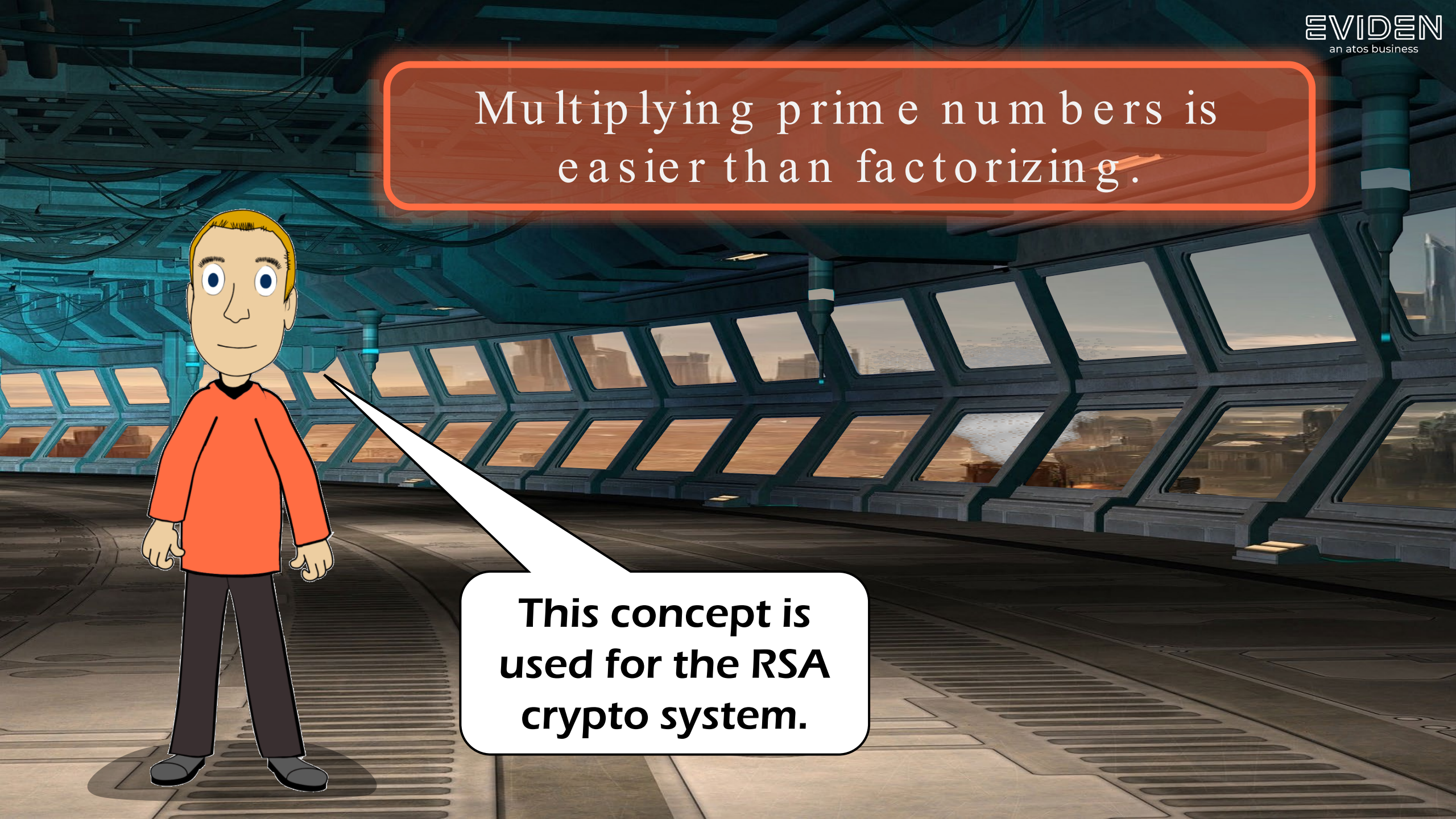
Even the best computer needs billions of years to factorize a 2048-bit number.


Klaus Schmeh, Marketing Editor at Eviden.


Book author, blogger

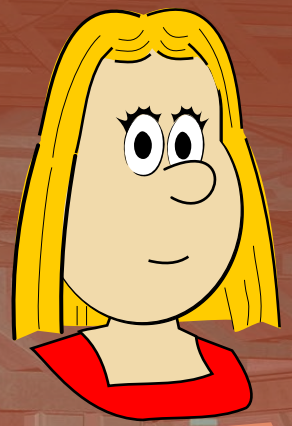
EVIDEN
an atos business

Multiplying prime numbers is easier than factorizing.



This concept is used for the RSA crypto system.

RSA Encryption



Alice

$$17 \cdot 23 = 391$$

Alice's private key for decryption

Alice's public key for encryption

Public key can easily be computed from private key, but not the other way around

Public key factorized => encryption is broken

In practice, public key has length of 700 digits

EVIDEN
an atos business

RSA is used almost everywhere.

Where is RSA used?

Smartphone

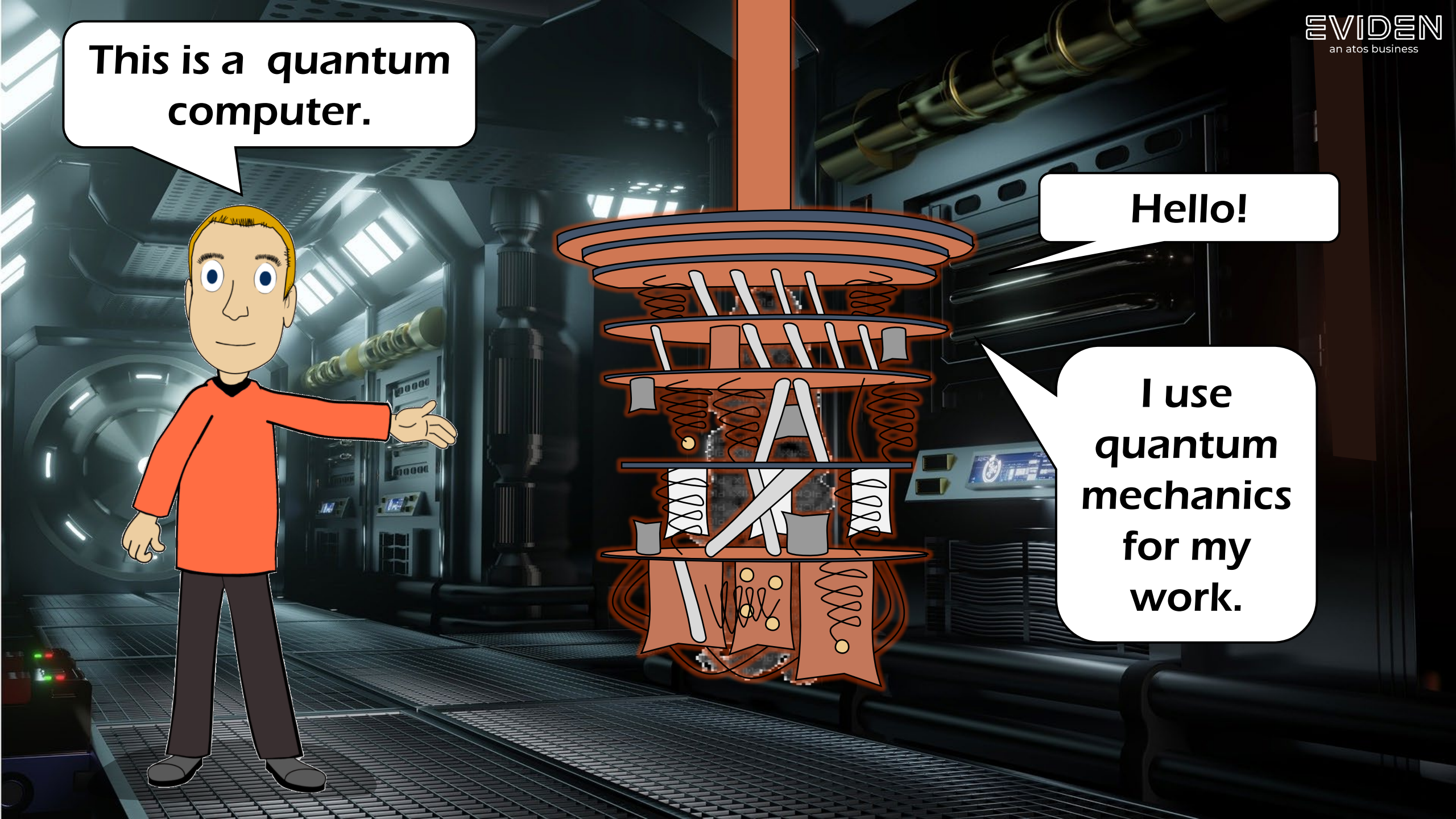
Web browser

Operating system

ATM

Email client

Not only for encryption, but also for signing.

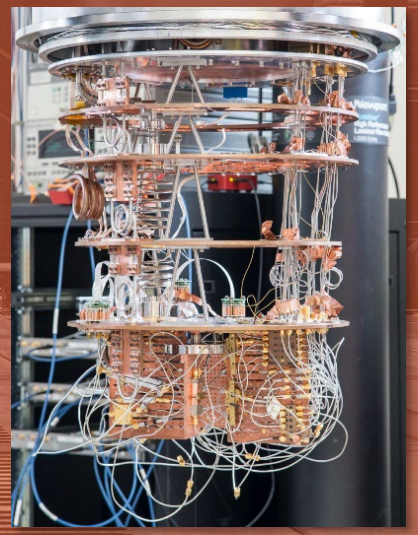

This is a quantum computer.
Hello!
I use quantum mechanics for my work.

Schrödinger‘s cat

Simultaneously
dead and alive

Until you look at it

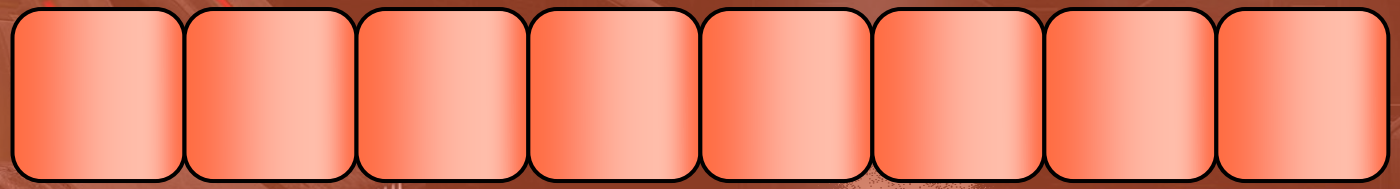
Quantum bit



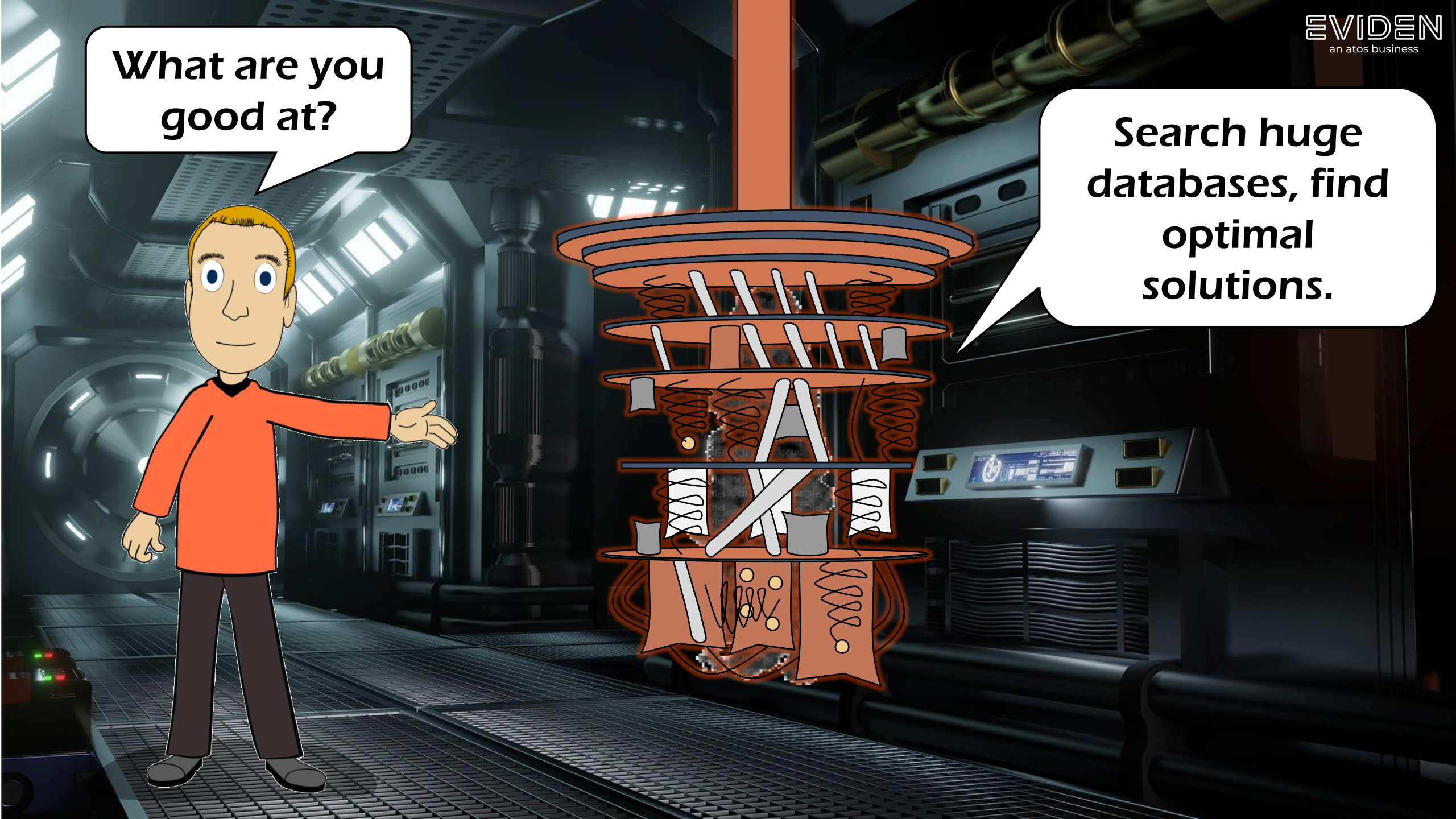
Simultaneously
0 and 1

Until you read it

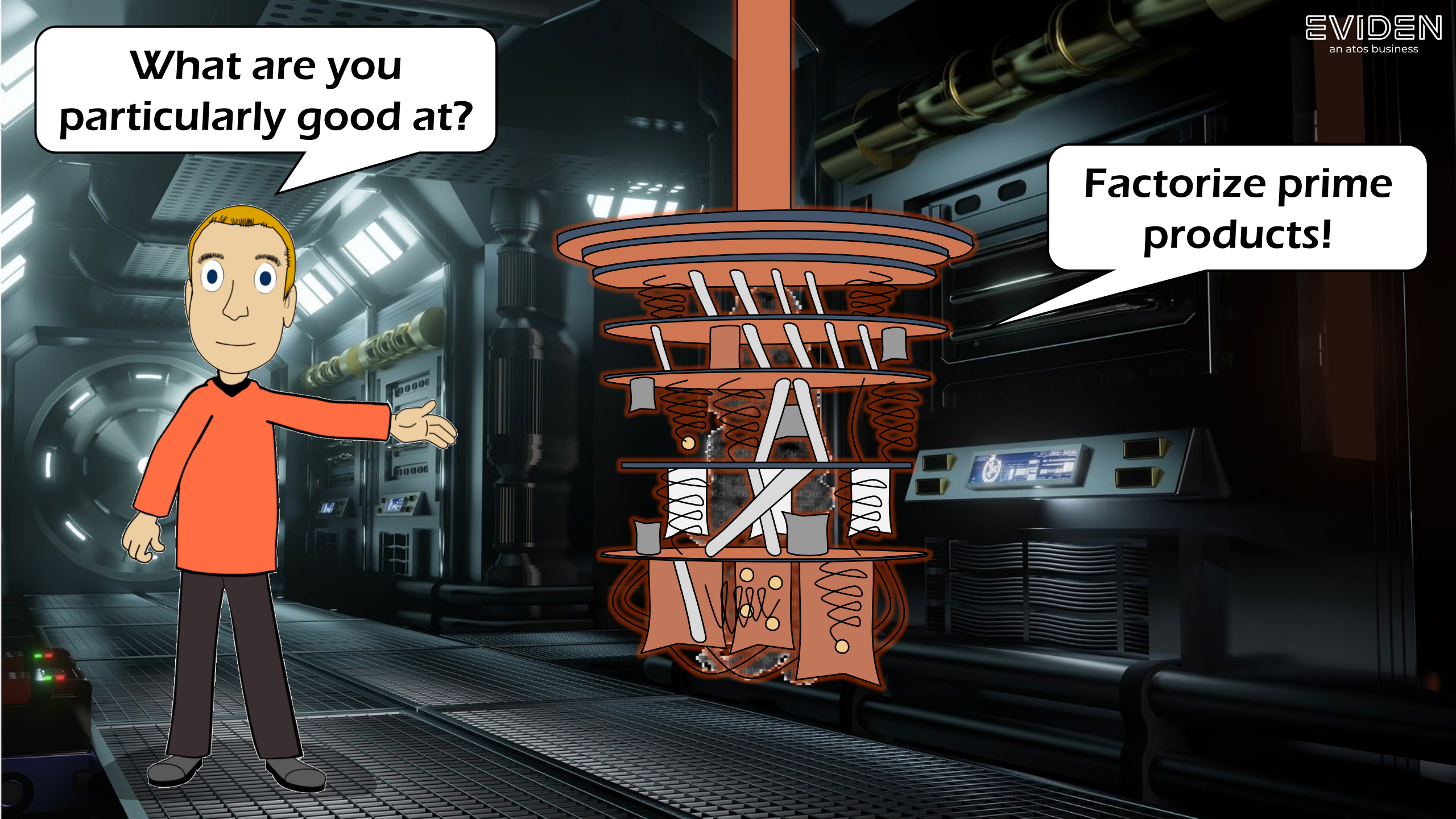
8 quantum bits

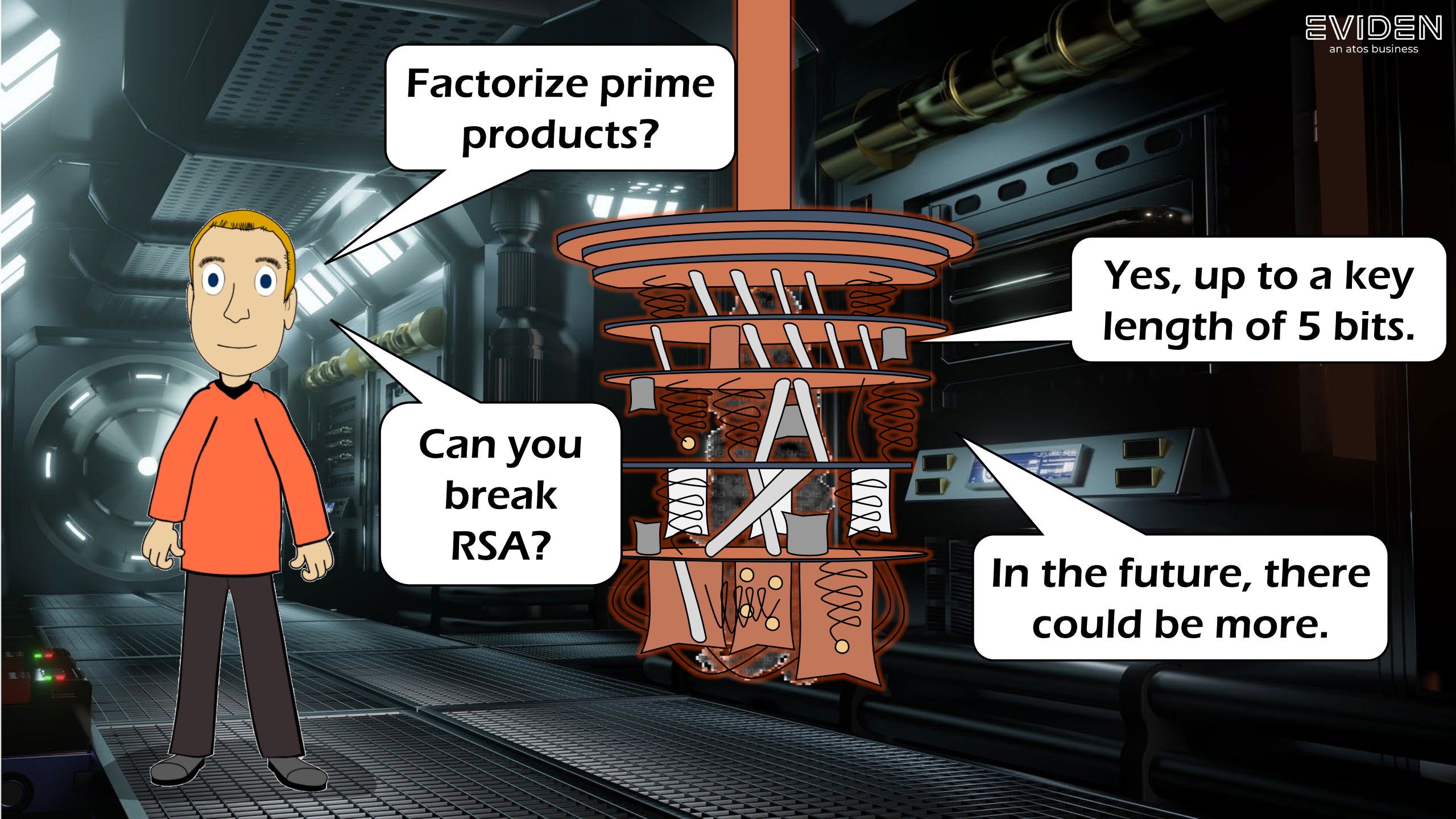


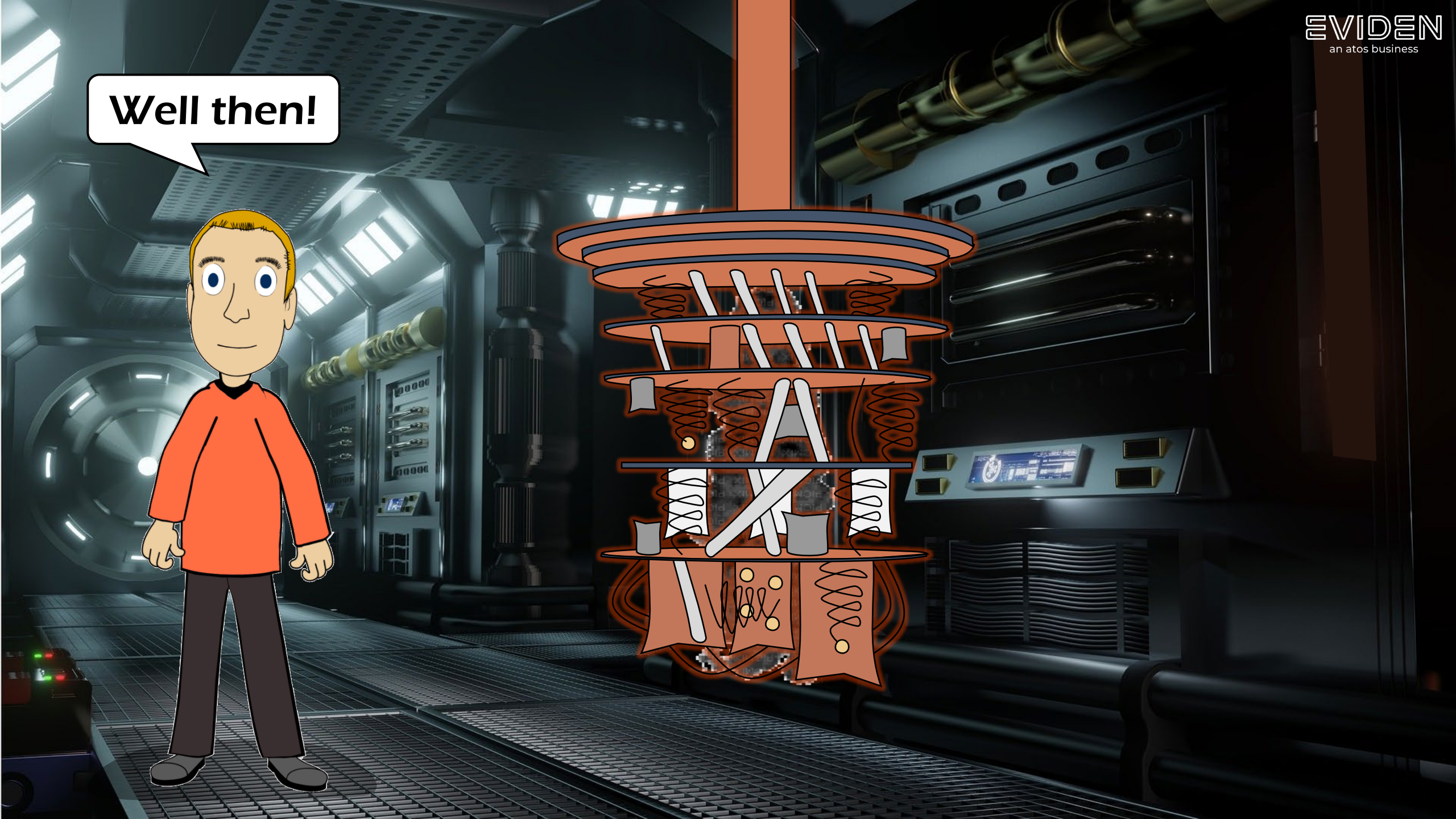
256 computations in
parallel, only one result


What are you good at?
Search huge databases, find optimal solutions.


What are you not good at?
Tasks that do not involve a single solution, such as sorting.


What are you particularly good at?
Factorize prime products!


Factorize prime products?
Can you break RSA?
Yes, up to a key length of 5 bits.
In the future, there could be more.


Well then!

EVIDEN
an atos business

Where is RSA used?

Smartphone

Web browser

Operating system

ATM

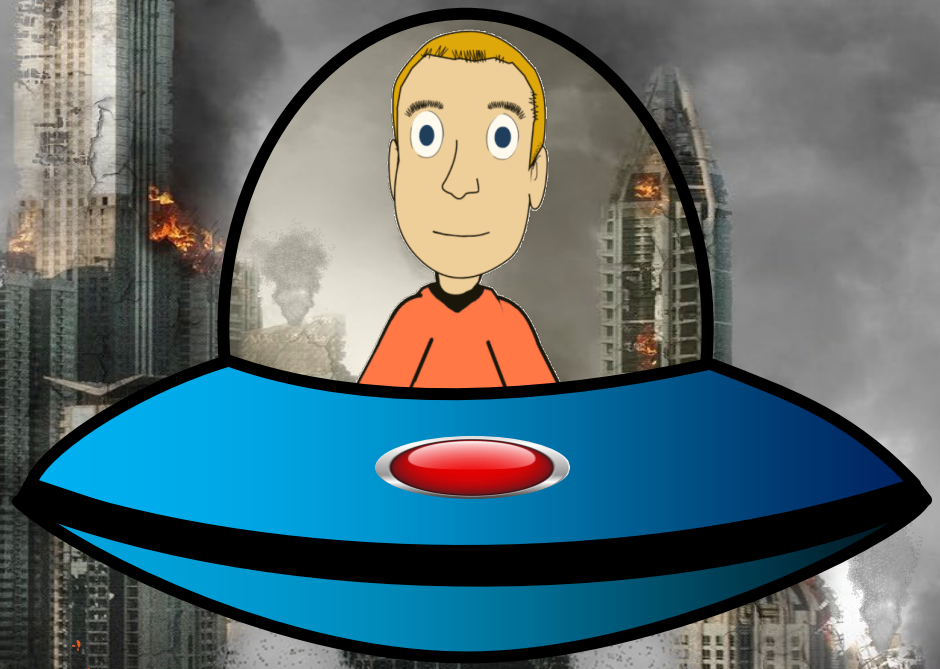
Email client

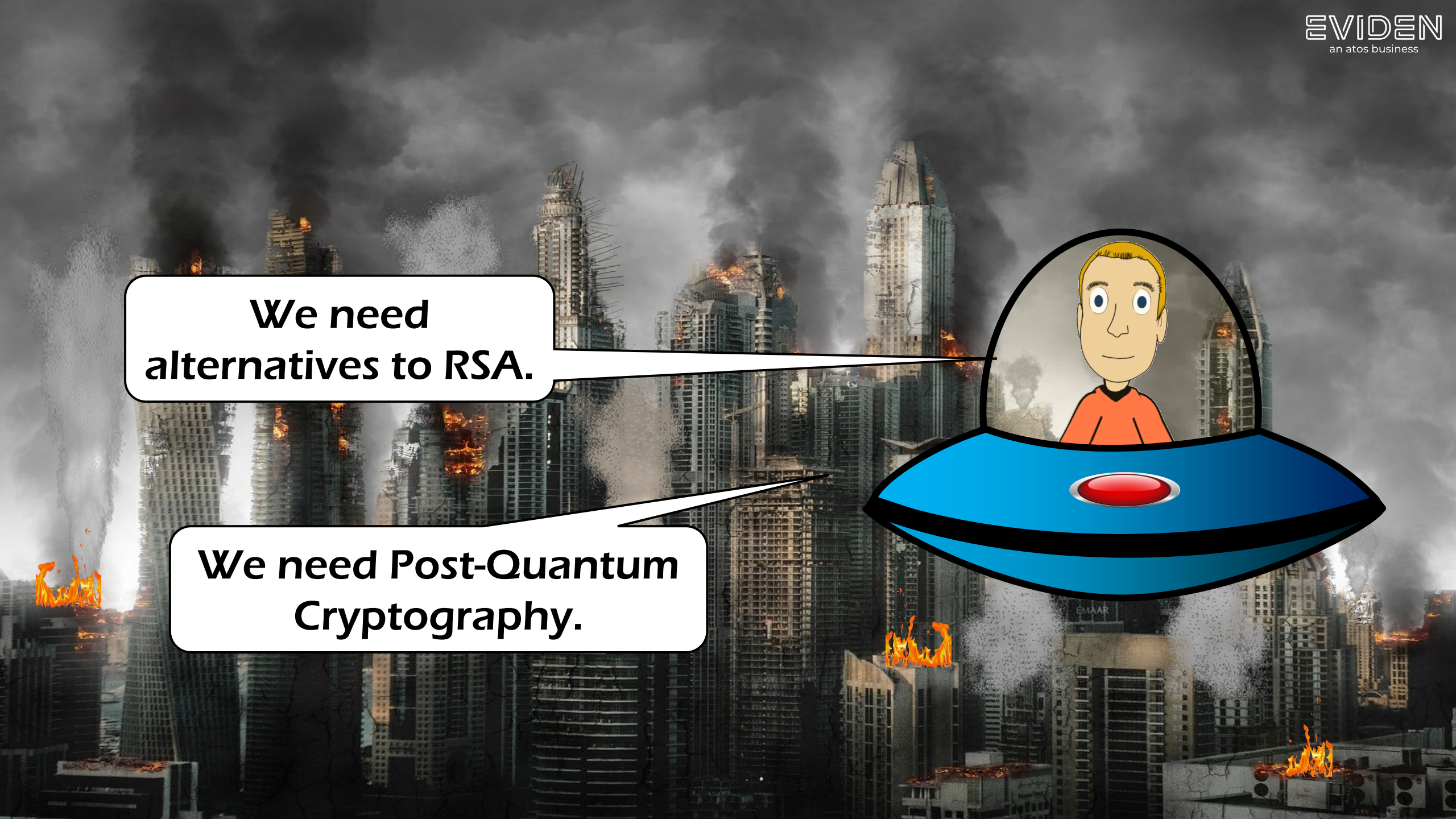

A disaster threatens!
EMAAR

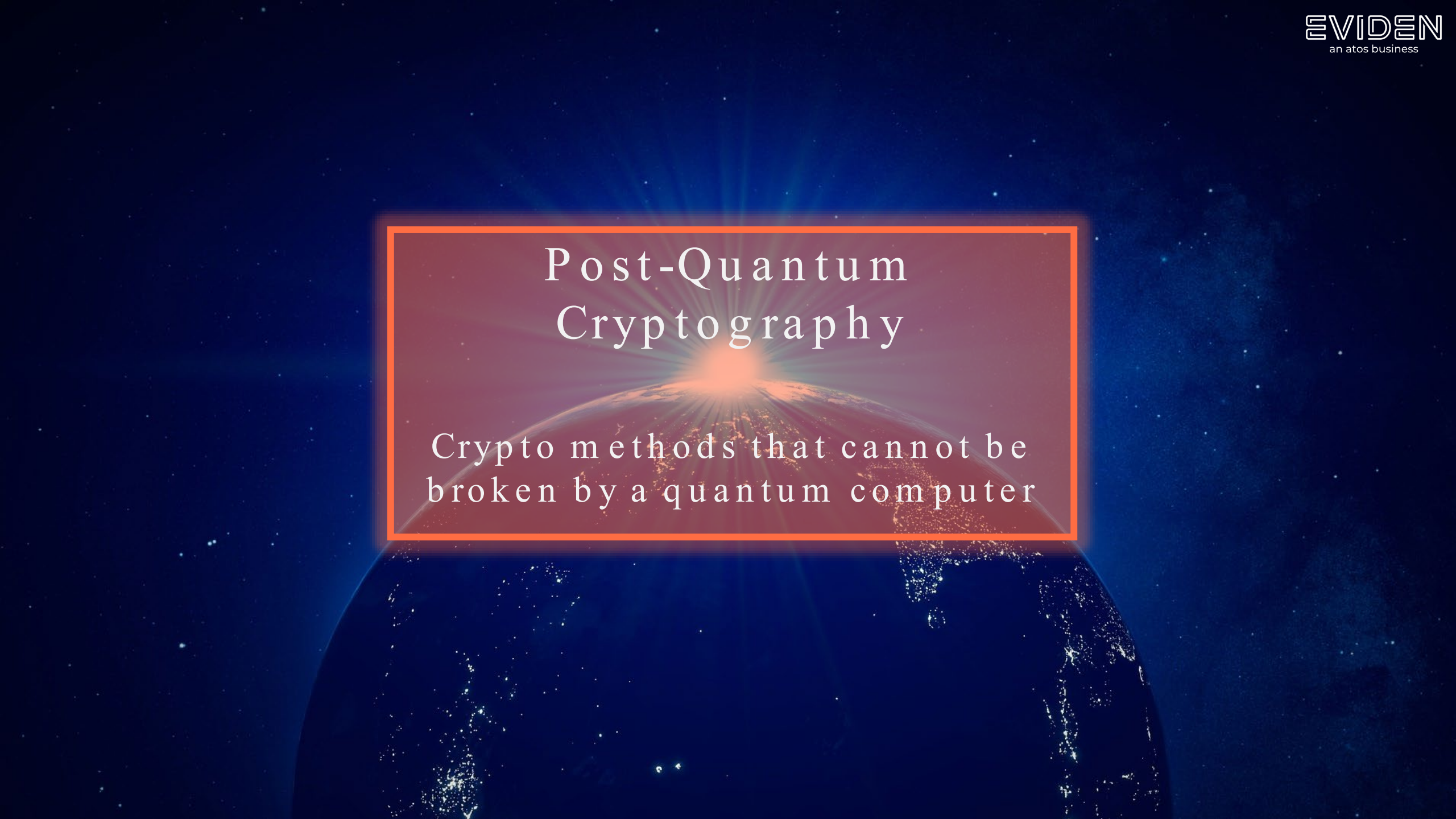
Q-Day and Y2Q

Q-Day: Day from which powerful quantum computers exist

Y2Q: Year of the Q-Day




We need alternatives to RSA.
We need Post-Quantum Cryptography.


EVIDEN
an atos business
Post-Quantum Cryptography
Crypto methods that cannot be broken by a quantum computer

EVIDEN
an atos business

2022

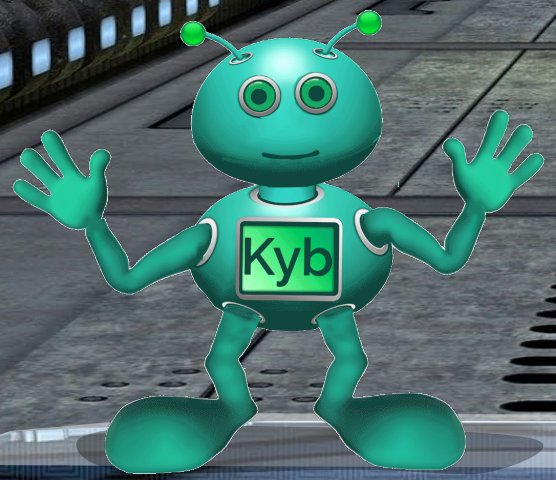
An important year for post-quantum cryptography

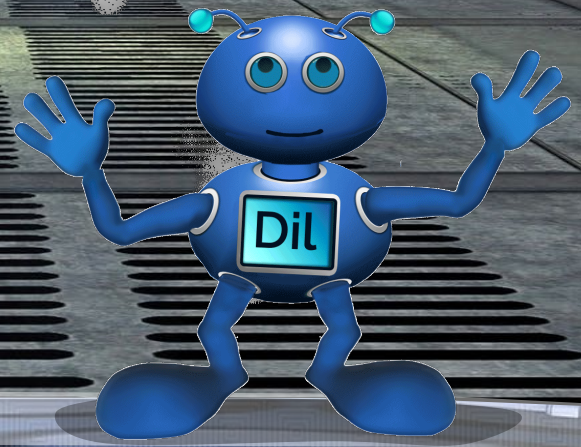
Because standardization has made progress

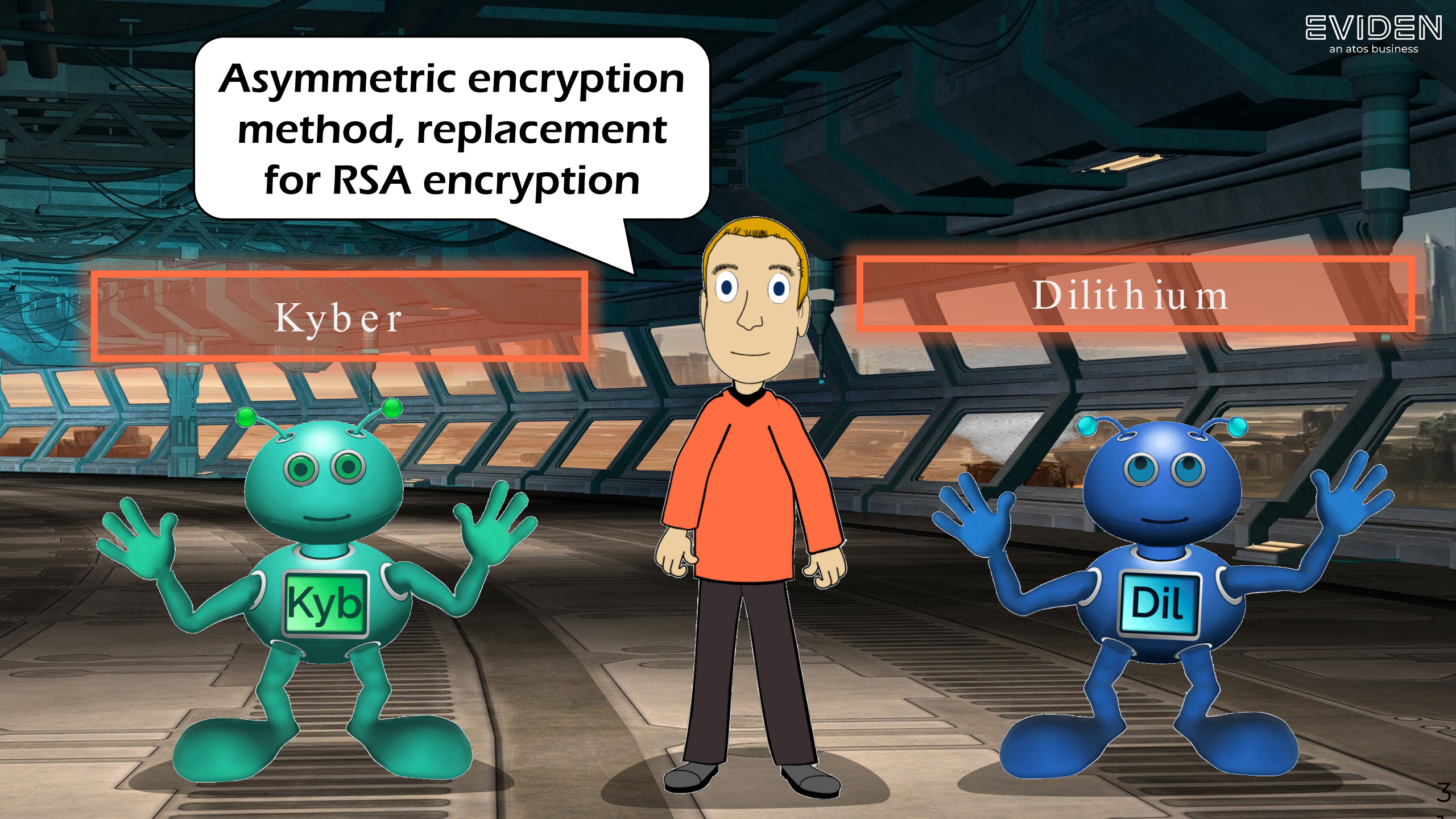
EVIDEN
an atos business

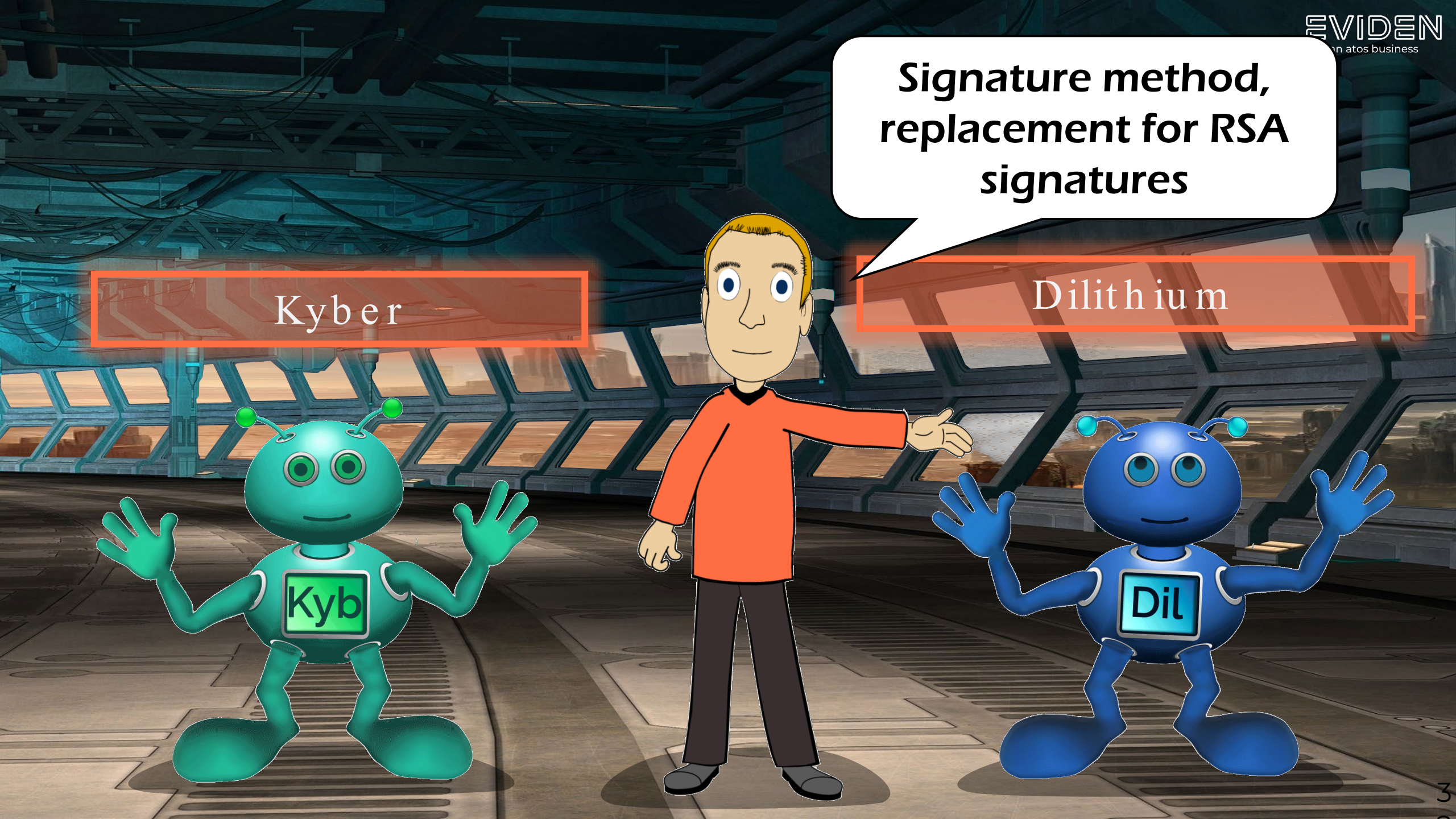
U.S. agency NIST names four post-quantum algorithms as competition winners

Among them CRYSTALS-Kyber and CRYSTALS-Dilithium






Asymmetric encryption method, replacement for RSA encryption
Kyber
Dilithium
Kyb
Dil


Signature method, replacement for RSA signatures
Kyber
Dilithium
Kyb
Dil


Both made in Germany
Kyber
Dilithium
Kyb
Dil

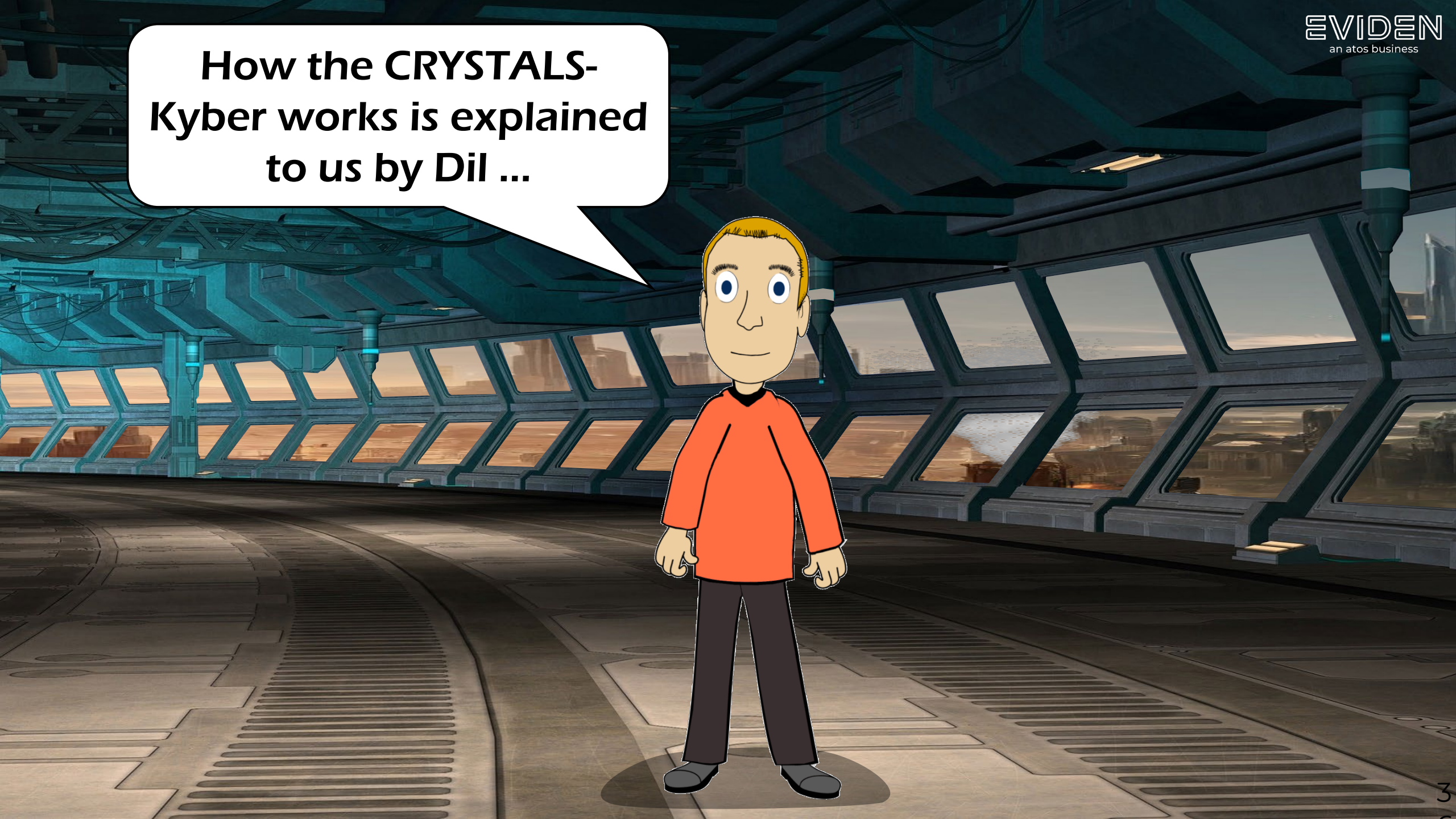
EVIDEN
an atos business

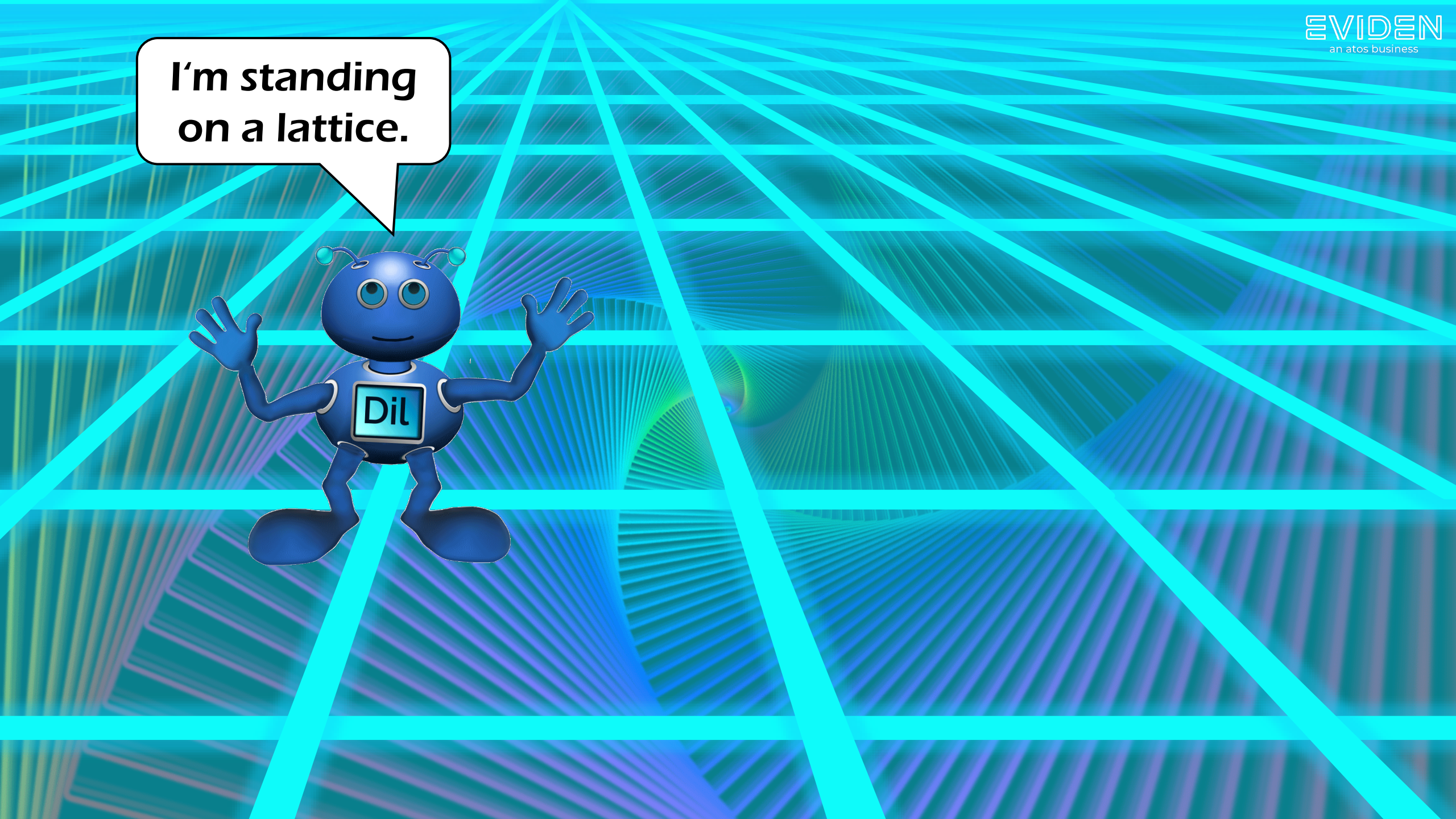
Eike Kiltz

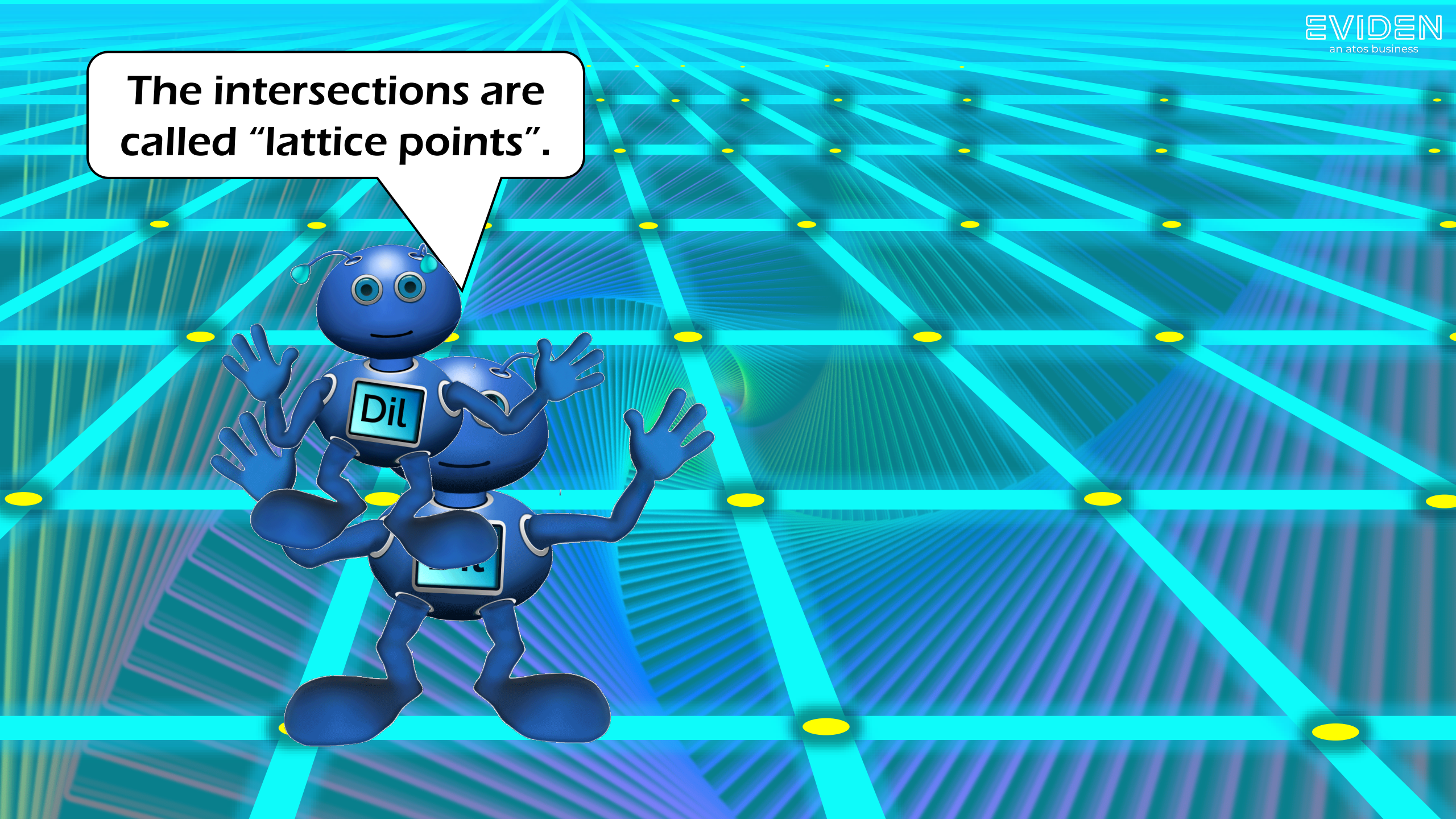
EVIDEN
an atos business

Eike Kiltz

Peter Schwabe

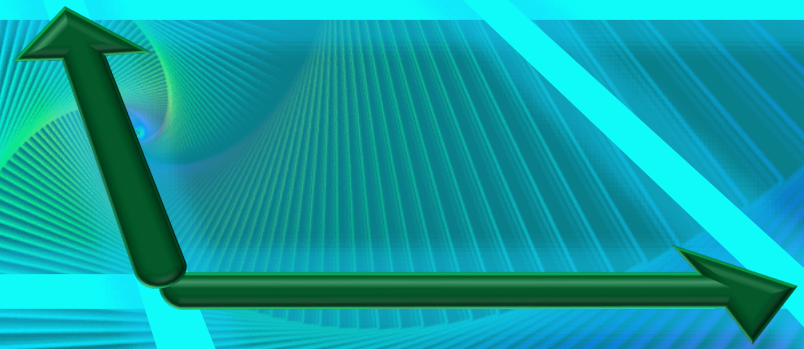

How the CRYSTALS-Kyber works is explained to us by Dil ...

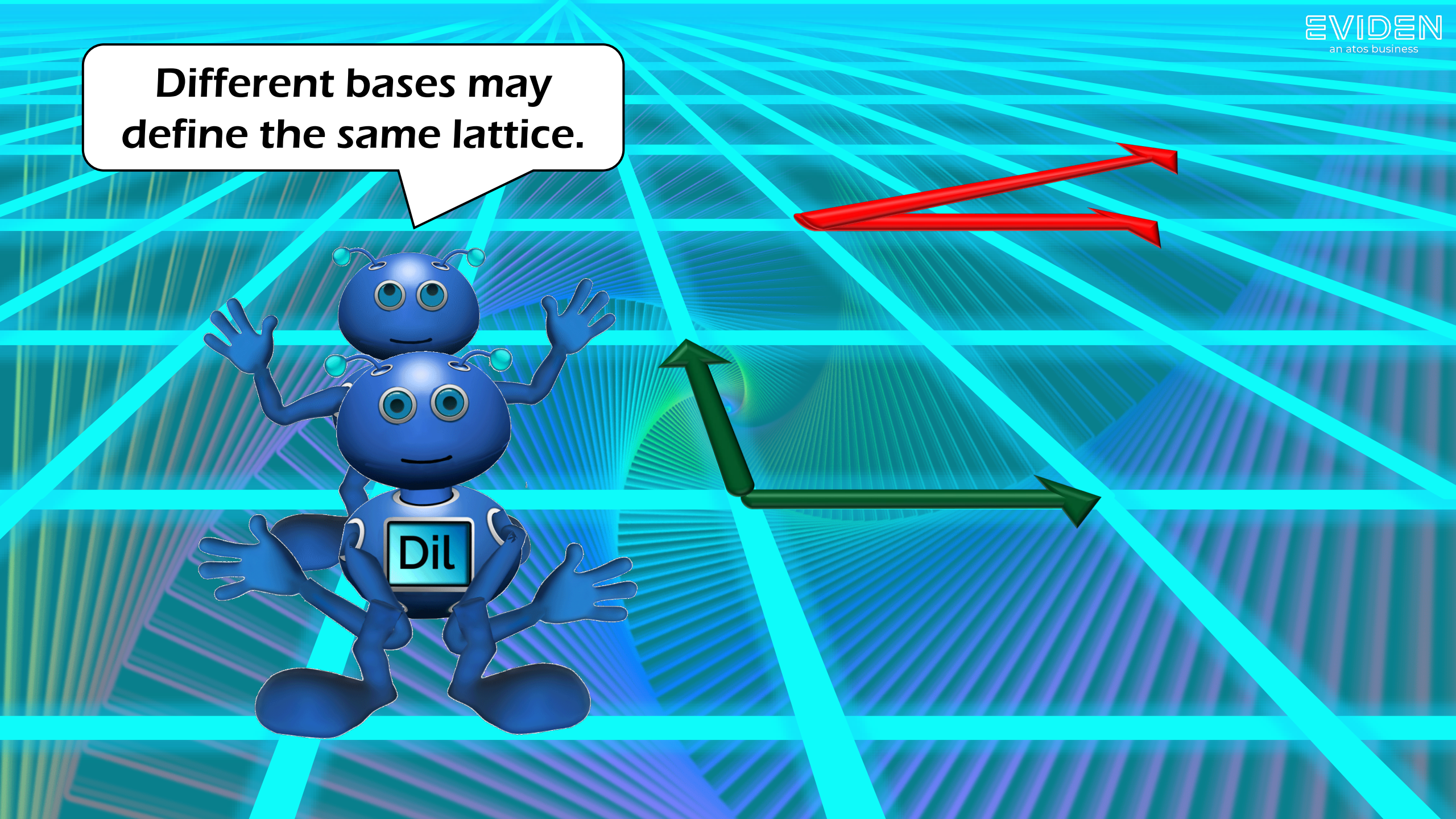

I'm standing on a lattice.
Dil

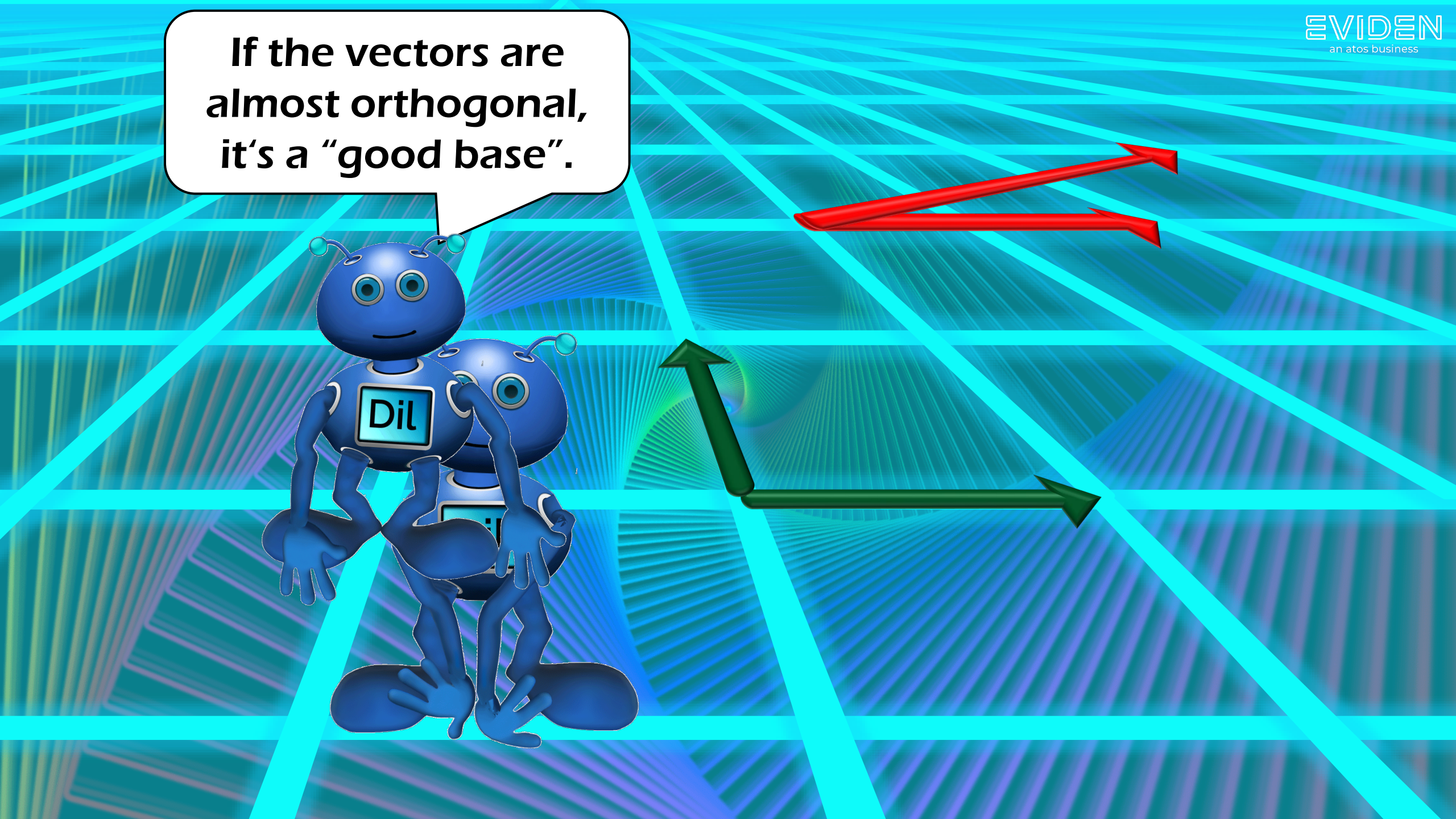

The intersections are called “lattice points”.
Dil

A lattice is defined with vectors.

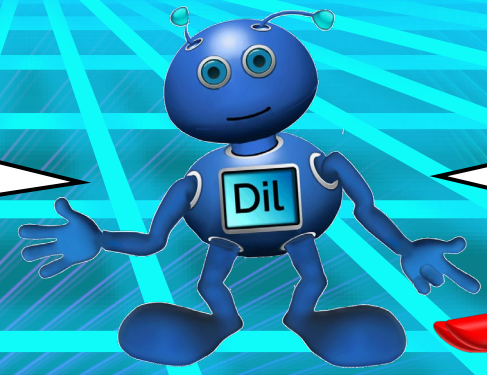
Reffered to as “base”.



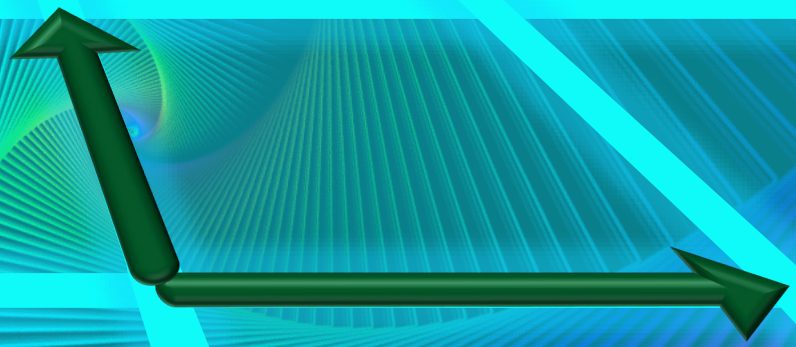

Different bases may define the same lattice.
Dil

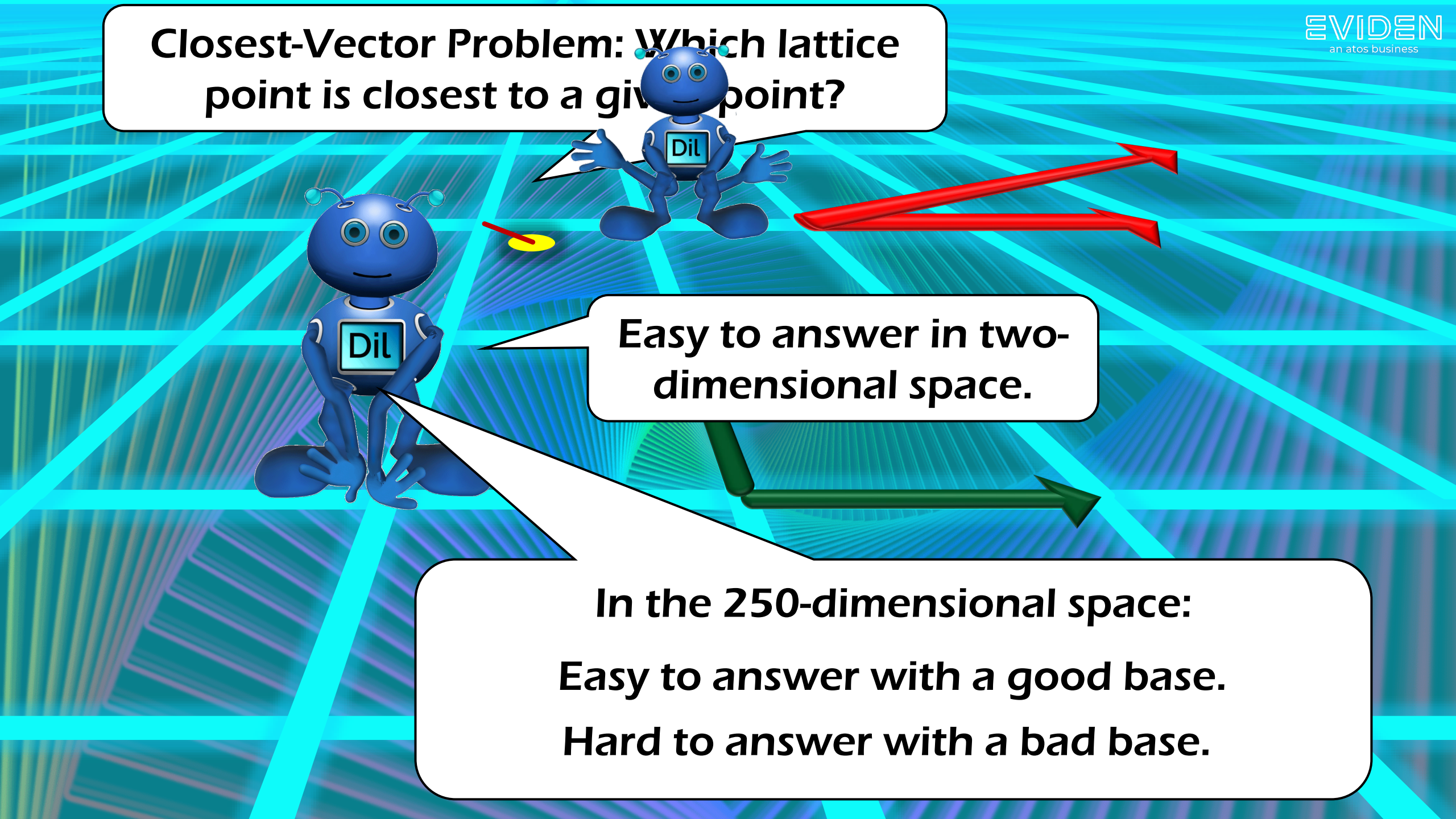

If the vectors are almost orthogonal, it's a "good base".
Dil

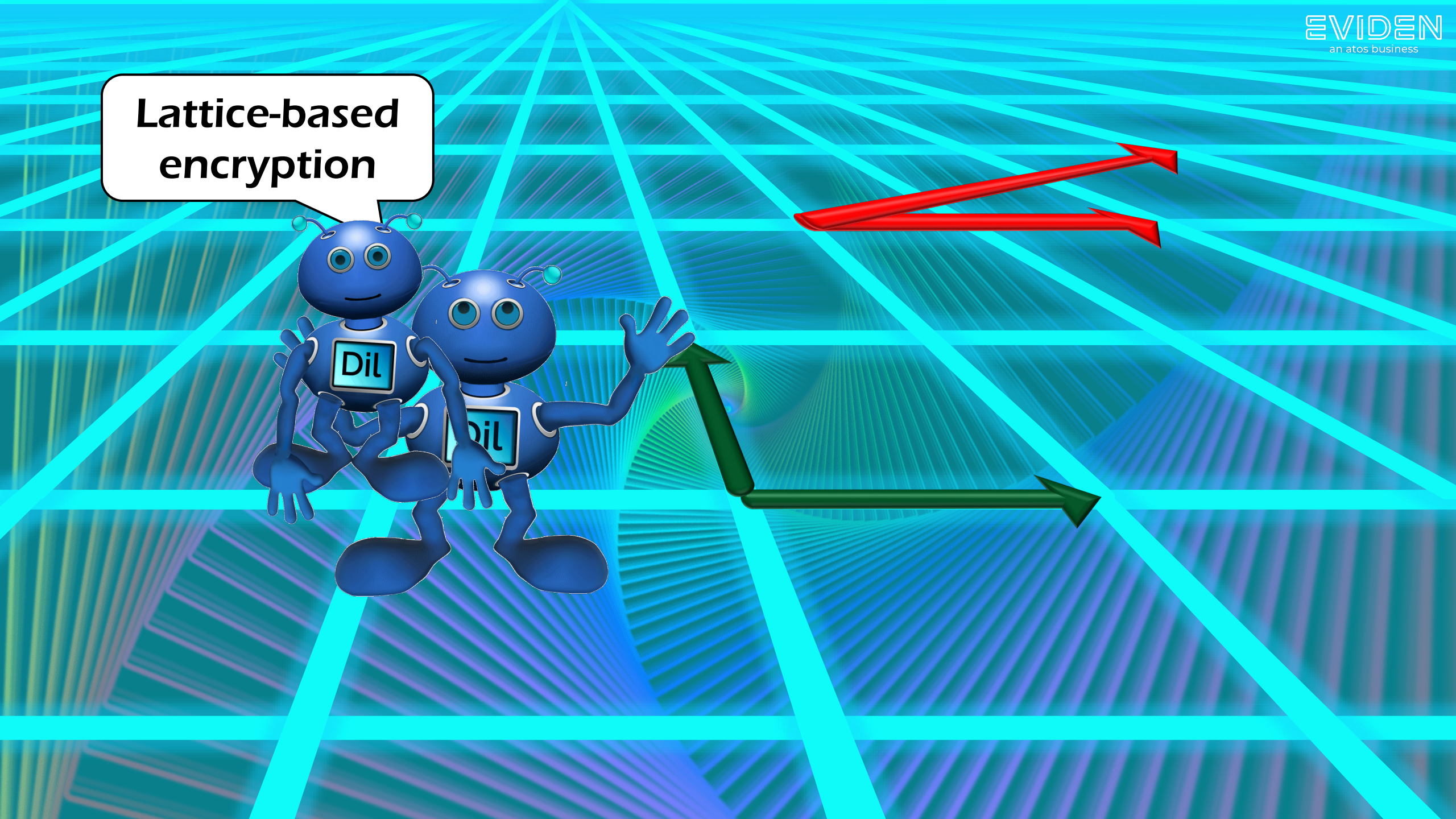
If the vectors are almost parallel, it's a "bad base".

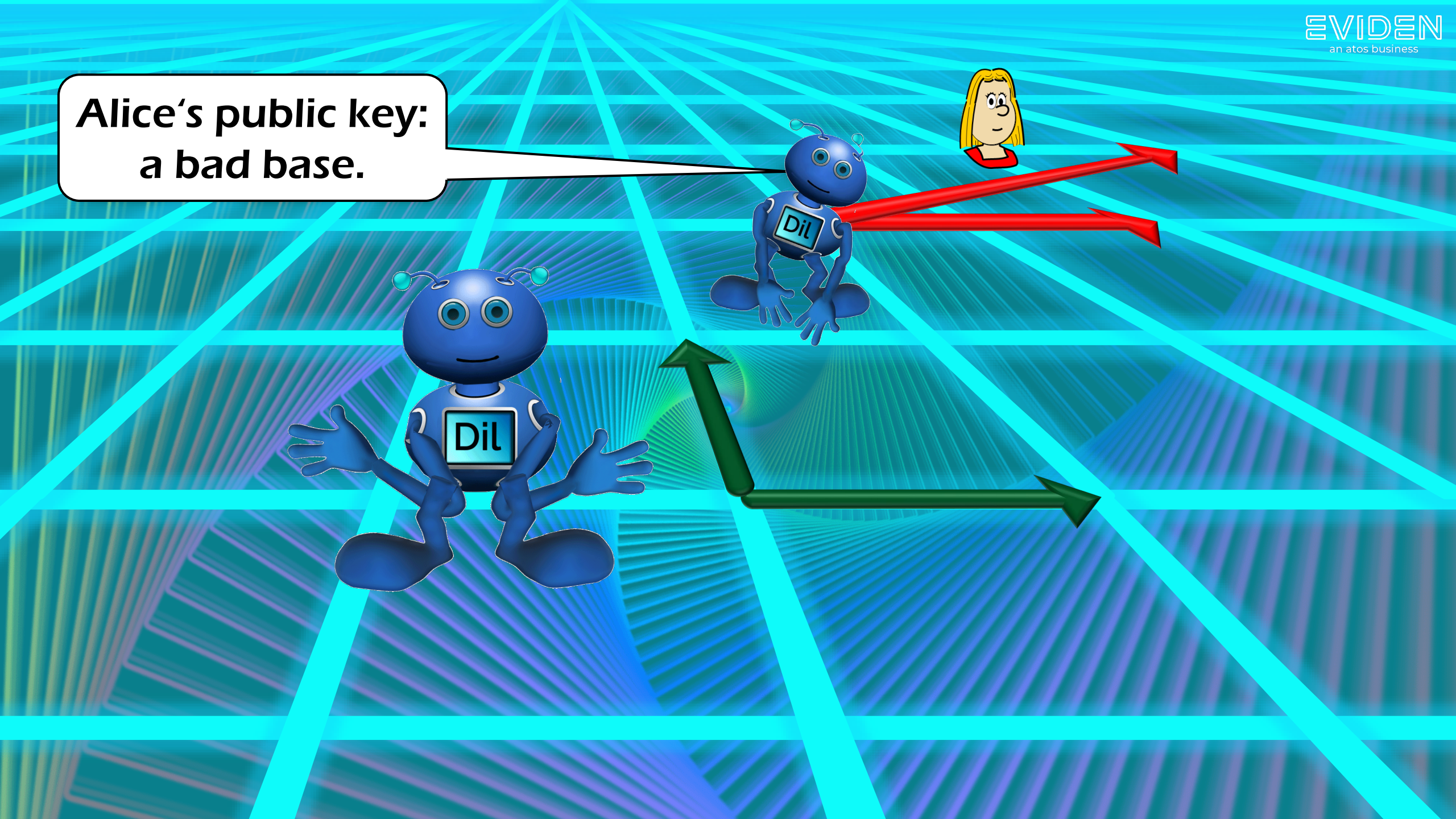


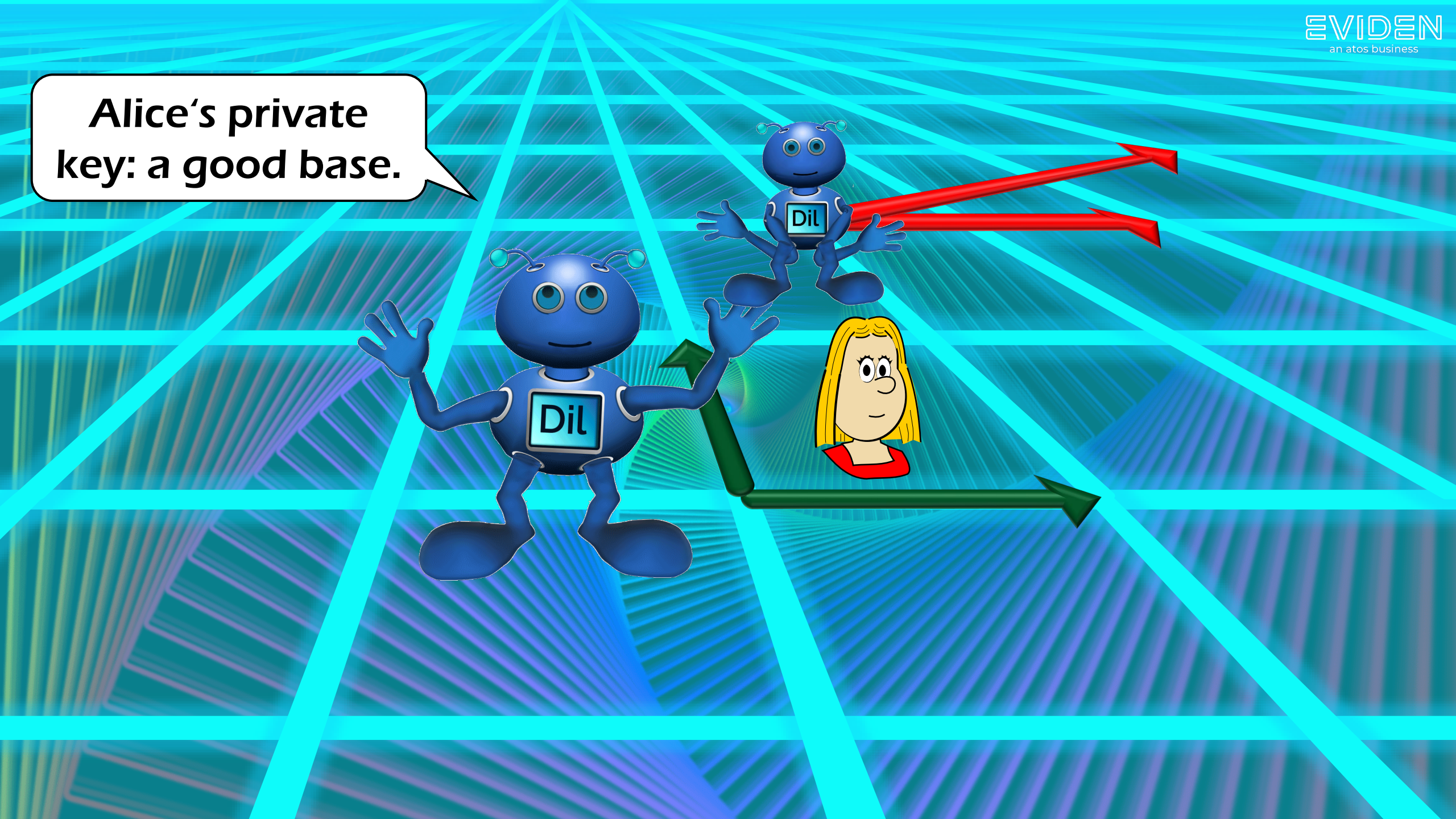
A bad base can be easily derived from a good one, but not the other way around.

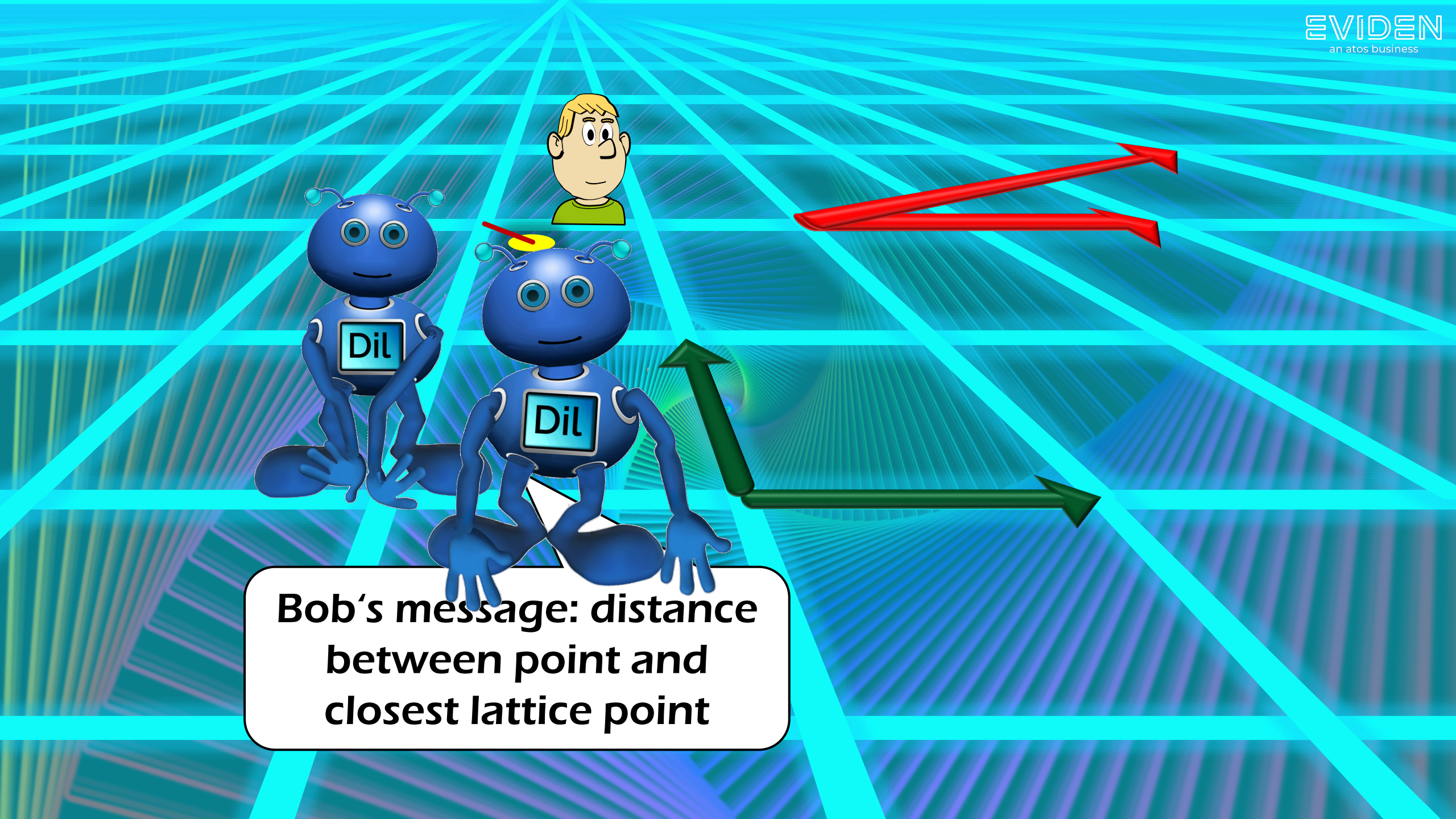


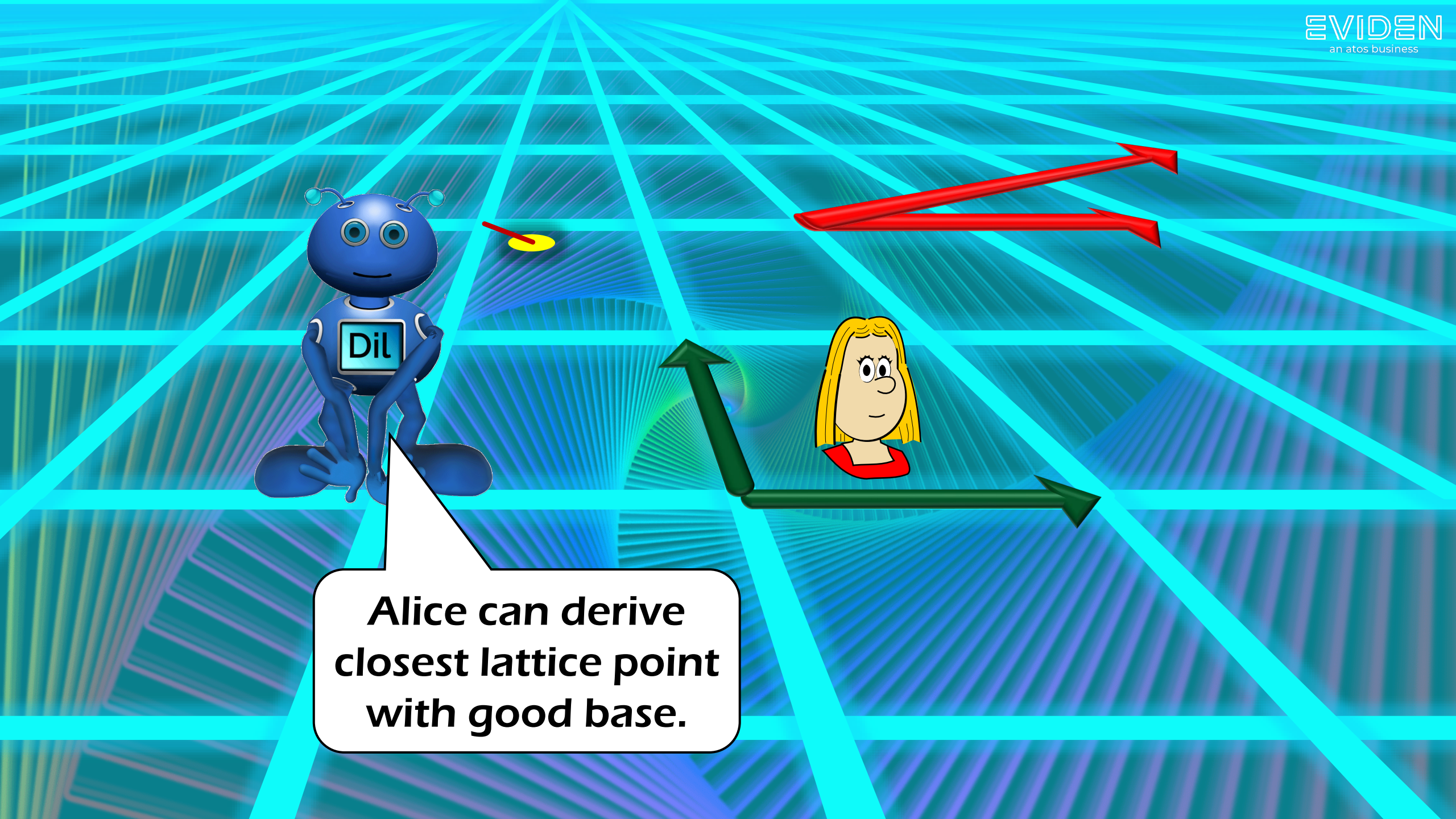

Closest-Vector Problem: Which lattice point is closest to a given point?
Dil
Dil
Easy to answer in two-dimensional space.
In the 250-dimensional space:
Easy to answer with a good base.
Hard to answer with a bad base.

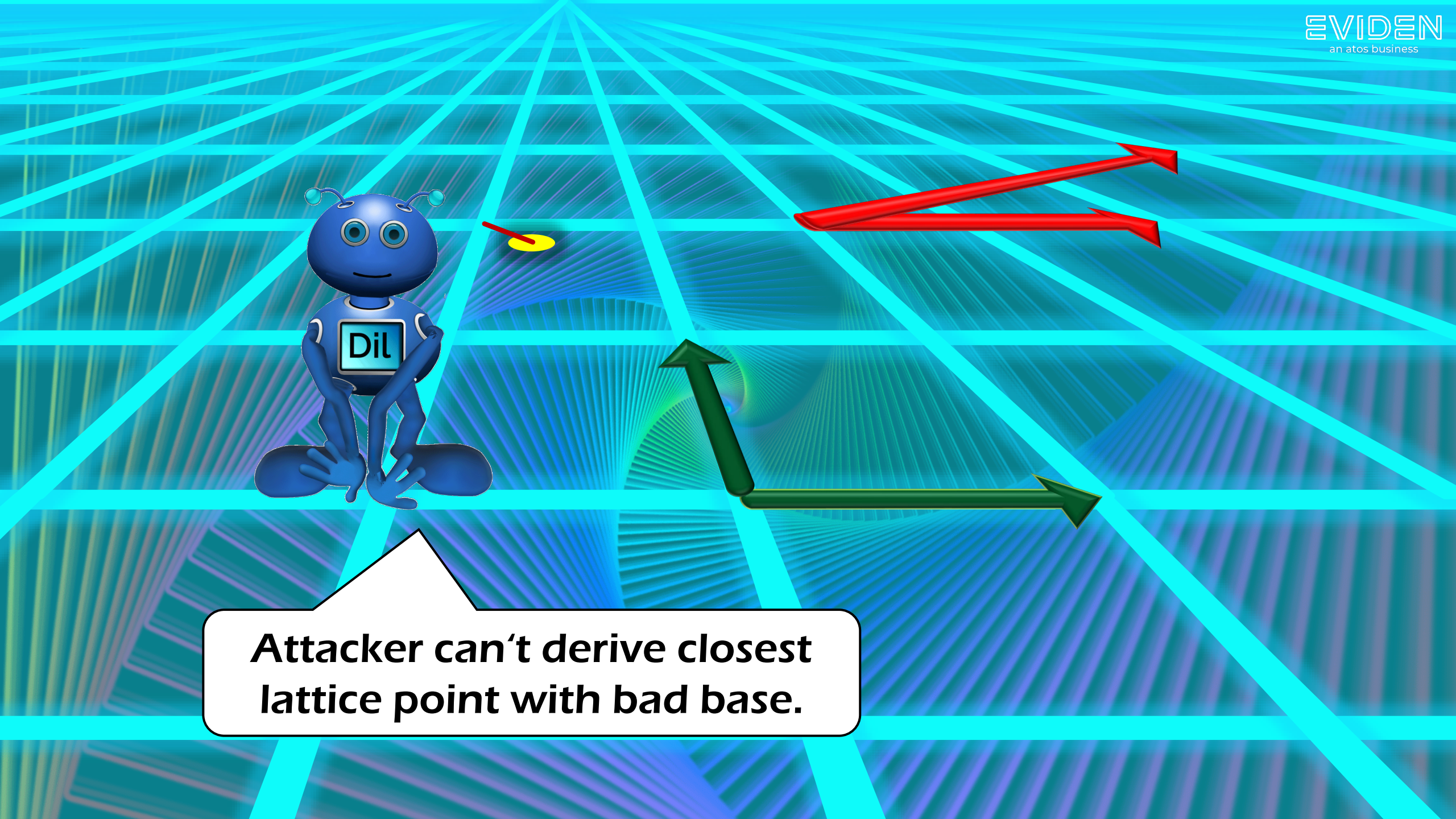

Lattice-based encryption
Dil
Dil

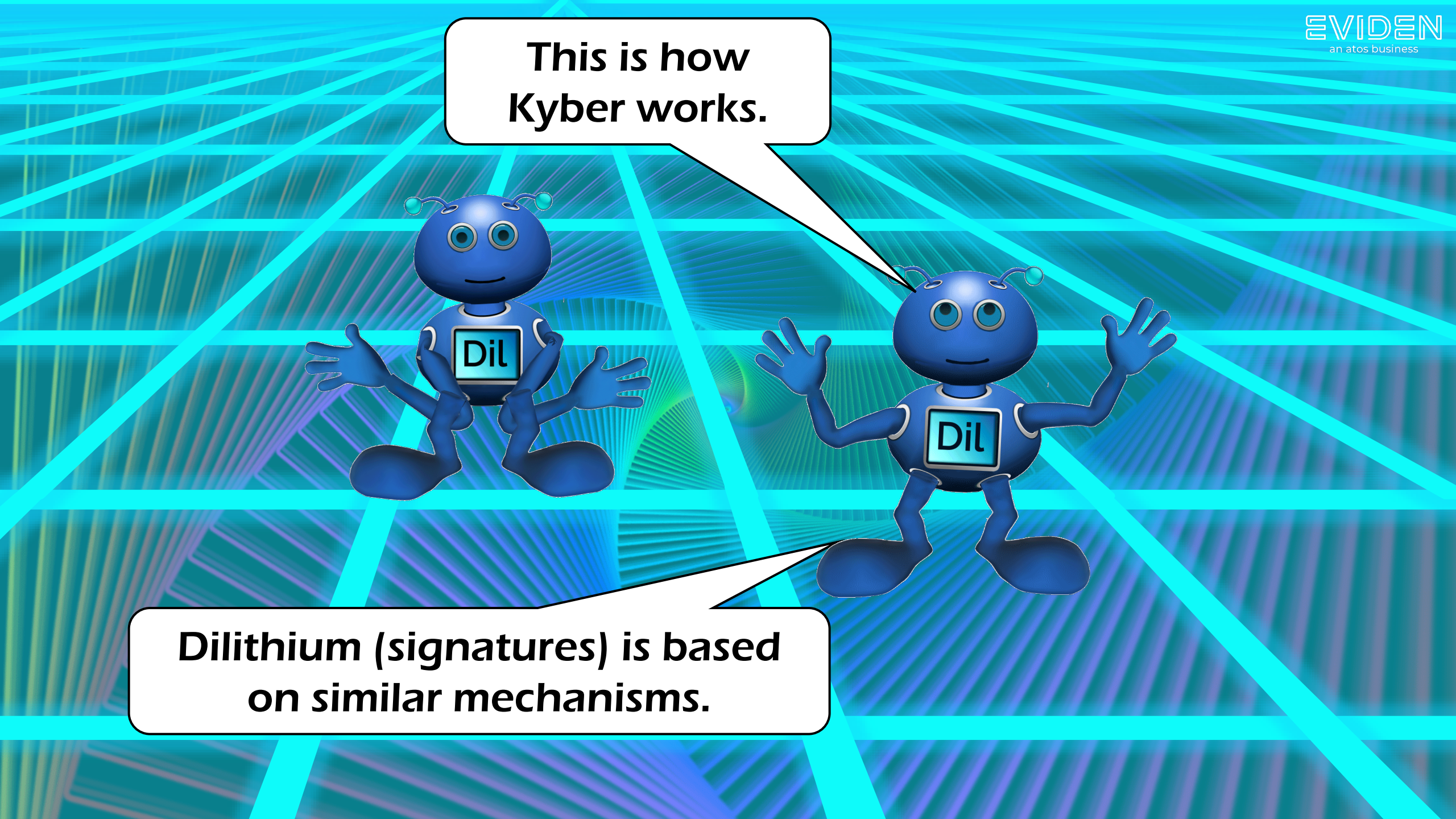

Alice's public key:
a bad base.
Dil
Dil

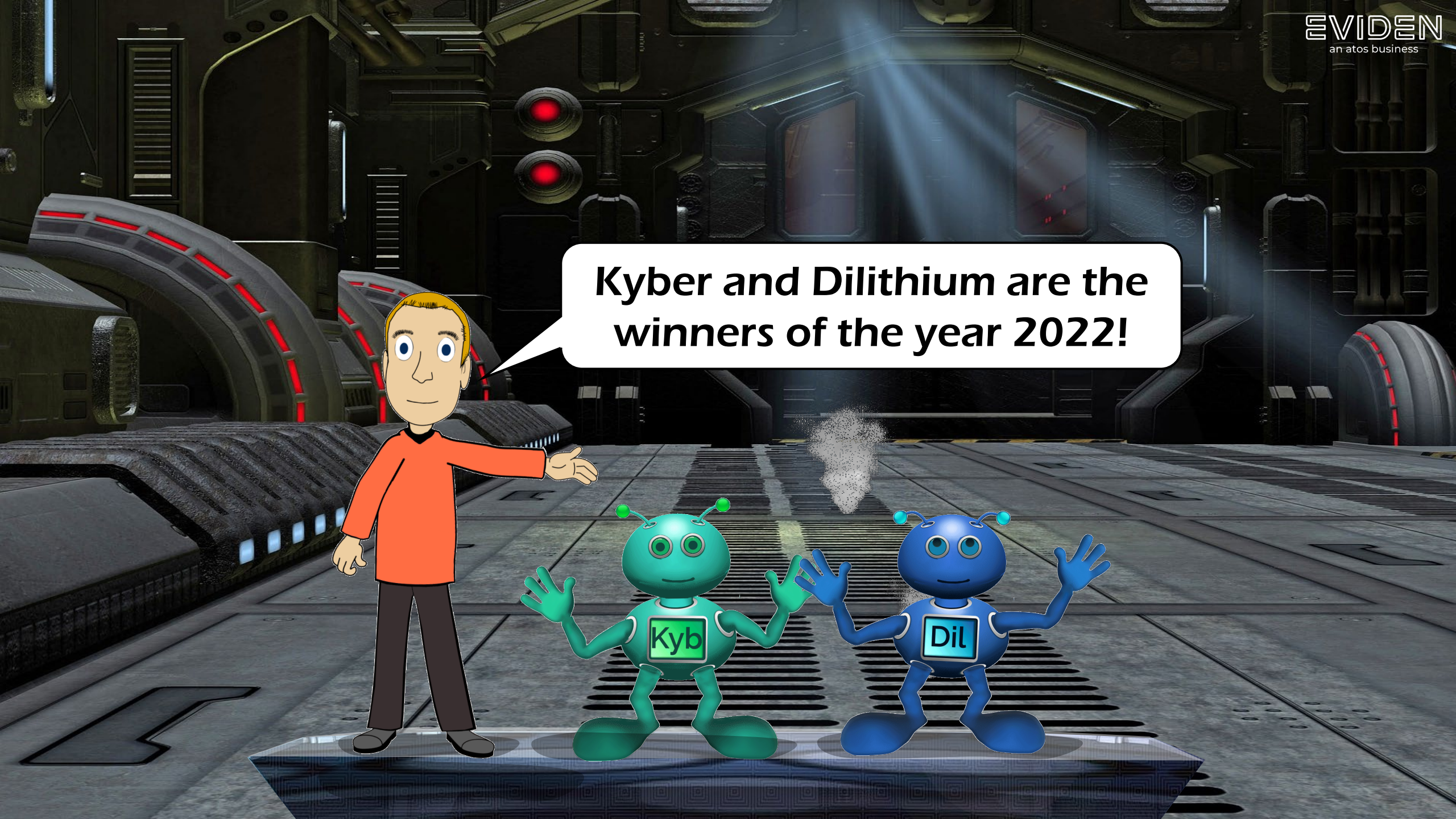

Alice's private key: a good base.
Dil
Dil


Dil
Dil
Bob's message: distance between point and closest lattice point


Dil
Alice can derive closest lattice point with good base.


Dil
Attacker can‘t derive closest lattice point with bad base.




Kyber and Dilithium are the winners of the year 2022!
Kyb
Dil

EVIDEN
an atos business

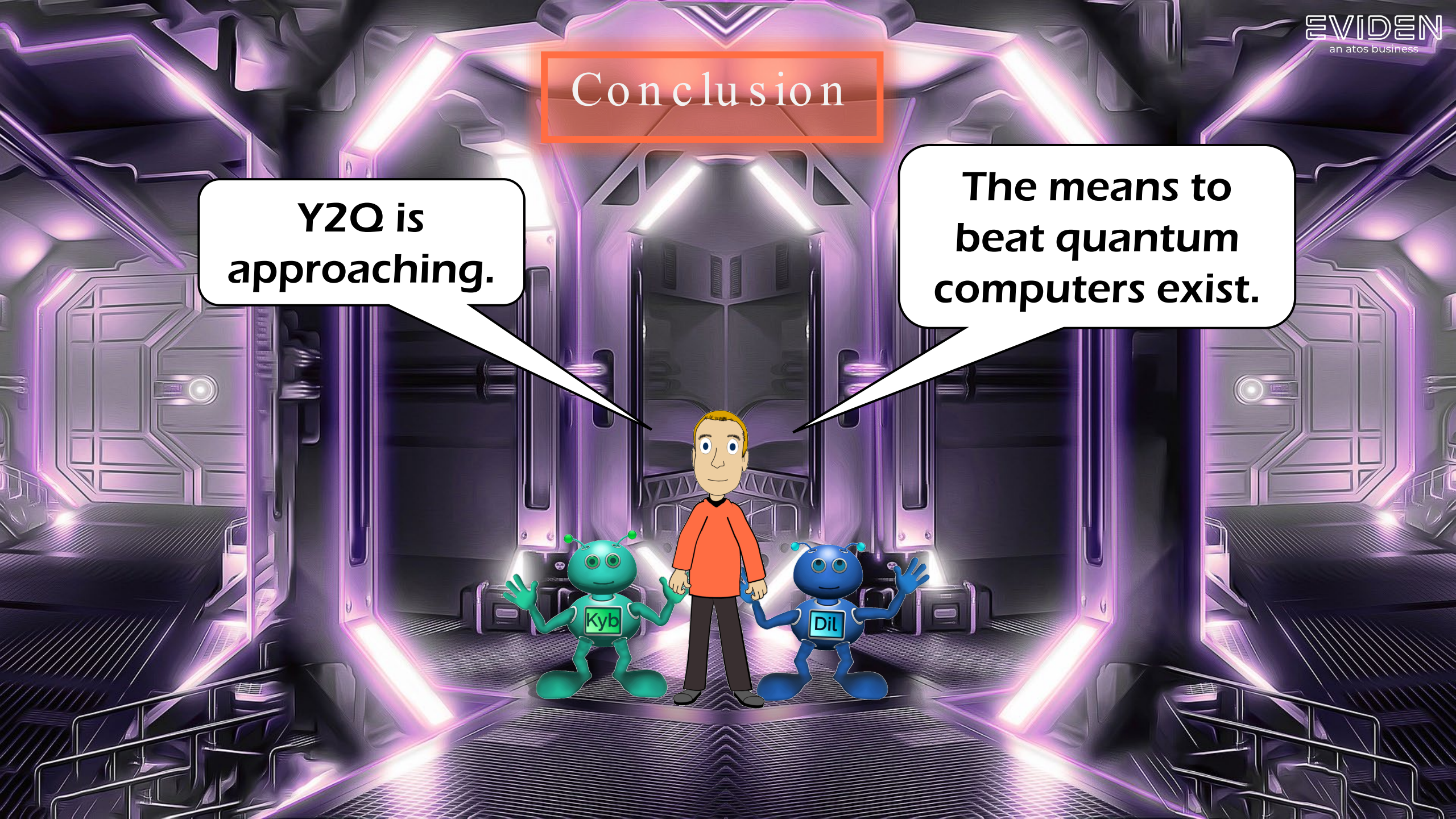
Public-key lengths

RSA: 2000 bit

Kyber: 6000 bit

Dilithium: 10000 bit

Conclusion

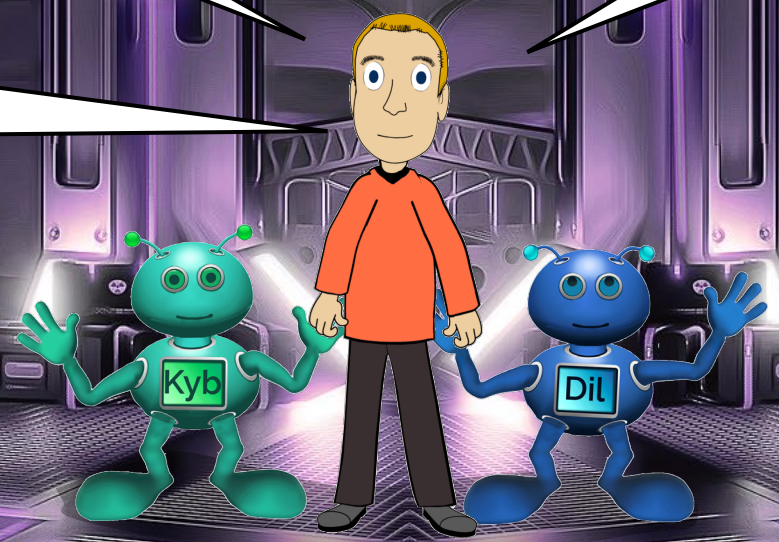

Y2Q is approaching.
The means to beat quantum computers exist.
Kyb
Dil

Conclusion

Standardisation is taking shape.

There's a lot to do, but it needs to be done.

Migration will be the next step.




EVIDEN
an atos business
END