

Cryptography is not enough

Cryptography is not enough

**A long(ish) Speech
on paradoxes and antinomies.**

Speech

Code = Speech

Speech = Code

Speech = Free

Speech = Free(dom)

Censorship \neq Free(dom)

Censorship = Tyranny

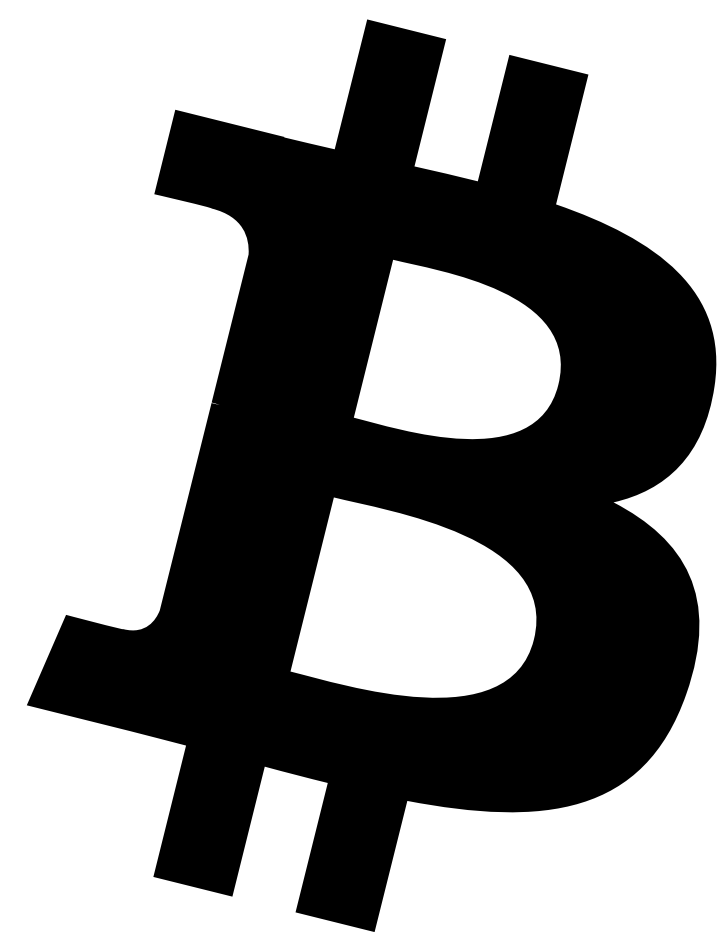
Privacy \neq Secrecy

**Running the
Numbers \neq Crime**

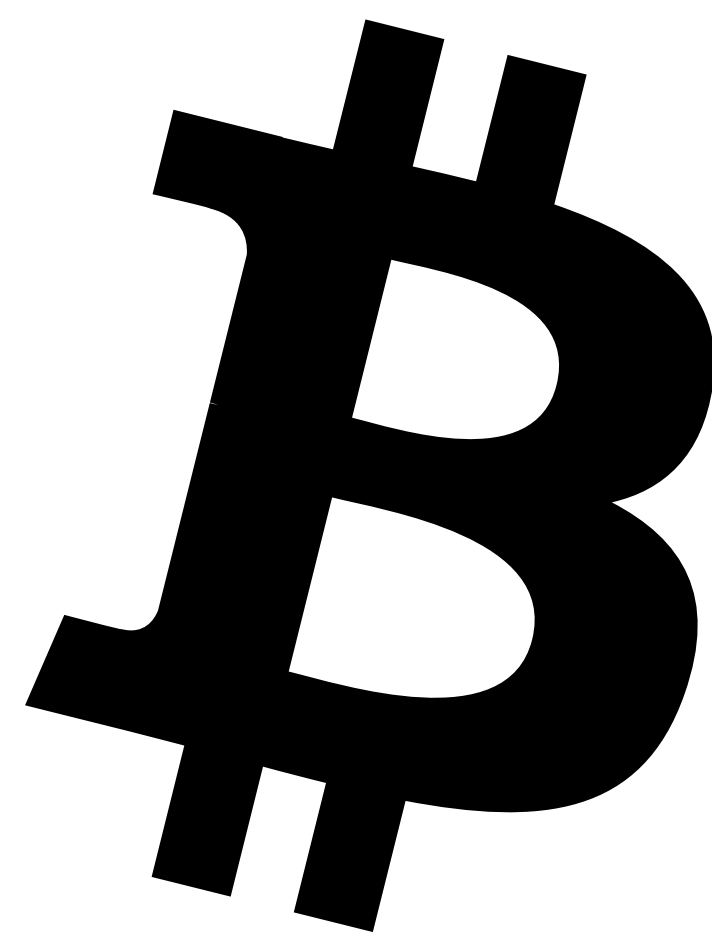
Numbers

3 Numbers

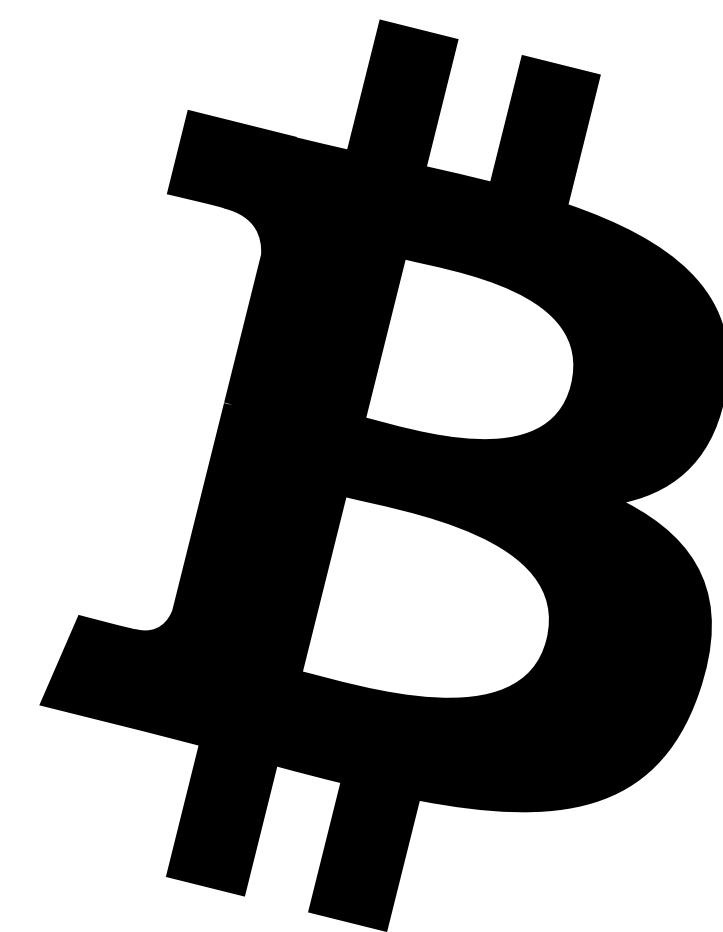




12

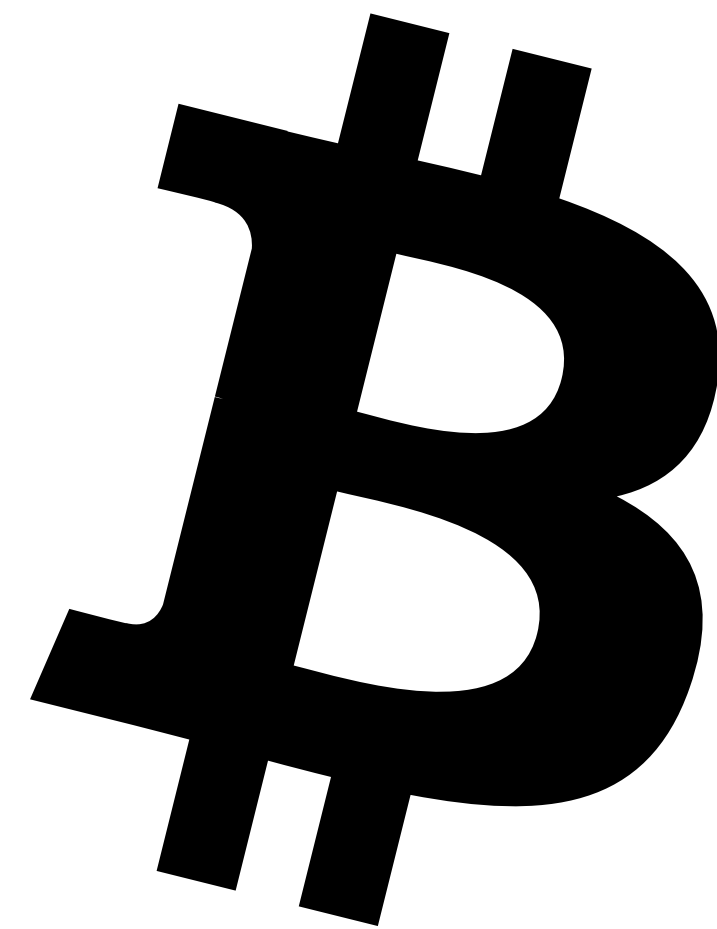


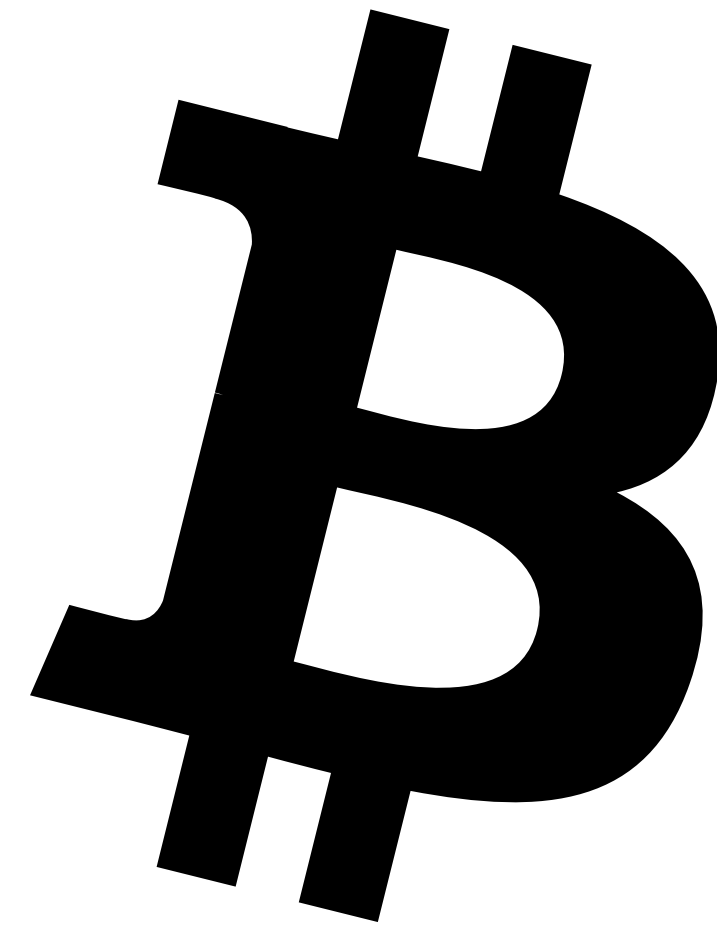
21



10

12

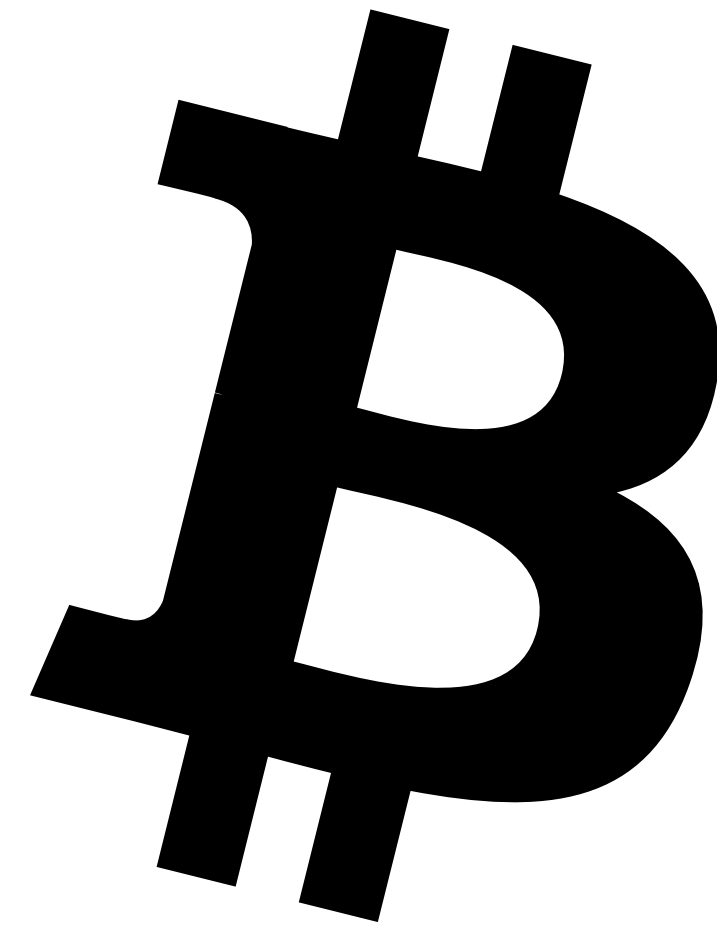




12

Act ONE

Bit



coin

Bitcoin = Code

Computer Code

Moral Code

Moral Code

**“You shall not inflate.
You shall not confiscate.
You shall not counterfeit.”**

“You shall not steal.”

—Bitcoin, basically

Bitcoin

Knowledge

Bitcoin = Knowledge

“Bitcoin = Knowledge”

“Knowledge = Power”

Knowledge = Power

France = Bacon

Bitcoin = Knowledge

Knowledge = Power

France = Bacon

Bitcoin = Knowledge

Knowledge = Power

France = **Bacon**

Bitcoin = Bacon

Bitcoin = Bacon

?

bacon bacon bacon
bacon bacon bacon
bacon bacon bacon
bacon bacon bacon

bacon bacon bacon
bacon bacon bacon
bacon bacon bacon
bacon bacon bacon

bacon bacon bacon
bacon bacon bacon
bacon bacon bacon
bacon bacon bacon

bacon bacon bacon
bacon bacon bacon
bacon bacon bacon
bacon bacon bacon



bacon bacon bacon
bacon bacon bacon
bacon bacon bacon
bacon bacon bacon

bacon bacon bacon
bacon bacon bacon
bacon bacon bacon
bacon bacon bacon

“bacon”

“bacon”

x 24

“flag”

“gas”

“great”

“slice”

“solution”

“bacon”

“summer”

“they”

“trade”

“trap”

“zebra”

x 24

“flag”
“gas”
“great”
“slice”
“solution”
“bacon”
“summer”
“they”
“trade”
“trap”
“zebra”

241

12

241

12

24

12

words

12

magic words

12x

“word”

word word word
word word word
word word word
word word word

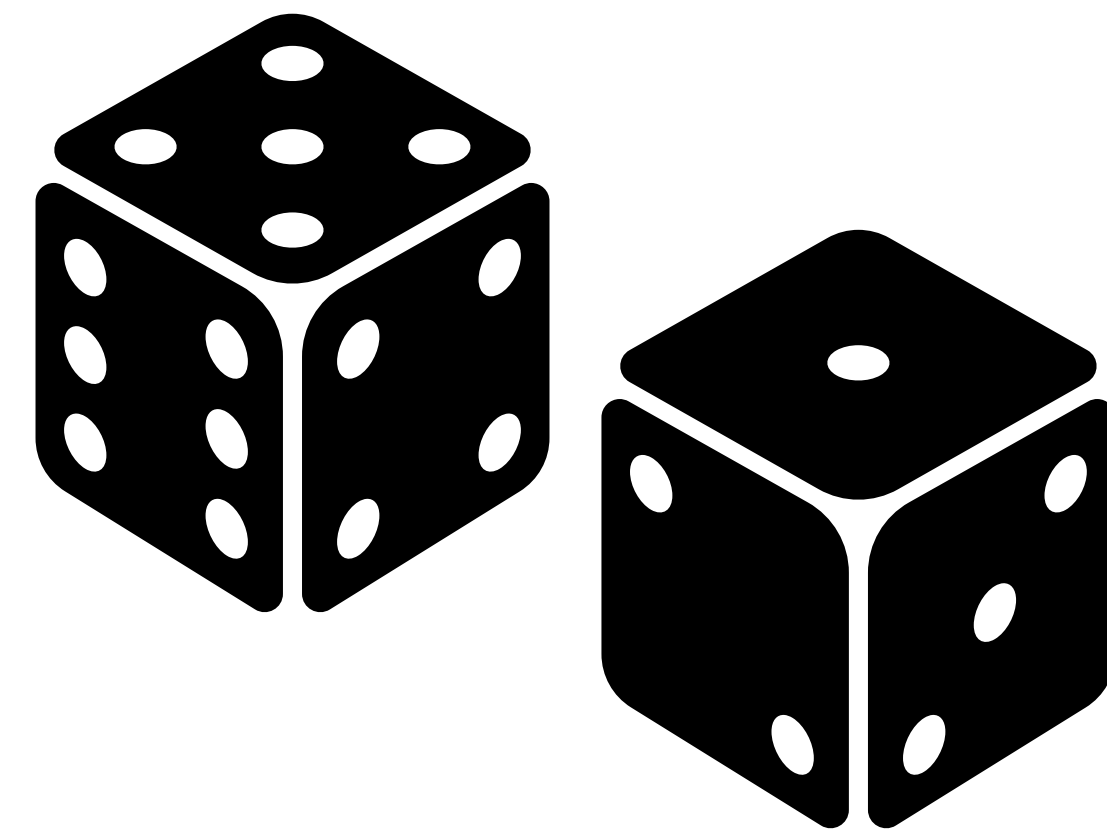
“word”

12

**twelve
magic
words**



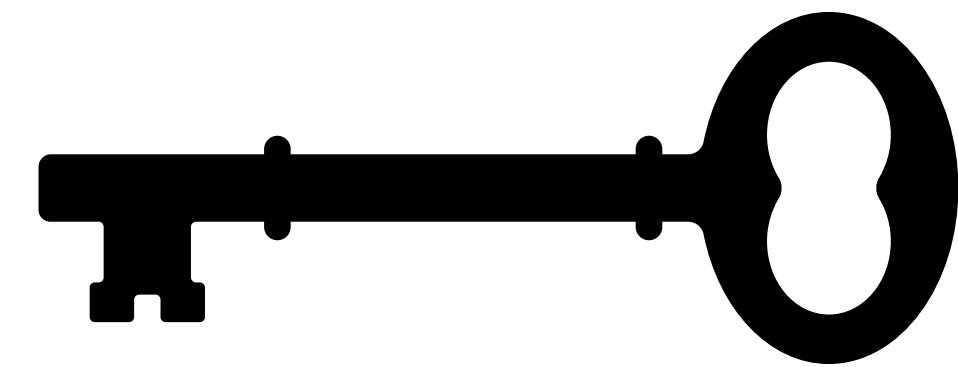
12
twelve
random
words



12
twelve
random
words

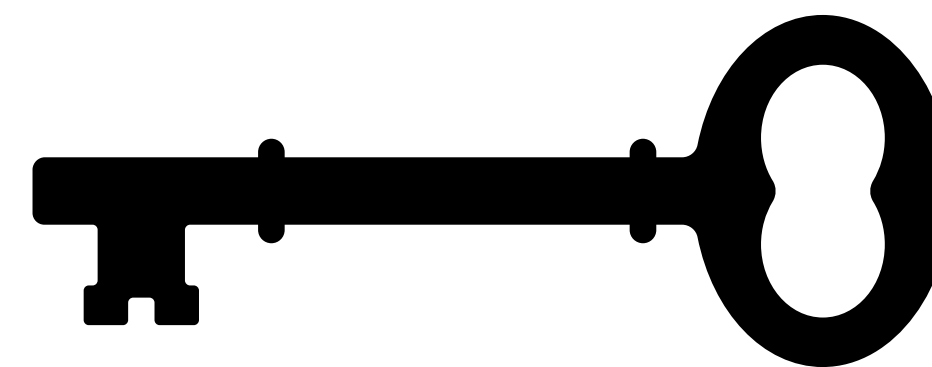


12
twelve
random
words



12

**twelve
valid
words**



12

**twelve
valid
words**



“flag”

“gas”

“great”

12

“twelve”

“valid”

“word”

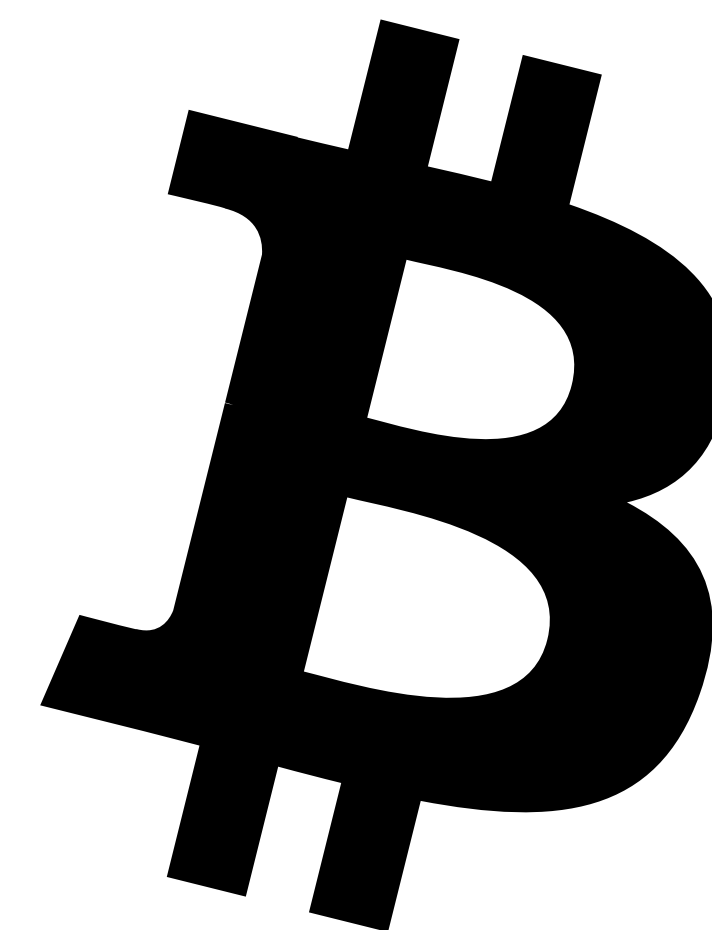


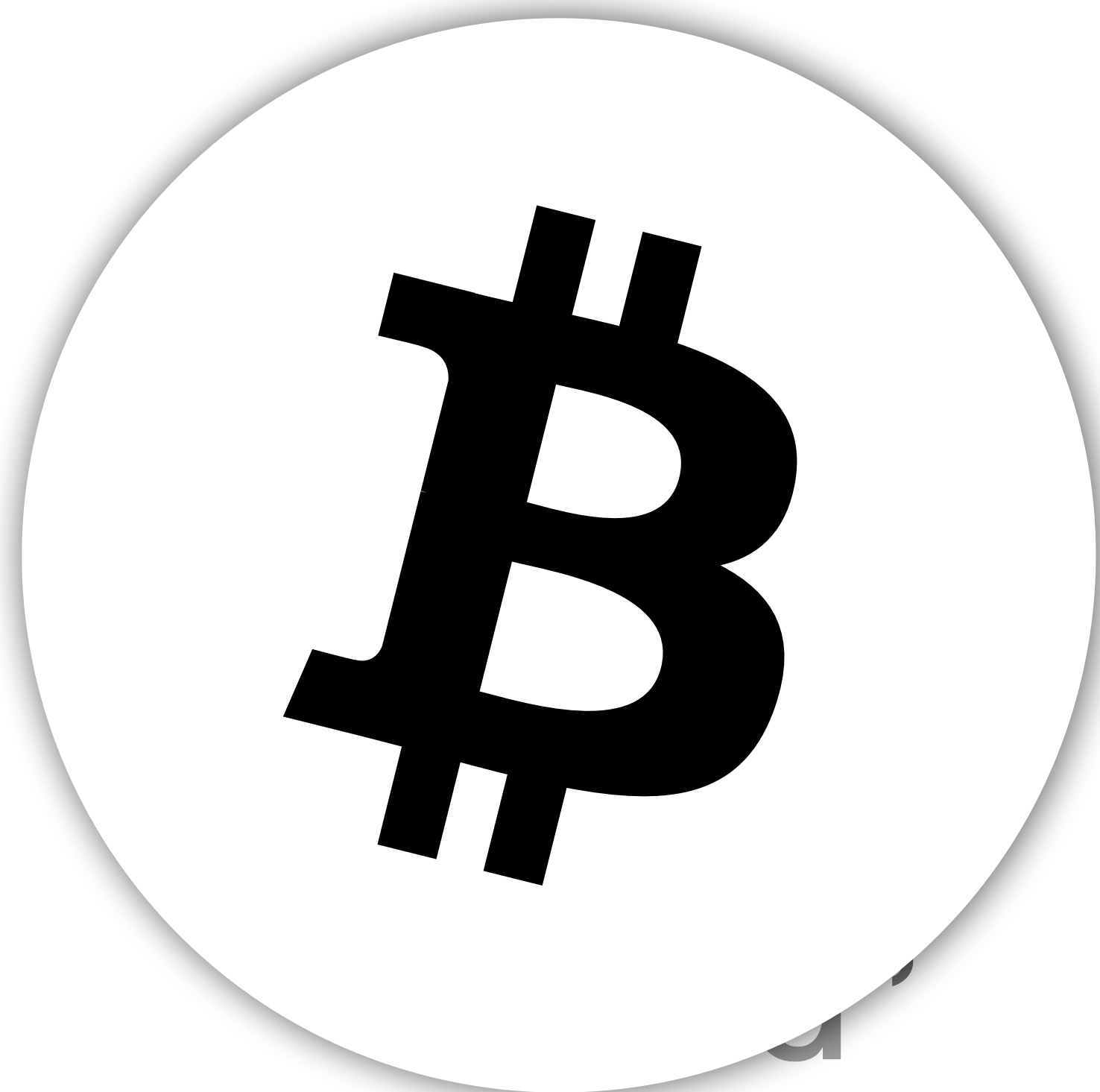
12

“twelve”

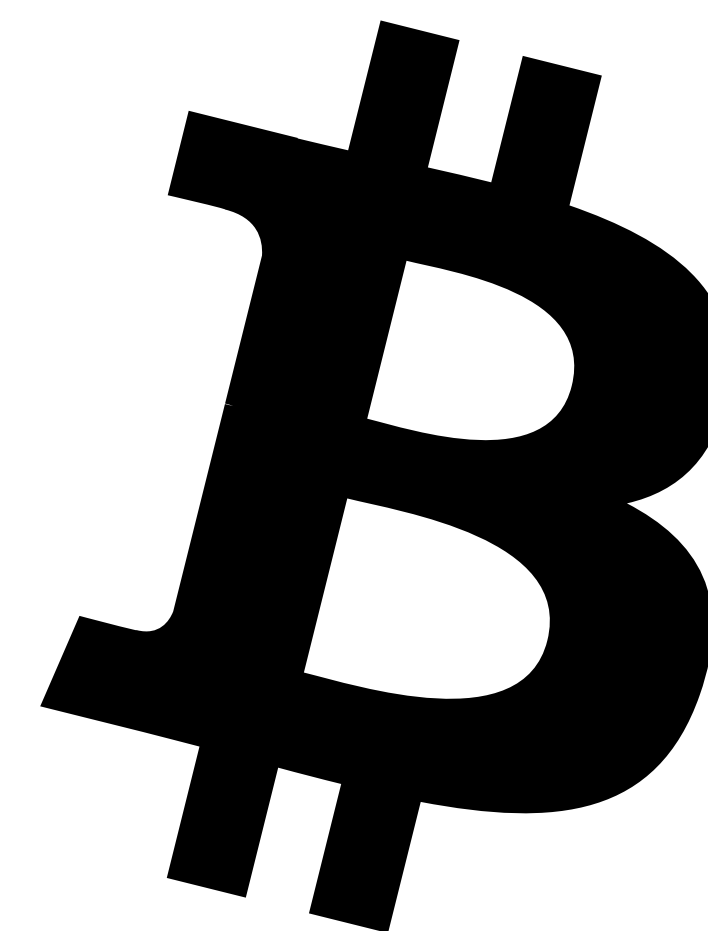
“valid”

“word”

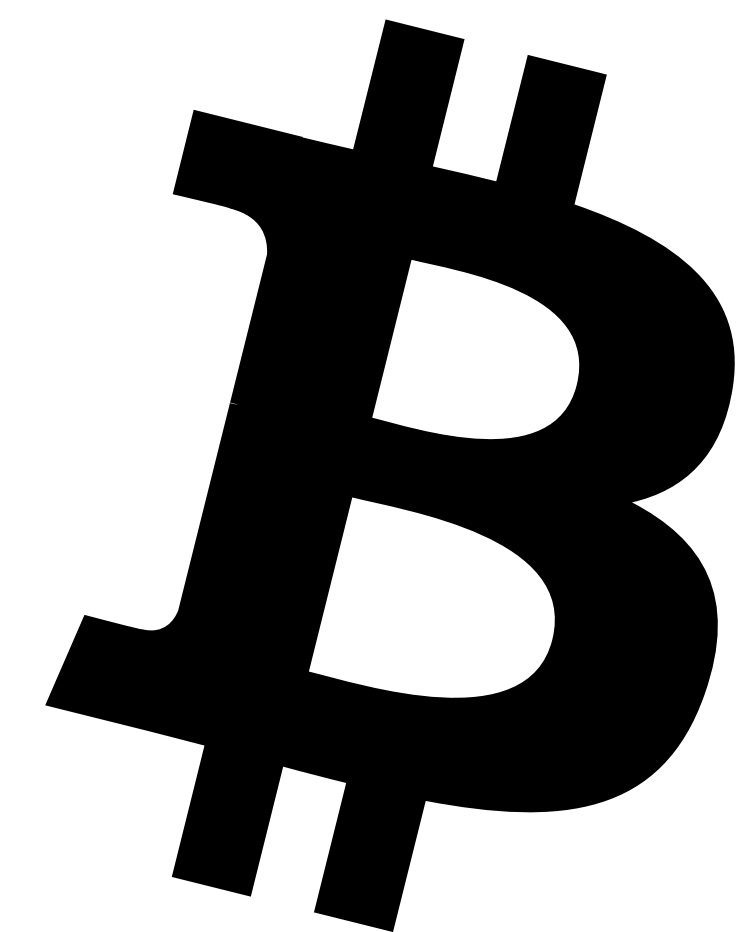




“word”



ACT



TWO

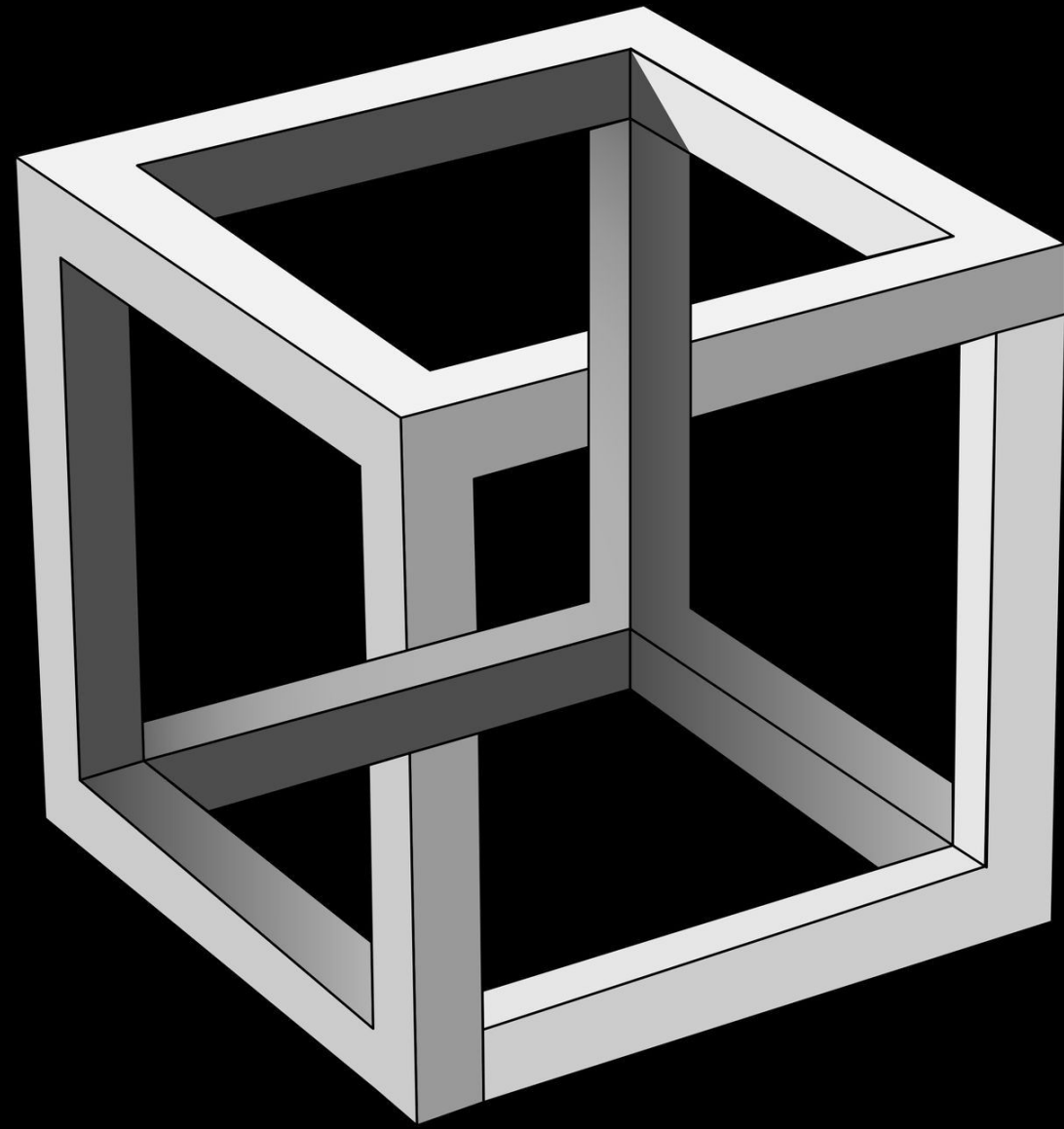
ACT



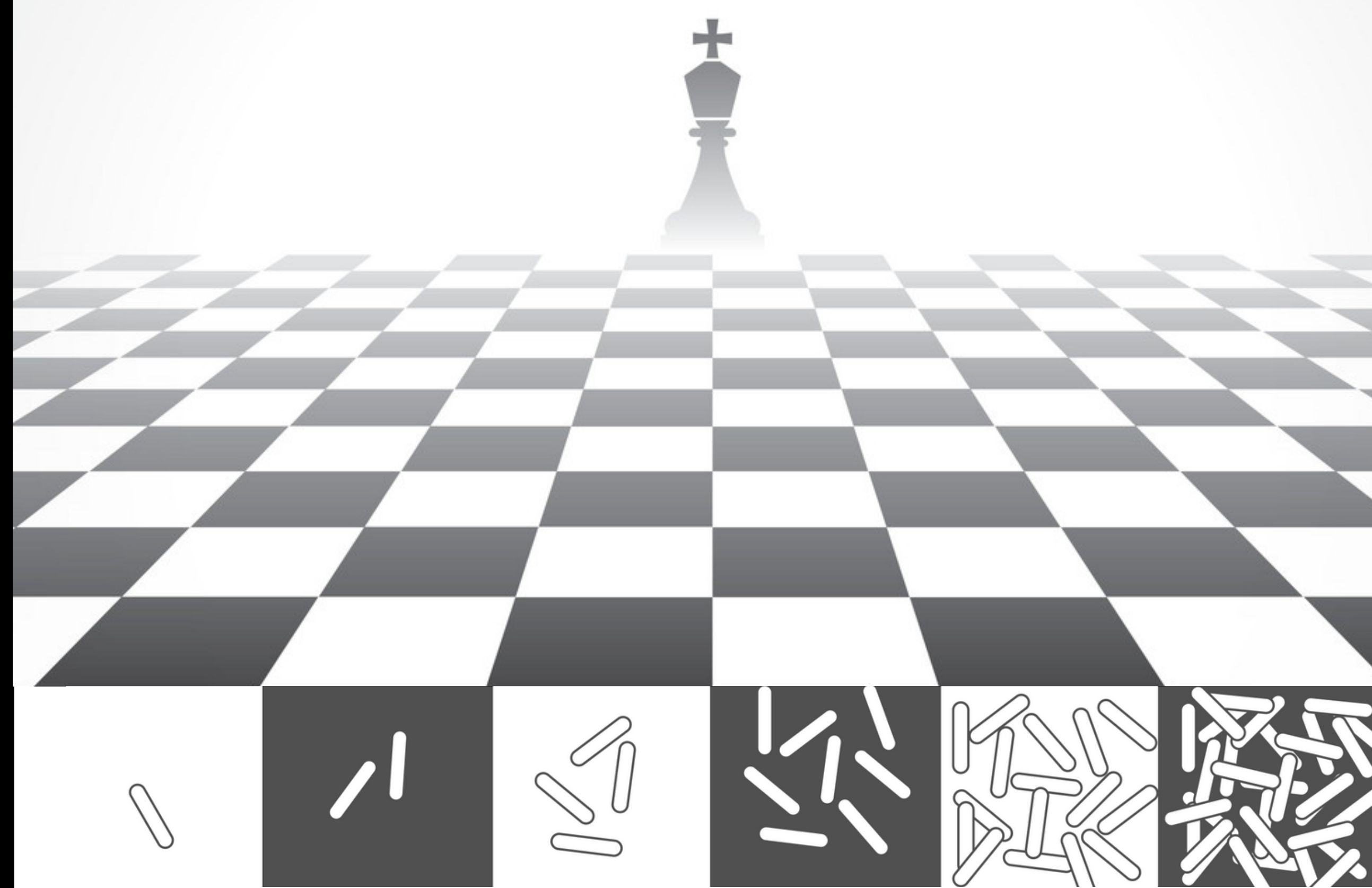
TWO



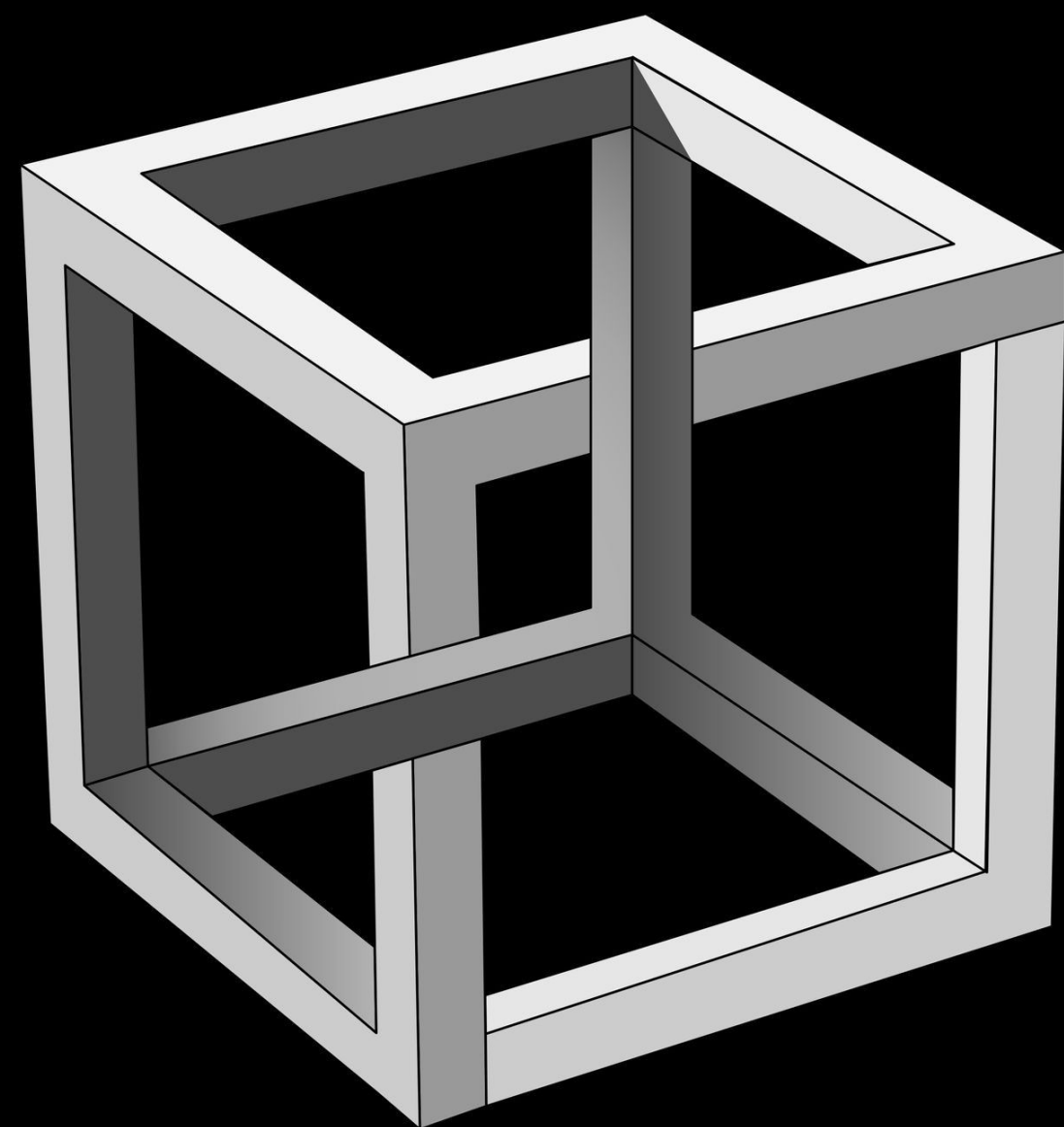
21



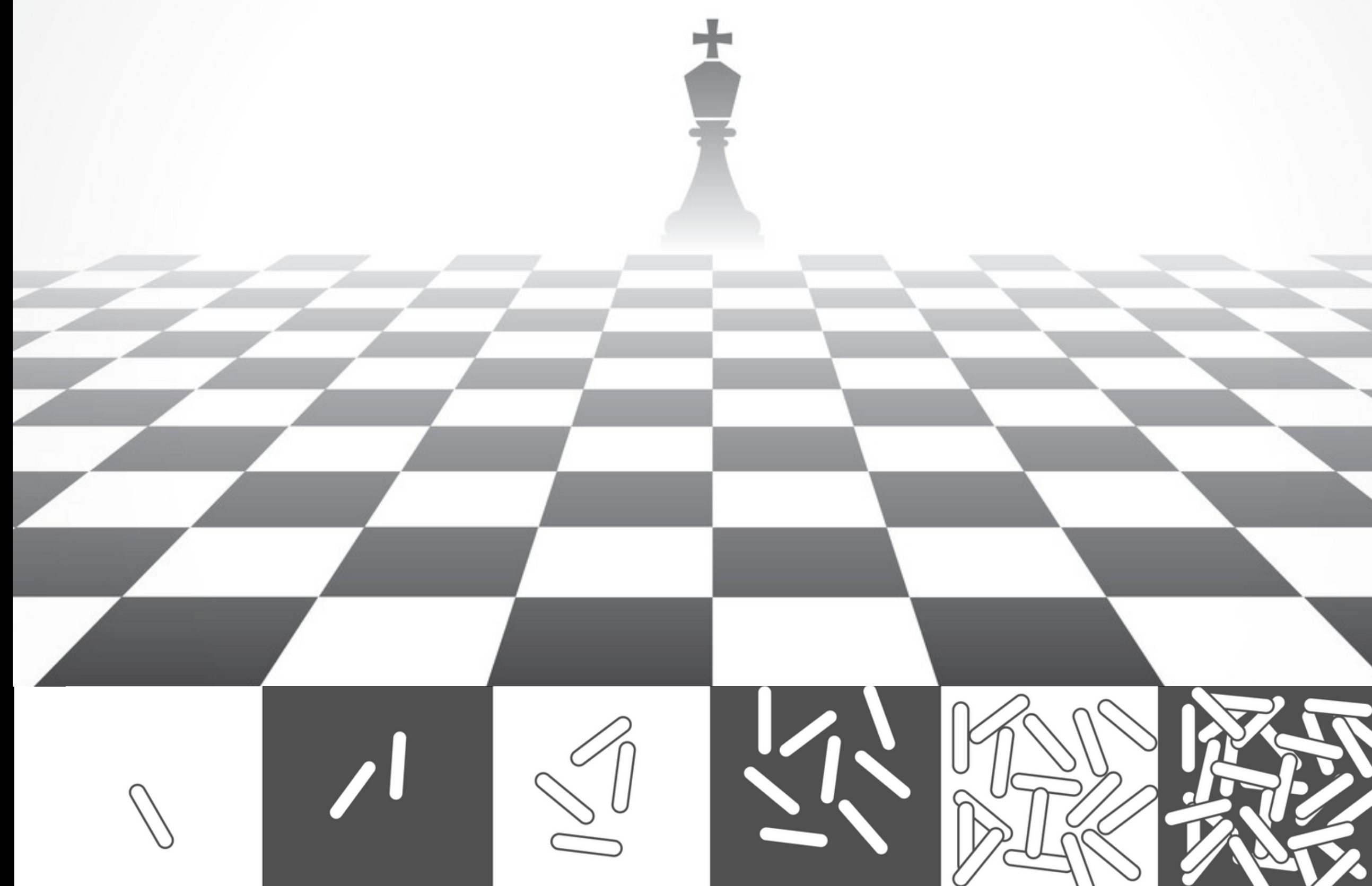
Paradoxical



Unintuitive

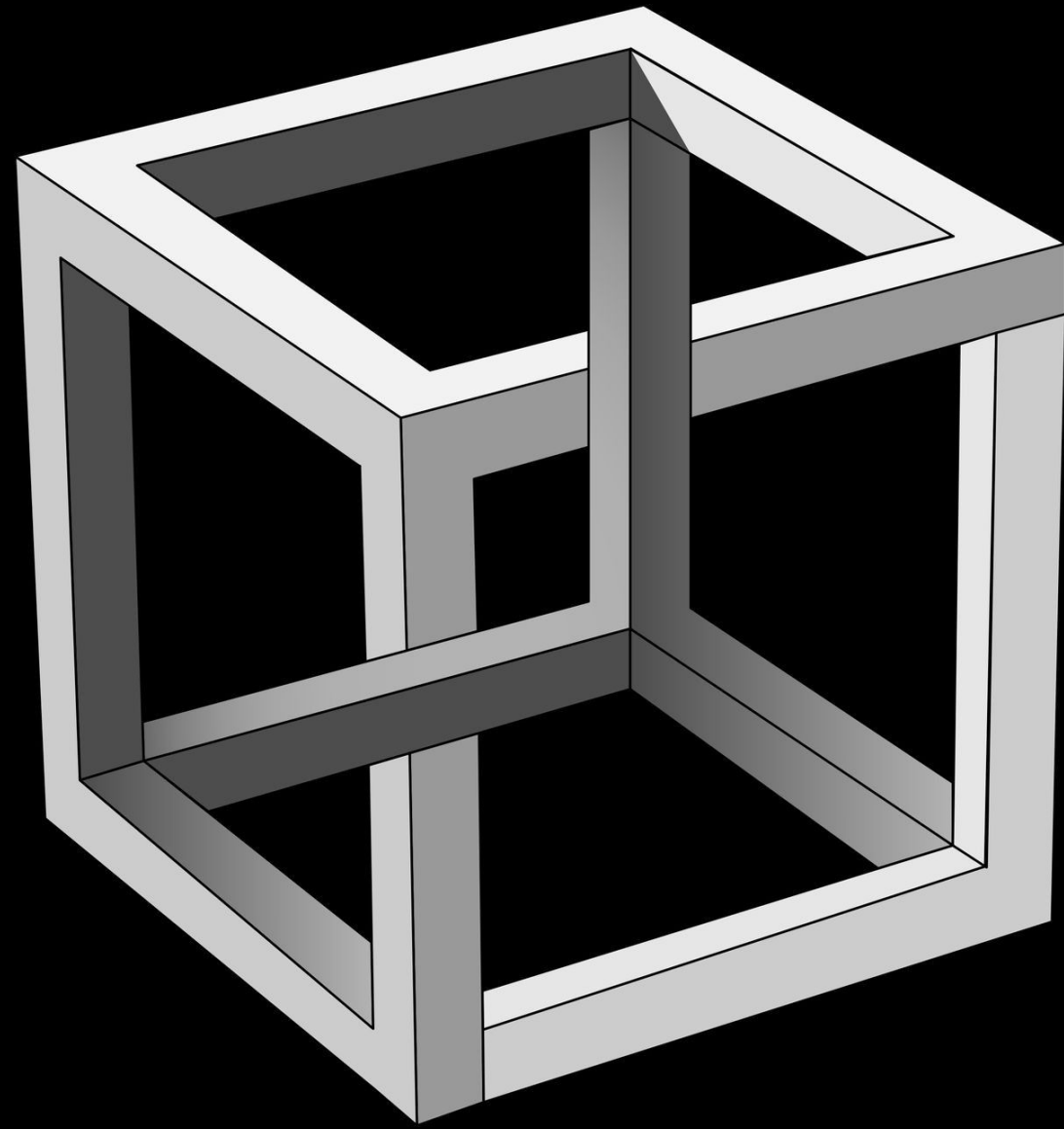


Paradoxical

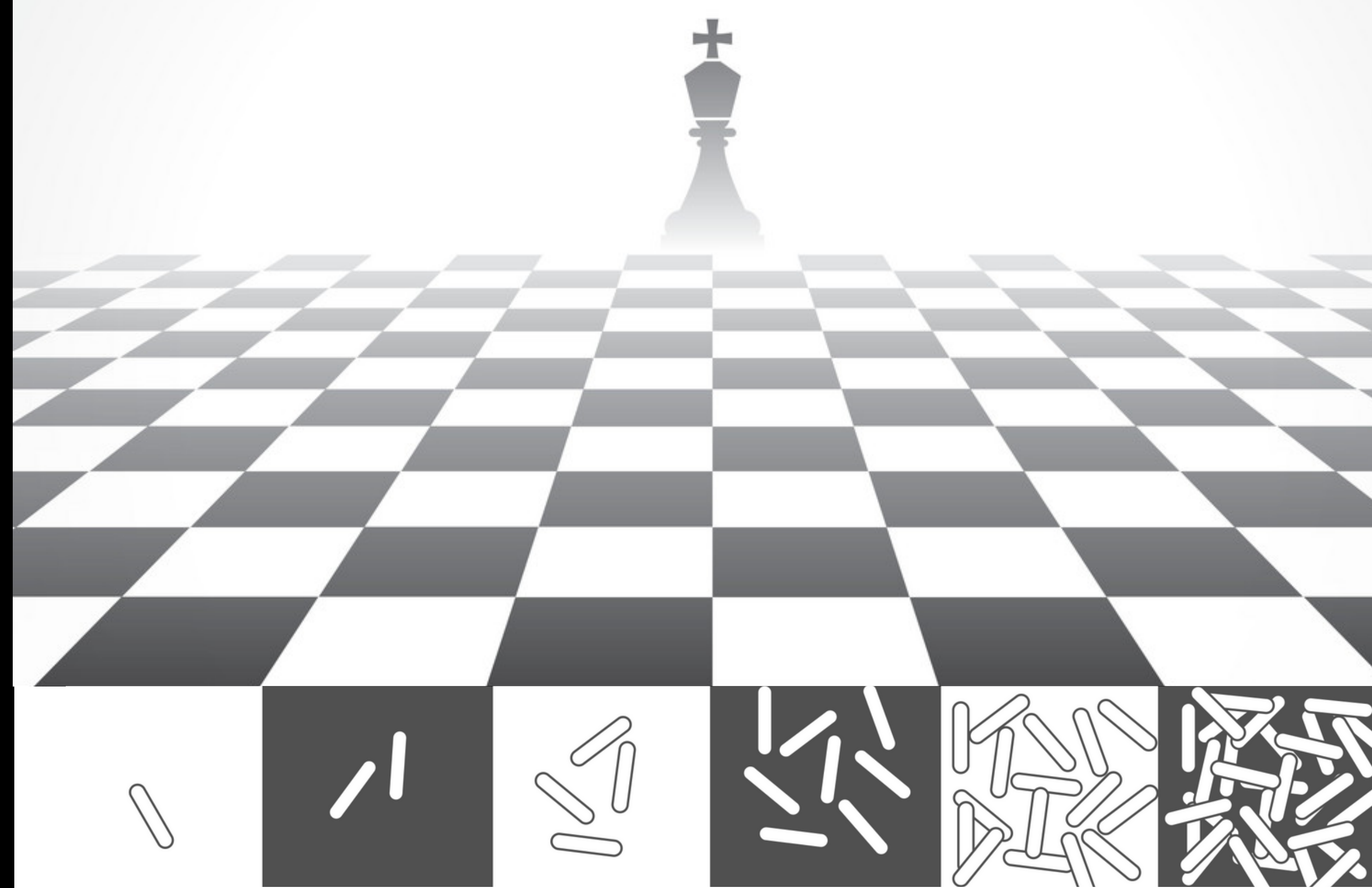


Unintuitive



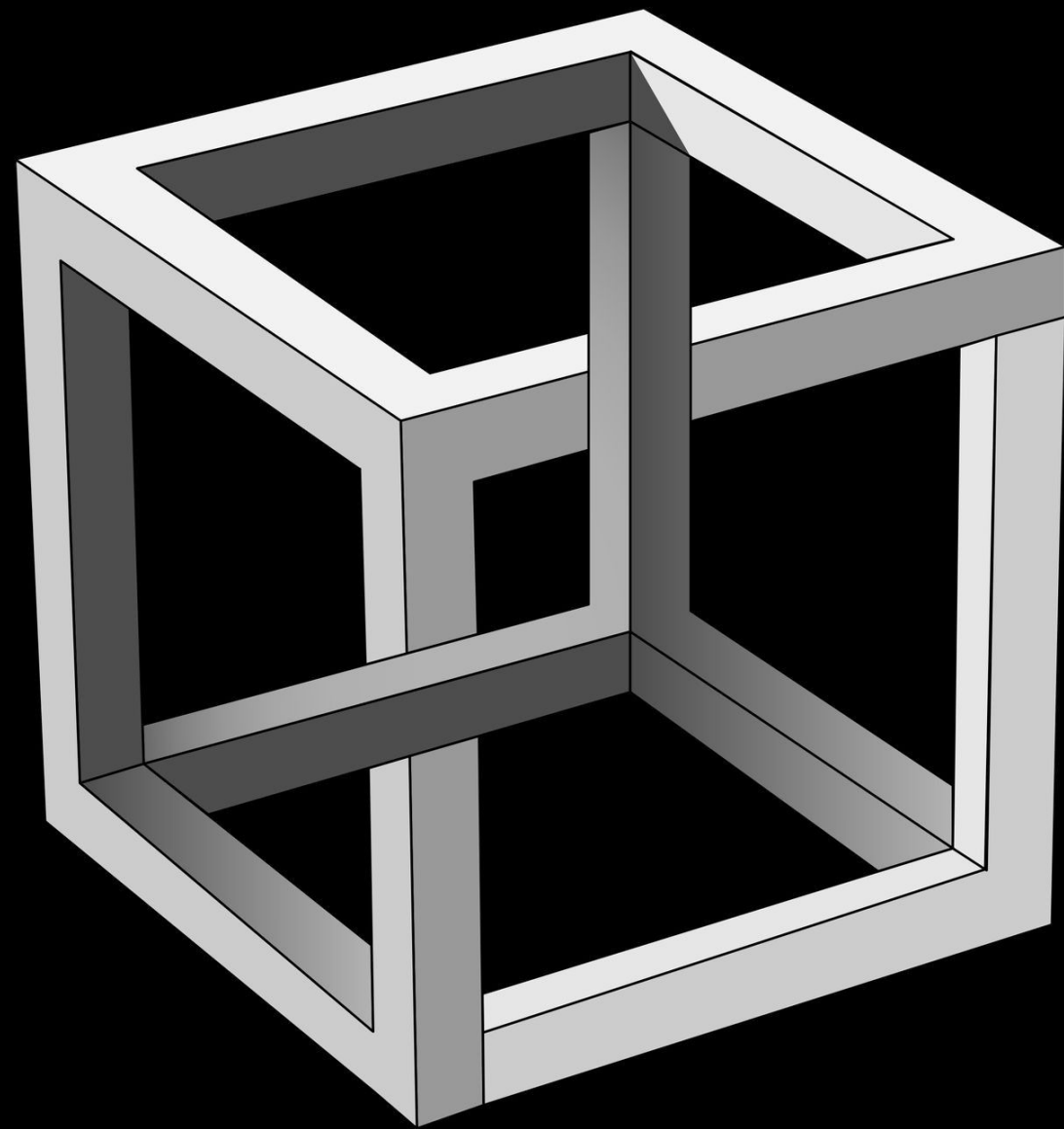


Paradoxical

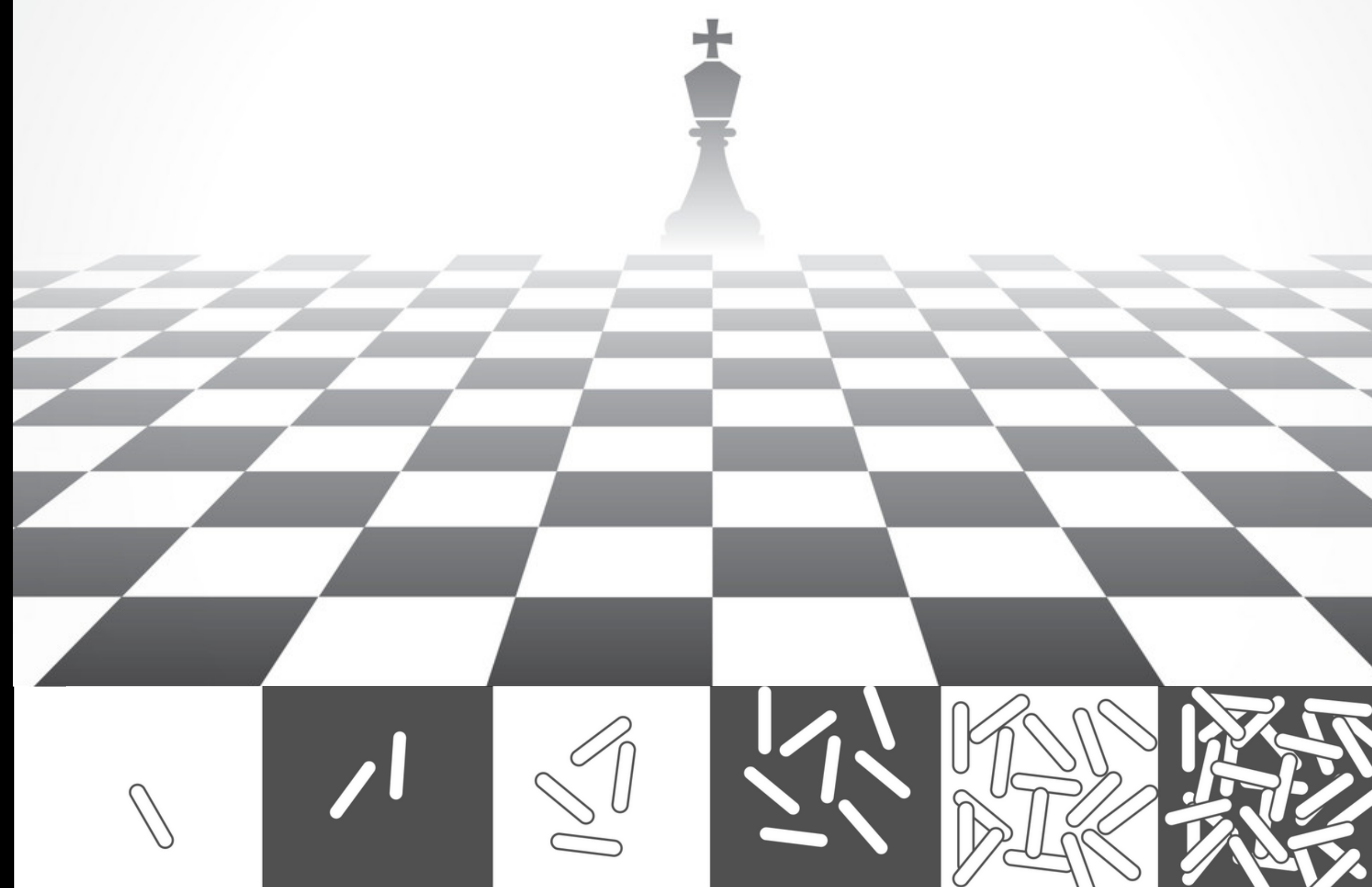


Unintuitive

~18 quintillion

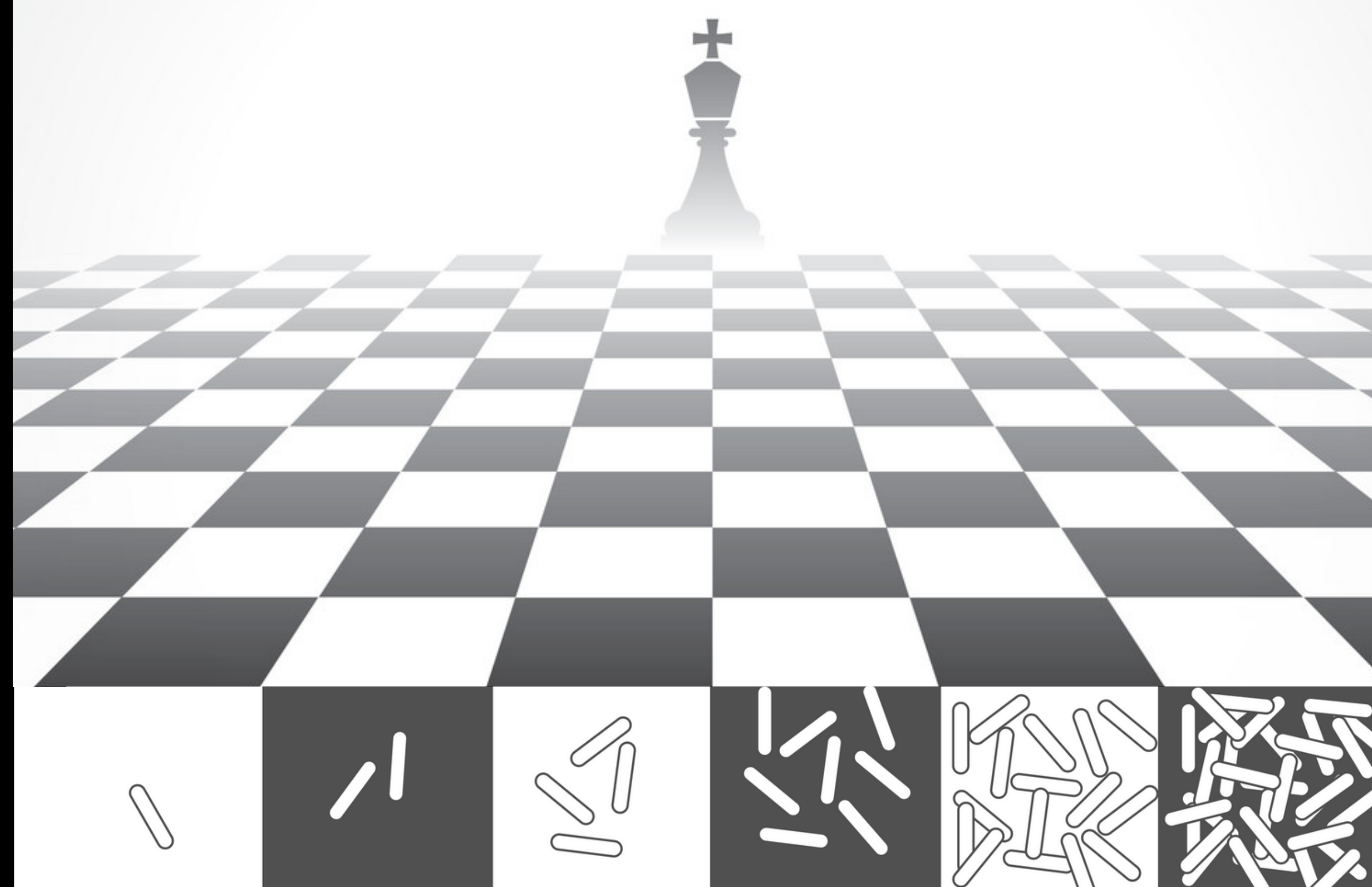
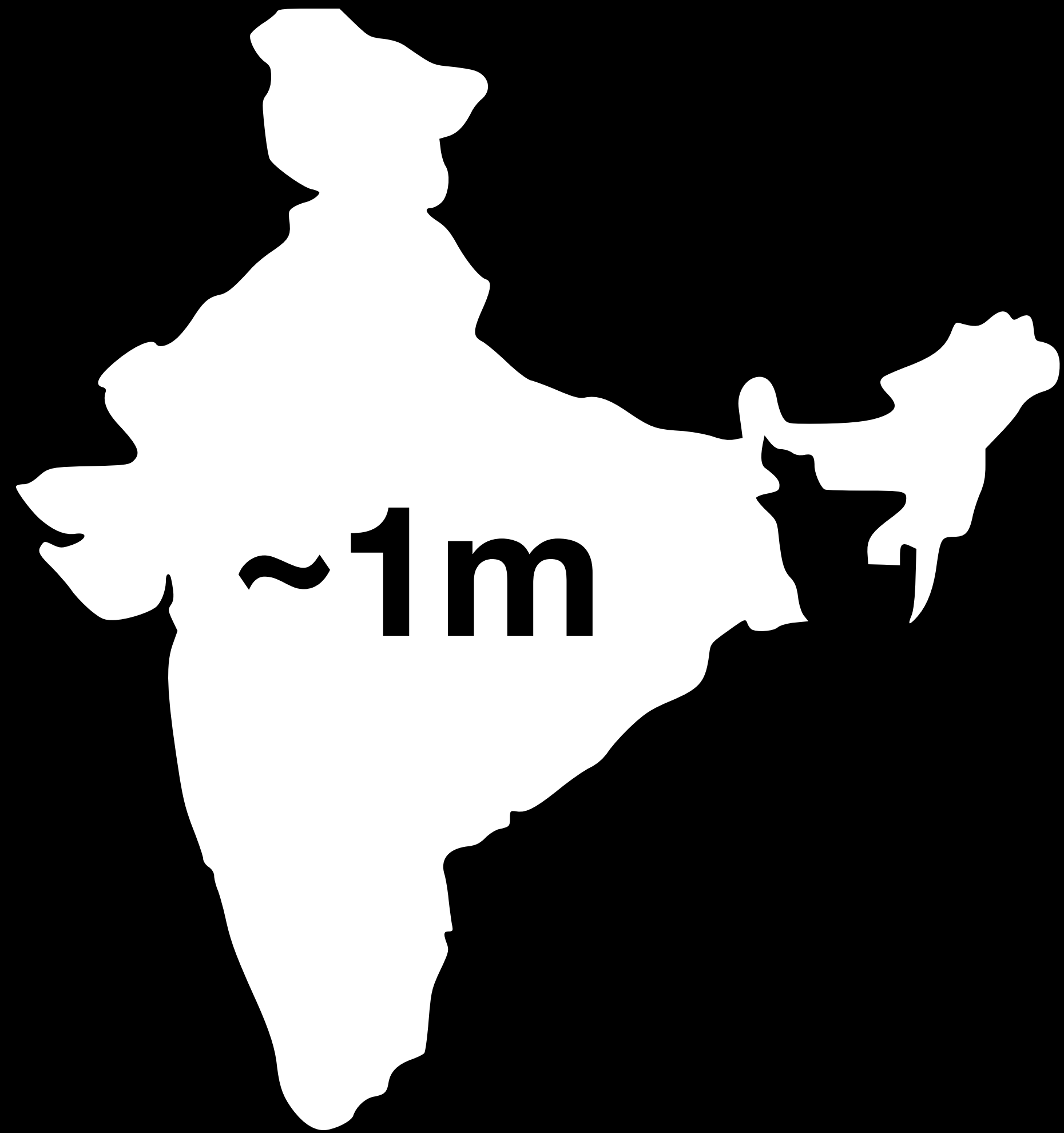


Paradoxical



Unintuitive

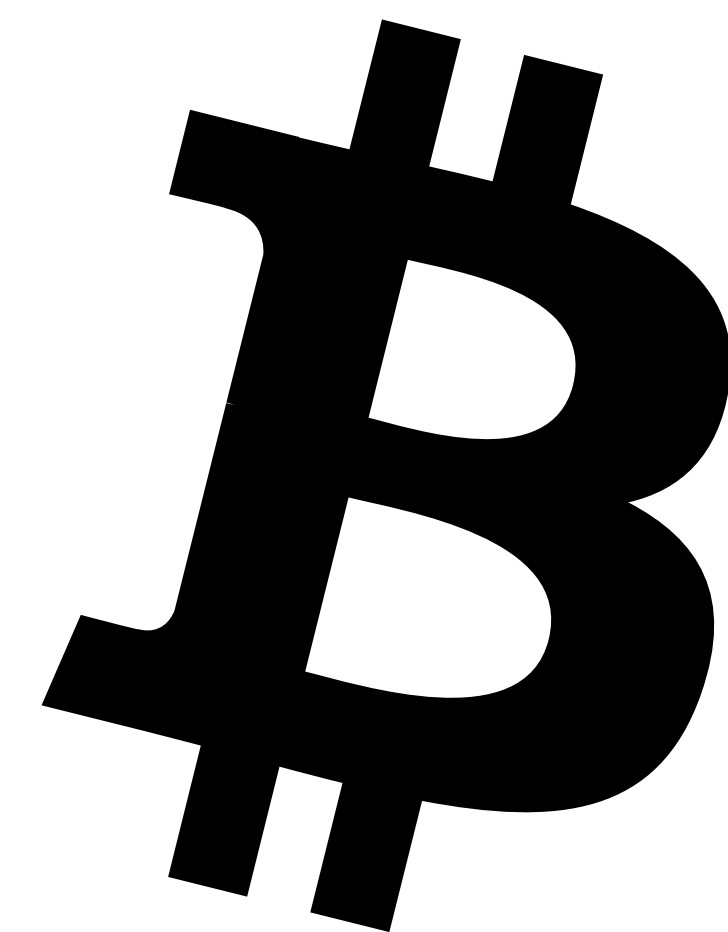
~210b tonnes
~18 quintillion



Unintuitive

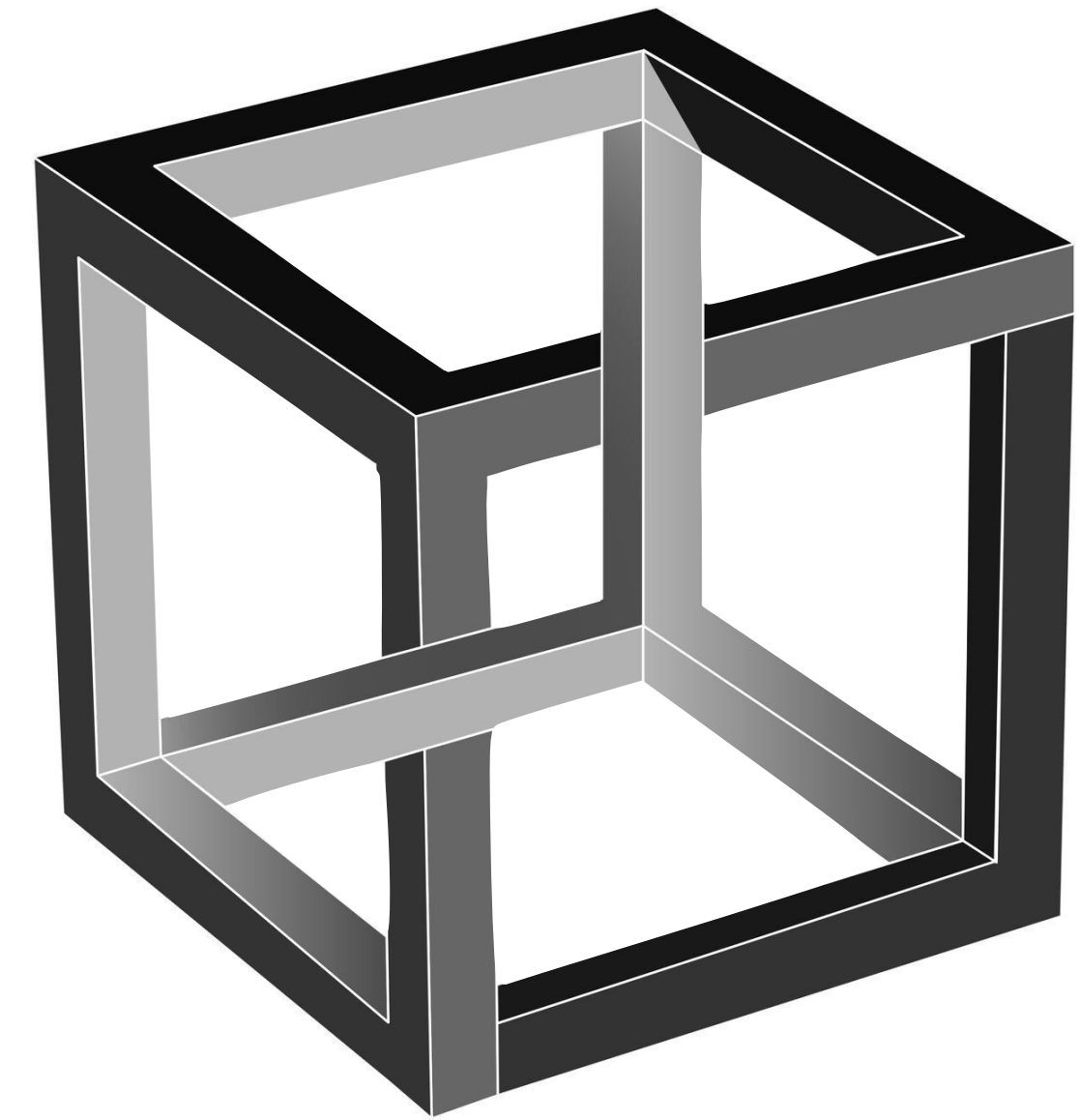
~210b tonnes
~18 quintillion

12
twelve
magic
words



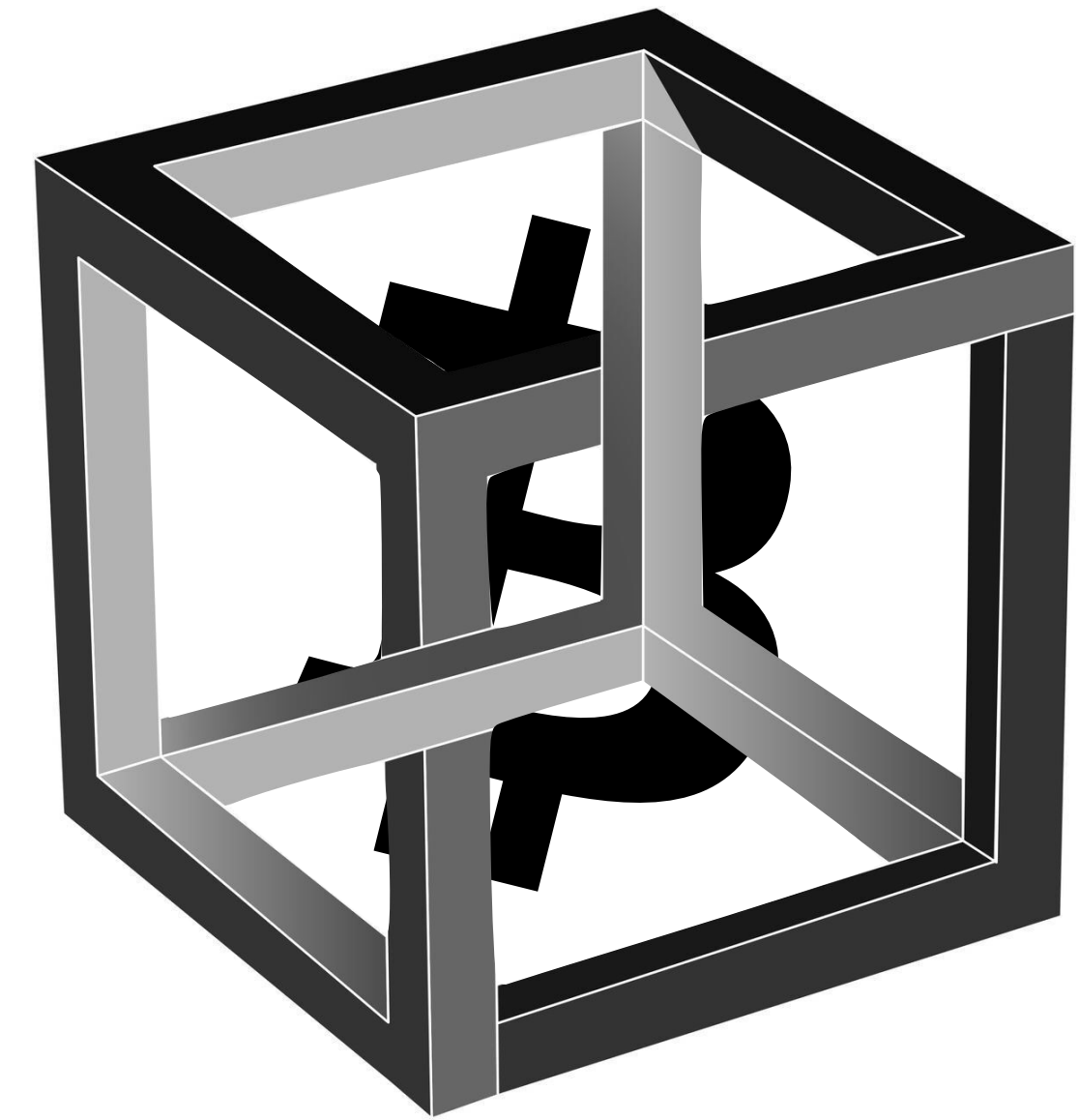
12

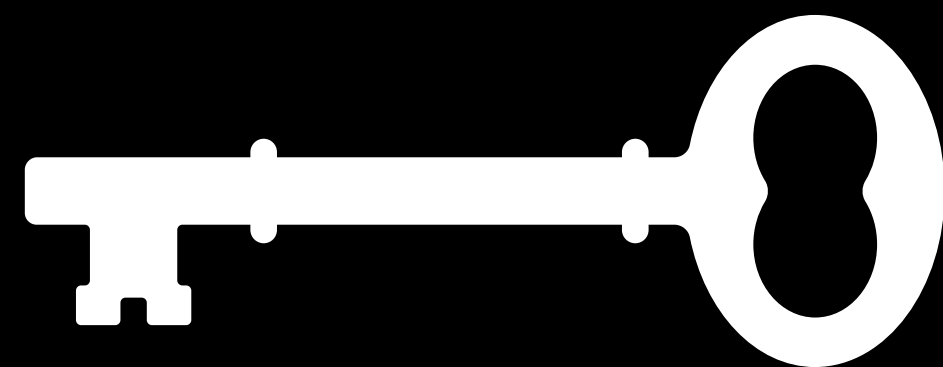
twelve
magic
words



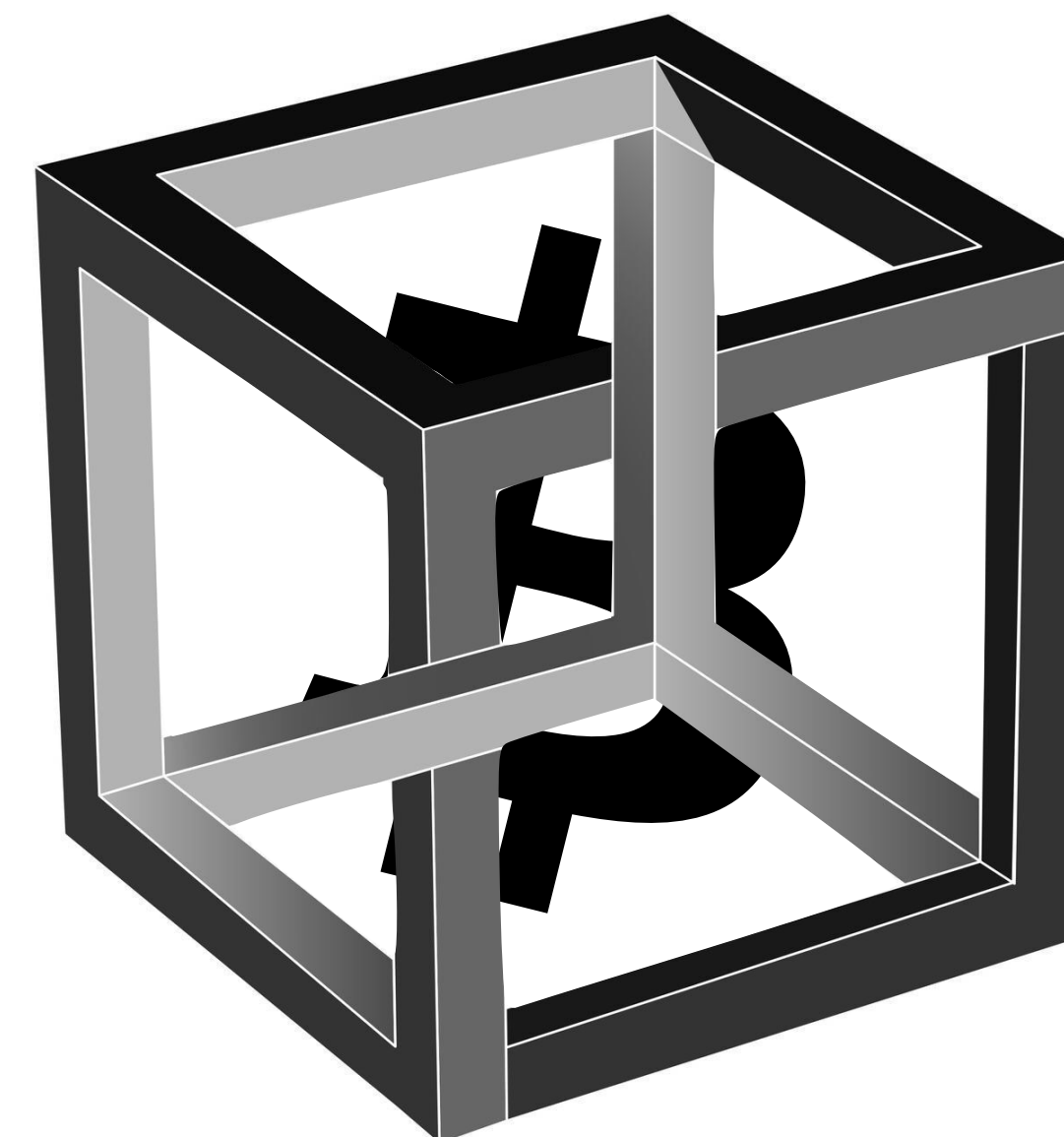
12

twelve
magic
words

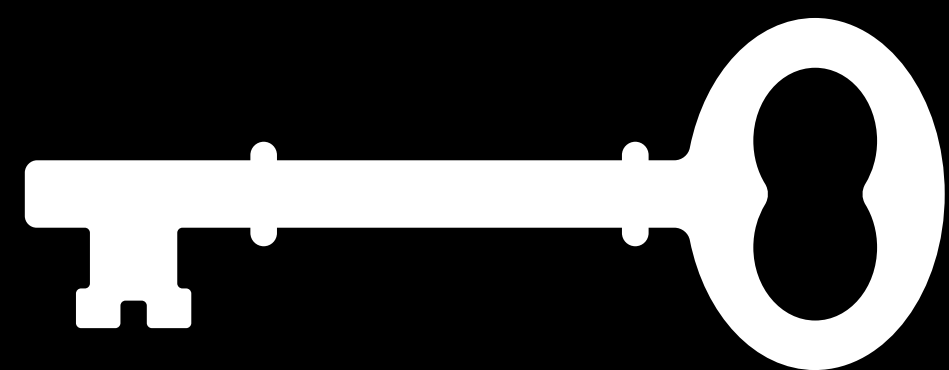




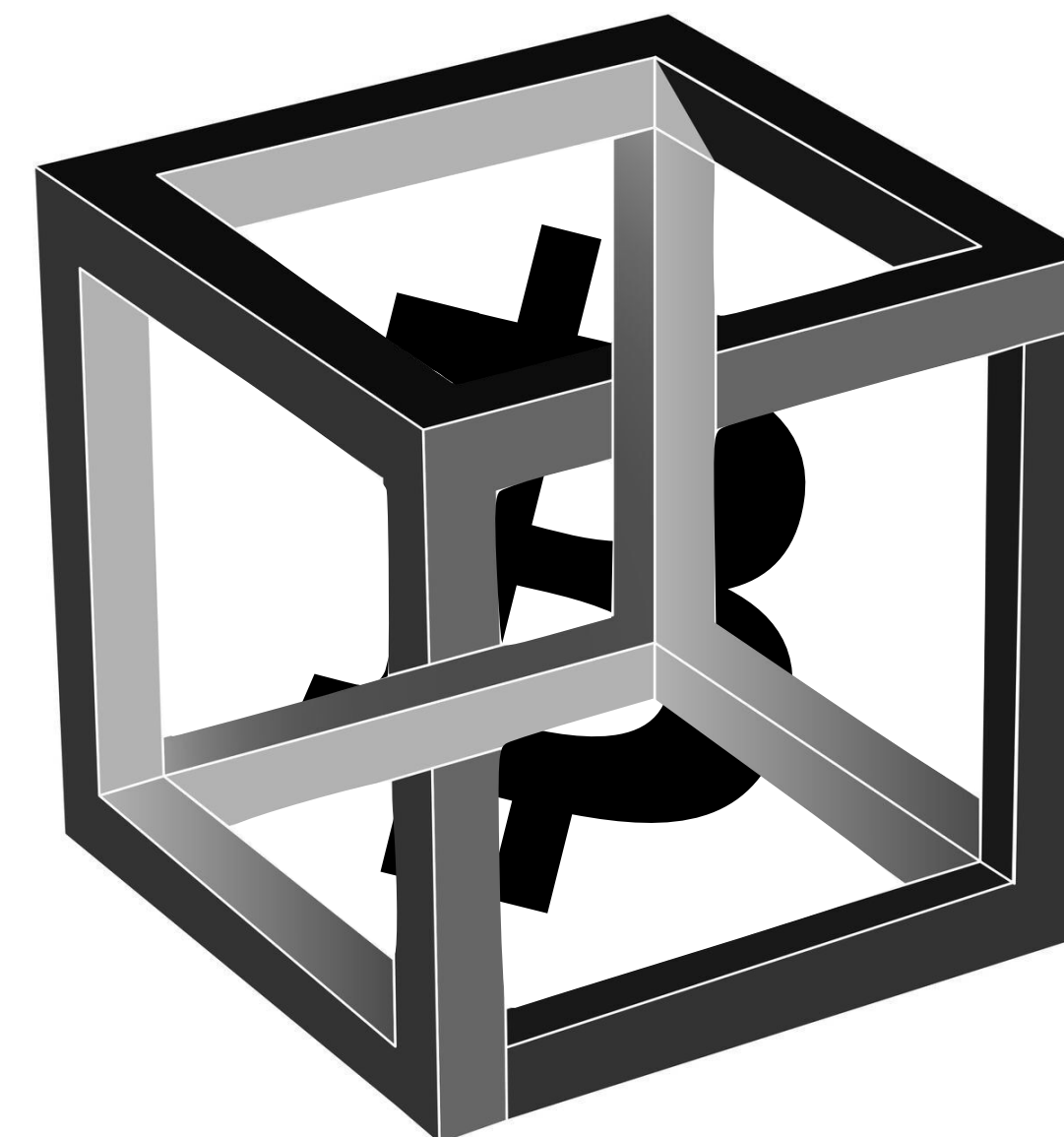
Private



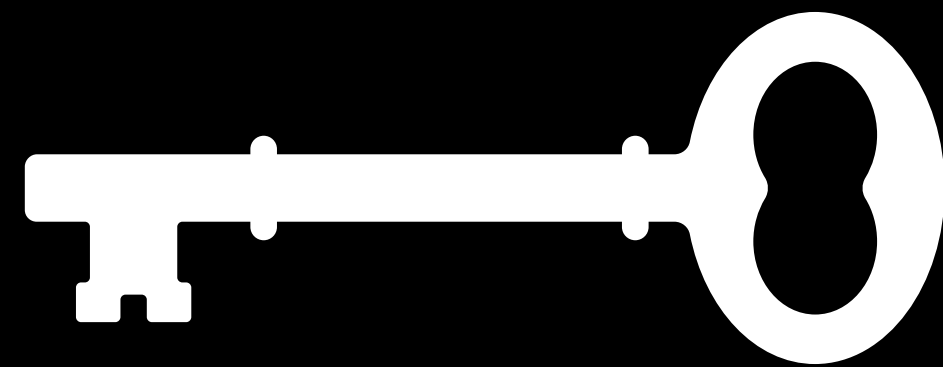
Locked



1,000,000 sats

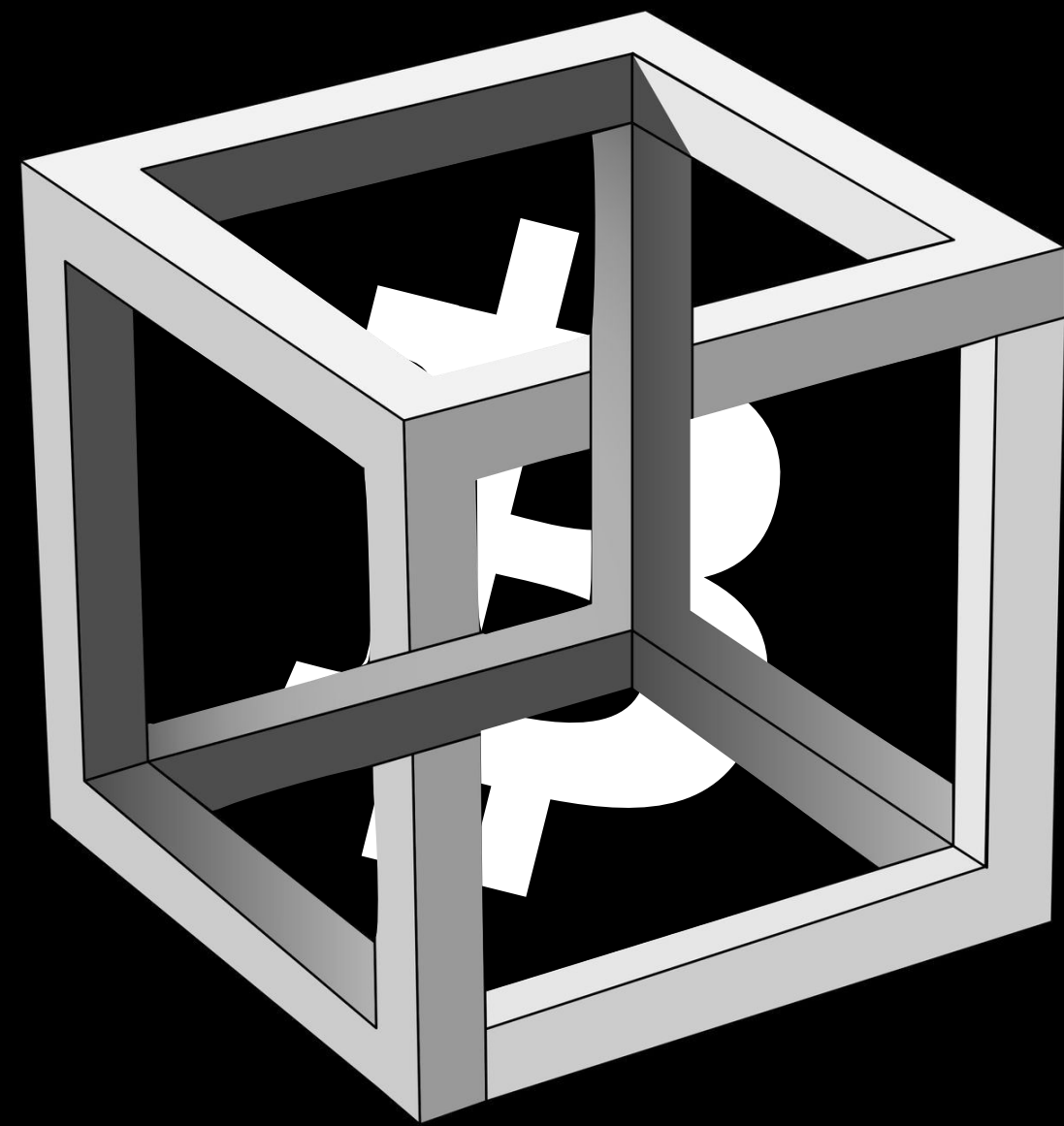


1,000,000 sats



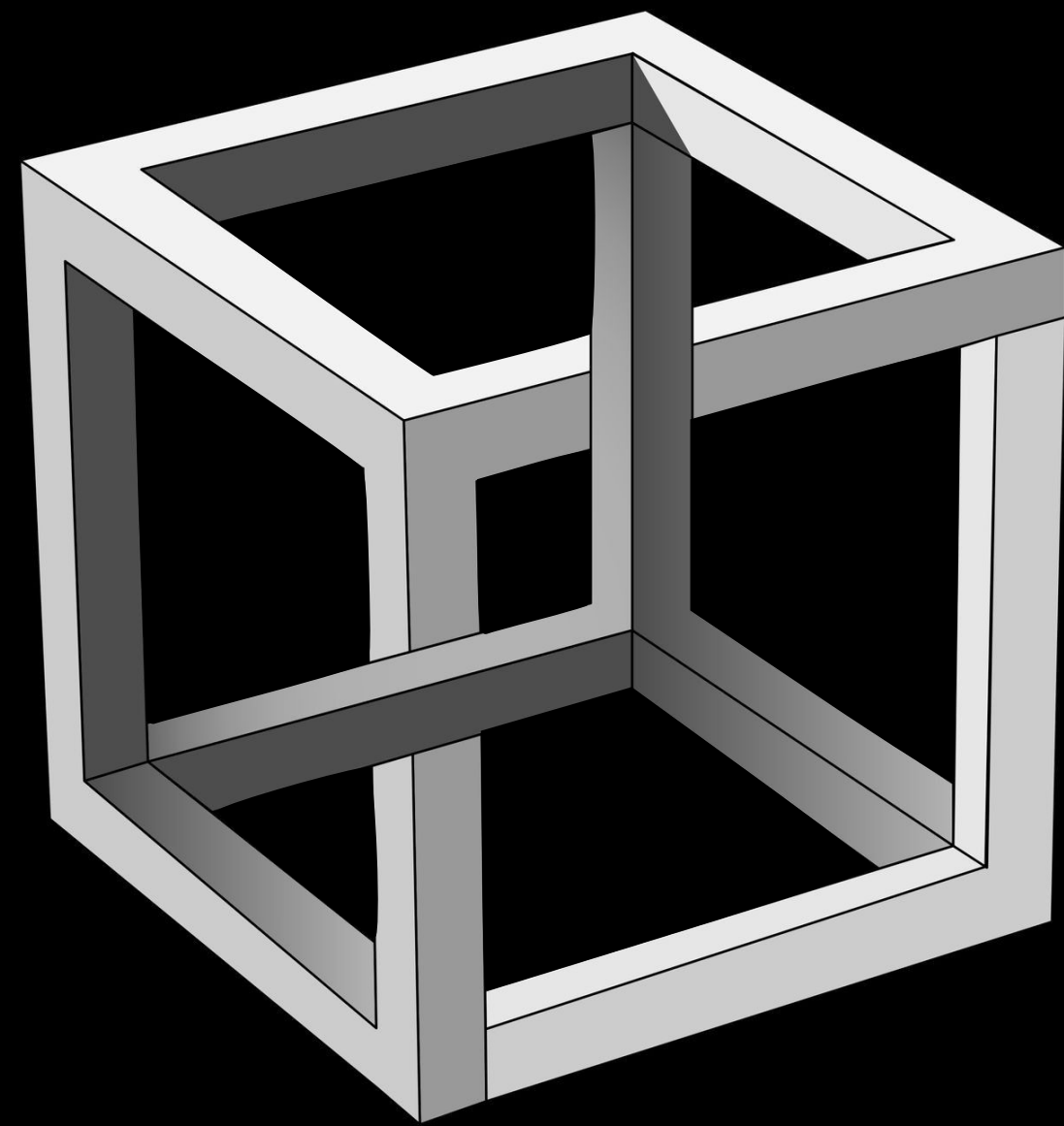
1,000,000 sats

**pattern
hour
video
shed
umbrella
today
they
alcohol
belt
shoe
oppose
smooth**



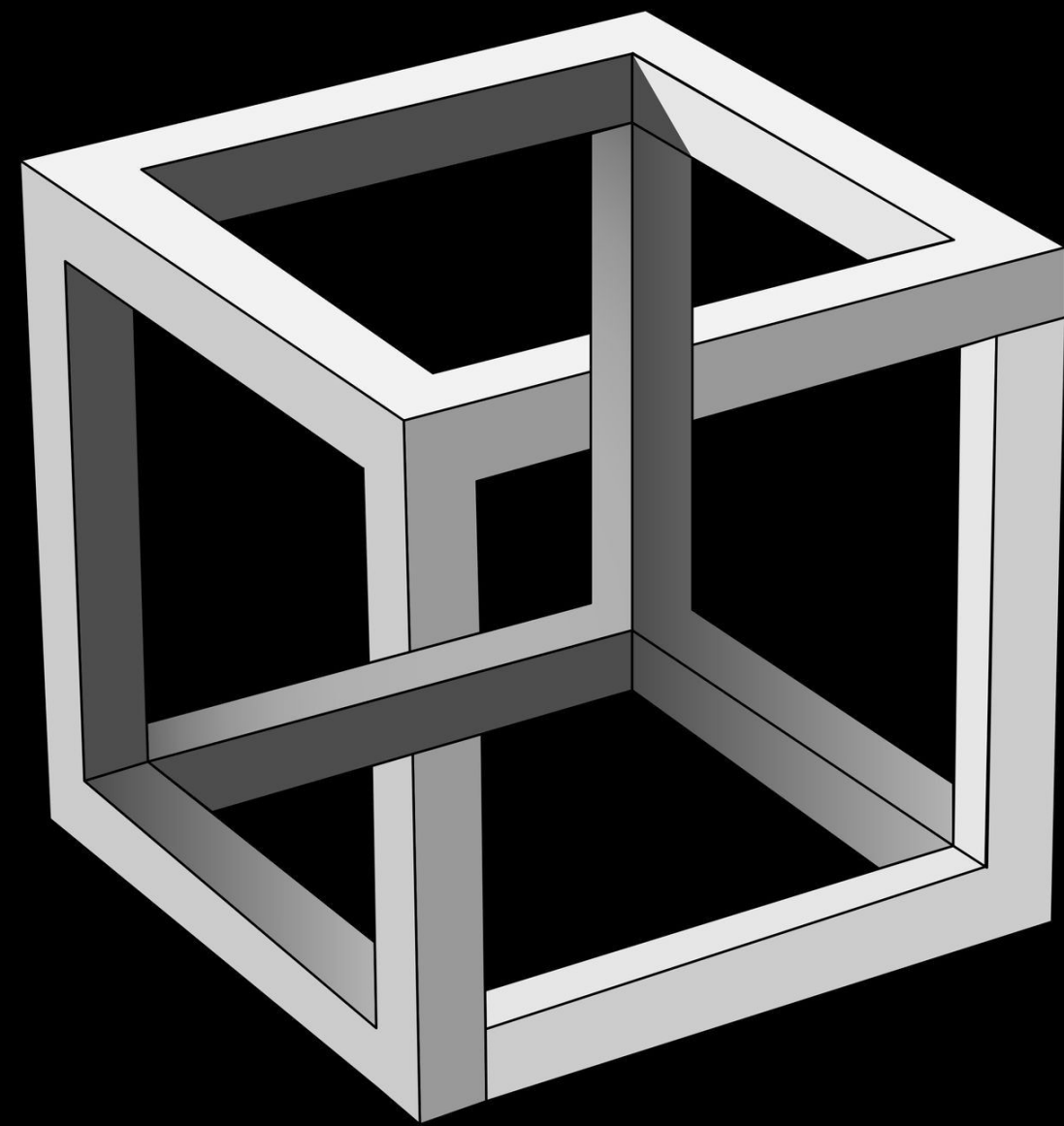
1,000,000 sats

**pattern
hour
video
shed
umbrella
today
they
alcohol
belt
shoe
oppose
smooth**



1,000,000 sats

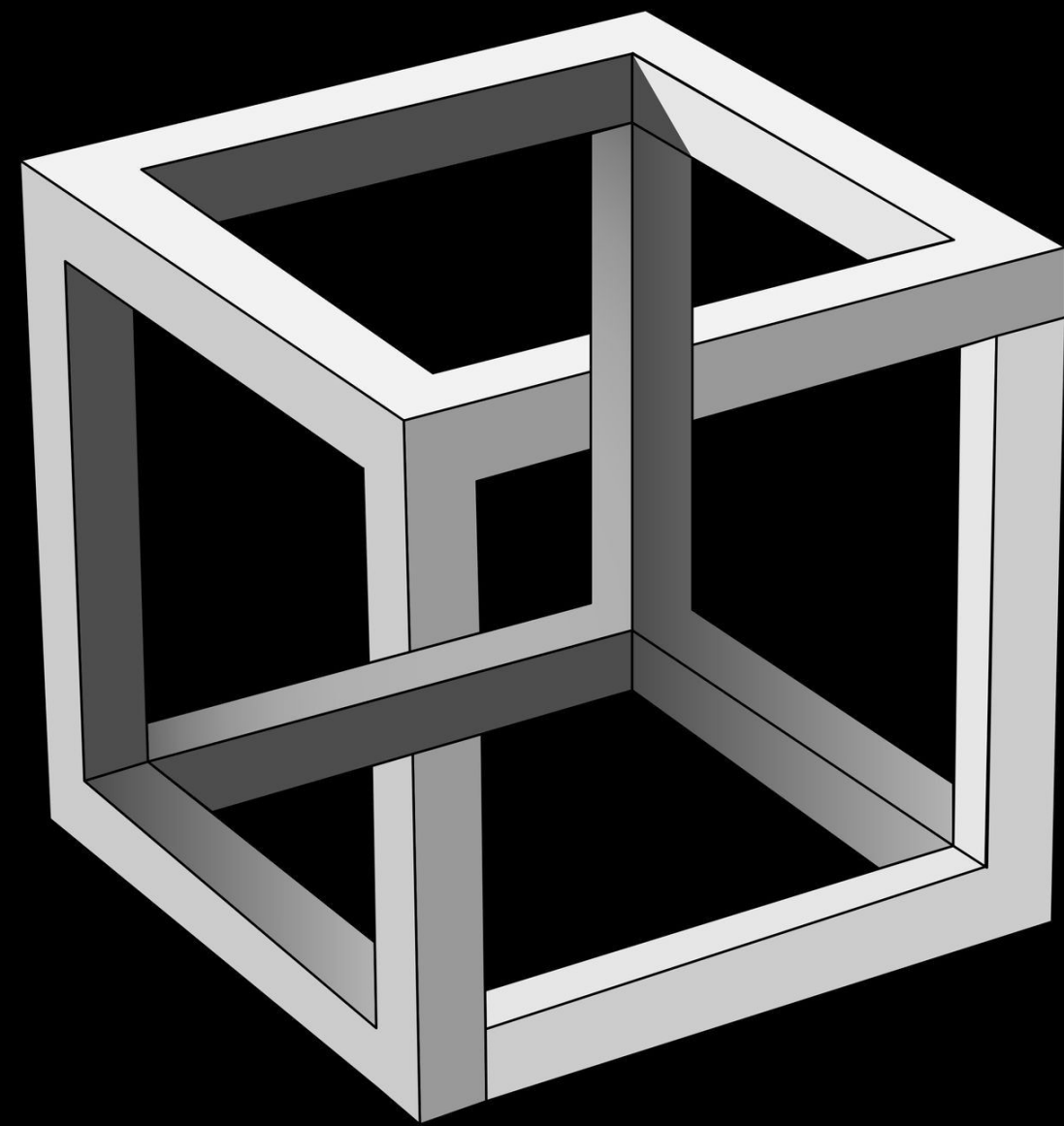
**pattern
hour
video
shed
umbrella
today
they
alcohol
belt
shoe
oppose
smooth**



1,000,000 sats

100%

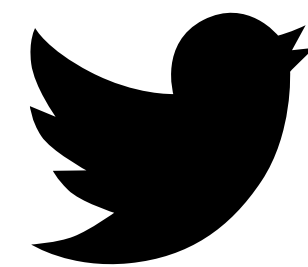
Gone.



1,000,000 sats

100%

Gone.



12
twelve
magic
words

Secure?

12

twelve
magic
words

2048¹²

12

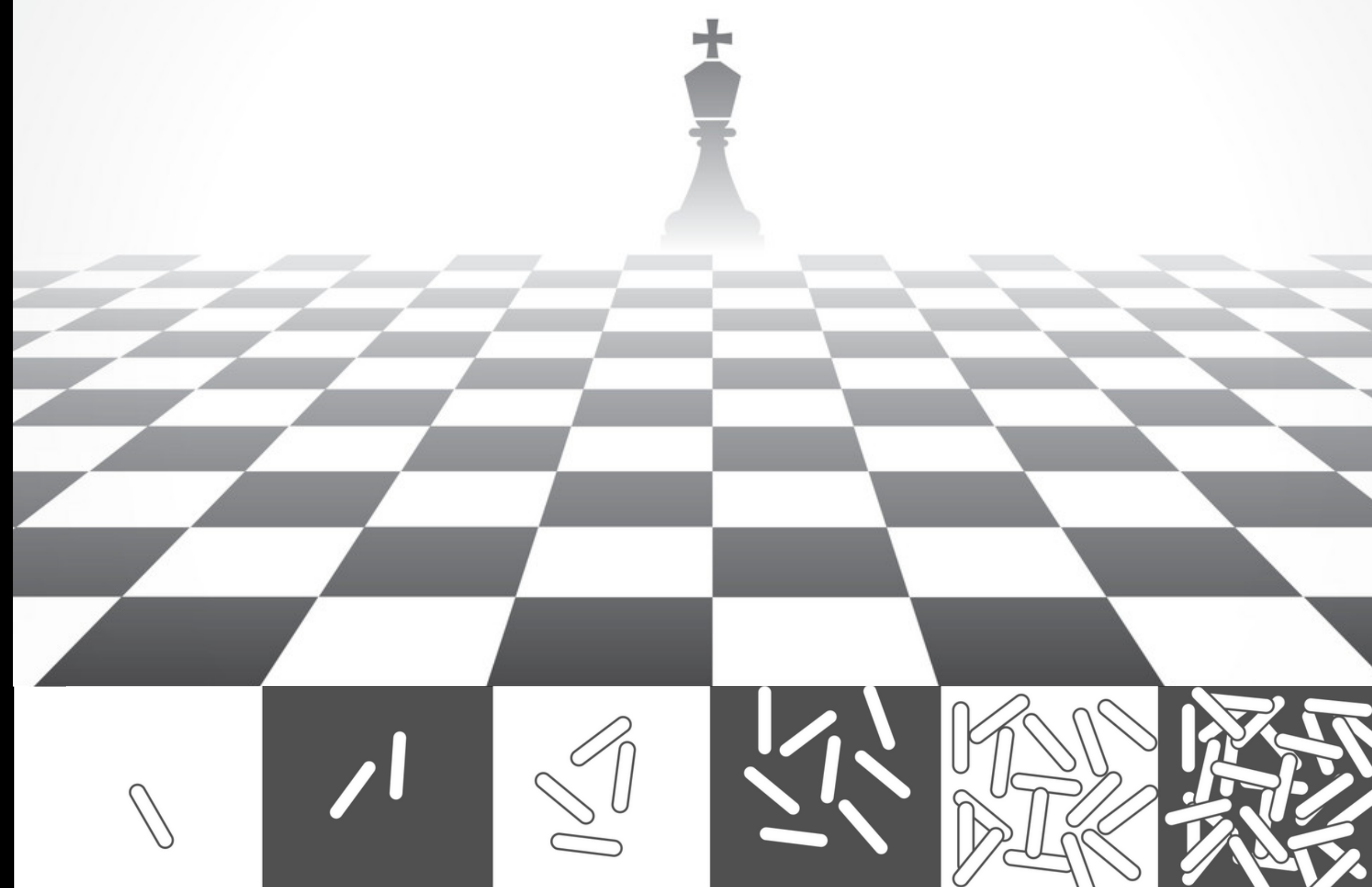
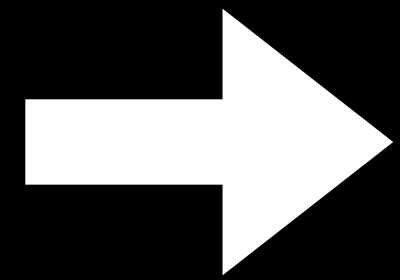
twelve
magic
words

$\sim 2^{128}$

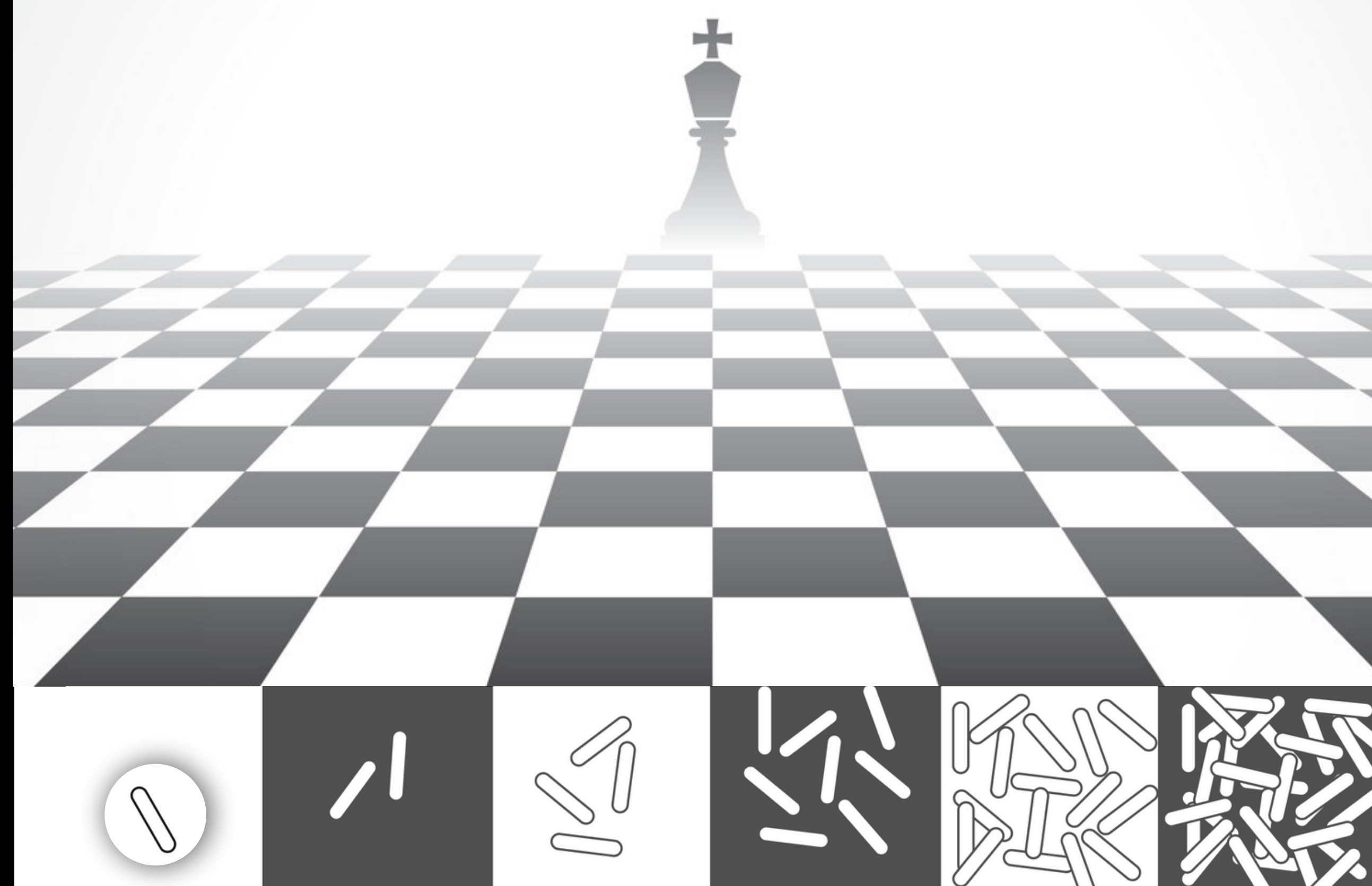
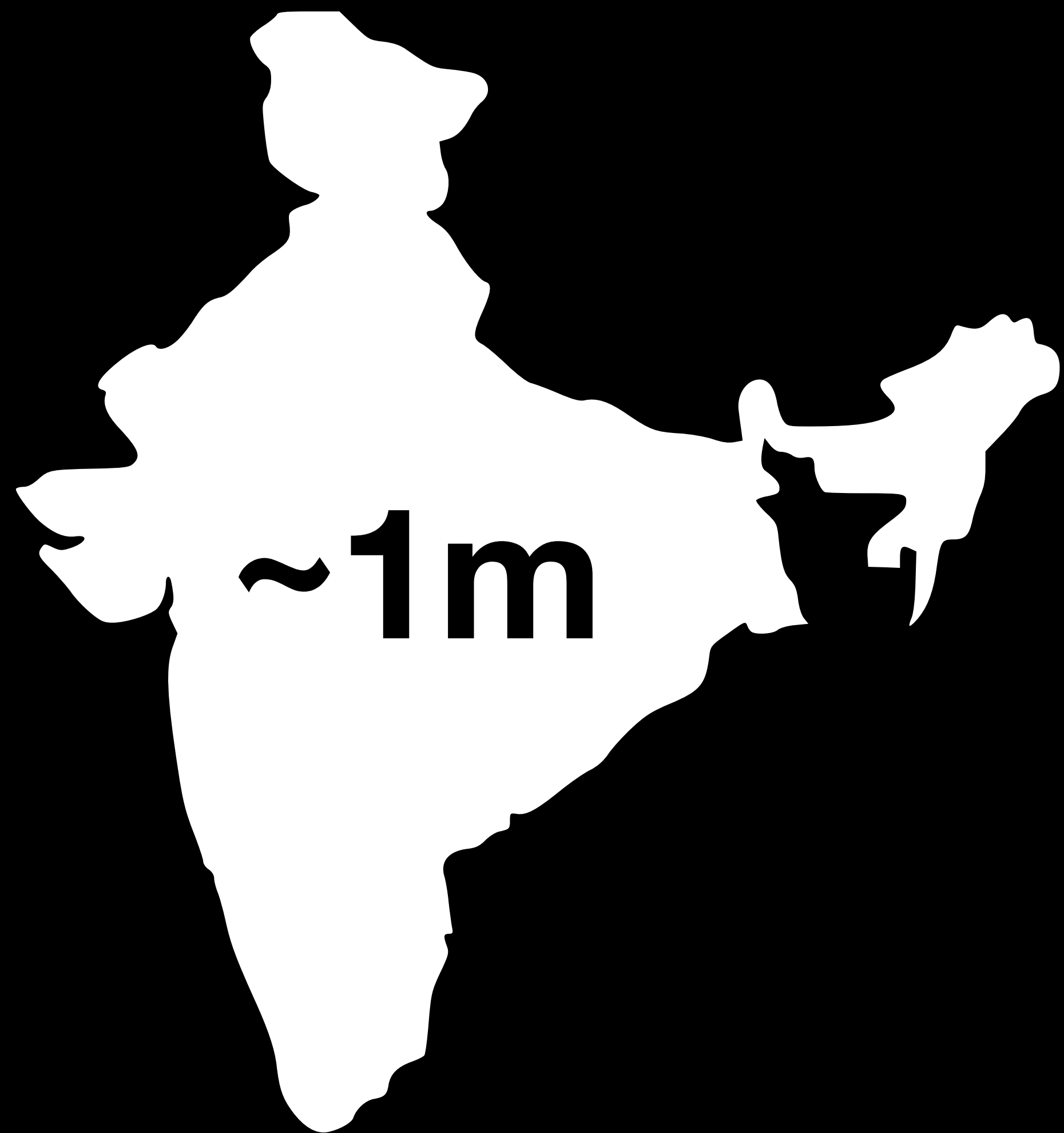
340 undecillion
282 decillion
366 nonillion
920 octillion
938 septillion
463 sextillion
463 quintillion
374 quadrillion
607 trillion
431 billion
768 million
211 thousand
456

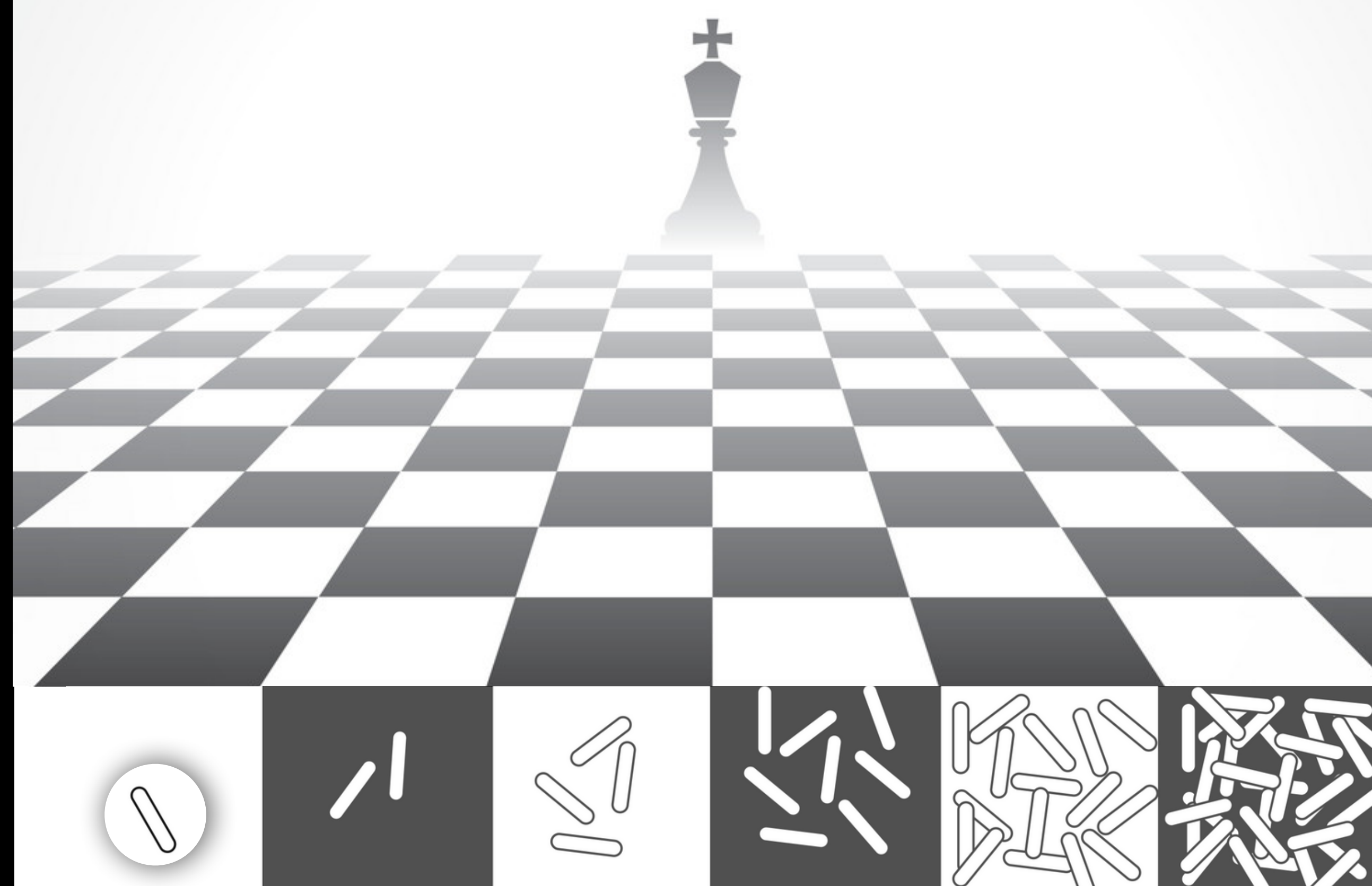
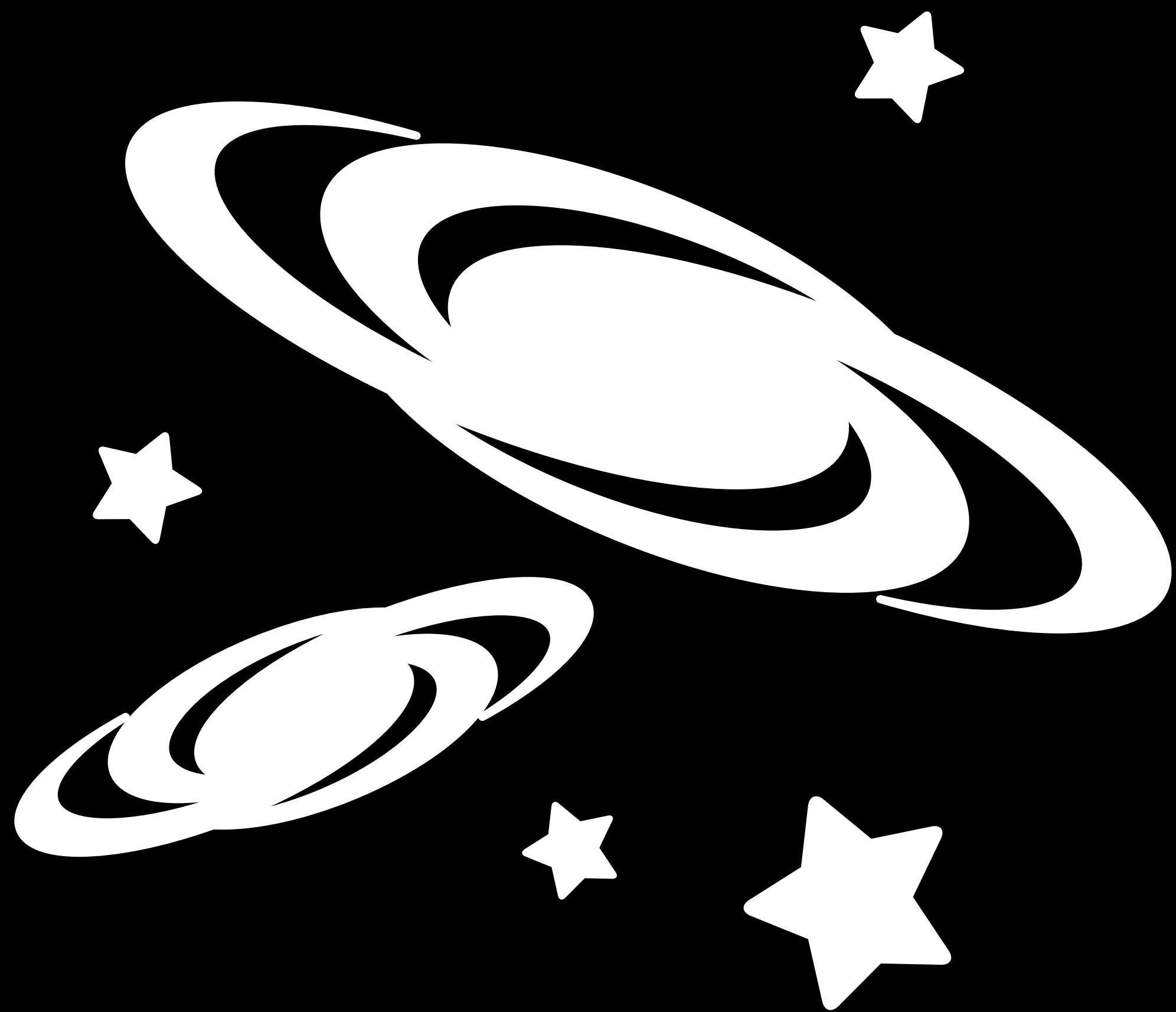
$$\sim 2^{128}$$

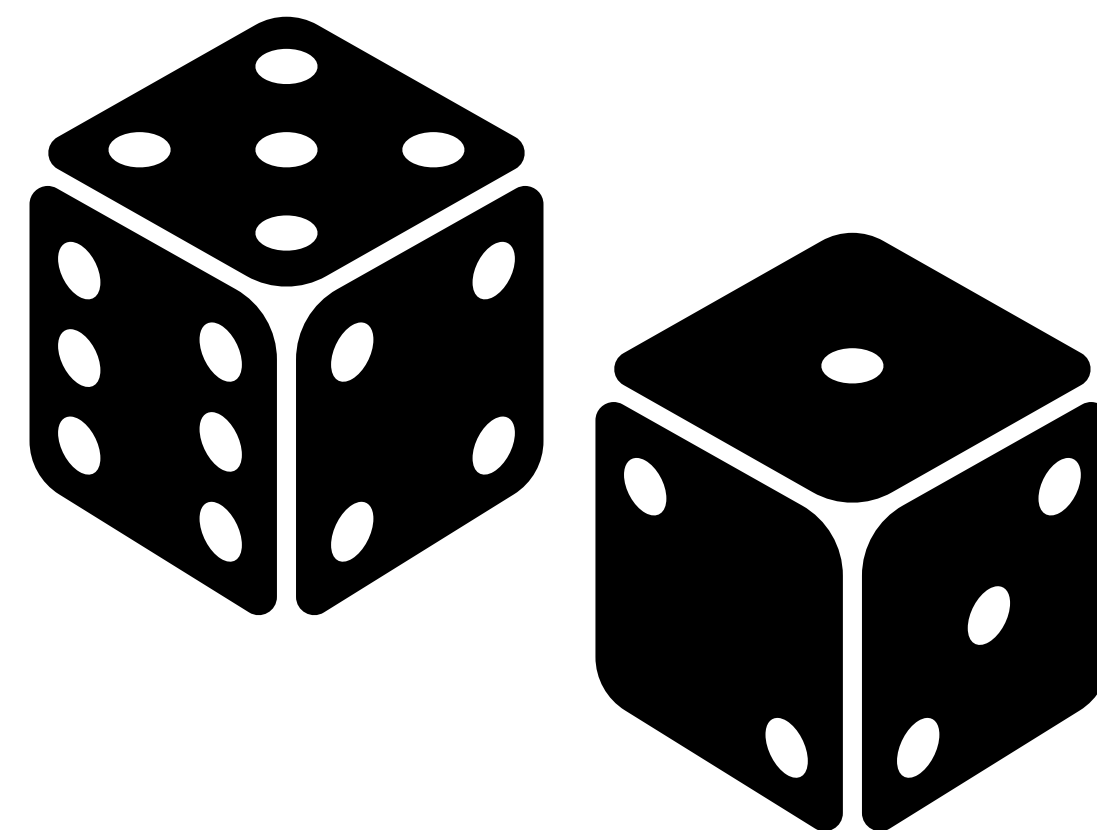
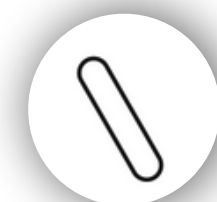
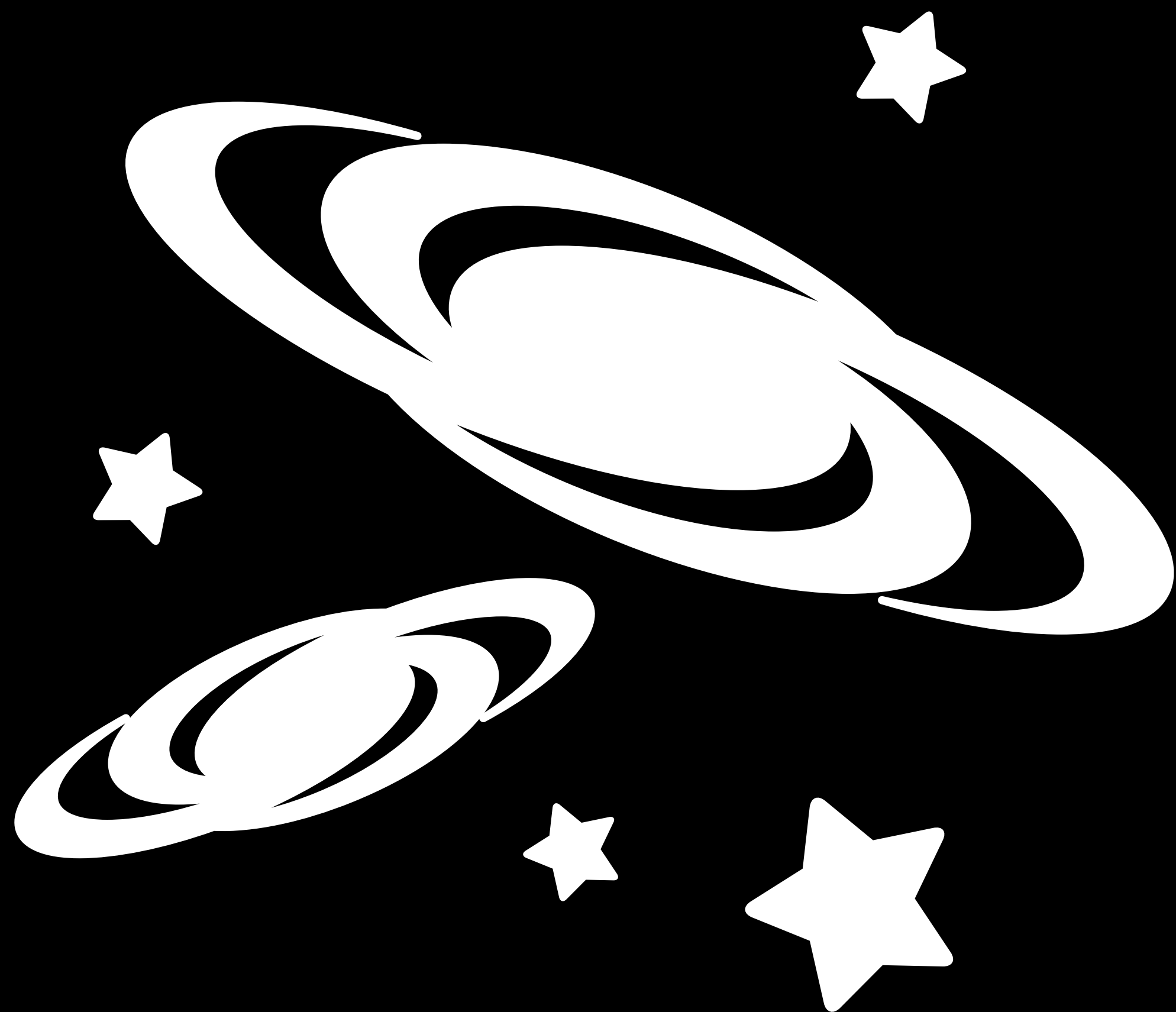
**340 undecillion
282 decillion
366 nonillion
920 octillion
938 septillion
463 sextillion
463 quintillion
374 quadrillion
607 trillion
431 billion
768 million
211 thousand
456**



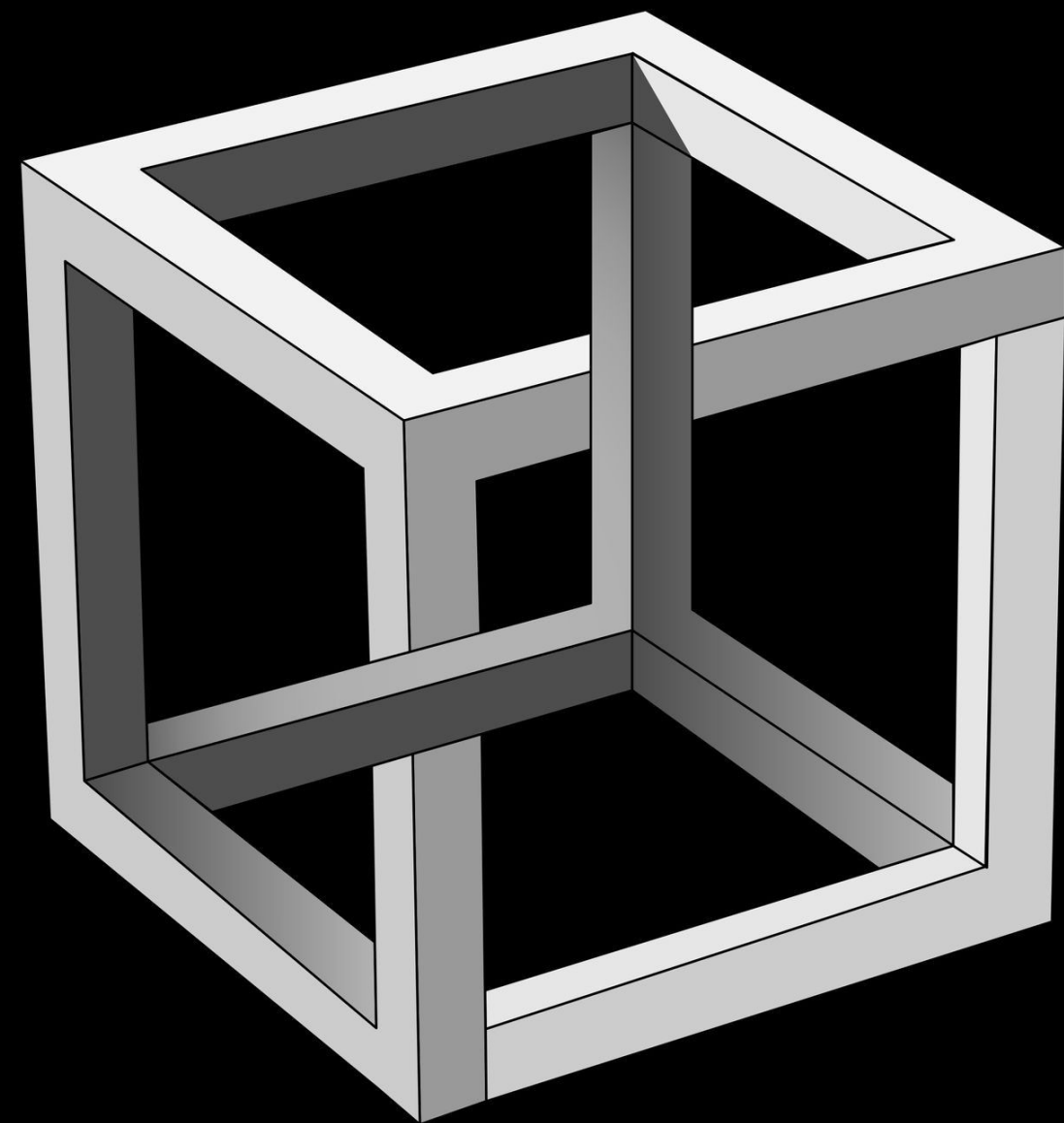
>18 quintillion



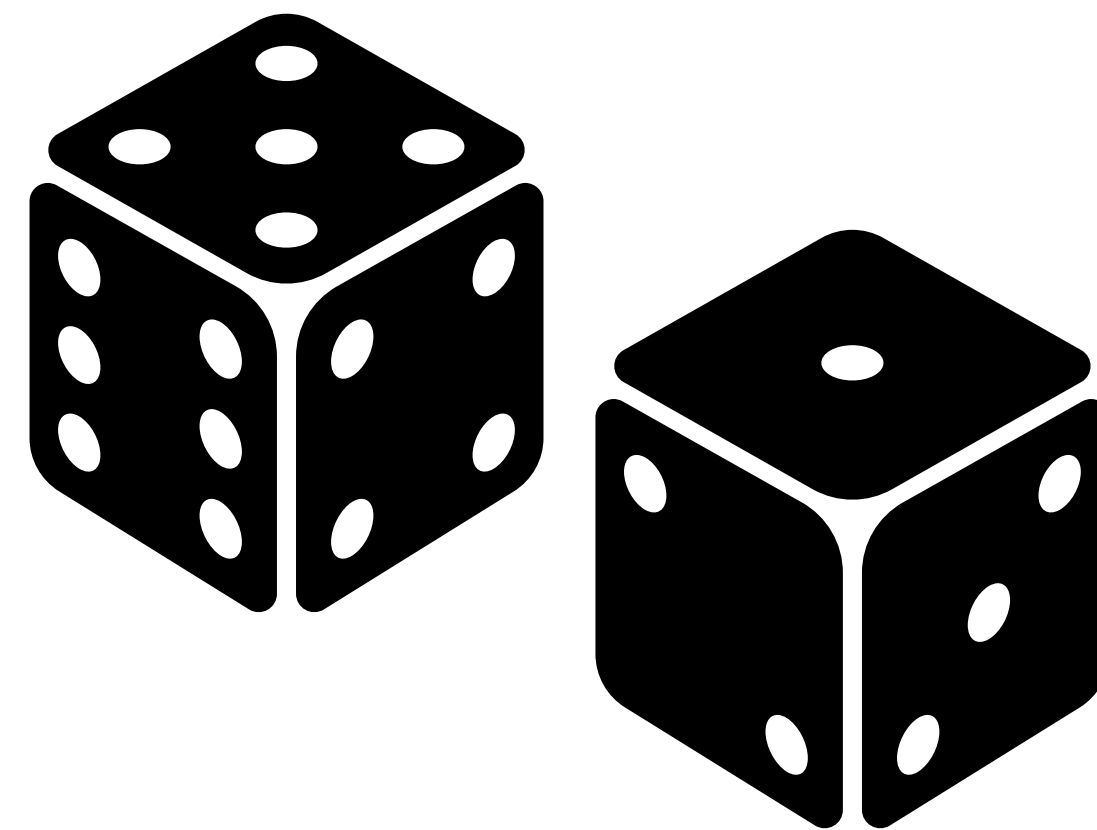




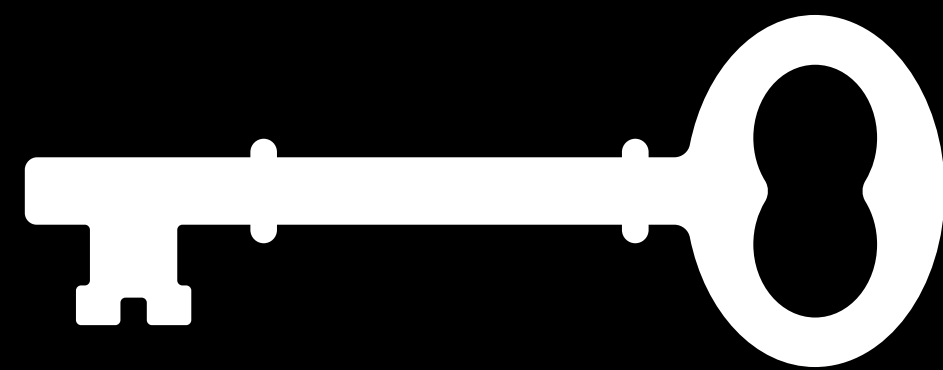
Random



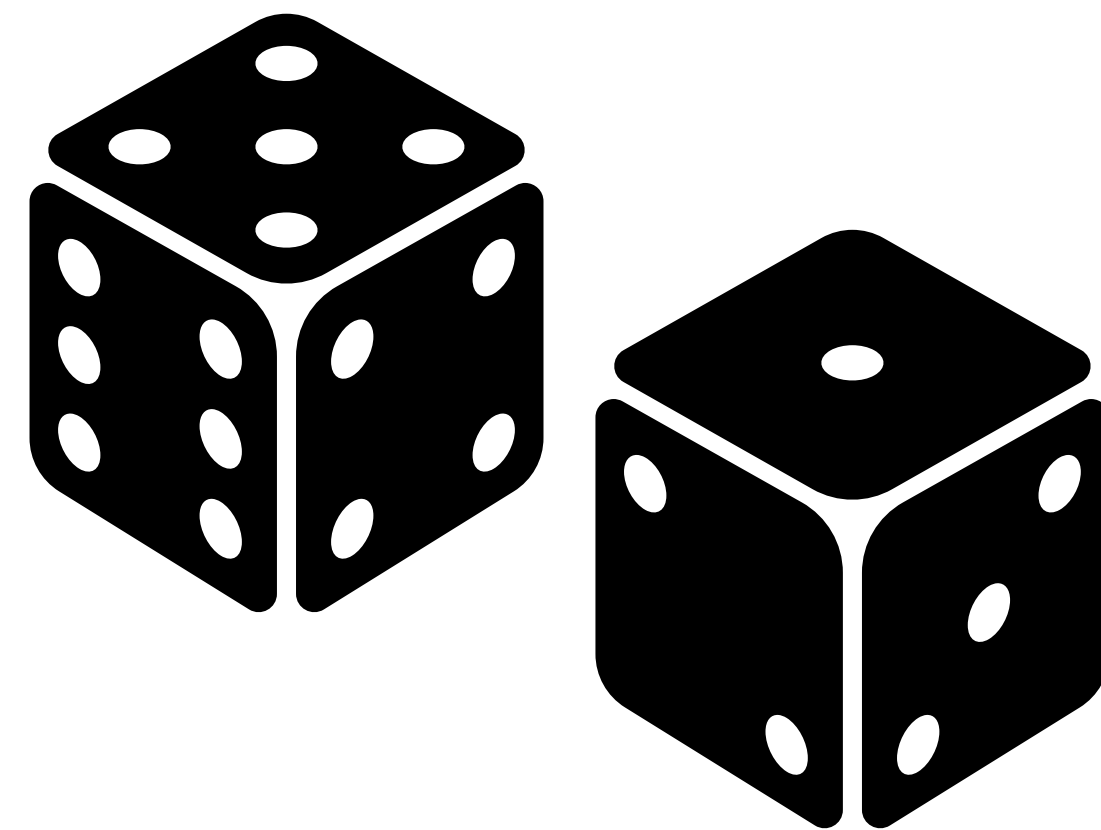
Secure



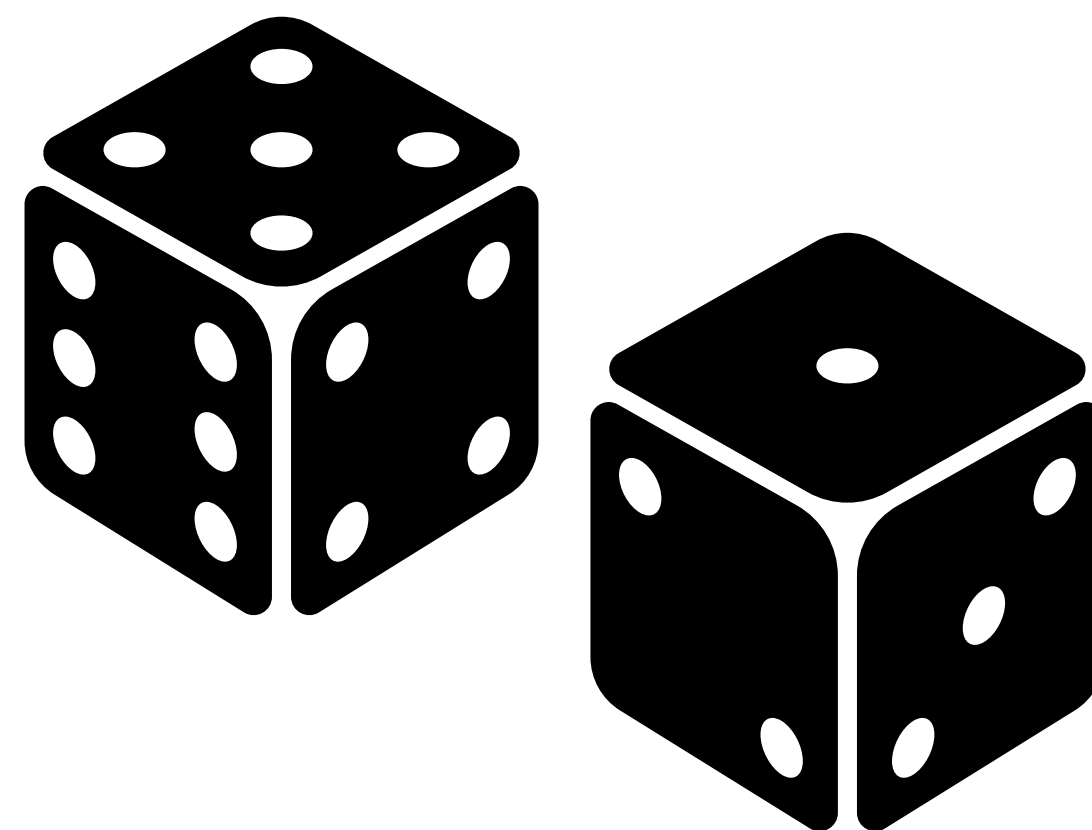
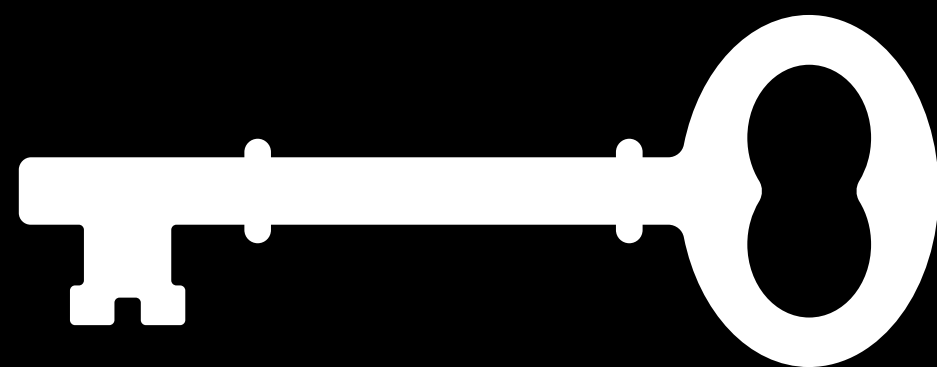
Random



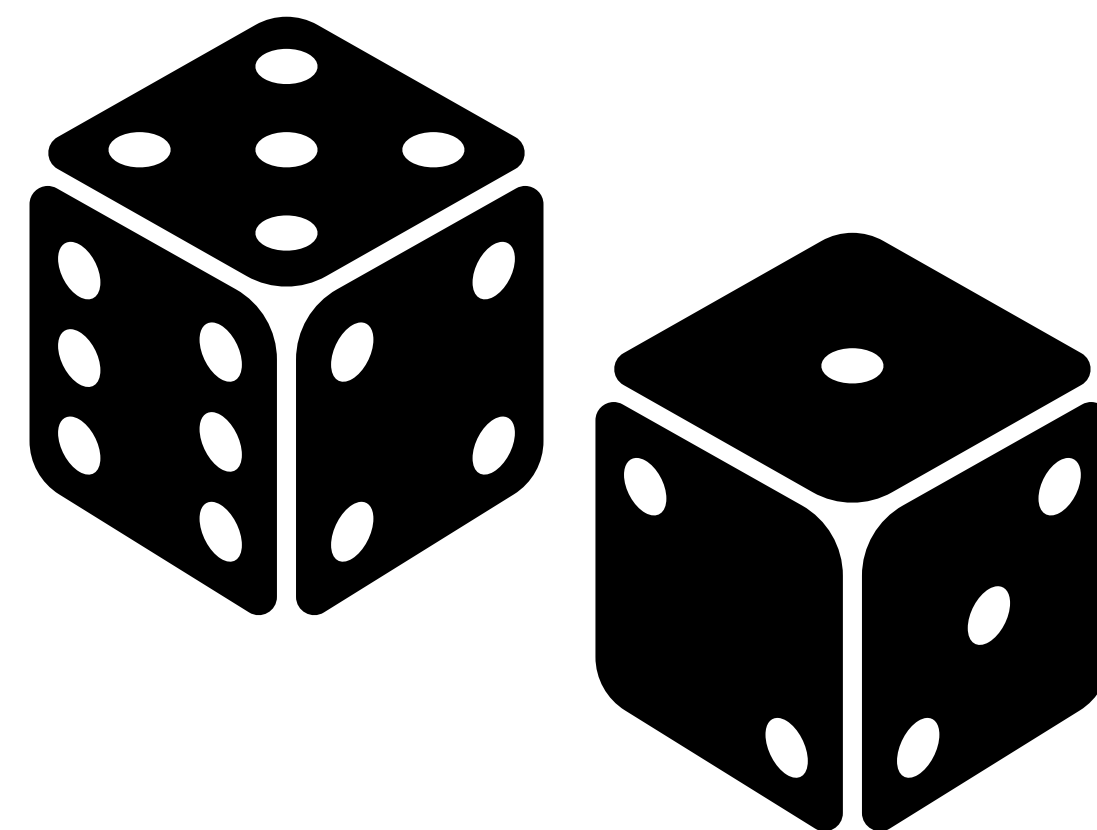
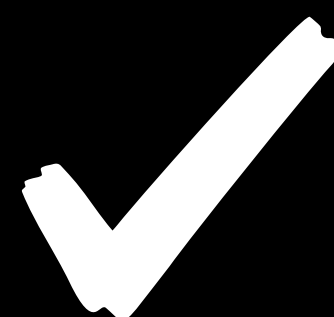
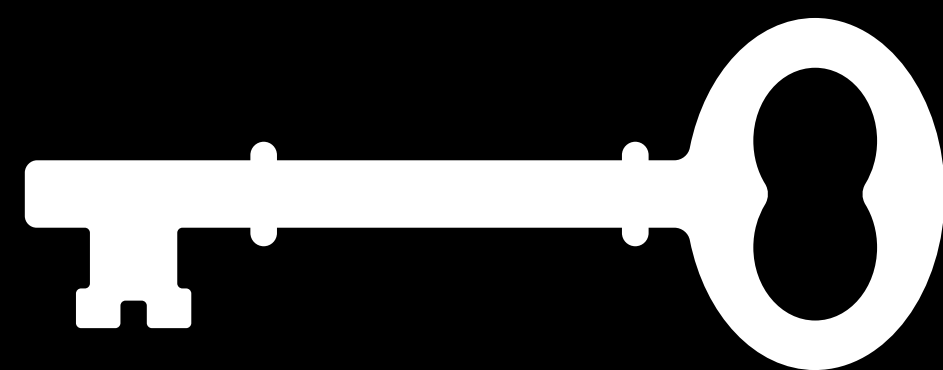
Private

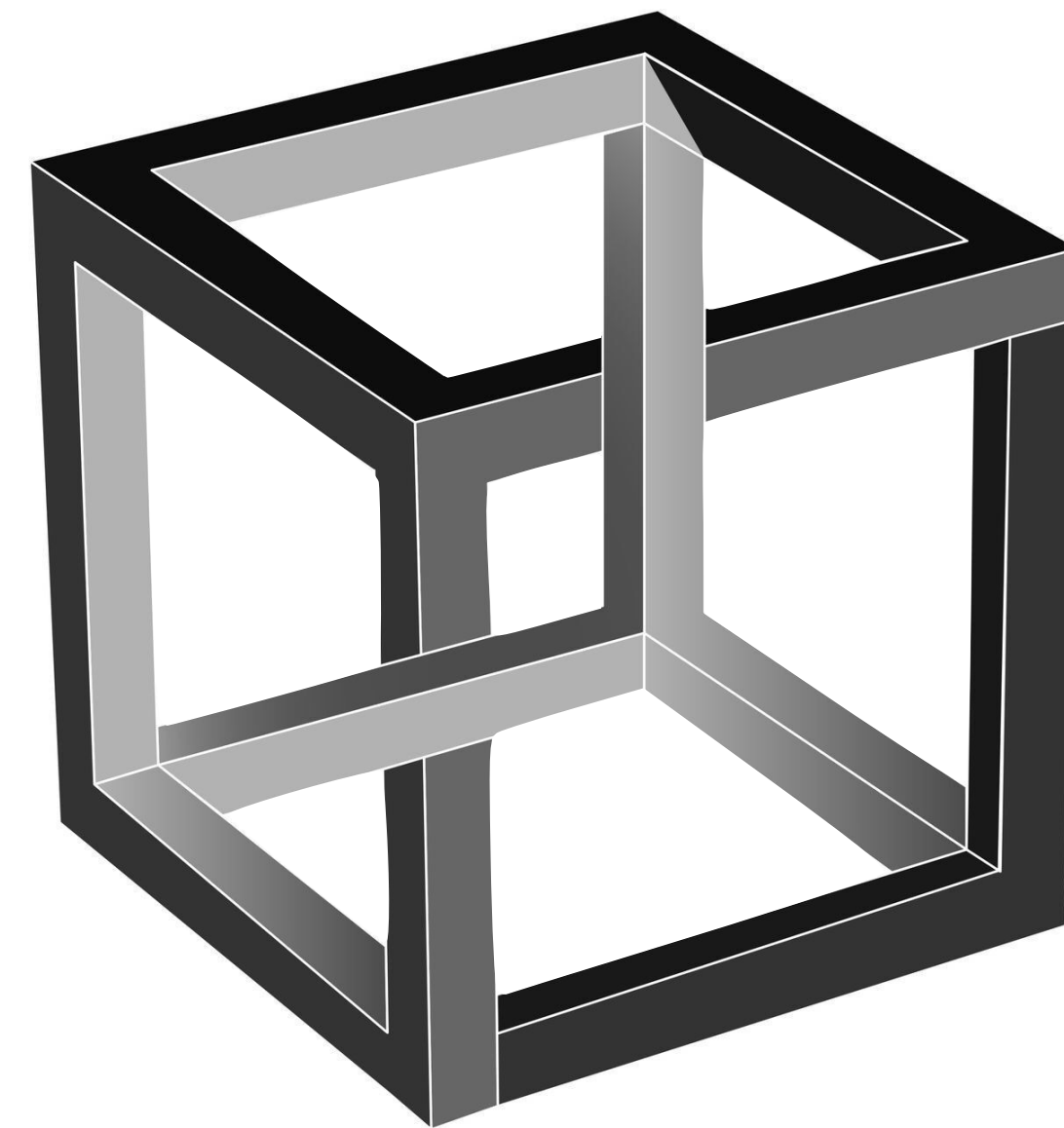
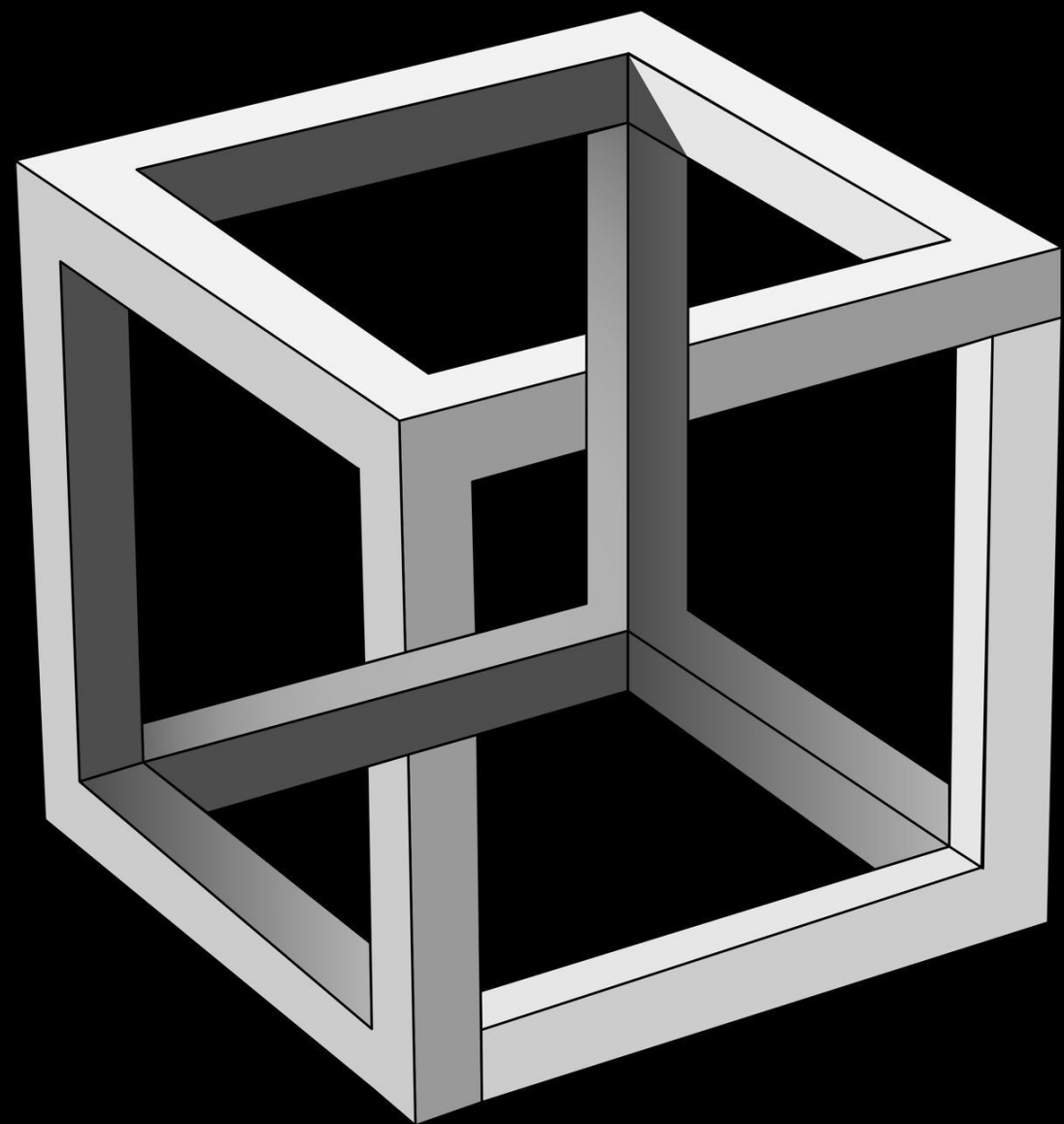


Random



Random





**You can't
possess
bitcoin.**

**You can be
possessed
by bitcoin.**

**Bitcoin is
everywhere.**

**Bitcoin is
nowhere.**

**Bitcoin can't
be copied.**

**Every part
of bitcoin can
be copied.**

**Bitcoin is
always
changing.**

**Bitcoin is
un-
changeable.**

**Bitcoin is
digital.**

**Bitcoin is
scarce.**

**Bitcoin is
dead.**

**Bitcoin is
alive.**

**Bitcoin is
a bubble.**

**Bitcoin is
the pin.**

**Bitcoin is
simple.**

**Bitcoin is
complicated.**

**Bitcoin is
elegant.**

**Bitcoin is
complex.**

**Bitcoin is
ugly.**

**Bitcoin is
beautiful.**

**Bitcoin is
worse.**

**Bitcoin is
better.**

**Bitcoin is
worthless.**

**Bitcoin is
too
expensive.**

**Bitcoin is
finite.**

**Bitcoin is
endless.**

**Bitcoin is
private.**

**Bitcoin is
transparent.**

**Bitcoin is
energy-
intensive.**

**Bitcoin is
efficient.**

**Bitcoin is
slow.**

**Bitcoin is
fast as
lightning.**

**Bitcoin
can't be
confiscated.**

**Bitcoin
can be lost.**

**Bitcoin is
text.**

**Bitcoin is
money.**

**Bitcoin is
time.**

**Bitcoin is
energy.**

**Bitcoin is
savings.**

**Bitcoin is
streaming
money.**

**Bitcoin is
conservative.**

**Bitcoin is
progressive.**

**Bitcoin is
political.**

**Bitcoin is
apolitical.**

**Bitcoin is
lawless.**

**Bitcoin is
the law.**

**Bitcoin is
math.**

**Bitcoin is
physics.**

**Bitcoin is
religion.**

**Bitcoin is
atheism.**

**Bitcoin
requires
randomness.**

**Bitcoin
creates order.**

**Bitcoin
price is
important.**

**Bitcoin
price is
unimportant.**

**Bitcoin
pays people.**

**Bitcoin
can't go
bankrupt.**

**Bitcoin is
intangible.**

**Bitcoin is
incorruptible.**

**Bitcoin
has rules.**

**Bitcoin
has no rules.**

**Bitcoin is
Love.**

**Bitcoin is
Fuck You!**

**Bitcoin
is a chain.**

**Bitcoin
ends slavery.**

—Ben Gunn

**Bitcoin is
12 words in
your head.**

**Bitcoin is
21 Million.**

**Bitcoin is
knowledge.**

**Bitcoin is
knowledge.**

**Knowledge is
power.**

Asymmetry

knowledge

of power via

asymmetry.

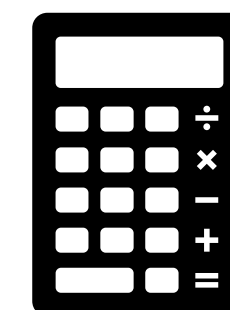
**Hard to
produce.**

**Easy to
verify.**

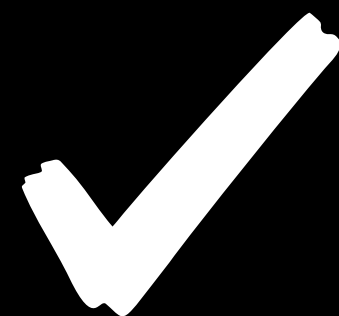
**Hard to
produce.**



**Easy to
verify.**



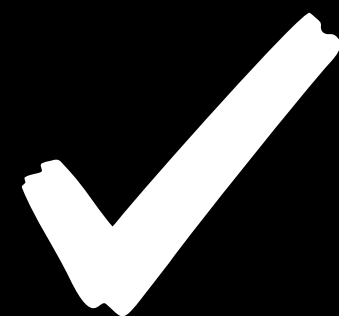
**Hard to
produce.**



**Easy to
verify.**



**Valid
signature.**



**Valid
block.**



**Valid
signature.**

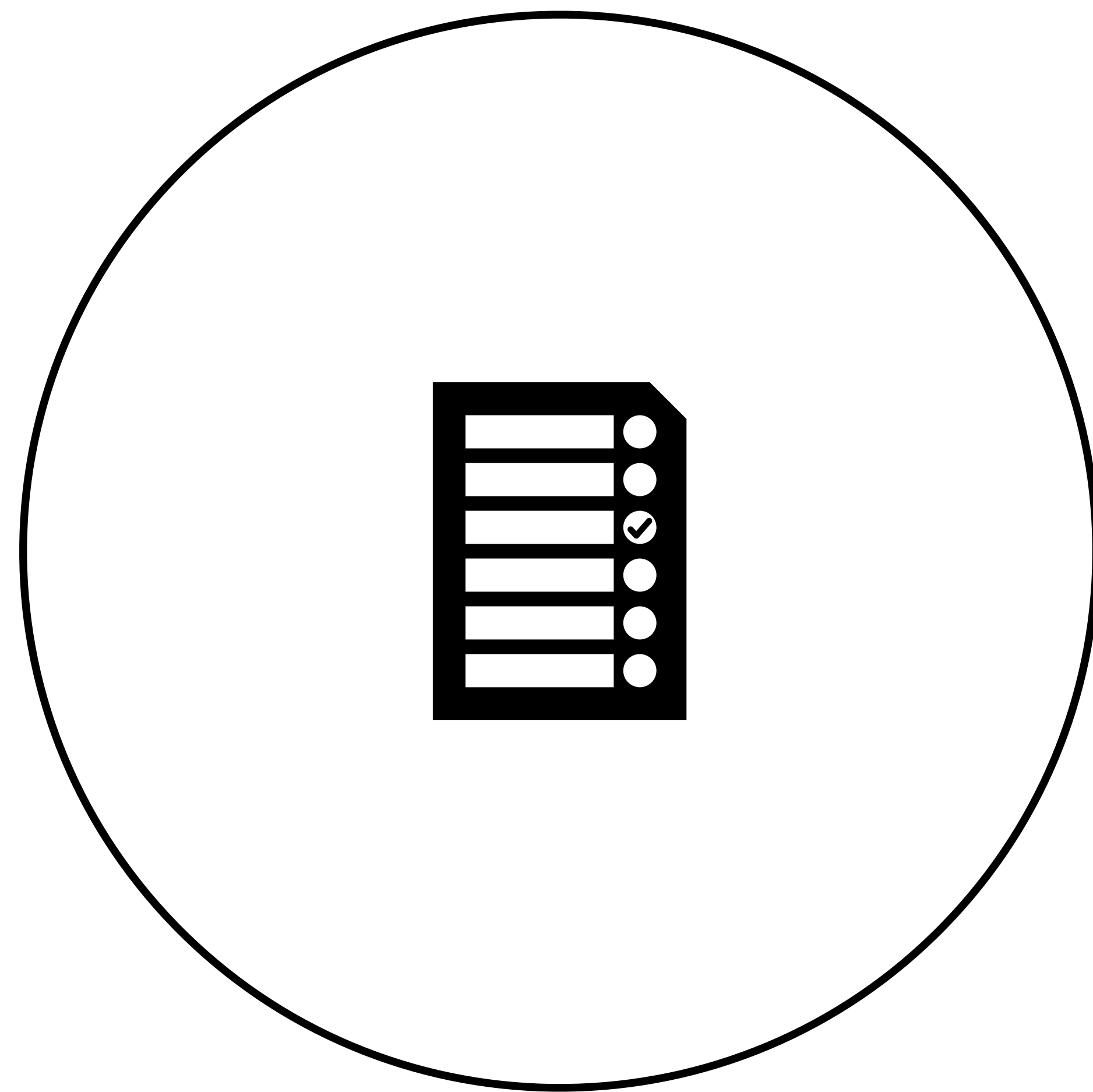
Private

**Valid
block.**

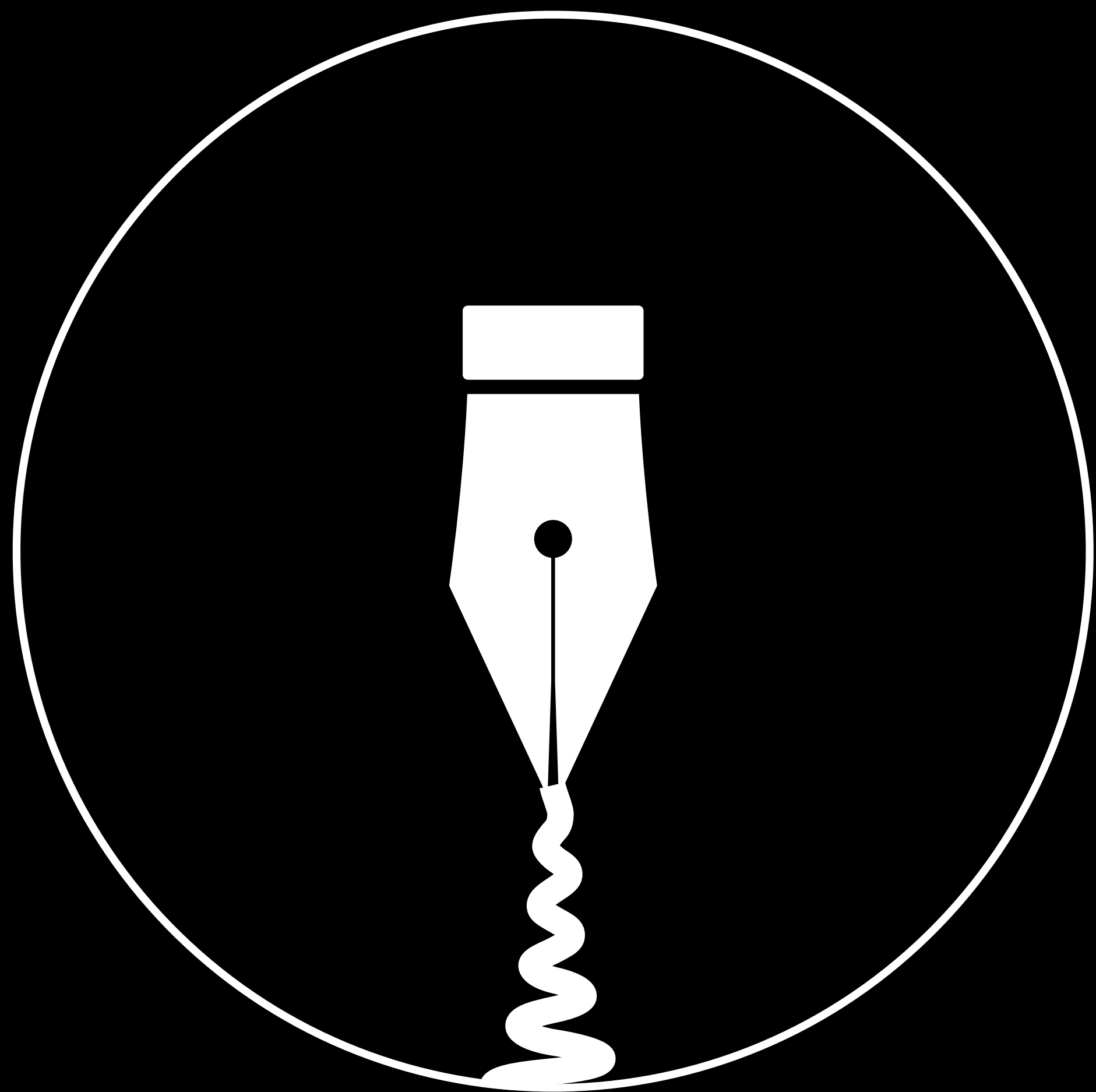
Public



Private



Public



Local



Global



Secret Information



Public Information



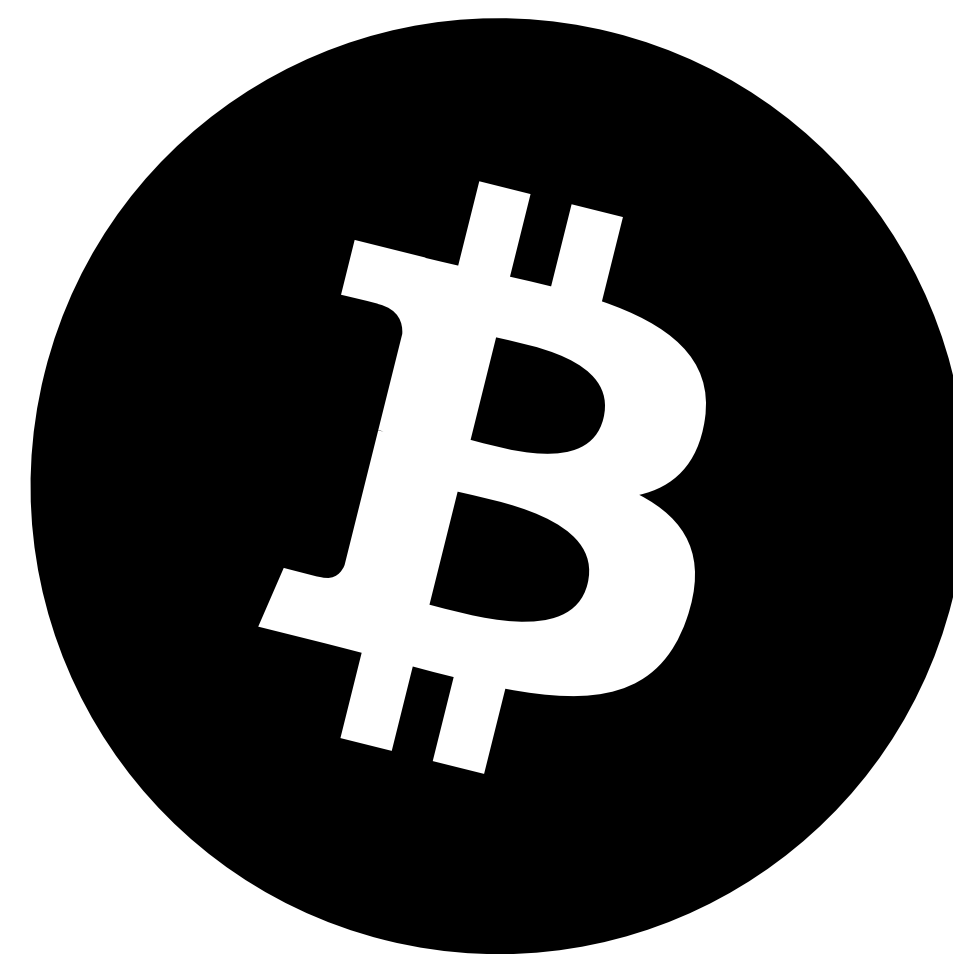
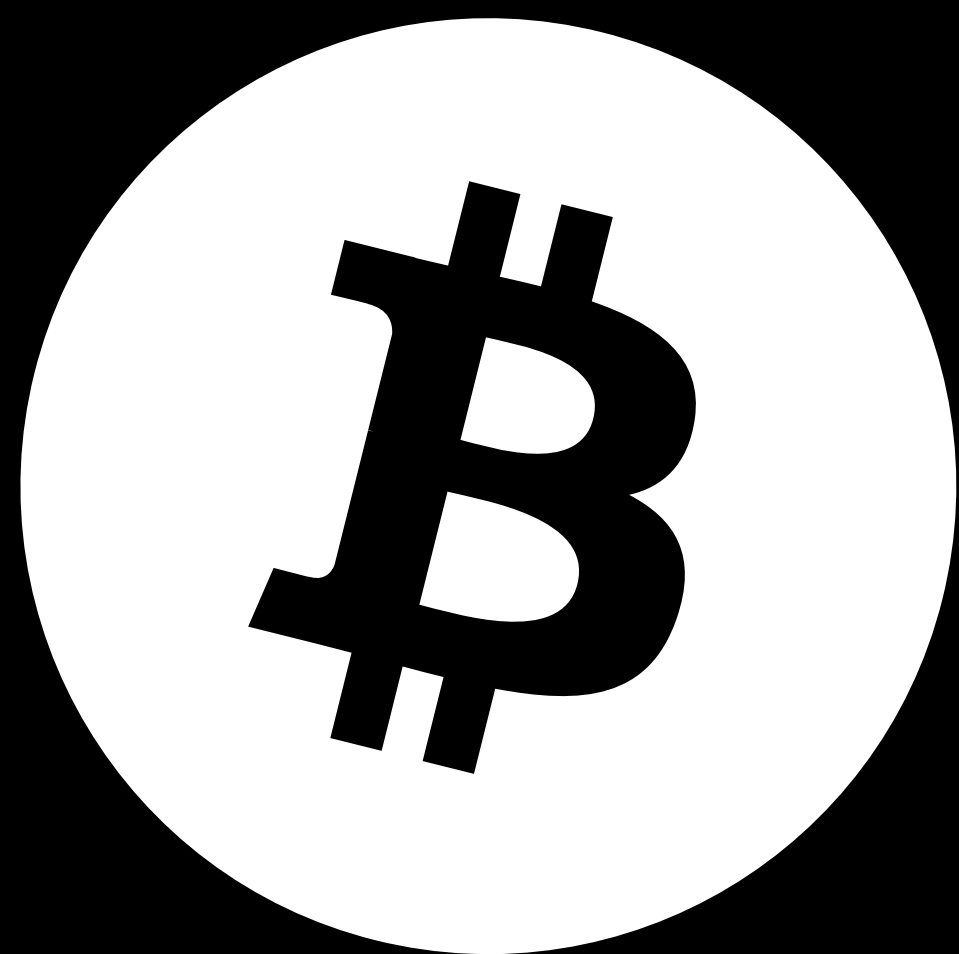
12

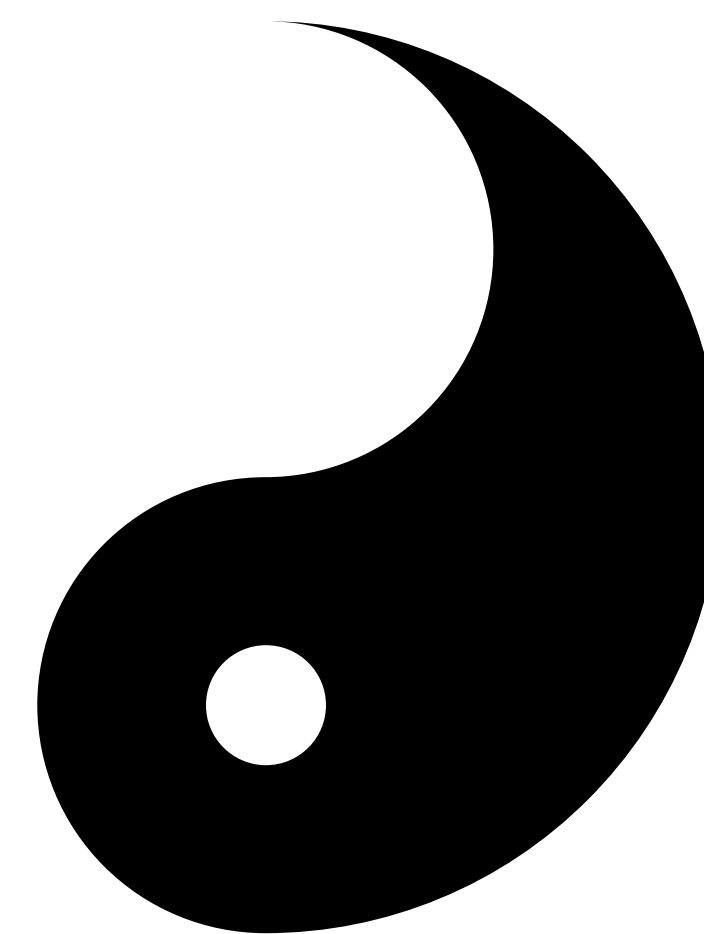
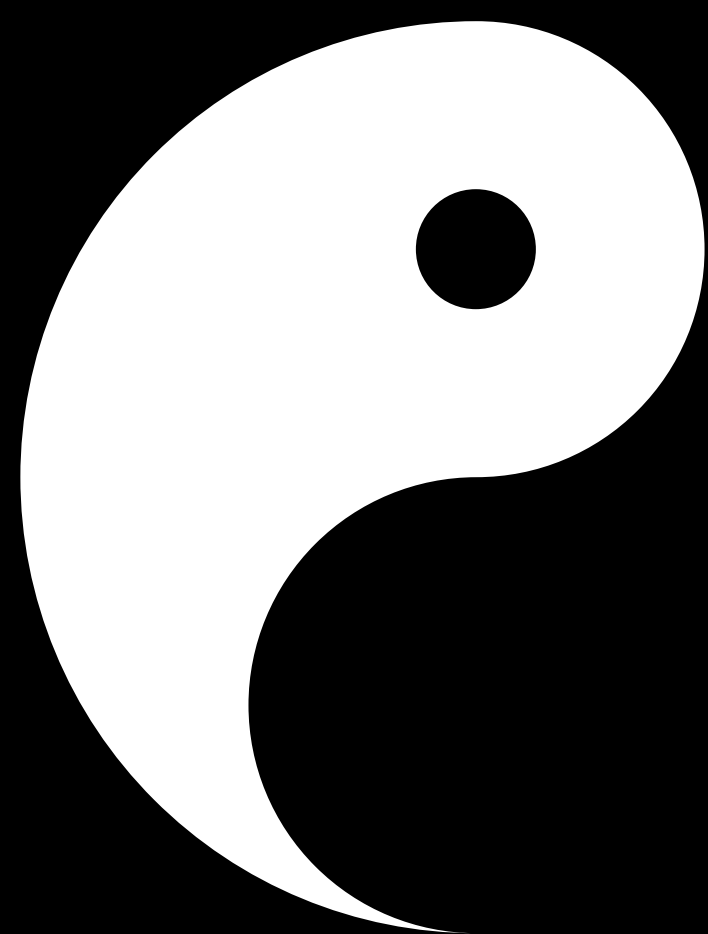
Words

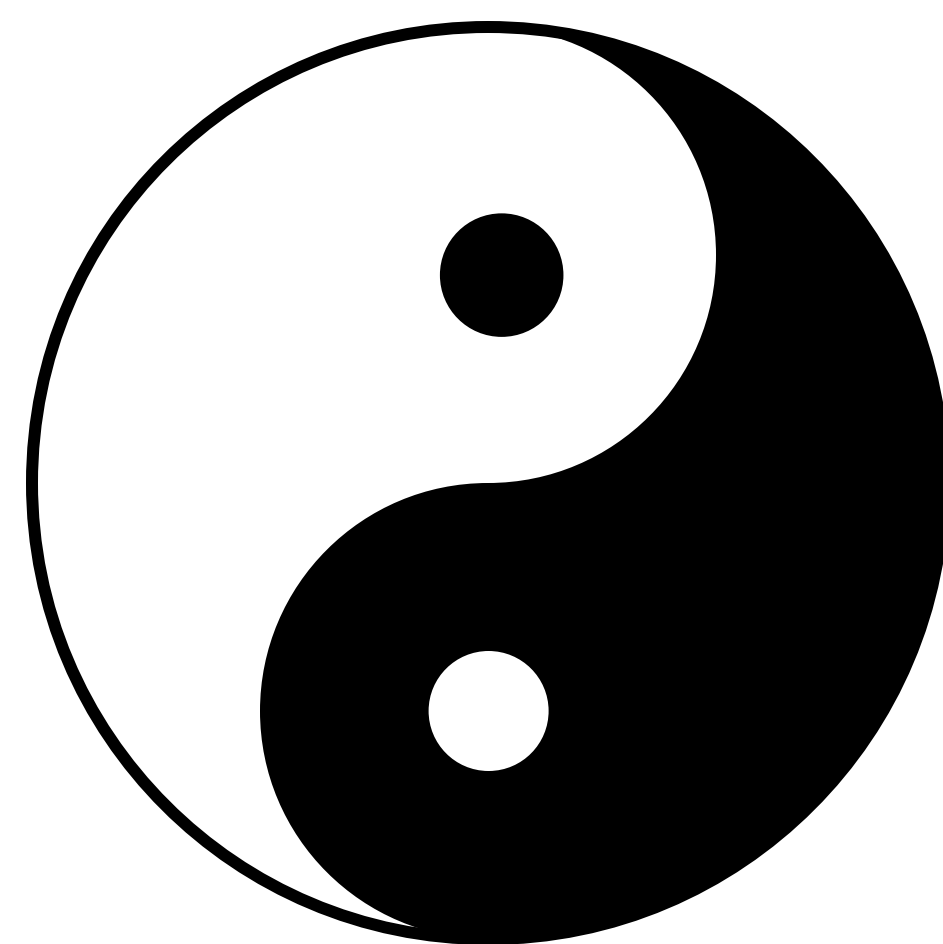


21

Million



















A bright orange is suspended by a thin black cord with a small metal bell at the top. The orange is in sharp focus, showing its textured peel. The background is a blurred winter scene with snow-covered ground and bare trees, creating a bokeh effect with soft light and dark shadows.

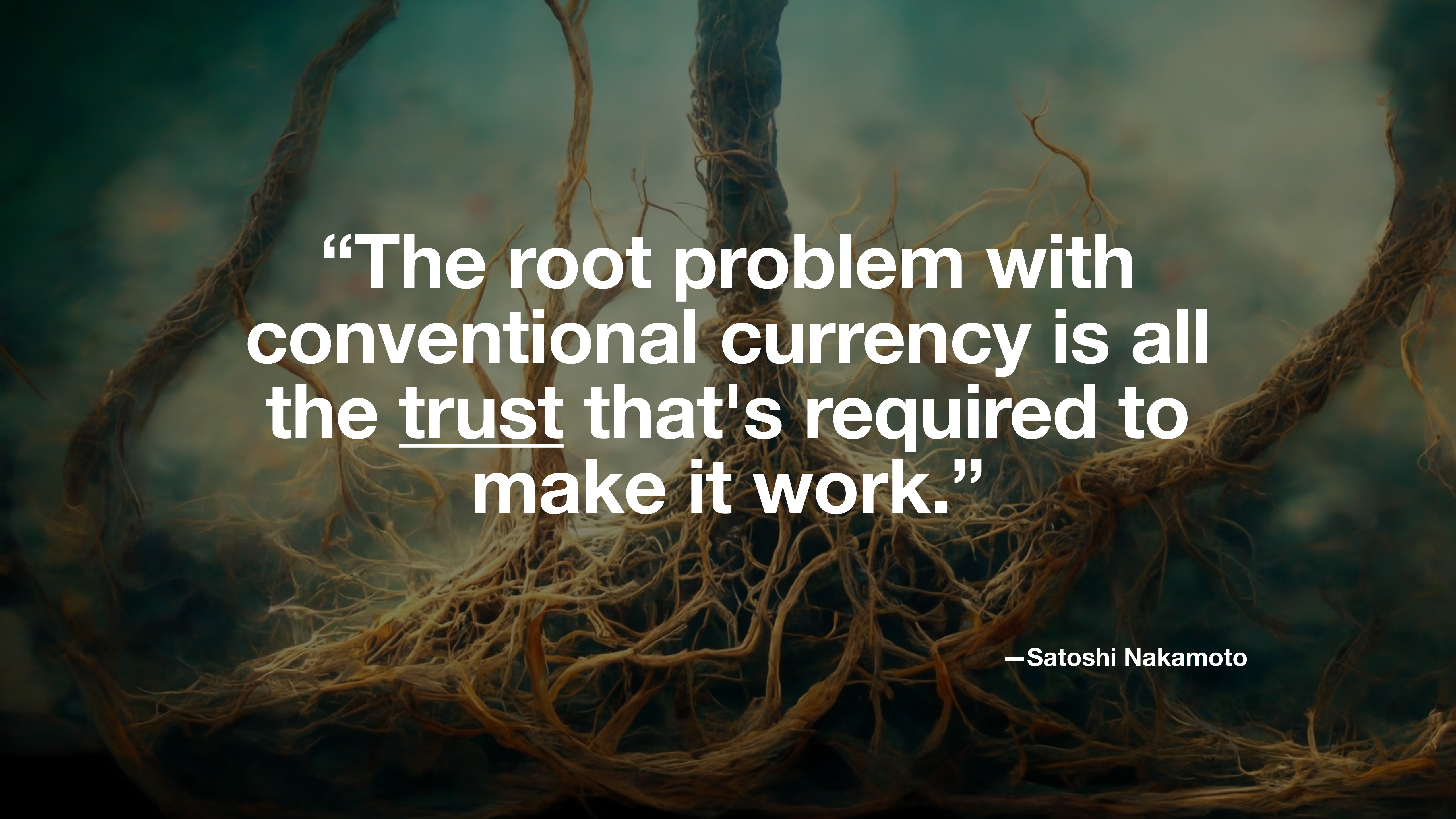
ACT THREE

ACT THREE









**“The root problem with
conventional currency is all
the trust that's required to
make it work.”**

—Satoshi Nakamoto

A large, gnarled tree root system is exposed, with many smaller roots branching out from a central trunk. The roots are light brown and appear to be submerged in or emerging from a body of water. The background is a soft, out-of-focus mix of blue and green, suggesting a natural outdoor setting. The text "Trust is the Root Problem" is overlaid in white, with the word "Trust" underlined.

Trust is the Root Problem



Trust

...can be abused



Trust

“Crypto Proof”

— Satoshi Nakamoto

A large, gnarled tree root system is exposed, with many smaller roots branching out from a central trunk. The roots are light brown and appear to be submerged in or emerging from a body of water. The background is a soft, out-of-focus mix of blue and green, suggesting a natural, outdoor setting.

**How was the
Trust problem solved
historically?**



“Trust us.”



“Trust us.”

— Authority



“Trust us.”

Cryptography



“Trust us.”



Cryptography



“Trust us.”



“Crypto”



“Trust us.”



— Crypto bro



“Trust us.”



— Politicians



“Trust us.” — Politicians



“Trust us.” — The State



Money

The State

A dramatic painting depicting a city under attack. A large, classical-style building with many columns is the central focus. It is being set on fire by a massive explosion or fire that is consuming the left side of the image. The sky is filled with thick, dark smoke and fire. In the foreground, there is a large crowd of people, some on horseback, watching the destruction. The overall tone is dark and apocalyptic.

Cryptography is not enough.





K
E
I
S
T
I
N
H
A
G
U
S
T
I
K
T
E
R



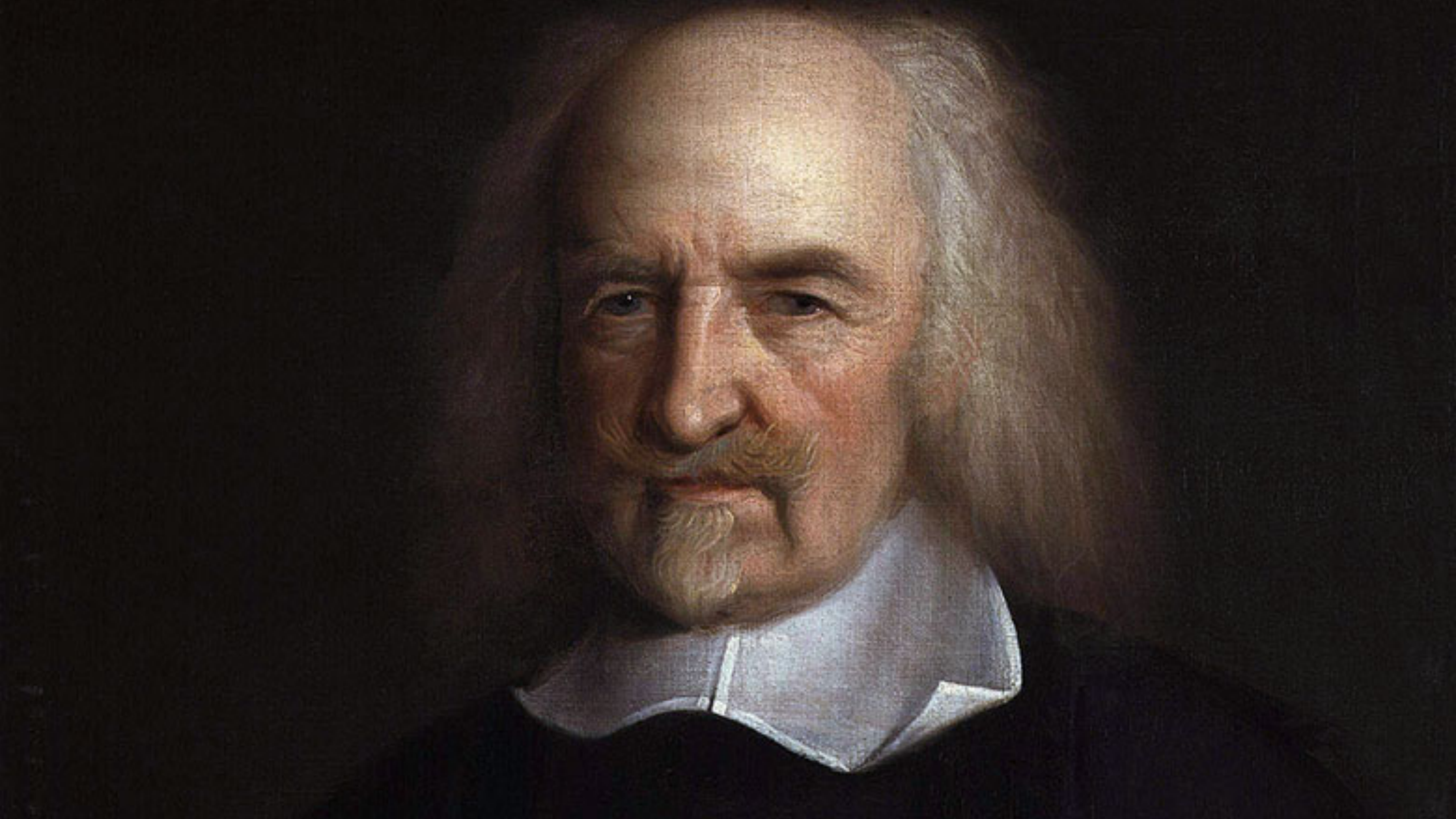


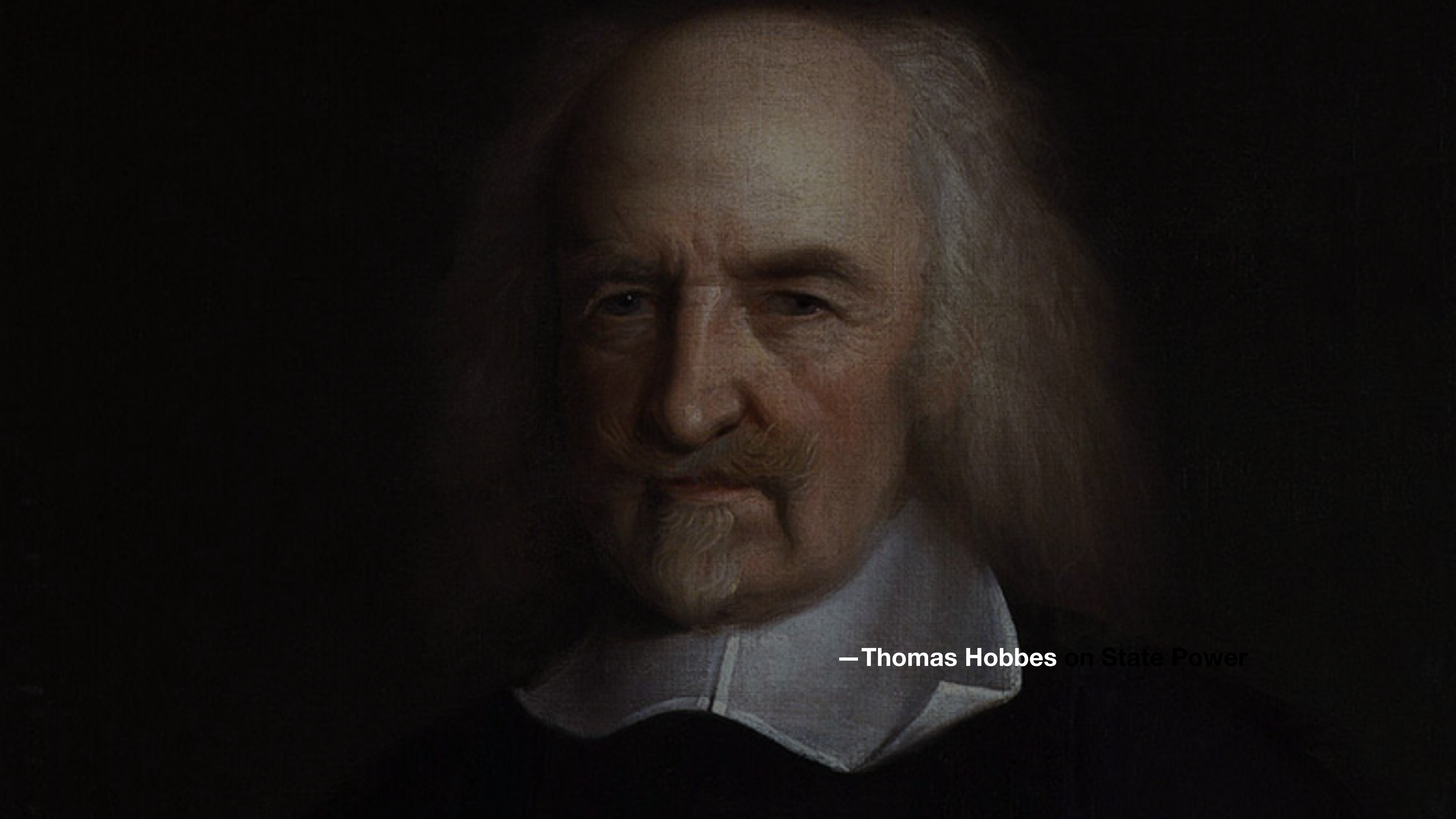
**Cryptography alone does not
provide integrity.**



**Cryptography alone does not
provide legitimacy.**





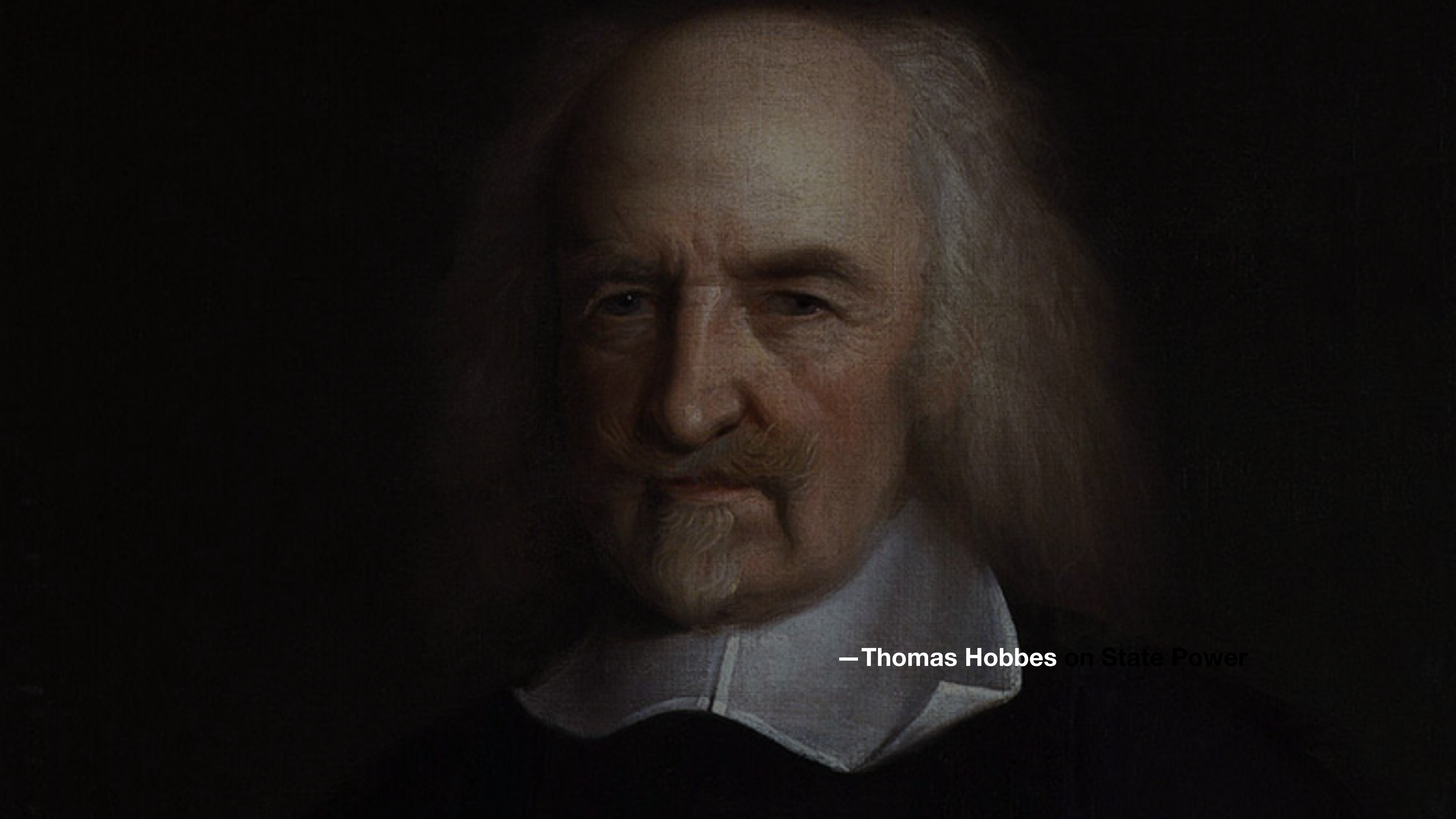


— Thomas Hobbes on State Power

A portrait of Thomas Hobbes, an English philosopher, is shown in the background. He is an older man with white hair and a beard, wearing a white ruffled collar. The portrait is centered and slightly faded, serving as a backdrop for the text.

**“Authority, not truth creates
legitimacy.”**

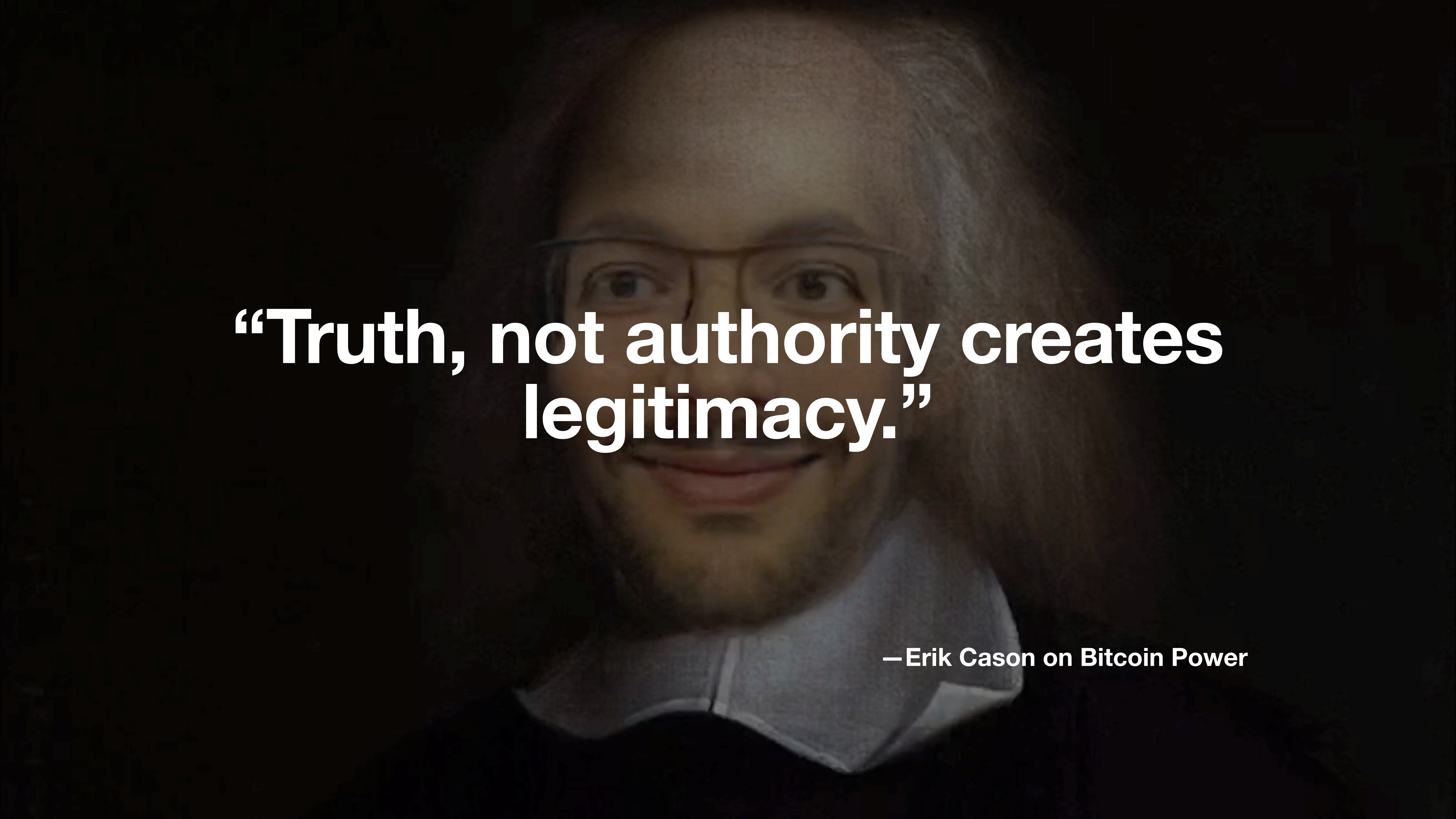
—Thomas Hobbes on State Power



— Thomas Hobbes on State Power



—Erik Cason on Bitcoin Power



**“Truth, not authority creates
legitimacy.”**

—Erik Cason on Bitcoin Power

Reclaim “Crypto”

—Erik Cason on cryptosovereignty.org





“Crypto”



Cryptography





Cryptography is not enough.



Cryptography requires secrecy.



Cryptography \neq Legitimacy



Cryptography \neq Reality



Cryptography \neq Scarcity

“Crypto” ≠ Scarcity



“Crypto” = Rugpulls





The background image is a painting of a landscape. In the foreground, a large, ornate rug with a complex geometric and floral pattern in shades of red, blue, and gold is spread out on the ground. The rug's pattern consists of interlocking diamond shapes. In the middle ground, there is a flat, grassy field. In the background, there are dark, silhouetted hills or mountains under a sky filled with large, billowing white and grey clouds. The overall lighting is somewhat dim, giving it a moody, atmospheric feel.

**“It ain’t what you don’t know
that gets you into trouble.**

**It’s what you know for sure
that just ain’t so.”**

—Mark Twain on Rugpulls

A landscape painting featuring a vast, ornate red and blue rug laid out on a grassy field under a dramatic, cloudy sky. The rug has a complex geometric pattern with deep red borders and blue central medallions. The background shows a line of trees and distant hills under a sky filled with large, billowing white and grey clouds.

**“Where there is trust in others,
there is a rug.”**

—Satoshi Nakamoto (paraphrased)

A surreal landscape painting. The foreground is dominated by a vast, ornate rug with a repeating geometric pattern in deep red, dark blue, and gold. The rug stretches across the entire ground, leading the viewer's eye into the distance. In the middle ground, a small, distant castle or fortress sits on a hill, with a few tiny figures standing nearby. The background features rolling hills and a dramatic sky filled with large, billowing white and grey clouds against a dark, teal-blue upper portion. The overall mood is one of grandeur and mystery.

“Bitcoin fixes this!”

A surreal landscape painting. In the foreground, a vast, ornate rug with a repeating geometric pattern in deep red, dark blue, and gold lies flat on a green field. The rug's pattern consists of interlocking diamond shapes. In the middle ground, a small group of figures stands on the horizon line. The background features rolling green hills and a dramatic sky filled with large, billowing white and grey clouds. The overall mood is one of grandeur and mystery.

Bitcoin \neq “Crypto”

A landscape painting featuring a vast, ornate rug with a red and blue geometric pattern laid out on a grassy field. In the background, there are rolling hills, a small cluster of trees, and a large, dramatic, cloudy sky. The overall tone is somber and atmospheric.

Bitcoin \neq Rugpull



Bitcoin = anti-rug tech



Bitcoin = Legitimacy

A surrealist landscape painting. The foreground is dominated by a vast, intricate rug with a repeating geometric pattern in deep red, dark blue, and gold. The rug appears to stretch across a flat, open landscape. In the middle ground, a small, dark, rocky outcrop stands on the horizon. The background features rolling hills and a distant, hazy horizon. The sky is filled with large, billowing clouds in shades of white, yellow, and grey, set against a dark, teal-blue background. The overall mood is dreamlike and expansive.

Reality & Cryptography



Physics & Math

Crypto & Proof

The image is a surreal landscape painting. In the foreground, a massive, intricately patterned rug with a repeating geometric design in deep red, dark blue, and gold tones is spread out across a green field. The rug's pattern consists of interlocking diamond and square shapes. In the middle ground, the field leads to a line of dark, silhouetted trees and hills. A small, isolated, and somewhat jagged structure, possibly a ruin or a small building, stands in the distance. The sky is filled with large, billowing clouds in shades of white, grey, and pale yellow, set against a darker, teal-blue upper portion. The overall mood is dreamlike and expansive.



Keys & Work



Keys \neq Work



Reality \neq Theory



Reality = What survives

The background is a painting of a vast, open landscape. In the foreground, a large, ornate rug with a complex geometric pattern in shades of red, blue, and gold is spread out across the ground. The rug's pattern consists of interlocking diamond and square shapes. In the middle ground, a flat, green field stretches towards a distant horizon. A few small figures of people are visible in the distance. The sky is filled with large, billowing clouds in shades of white, yellow, and grey, set against a dark, teal-blue background. The overall mood is dramatic and expansive.

“Only the strong survive.”

—Allen Farrington





—Adam Back



Proof of Work

—Adam Back

A highly detailed oil painting of a muscular man's back and arms, viewed from behind. The man's skin is a warm, golden-brown color, and his muscles are extremely well-defined, showing deep ridges and valleys. The lighting comes from the upper left, casting shadows that emphasize the three-dimensional quality of the musculature. The background is a dark, textured blue-green. In the center of the image, the letters 'PoW' are written in a bold, white, sans-serif font.

PoW

A classical painting of a muscular man's back and arms, rendered in a realistic style with detailed musculature. The man's skin is a warm, brownish-tan color, and his muscles are highly defined, showing deep shadows and bright highlights. He is positioned against a dark, textured background that appears to be a deep blue or black. The overall composition is centered, with the man's back and arms filling most of the frame. Overlaid on the center of the image is the text "PoW = self-evident" in a bold, white, sans-serif font.

PoW = self-evident



PoW = Transformation

The background of the image is a highly detailed painting of a muscular, brown-skinned figure, possibly a deity or warrior, with a dark, starry background. The figure is shown from the waist up, with its arms raised and bent, revealing intricate muscle detail. The lighting is dramatic, highlighting the contours of the muscles. The overall tone is dark and mystical.

PoW = Computation

A classical painting of a muscular man's back and arms, rendered in a dark, textured style. The man's back is the central focus, showing intricate muscle detail. His arms are bent, with hands near his waist. The background is a dark, mottled blue-green. The text "PoW = Electricity" is overlaid in the center in a bold, white, sans-serif font.

PoW = Electricity



PoW = Energy



PoW = Costly



PoW = Integrity

A classical painting depicting a muscular man wrestling a large tortoise. The man is on the left, leaning over the tortoise, with his arms extended. The tortoise is on the right, facing the man. The background is dark and textured. The text is overlaid in the center.

**PoW = Integrity
w/o Authority
w/o Crypto keys
w/o Secrecy**

A classical painting of a muscular man's back and arms, rendered in a realistic style with detailed musculature. The man's skin is a warm, brownish-tan color, and his muscles are highly defined, showing deep shadows and bright highlights. He is positioned against a dark, textured background that appears to be a deep blue or black. The lighting comes from the upper left, casting strong shadows on the right side of his back and arms. The overall composition is centered, with the man's back filling most of the frame. Overlaid on the center of the image is the text 'd.a. PoW = Solution' in a bold, white, sans-serif font.

d.a. PoW = Solution





**Last block:
9 min ago**

**Next block:
???**



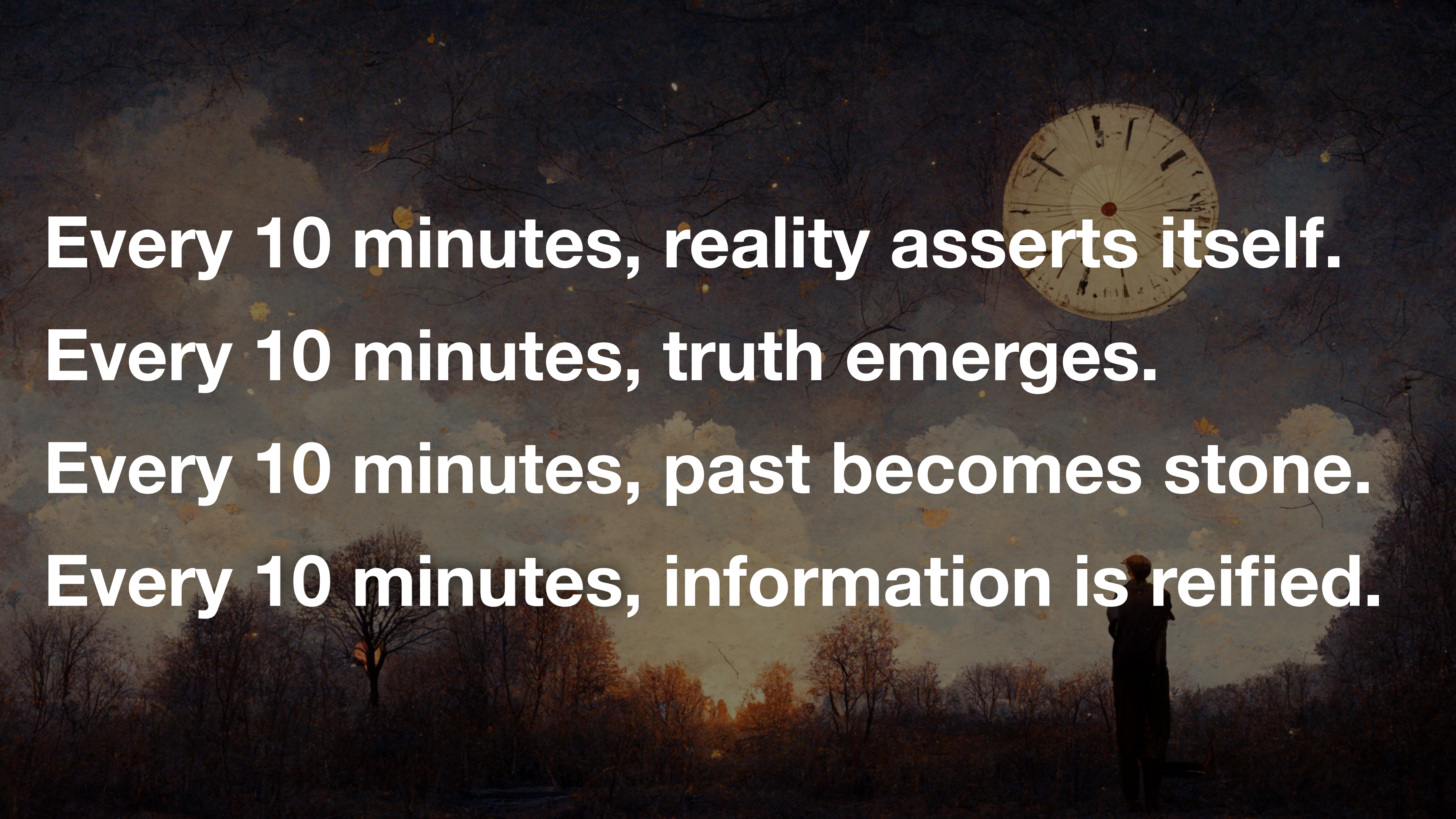
**Last block:
9 min ago**

**Next block:
10 minutes**



10 minutes





Every 10 minutes, reality asserts itself.
Every 10 minutes, truth emerges.
Every 10 minutes, past becomes stone.
Every 10 minutes, information is reified.

duration

10 minutes





**Bitcoin measures
duration via computation.**

10 minutes



**Bitcoin measures
duration via computation
& settles**

**10 minutes of history,
every 10 minutes.**

A surreal landscape painting. In the upper right, a large, white, antique-style clock face floats in a dark, starry sky. The clock has a red center and black hands. Below the sky, a layer of soft, white and grey clouds stretches across the middle. In the foreground, a person in a long, dark coat stands with their back to the viewer, looking up at the clock. The ground is dark and covered with trees and bushes, some of which have autumn-colored leaves. Numerous yellow and orange leaves are shown falling through the air, creating a sense of motion. The overall mood is contemplative and mysterious.

10 minutes of history.

A surreal landscape painting. In the upper right, a large, circular clock face is superimposed on a dark, starry sky. The clock face is white with black hands and numbers, and a small red dot at the center. Below the clock, a person in a long, dark coat stands with their back to the viewer, looking up at the sky. The foreground is filled with dark, silhouetted trees and falling yellow leaves. The overall mood is contemplative and mysterious.

**10 minutes of history.
of the future.**



**10 minutes of history.
of the future.**



Year 2140



**10 minutes of history.
of the future.**



Year 2140



**10 minutes of history.
of the future.**



Year 2140



**10 minutes of history.
of the future.**



“Bitcoin is Time”



**10 minutes of history.
of the future.**



“Bitcoin is Time”

10 minutes

past
future



**Difficulty-adjusted
Proof of Work
creates**

**unforgeable
history.**



**Difficulty-adjusted
Proof of Work
solves the root problem.**



**Difficulty-adjusted
Proof of Work
solves the root problem.**

“Double spending”



**Difficulty-adjusted
Proof of Work
provides Trust & Integrity**




A person stands in a dark, wooded area, looking up at a large, glowing clock face that appears to be floating in the sky. The clock face is white with black hands and numbers, and a red center. The background is a dark, cloudy sky with some light filtering through. The overall mood is mysterious and contemplative.

**Difficulty-adjusted
Proof of Work
provides Trust & Integrity
without relying
on secrecy.**

**Difficulty-adjusted
Proof of Work
solves all the problems
of monies
past.**

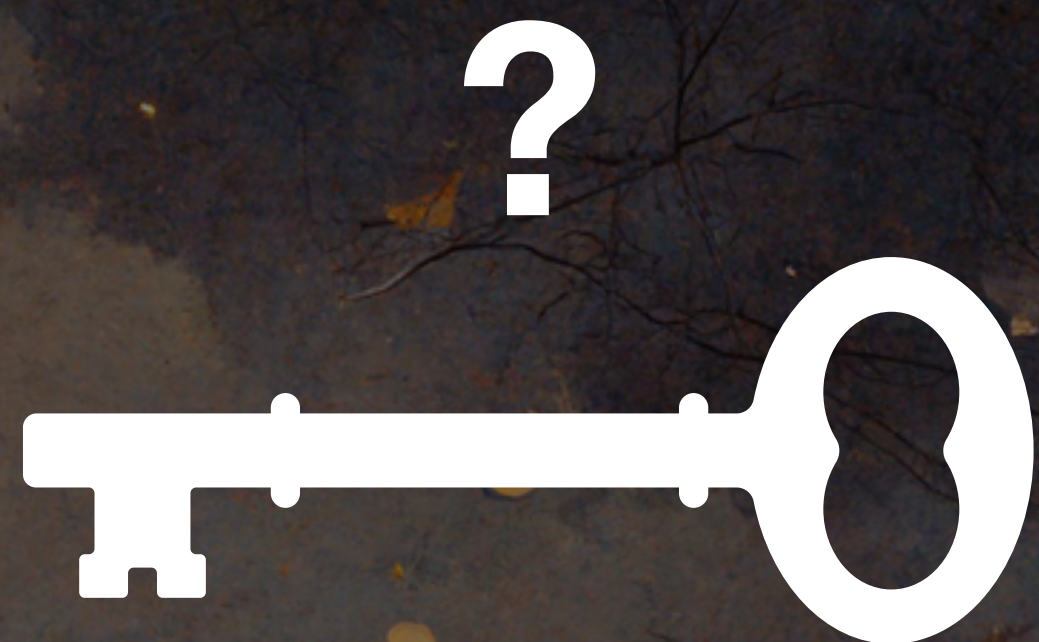




**Trustless issuance.
Decentralized time-stamping.
Cryptanalytic stability.
Digital scarcity.
Data integrity.**

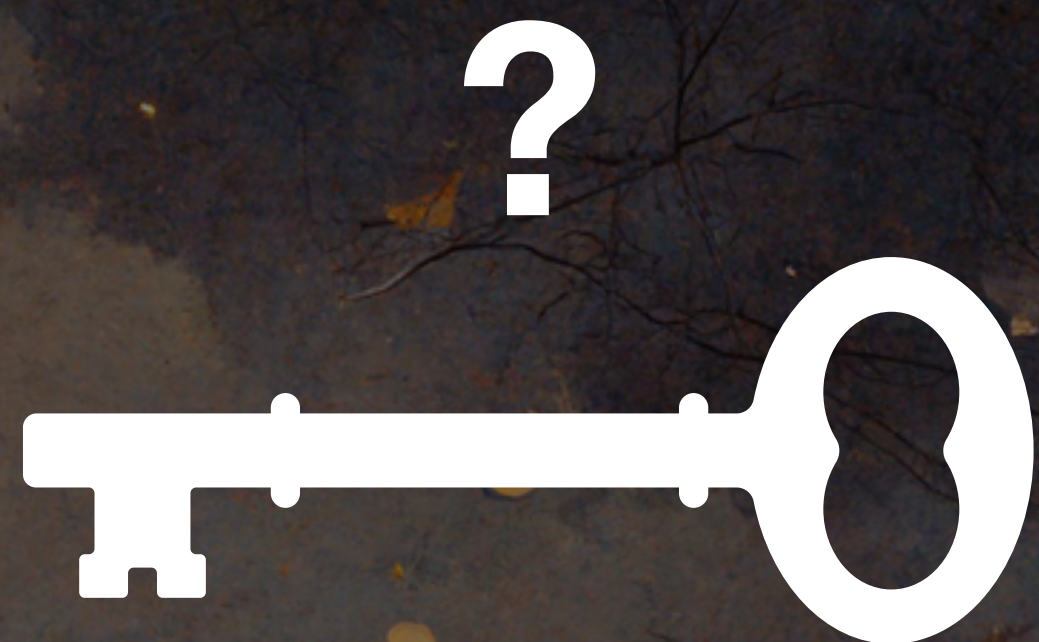
A surreal landscape painting. In the upper right, a large, white, antique-style clock face floats in a dark, starry sky. The clock has a red center and black hands. Below the sky, a layer of soft, white, ethereal clouds stretches across the middle. In the foreground, a person in a long, dark coat stands with their back to the viewer, looking up at the clock. The ground is dark and covered with trees and bushes, some of which have autumn-colored leaves. Numerous yellow and orange leaves are shown falling through the air, creating a sense of motion. The overall mood is contemplative and mysterious.

Data integrity?



Data integrity?





Data integrity?



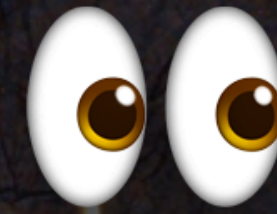
Data integrity?



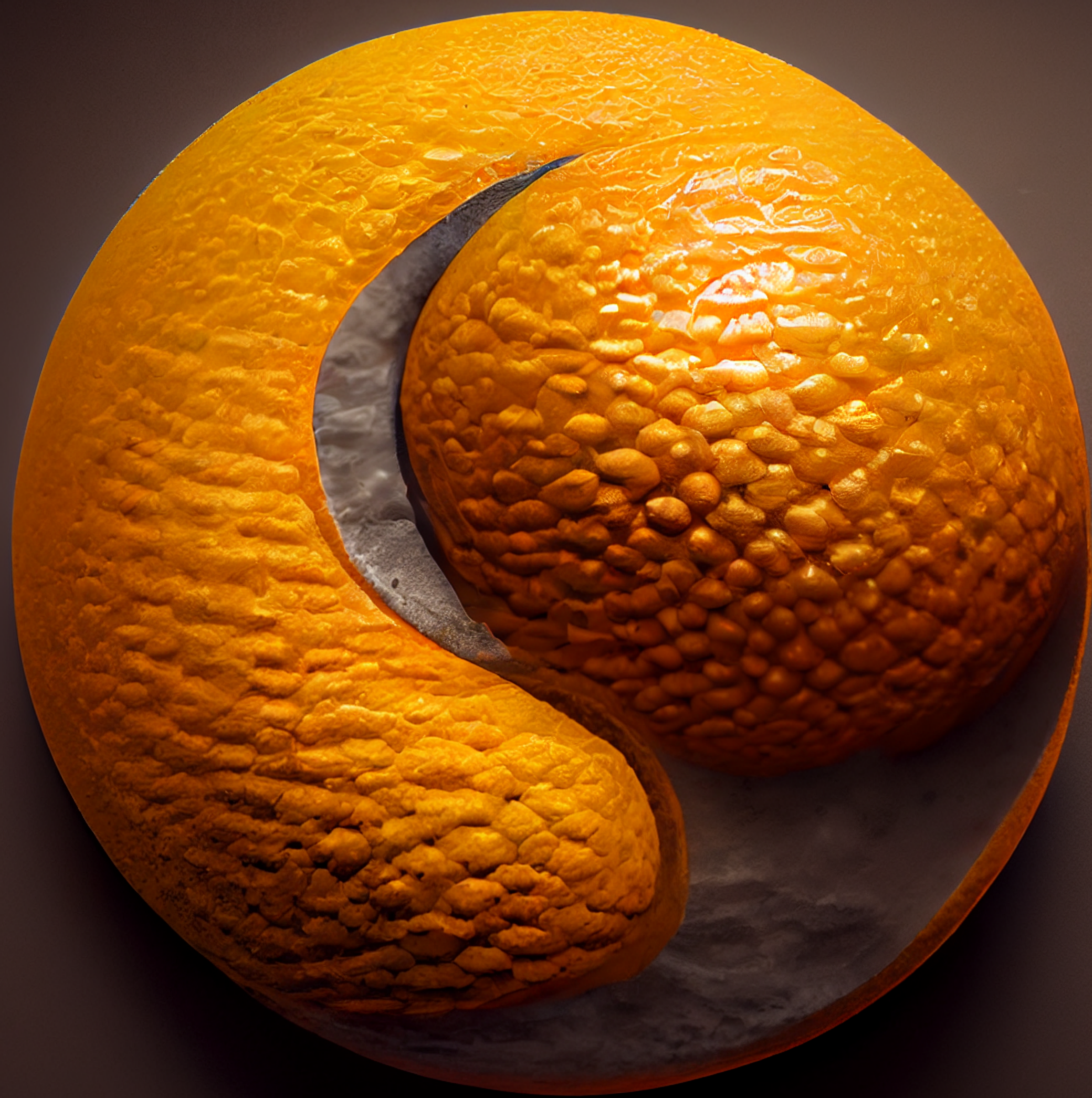
**Data integrity
without any private keys.**



**Data integrity
without any private keys.**



**Data integrity
without any private keys.**





Integrity & Validation



Words



Million



Keys



Ledger(s)











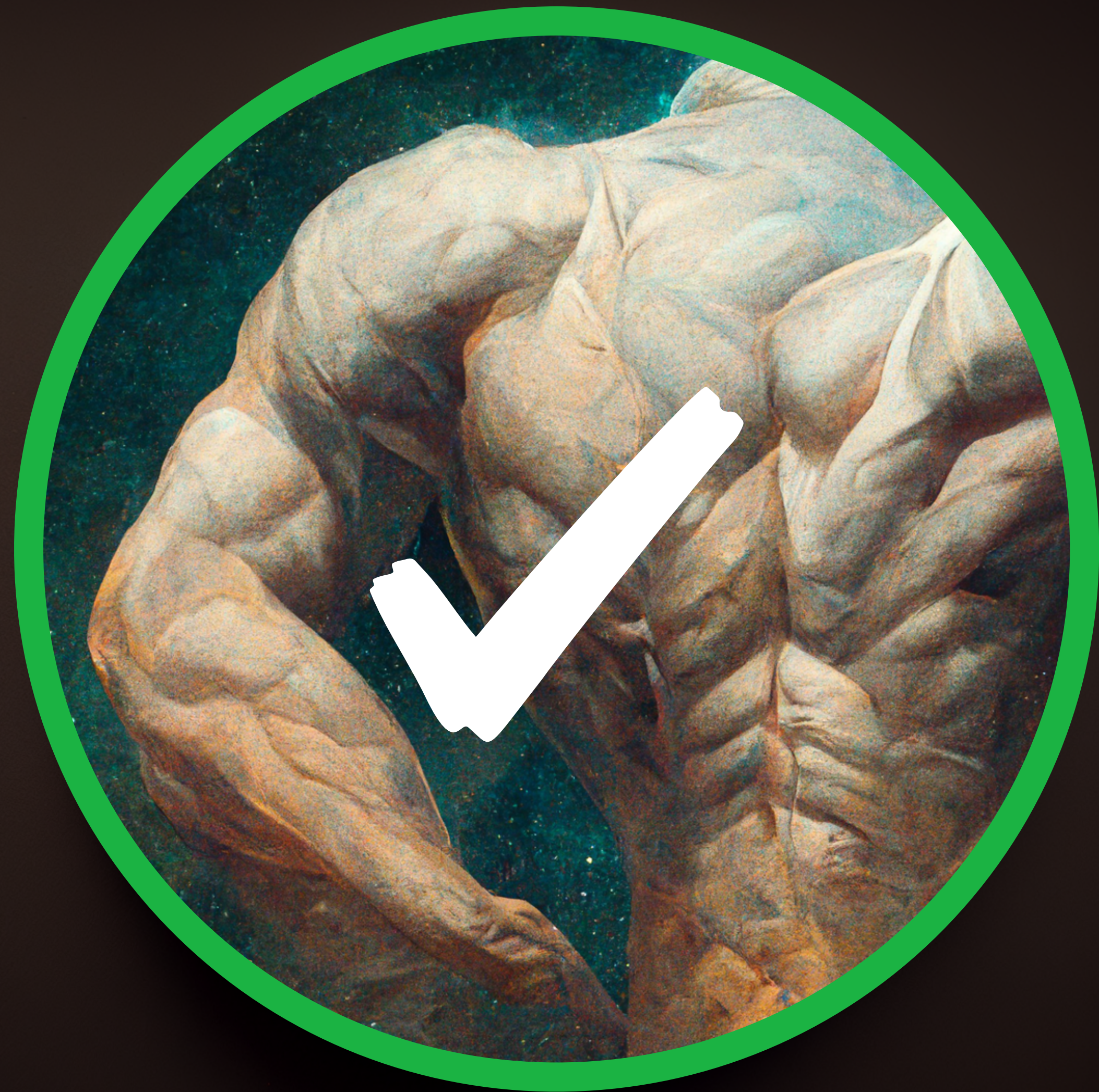
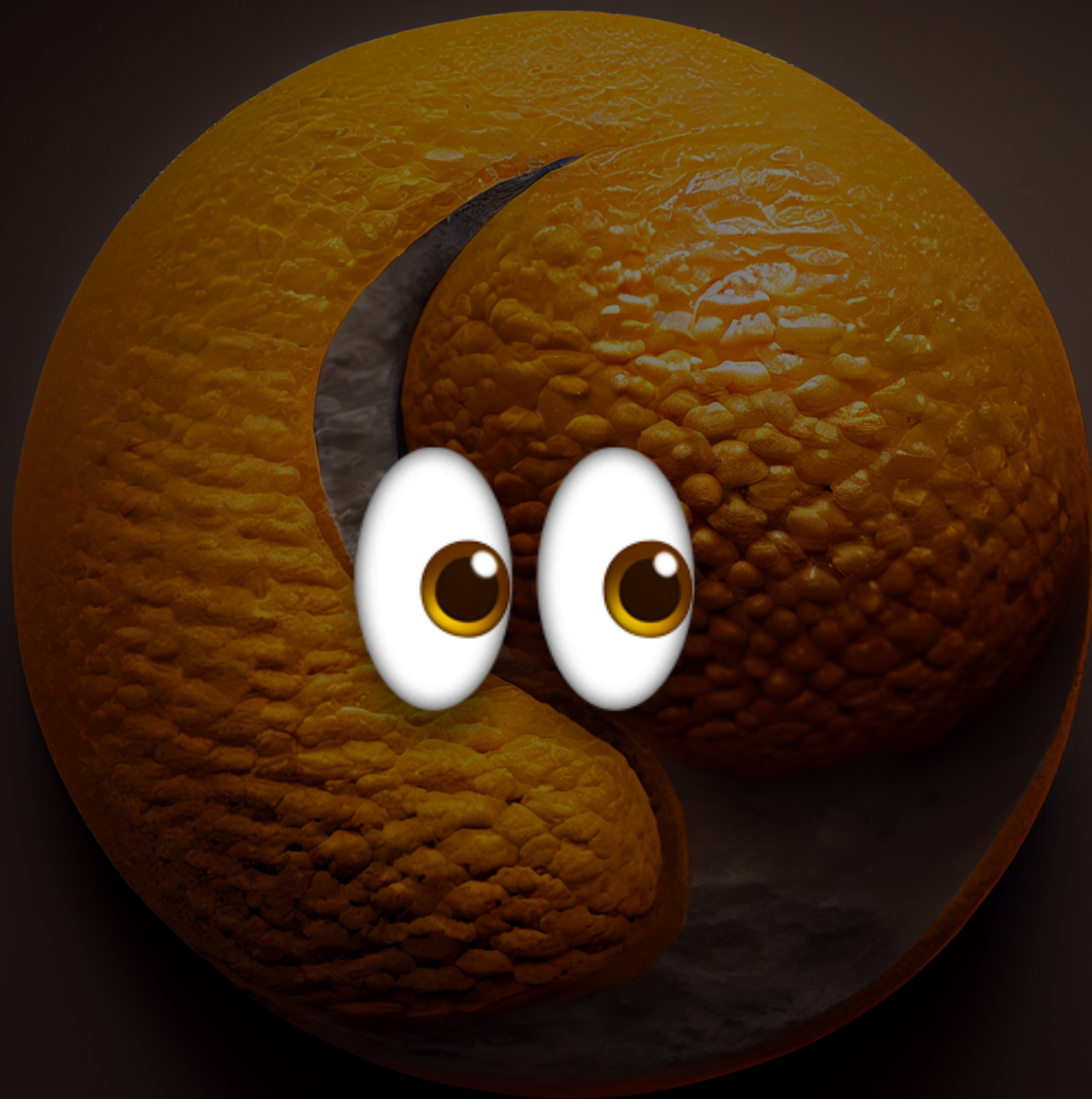


















—Satoshi Nakamoto



think

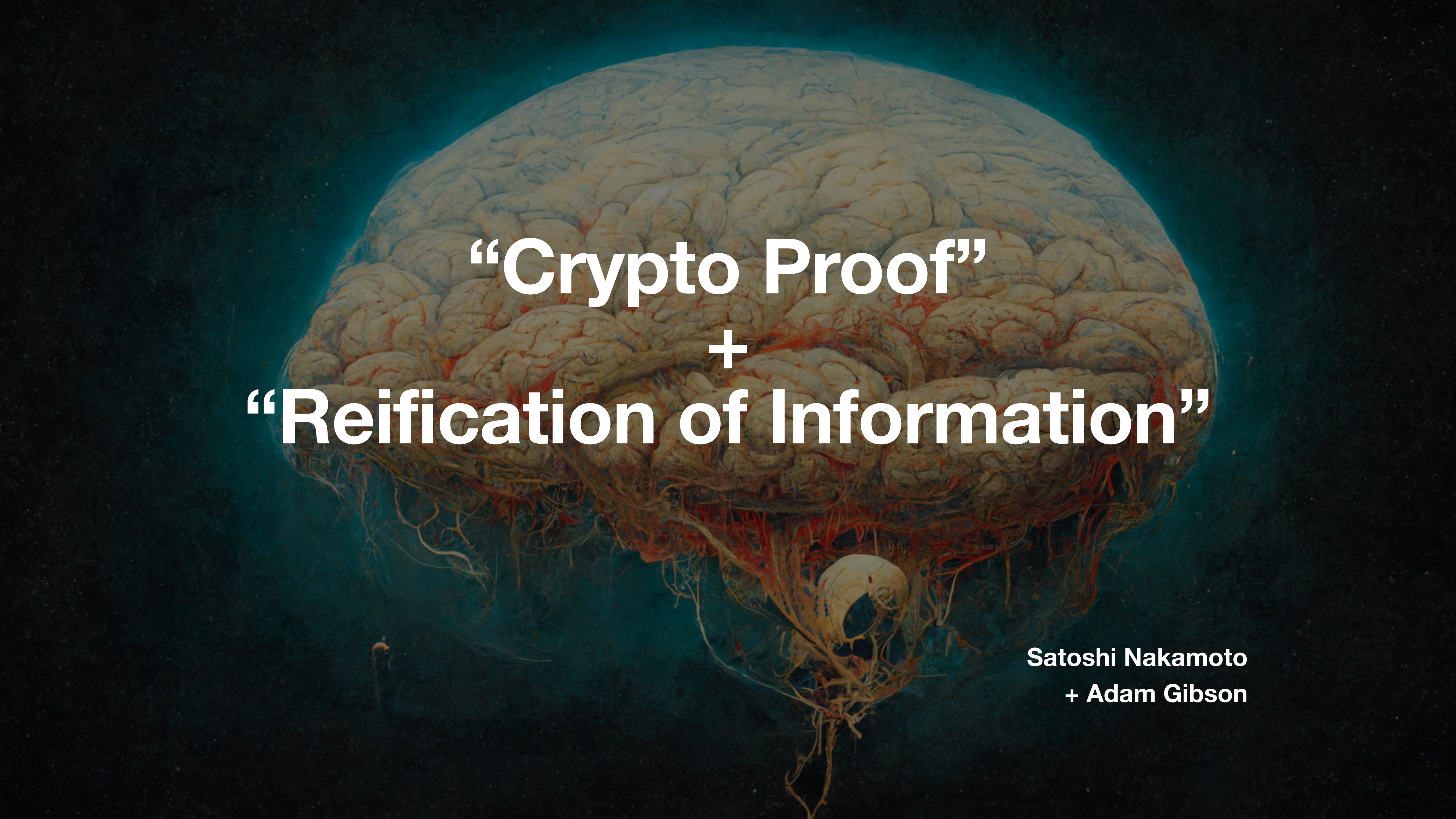
decentralized

—Satoshi Nakamoto



**“I think this is the first time
we're trying a decentralized,
non-trust-based system.”**

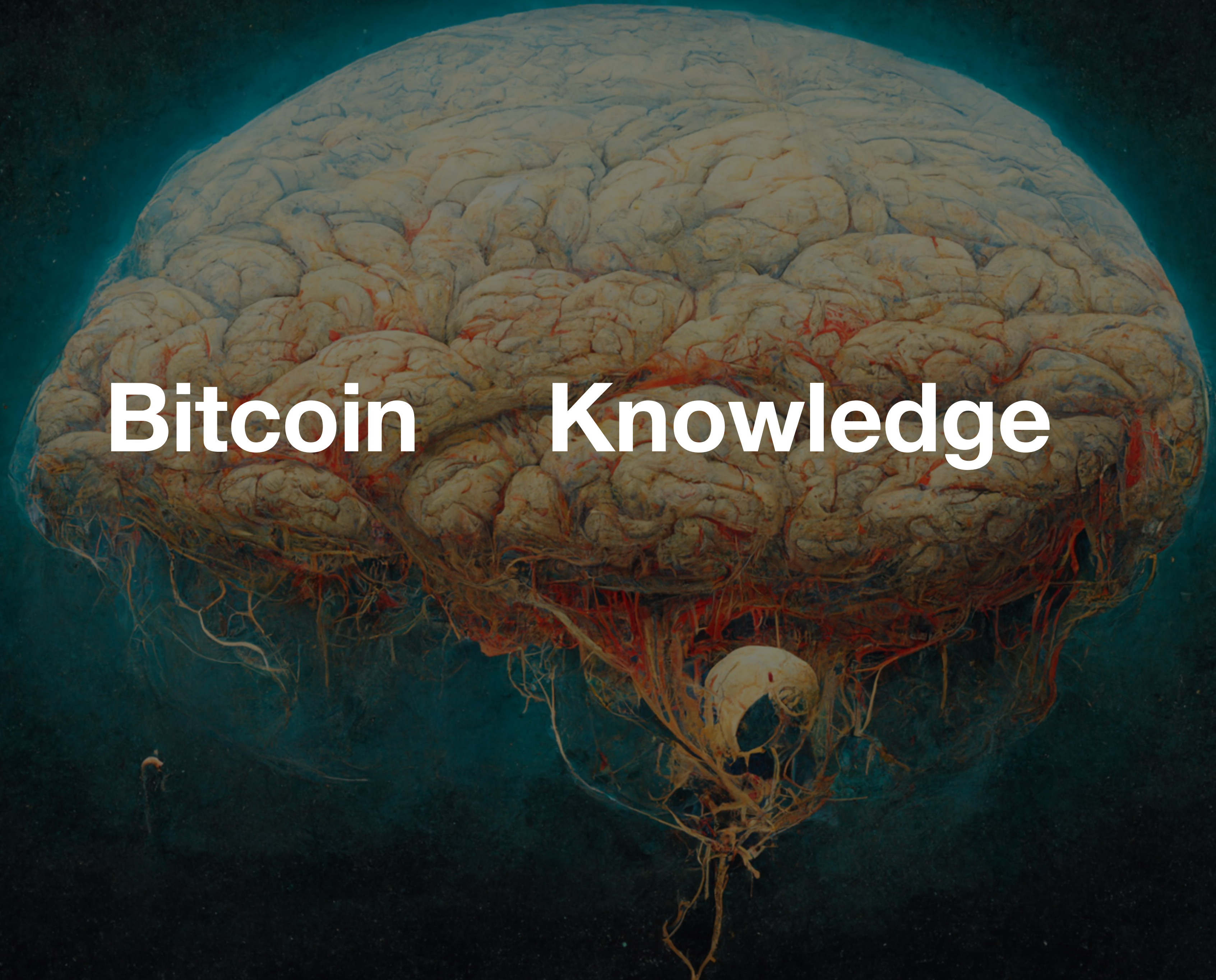
—Satoshi Nakamoto



“Crypto Proof” + “Reification of Information”

**Satoshi Nakamoto
+ Adam Gibson**

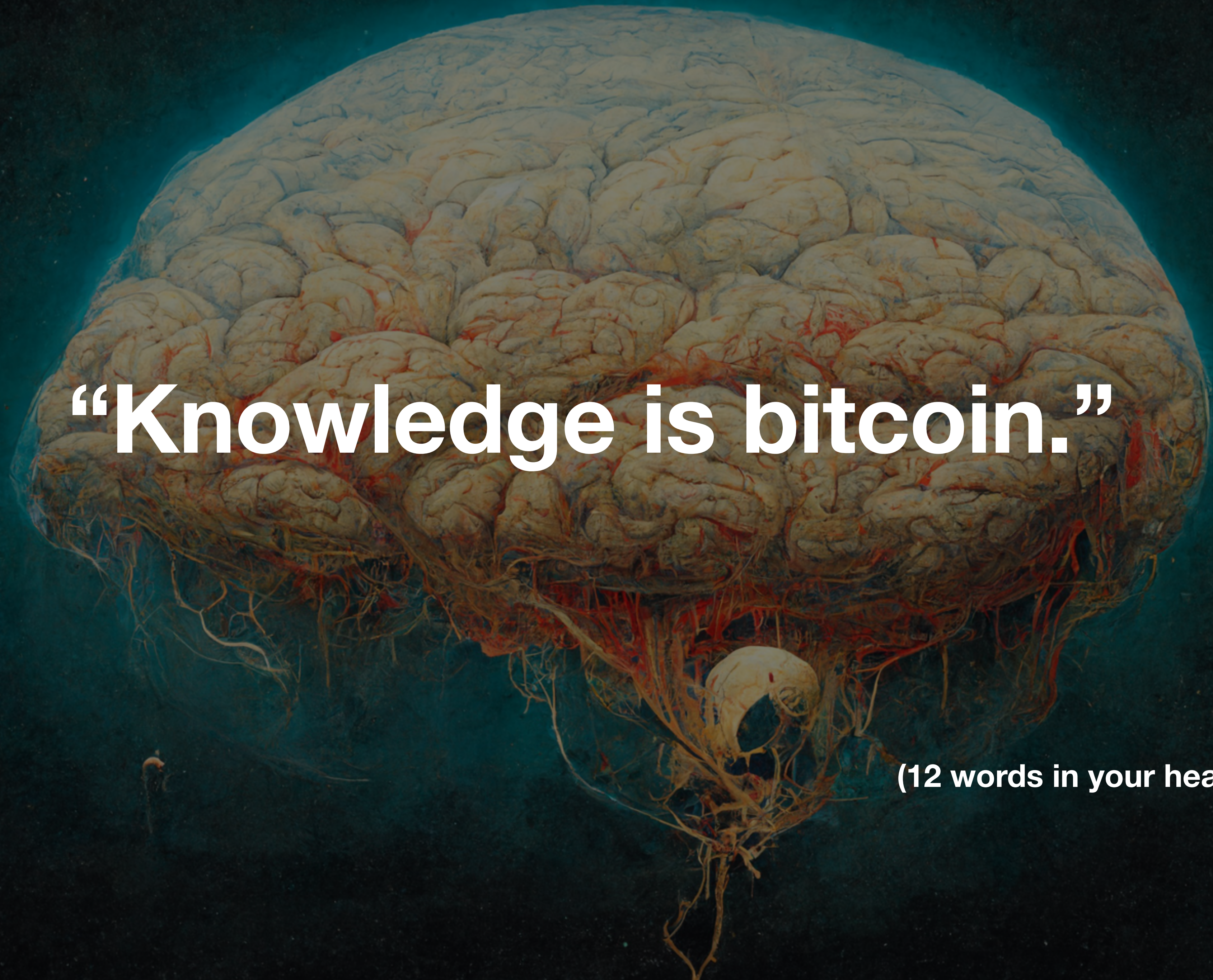
Bitcoin Knowledge





“Bitcoin is Knowledge.”

(Integrity of system, monetary policy, 21 Million)



“Knowledge is bitcoin.”

(12 words in your head)



Knowledge



Bitcoin



Knowledge

Private



Bitcoin



Words





Words



Public & Transparent



Words



Million

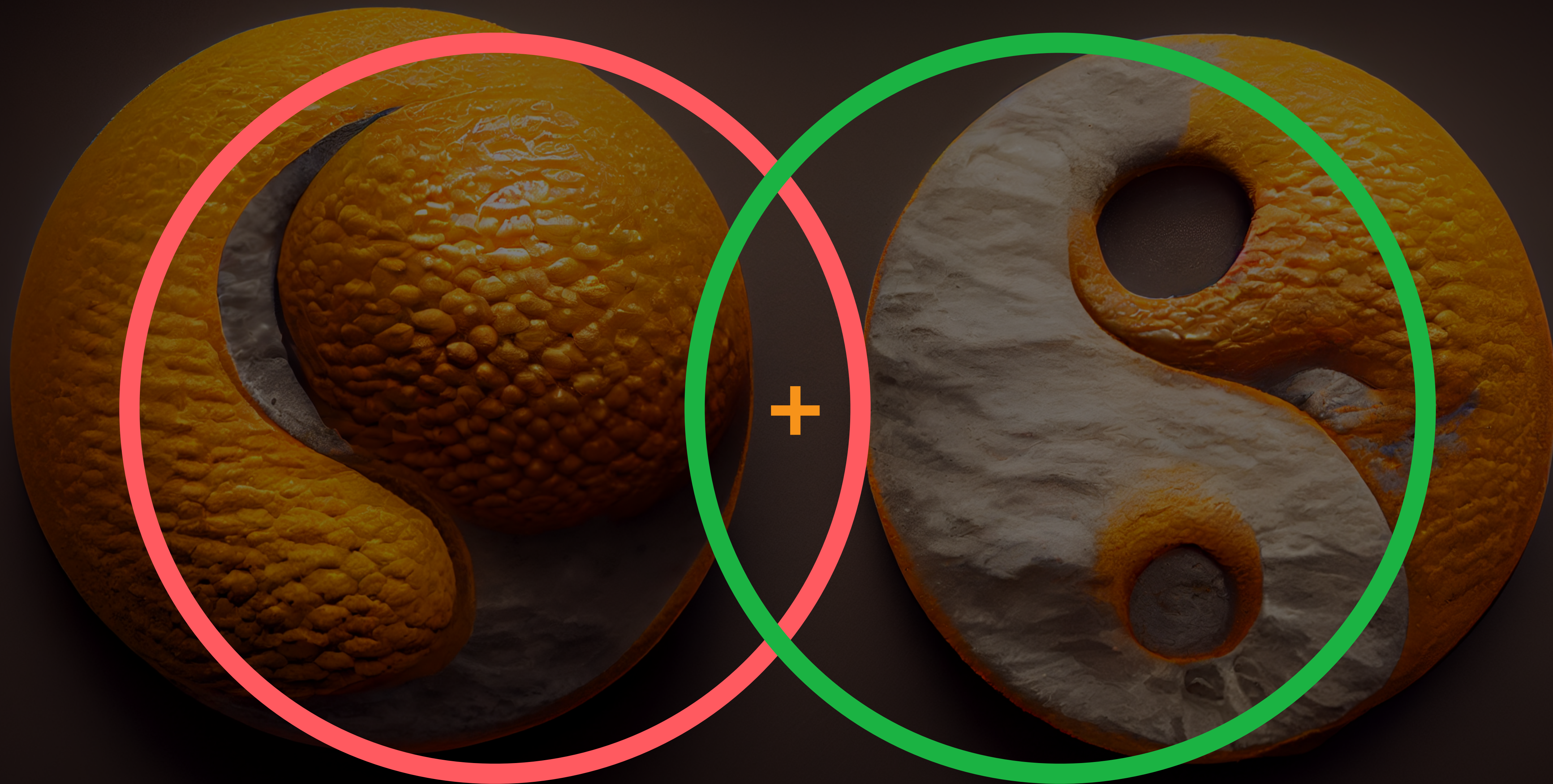


Private Key

+



Public Ledger

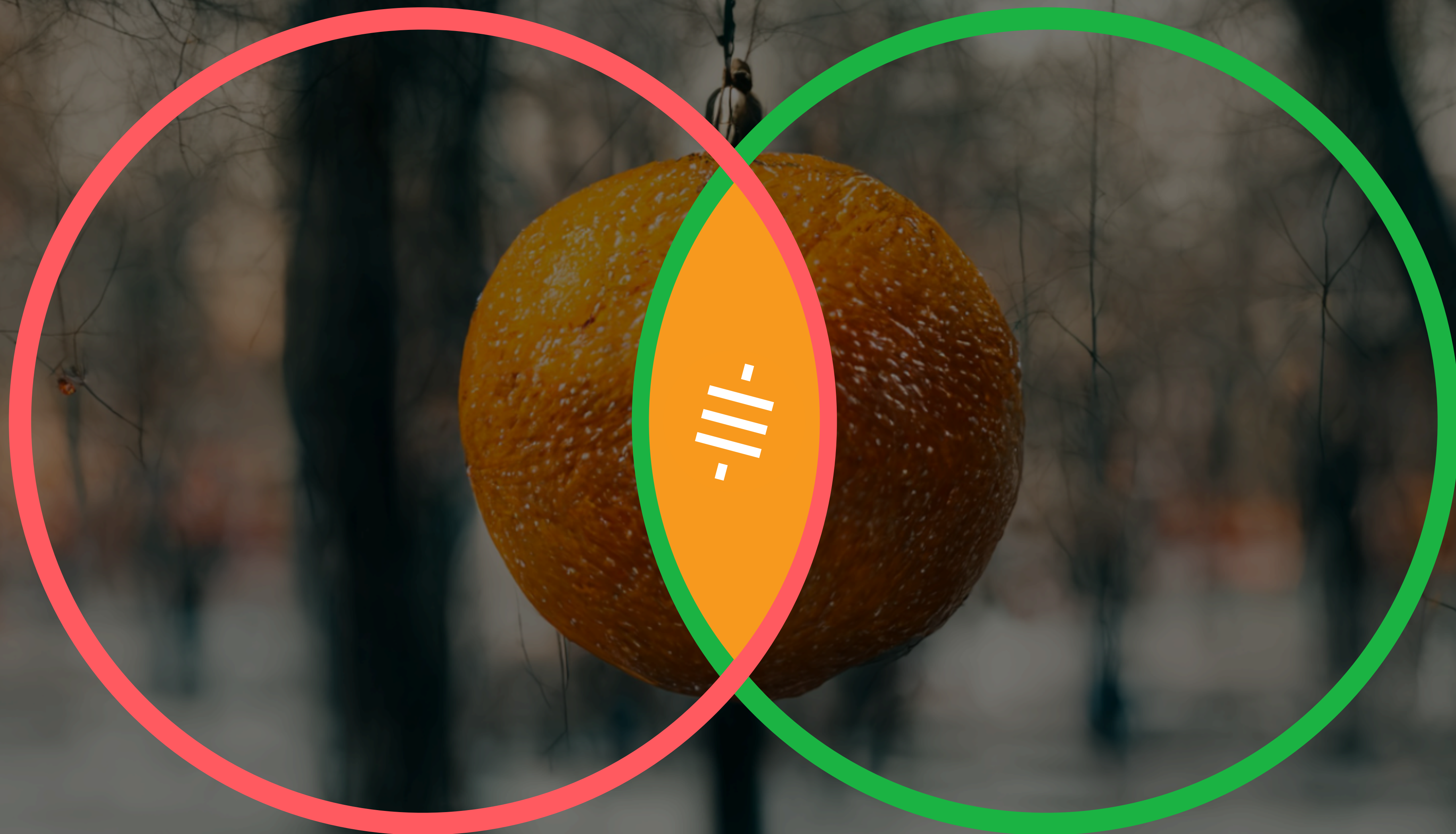




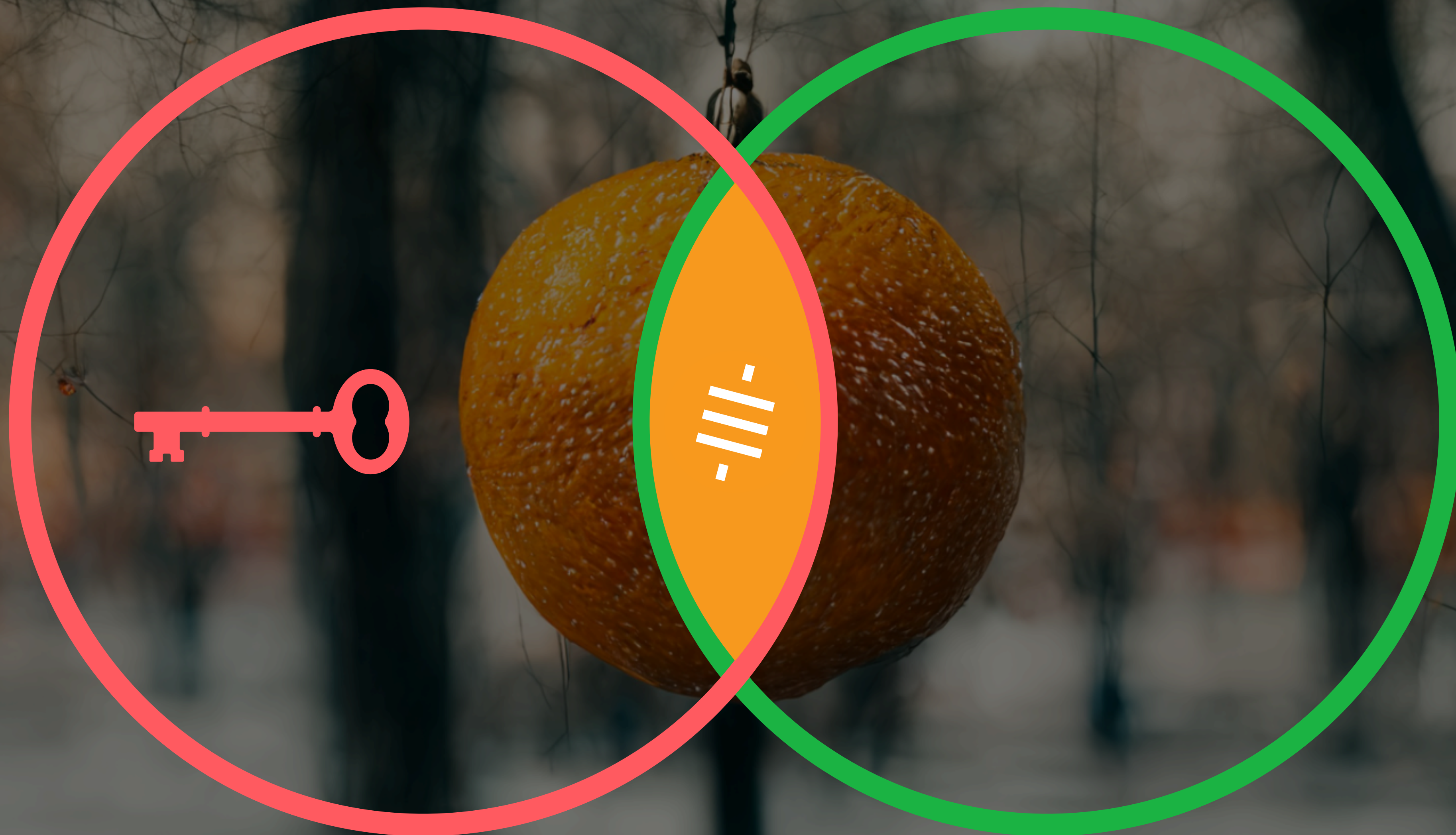
Alice



Bob



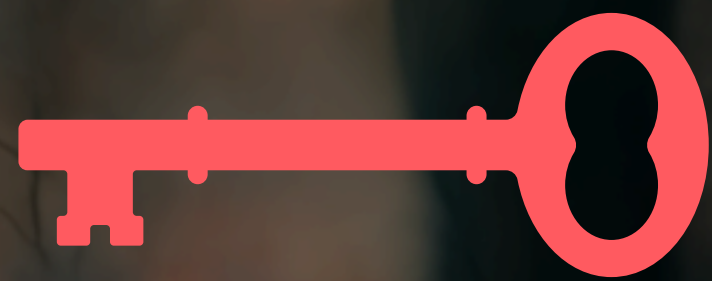
Alice



Bob



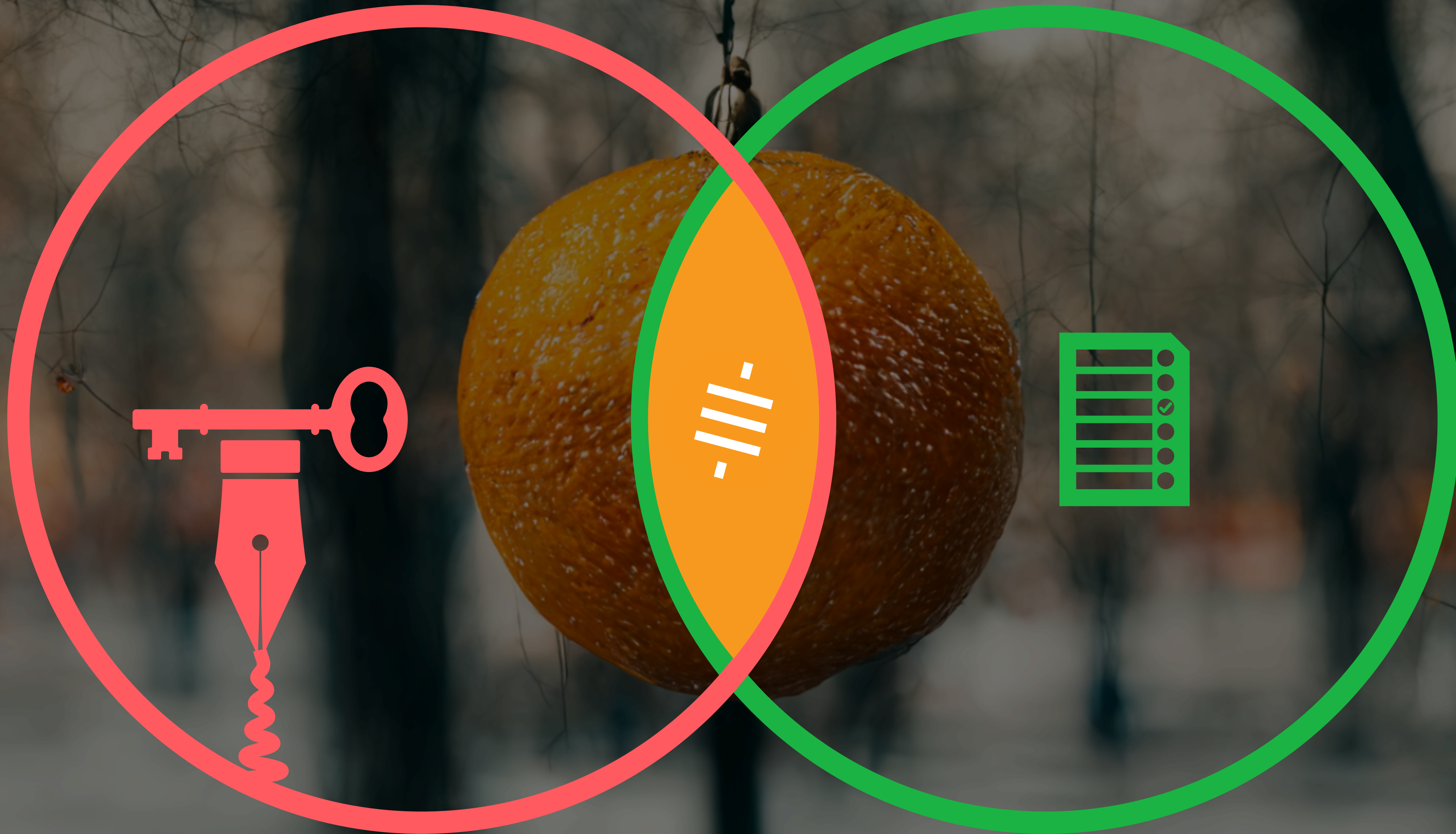
Alice



Bob



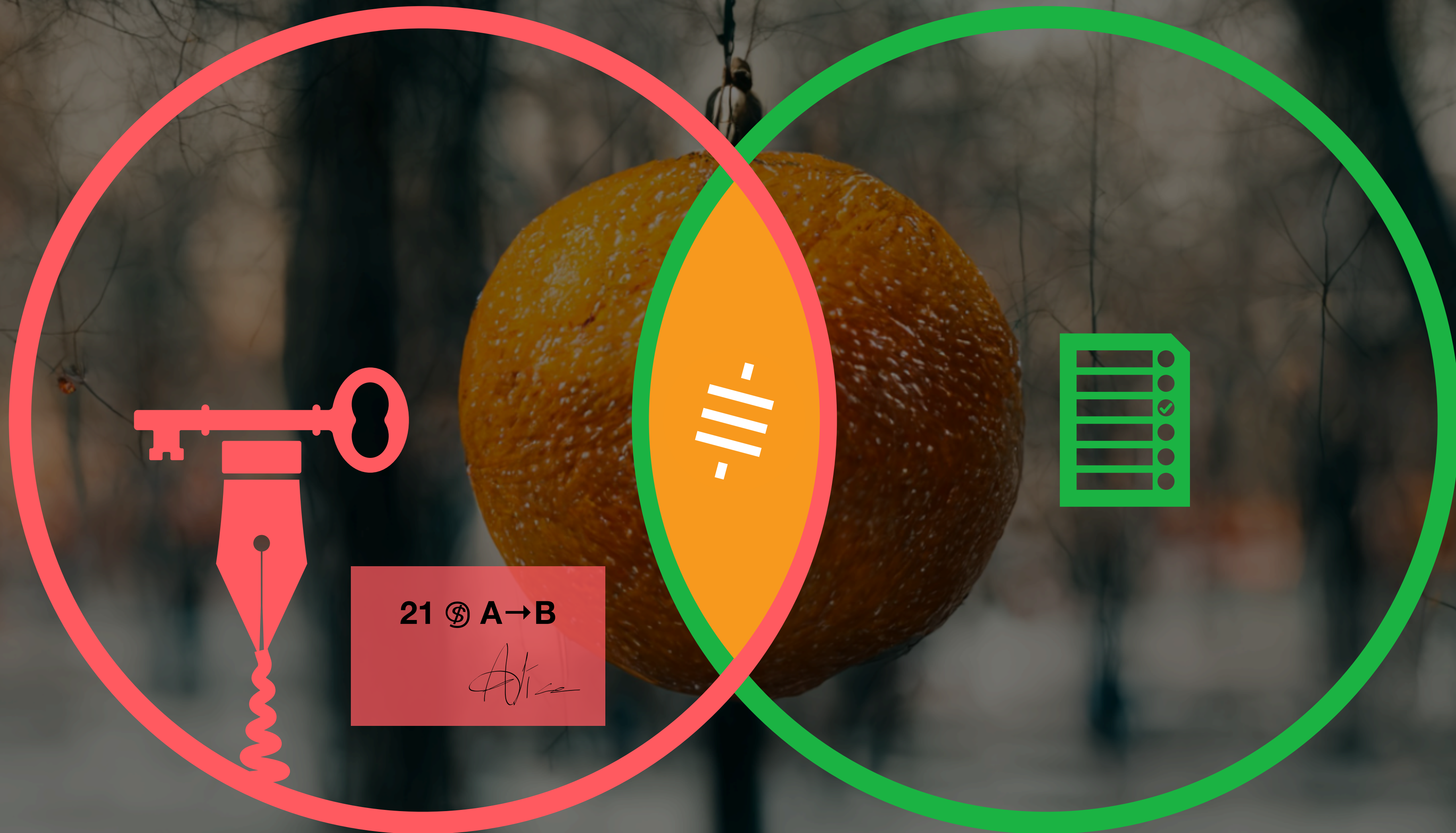
Alice



Bob



Alice



21 \$ A→B

Alice



Network

Alice



Network

21 \$ A→B

Alice

Alice

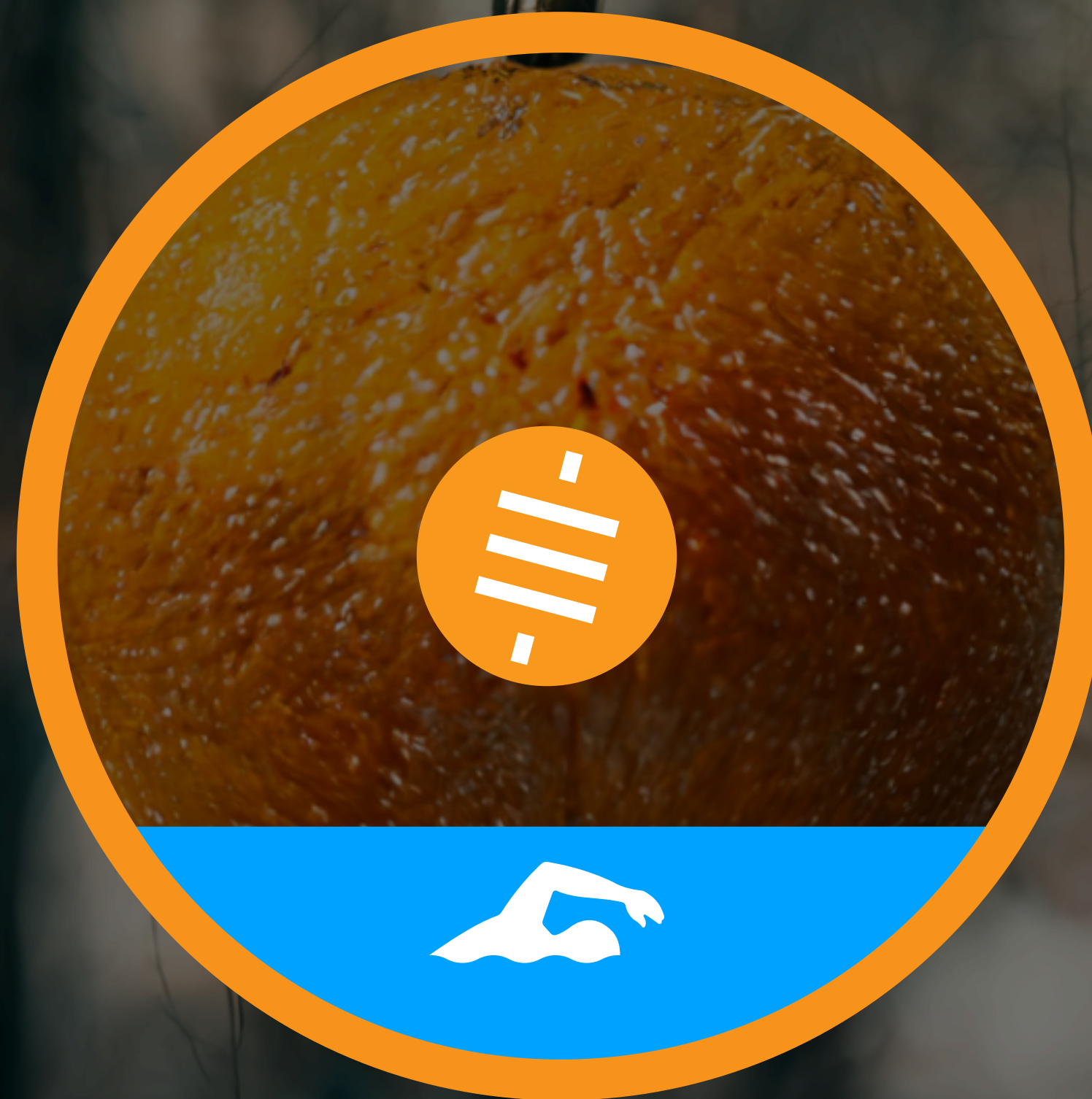


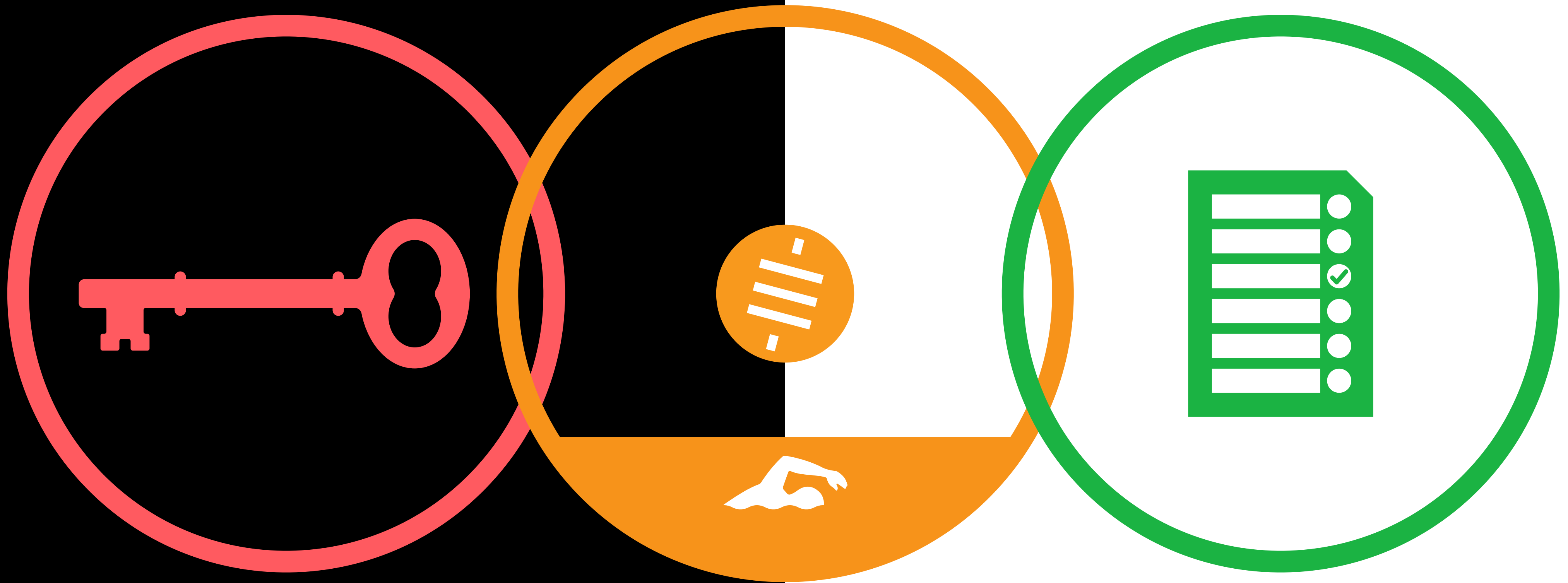
Network

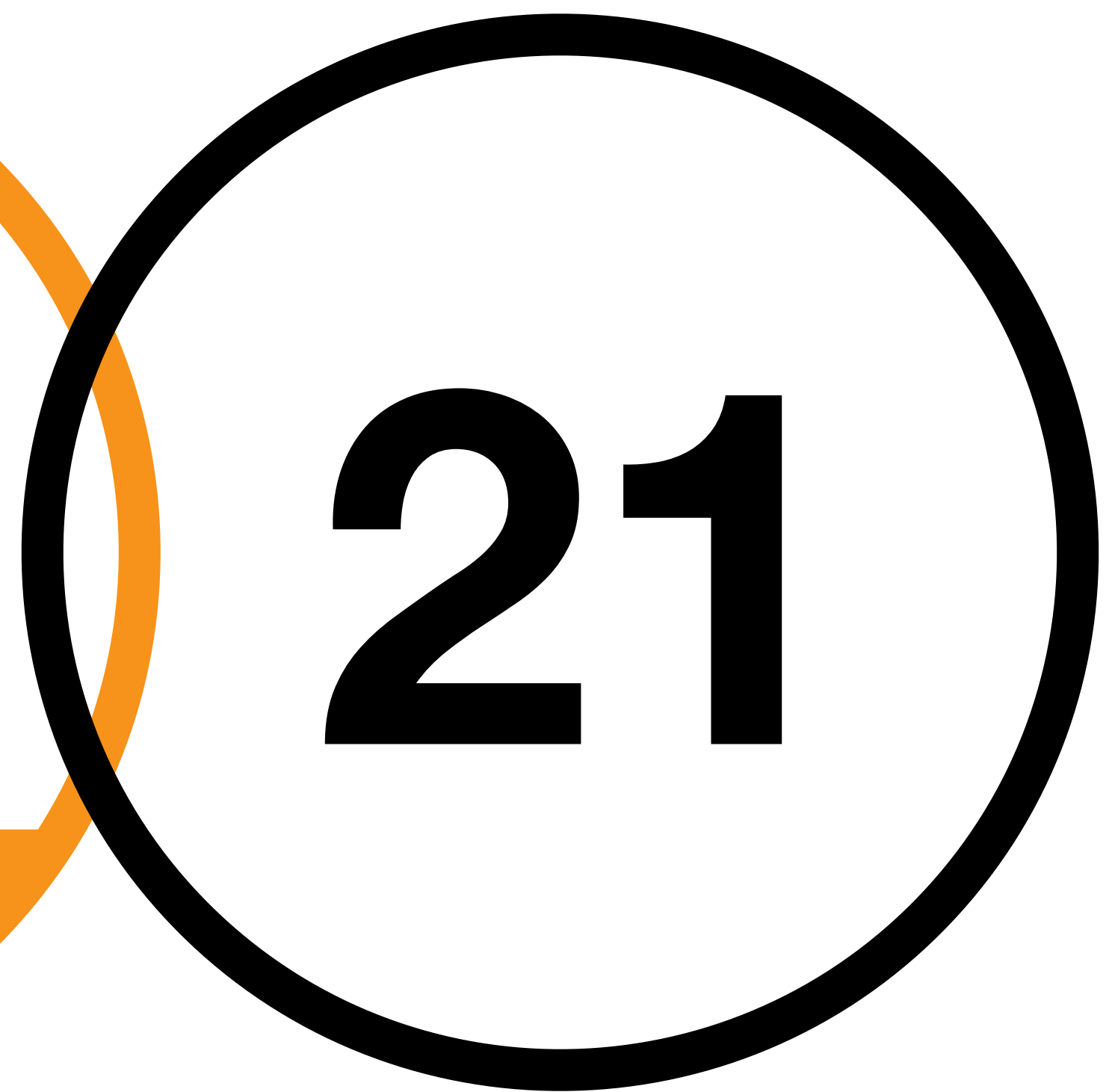
Alice



Network

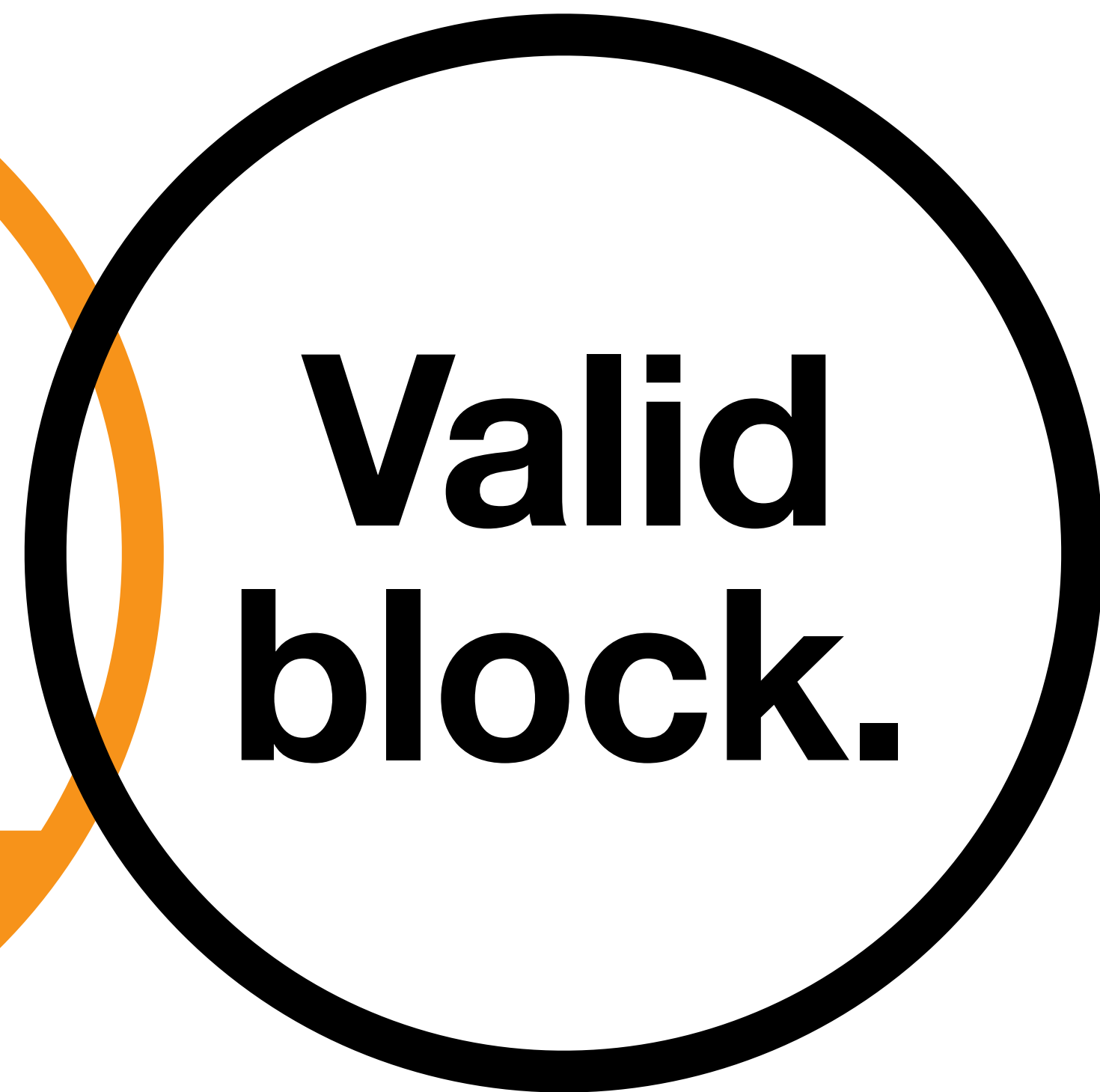








**Valid
sig.**



**Valid
block.**



12



~ 10



21



A large, semi-transparent Bitcoin logo is centered in the background. It consists of a light orange circle with a white Bitcoin symbol (a stylized 'B' with two vertical bars) in the center.

“Transaction confirmed.”



A large, semi-transparent Bitcoin logo is centered in the background. It consists of a light orange circle with a white Bitcoin symbol (a stylized 'B' with two vertical lines) in the center.

“Integrity confirmed.”



A large, semi-transparent Bitcoin logo is centered in the background. It consists of a light orange circle with a white Bitcoin symbol (a stylized 'B' with two vertical bars) in the center.

“Moral code confirmed.”





“You shall not inflate.”
“You shall not confiscate.”
“You shall not counterfeit.”
“You shall not steal.”

—Bitcoin, every 10 minutes.
Without relying on trust.



dergigi.com/support