CatVM: There and Back Again

Abstract

Any attempt to bring off-chain computation to Bitcoin must rely on pre-signed transactions. Pre-signed transactions require either trusted signers or trusted participants, and are typically capital inefficient for operators.

To break out of this model, Bitcoin consensus rules need covenants (i.e. the ability to restrict the future flow of coins). OP_CAT provides covenant functionality and also enables Bitcoin Script to simulate finite state machines. CatVM utilizes both of those properties to encumber BTC with arbitrary computation via a permissionless optimistic withdrawal path.

Our story begins with **Young Rijndael** awakening in a strange land.

Young Rijndael: *Wh... Where am I???*

Clouds appear in the sky to form **Satoshi, the Great Spirit** of the **Isle of Chain**.

Satoshi: *It is I who summoned you to the Isle of Chain!*
Our citizens face a plight. They cannot safely reach the riches of our neighboring isle, Off-Chain.
You are a renowned builder in your land. Can you help us bridge our two lands?

Young Rijndael: *This is a strange land indeed...*
But I will do my best to help your people, Great Spirit!

Satoshi: *Thank you, Young Rijndael.*
Explore the Isle of Chain and see what attempts our citizens have made to reach Off-Chain.
Perhaps their attempts will inspire you...

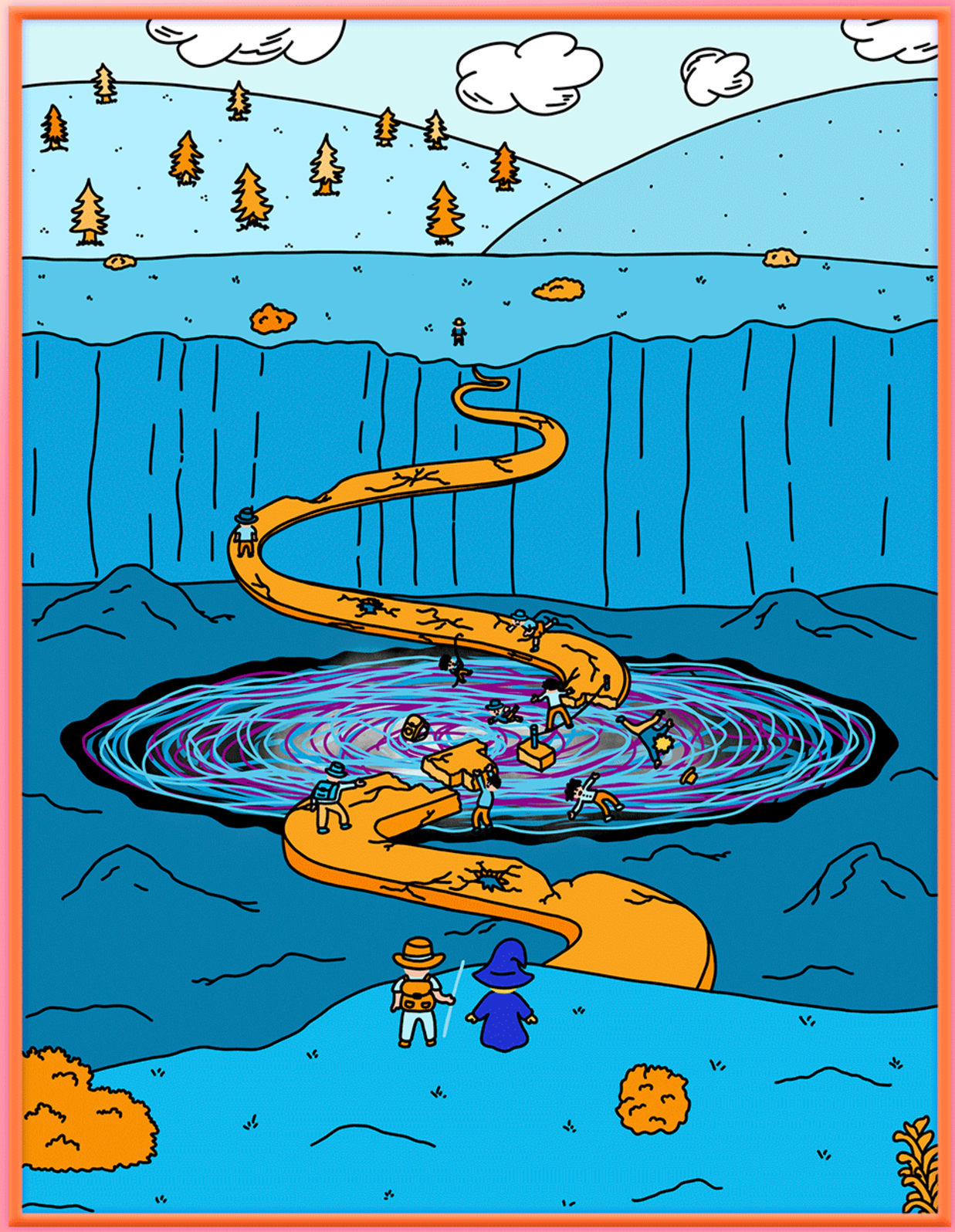
As the **Great Spirit Satoshi** fades away, Young Rijndael begins his exploration of the Isle of Chain.

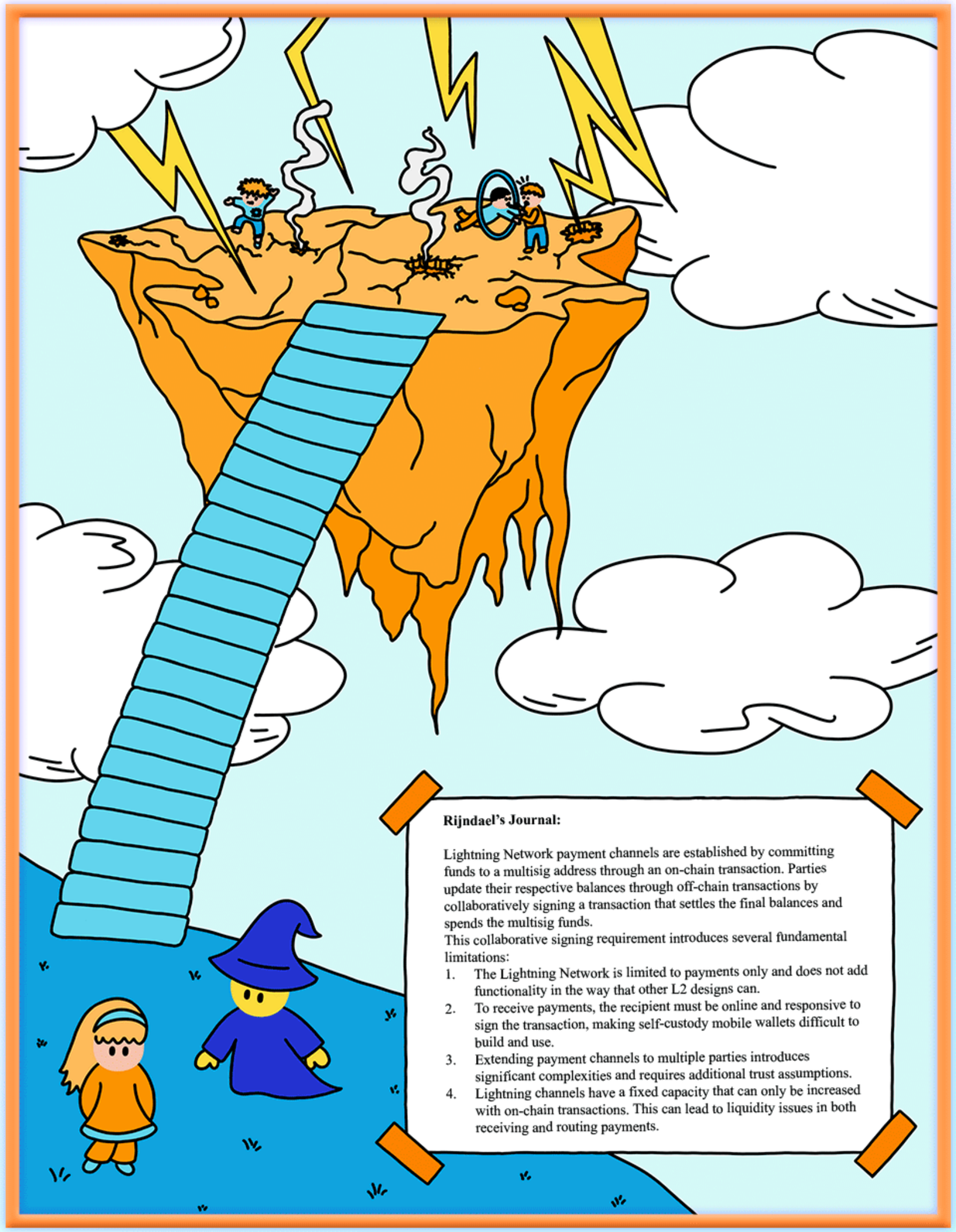
Young Rijndael begins his journey in the **Multisig Madlands**. The region is chaotic and full of **Adventurers** who are attempting to cross the **Multisig Bridge**.

Young Rijndael: *Greetings, brave Adventurer!*
This bridge looks like it could break at any moment.
What if it collapses and you cannot return home???

Adventurer: *That's just the risk we take as adventurers to Off-Chain.*
We know the wormhole will appear and collapse the bridge many times a year.
And we know hackers lie in wait on the other side.
But this is why the Multisig Bridge is only crossed by the bravest and most degenerate adventurers!

Young Rijndael wishes the adventurer luck on his journey across the **Multisig Bridge**. As **Young Rijndael** leaves the **Multisig Madlands**, he glances back and sees the bridge collapsing...





Young Rijndael exits the **Multisig Madlands** and journeys to the **Presigned Peninsula**. There, he first encounters the **Bridge to Nowhere** that leads to the **Lightning Wastelands**. A **Local** is strolling by the bridge. Across the bridge, a sparse number of citizens appear to be doing acrobatics...

Young Rijndael: *Hello madam!*
Why is there a bridge to this barren land?
And is that an acrobat I see amongst the vast nothingness?

Local: *The Lighting Wastelands were once thought to contain the riches of Off-Chain.*
A few delusional citizens still believe riches can be unearthed there.
They continue their mental gymnastics to this day.

Young Rijndael: *The Bridge to Nowhere does look sturdy...*
However, it clearly relies on presigned transactions and cooperative citizens to support it.

Regardless, it doesn't lead anywhere useful.
This is clearly not the bridge the Great Satoshi wishes to see built.

Young Rijndael thanks the Local for her help and continues down the **Presigned Peninsula**.

Young Rijndael continues along the **Presigned Peninsula** until he encounters the thriving **L2 Village**. The L2 Village is flooded with **Builders** and boasts a magical pot of VC gold that never depletes.

Builder: *Ser! I have not seen you around before.*
Come with me and see the marvel we have achieved!

Young Rijndael, eager to see what these exuberant engineers have achieved, follows quickly behind the Builder to the **BitVM Bridge** construction site.

Builder: *Feast your eyes upon this feat of innovation!*
We're basically already to Off-Chain!

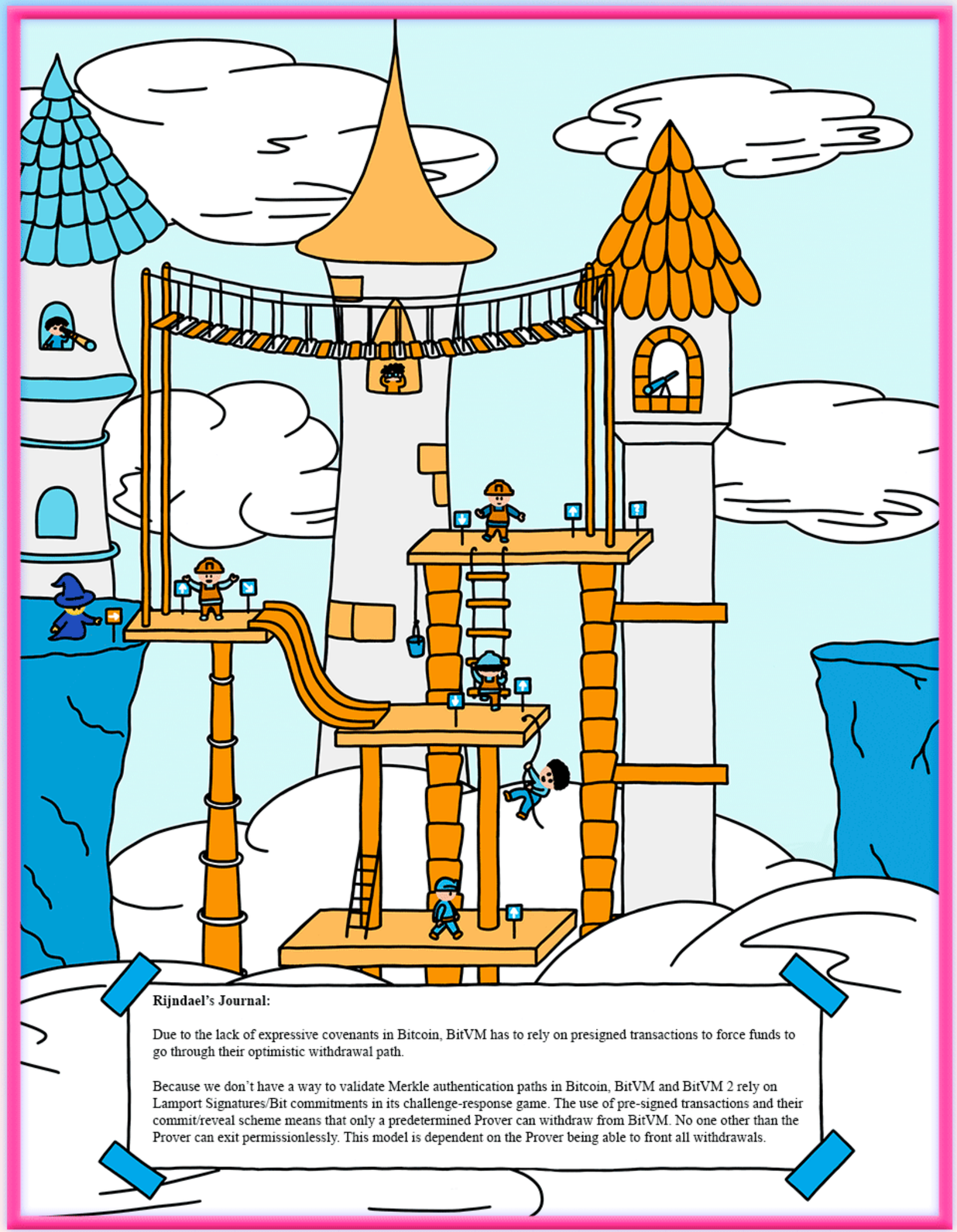
Young Rijndael is taken aback by the horrendously complicated Rube Goldberg construction that lies half complete in front of him. He inspects it closely...

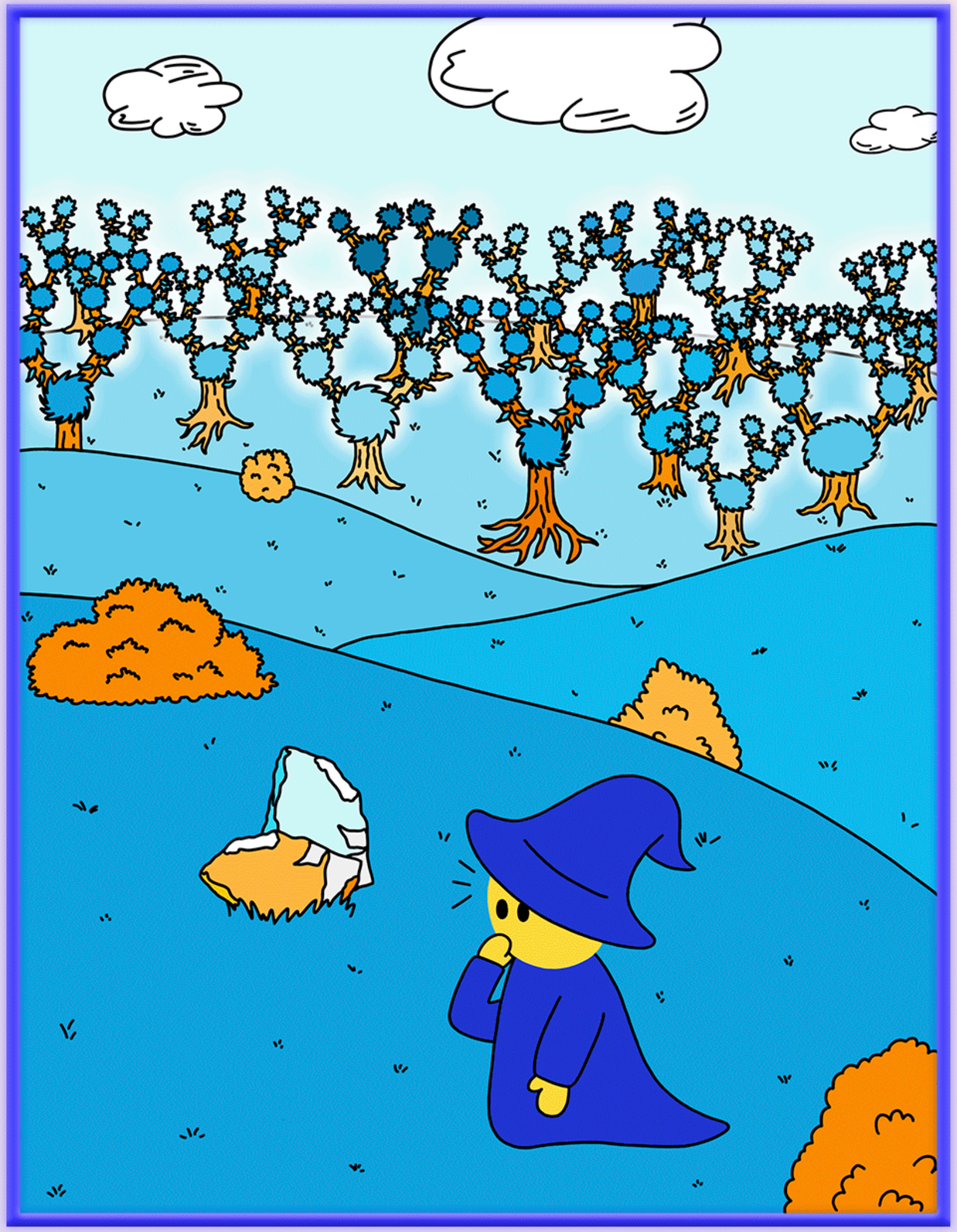
Young Rijndael: *But Builder, isn't this just like the Bridge to Nowhere but infinitely more complicated?!?!*

Builder glances over at the acrobats in the **Lightning Wastelands** and looks offended...

Builder: *No. No!*
This is SO much better!
Our structure combines presigned transactions, hashlock commitments, Merkleized ZK-proof traces, and an EXTENSIVE network of watchtowers watching the bridge to make sure it is safe and supported. As long as we can manage all these presigned transactions and the bridge operator can front all withdrawals, it works perfectly!

Young Rijndael takes a final befuddled look at the **BitVM Bridge** and informs the **Builder** he must be on his way.





After leaving the L2 Village, **Young Rijndael** wanders around the Isle of Chain and contemplates his next steps. He walks by **Permissionless Point** and makes a mental note that it would be a great place to build a bridge from.

Young Rijndael: *I fear that the citizens of Chain will never safely reach Off-Chain.*
The Multisig Madlands will never be stable.
And the Presigned Peninsula is plagued with false promise.

I have explored all the bridges on the isle, and none are safe, functional, and practical.
Surely there must be some construction that can achieve all of this.

It just feels like something is missing...

Young Rijndael grows weary from his journey around the Isle of Chain. He spies a **Merkle Tree Forest** and decides to seek shade there.

As **Young Rijndael** walks into the **Merkle Tree Forest,** a shimmering wave emanates from the woods. The **Quantum Cat** slowly coalesces in the air before him.

Young Rijndael: *Who are you???*

Quantum Cat: *Meow.*

Young Rijndael: *The Quantum Cat you say?*
You were around when Satoshi created the Isle of Chain?

Quantum Cat: *Meow!*

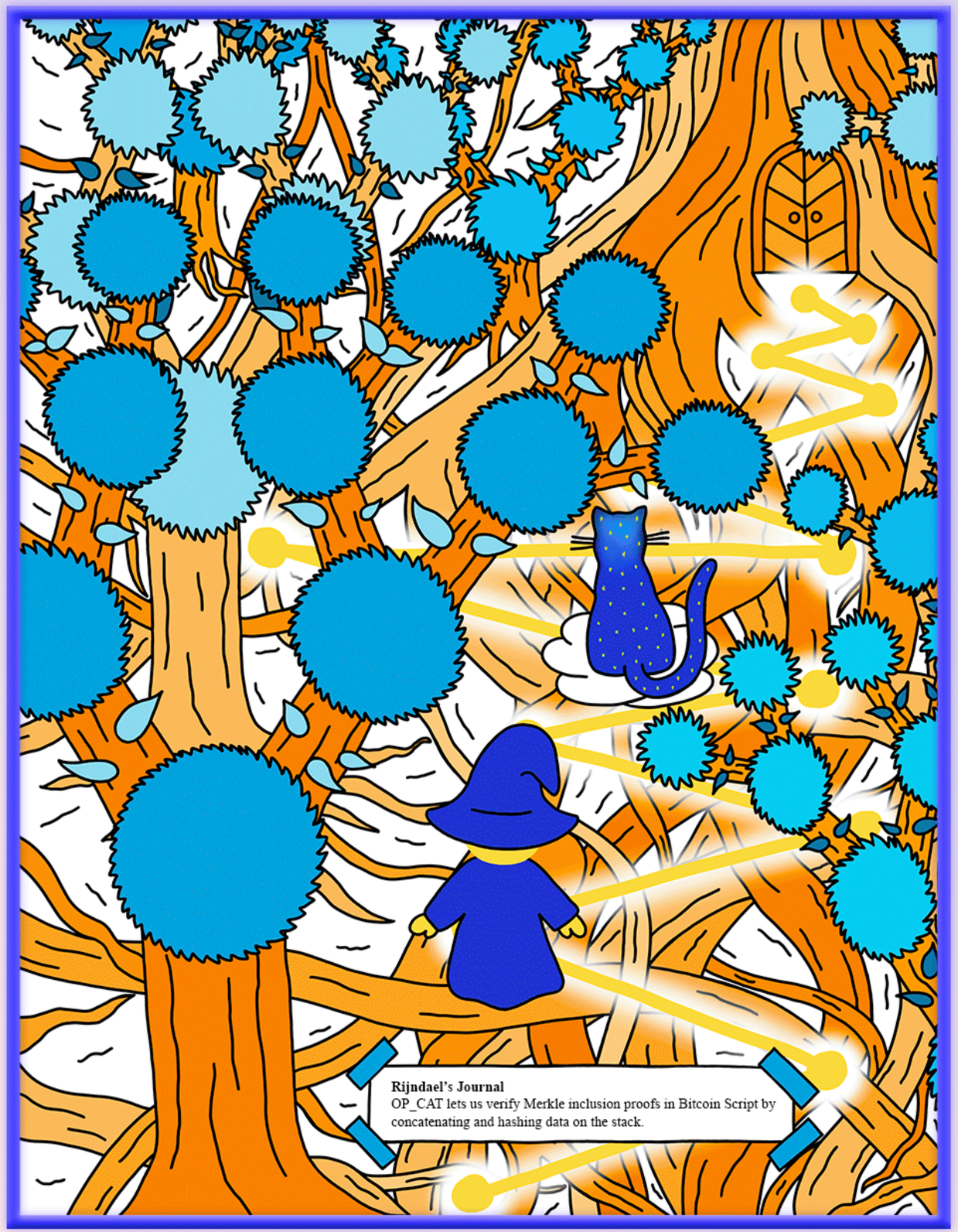
Young Rijndael: *And you were banished to this forest many moons ago?*

Quantum Cat: *Meow!!!*

The **Quantum Cat** begins to float down one of many paths into the **Merkle Tree Forest**. **Young Rijndael** decides to follow... After traversing many branches in the paths, the **Quantum Cat** stops at a collection of massive tree roots.

Young Rijndael: *Wow Quantum Cat!*
You just helped me trace a valid path through the Merkle trees all the way to the roots.
You must be a creature of some power.

Among the roots, **Young Rijndael** spies a door inlaid in a tree trunk and pushes it open...



As he steps through the doorway, **Young Rijndael** finds himself standing among the soaring shelves of the **Library of Spells.** Roots and branches intertwine to house a treasure trove of spellbooks that stretch towards the sky. There is an ephemeral pink luminescence emitted by magical tulips that line each row.

Young Rijndael: *What secrets this hidden library must hold!*
I feel the pull of arcane magic long forgotten...

Young Rijndael begins to stroll down the aisles.

As he compasses the library, the **Quantum Cat** floats behind **Young Rijndael** emitting a soft glow. **Young Rijndael** stops as one book's binding glints in the light.

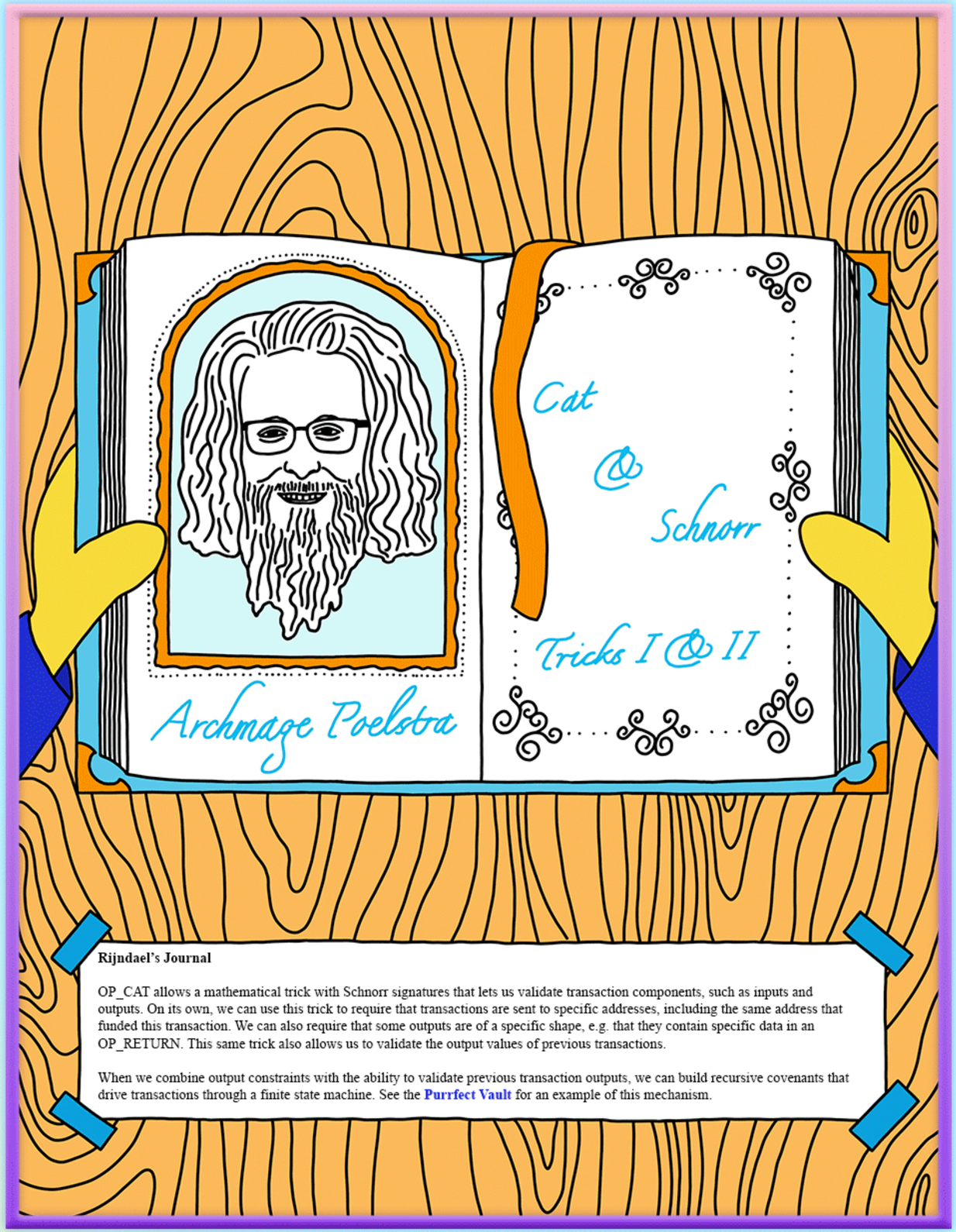
Young Rijndael: *What is this book that seems to be calling to me?*
Cat & Schnorr Tricks: A Spellbook by Archmage Poelstra
I must uncover the mysteries of this spell!

2 hours later, **Young Rijndael** looks up from the Spellbook. His eyes alight with the joy of new knowledge.

Young Rijndael: *Quantum Cat, I've learned that with your powers this spell will let me create recursive covenants and simulate finite state machines!*

This is an incredible breakthrough that I can apply to bridge design.

Young Rijndael decides he must continue to search this library for more forgotten spells.



Young Rijndael continues his exploration of the **Library of Spells**. He walks by one massive book that lays open on a table and dwarfs all the others in the library.

Young Rijndael: *Hmm, this enormous tome is simply called Simplicity.*
Yet it looks like a spell that will never be completed...
I don't believe this is what I'm looking for.

Young Rijndael and the **Quantum Cat** continue searching and find a book slightly ajar from the rest. It has a red hue and the title reads: *MATT - A Spell by Salvatore*. **Young Rijndael** begins reading.

Young Rijndael: *This mage Salvatore must have been truly ingenious!*
His spell describes how to design a bridge that will stand the test of time.

Salvatore has an interesting insight:
The ability to verify a Merkleized program trace combined with a covenant powerful enough to simulate finite state machines will allow us to perform optimistic withdrawals based on arbitrary computation.

Unfortunately it appears to require sorcery inaccessible in this world called OP_CHECKCONTRACTVERIFY.

Young Rijndael paces the library with the Quantum Cat. His mind reels from the mystical knowledge he's just acquired.

Young Rijndael is rejuvenated by the new knowledge he gained. He feels like he's teetering on the edge of a breakthrough.

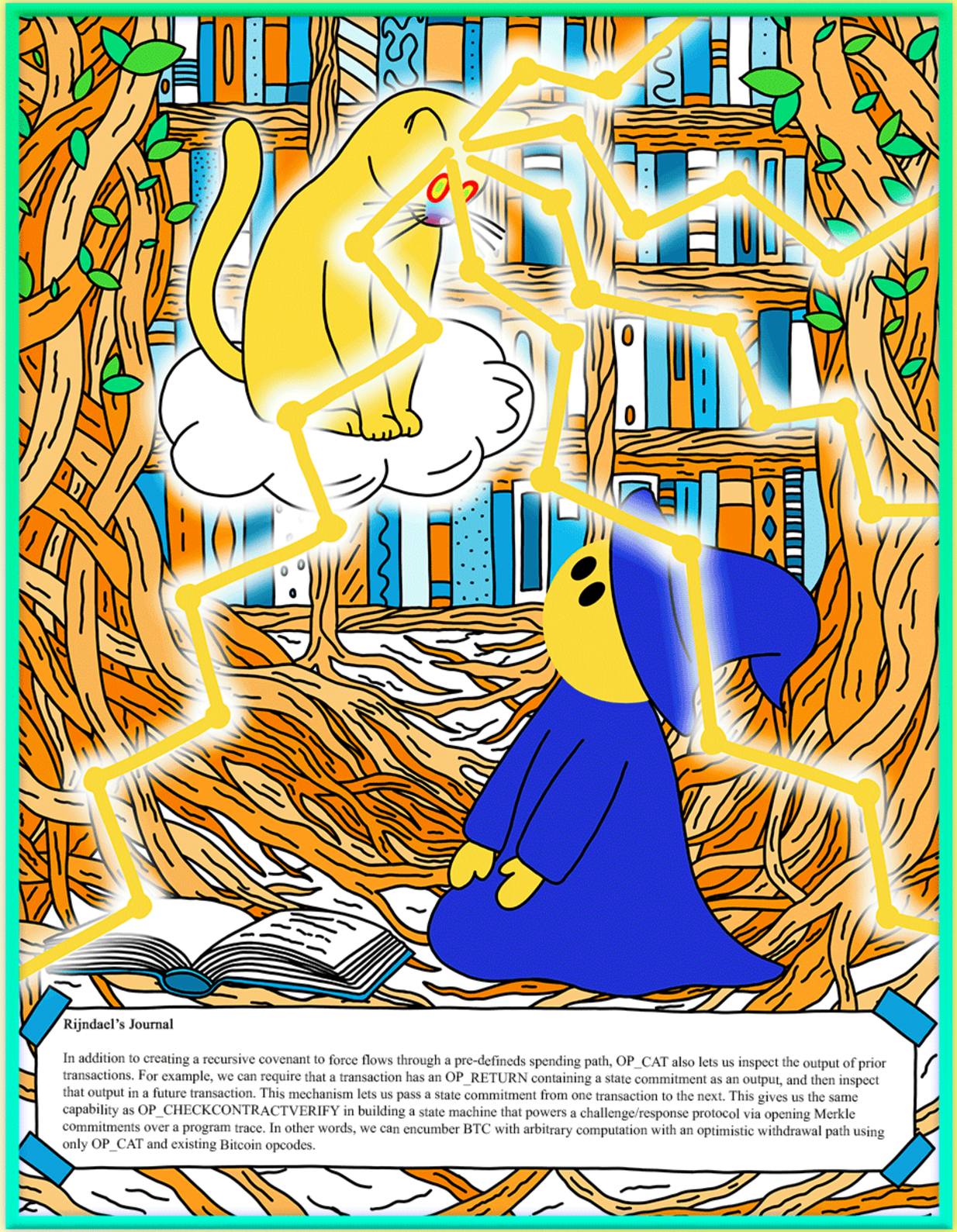
Young Rijndael: *WAIT A MINUTE!*

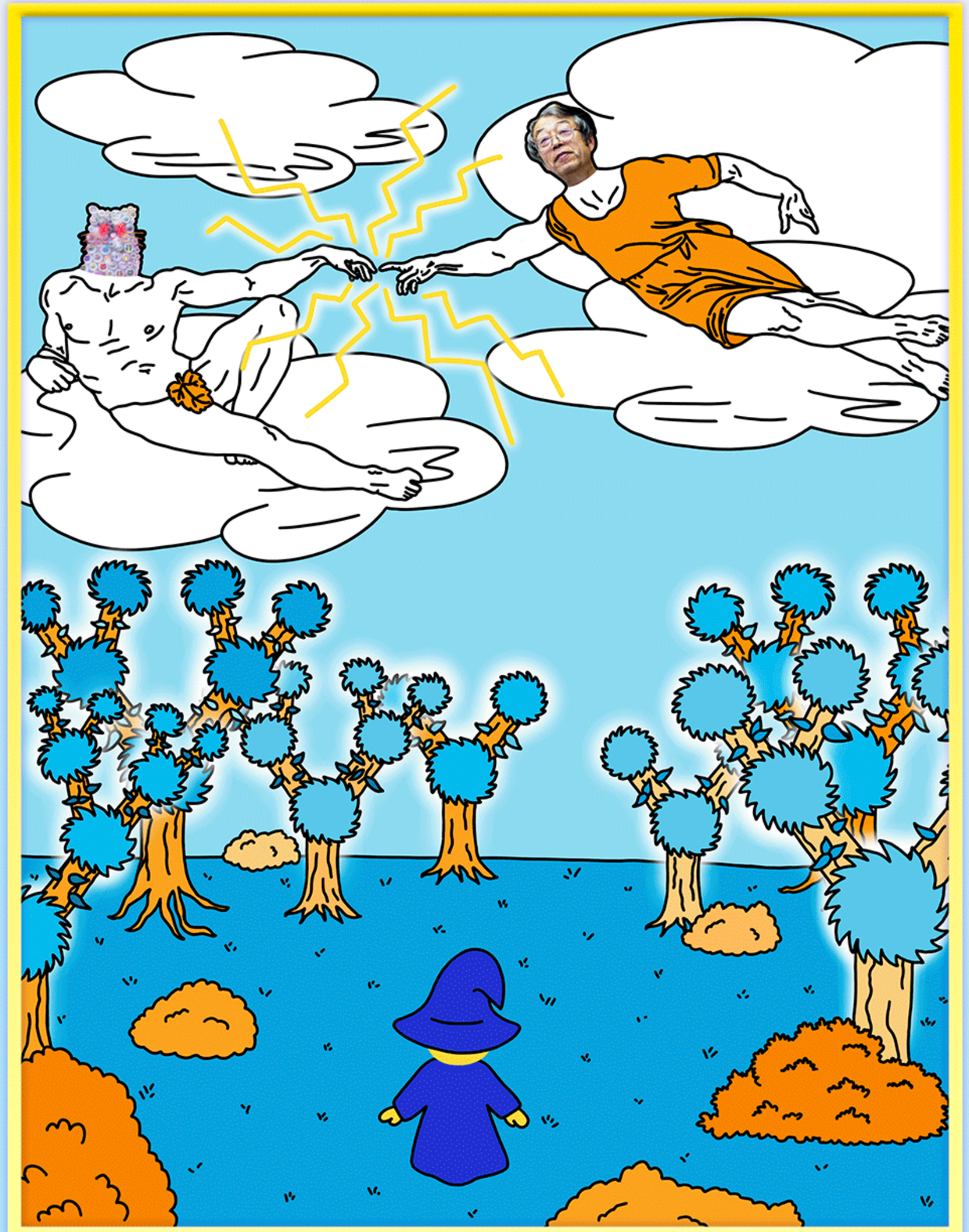
Quantum Cat, your powers let us verify a Merkleized program trace. You showed me that when you led me on the path through the forest!

*And I learned from the Archmage Poelstra that we can simulate finite state machines with your powers too! That means I can cast Salvatore's Spell and construct a permissionless bridge that relies on optimistic validation of arbitrary computation with just OP_CAT!!! I'll call this creation... **CatVM**!*

*Come on Quantum Cat! We have to go to Permissionless Point and begin construction on **CatVM** immediately!*

Young Rijndael rushes through the Library of Spells and back through the **Merkle Tree Forest**. The **Quantum Cat** floats quickly behind. However, as he reaches the edge of the forest, the **Quantum Cat** stops...





Young Rijndael pauses at the edge of the forest and remembers the **Quantum Cat** was banished here by the **Great Spirit Satoshi**. He decides to call upon **Satoshi** and ask for the **Quantum Cat** to be freed.

Young Rijndael: *Great Spirit Satoshi!*
I have journeyed to the Library of Spells in the Merkle Tree Forest.
There I conceived of new magic that will allow me to construct an ideal bridge off of Permissionless Point.
*Behold! I call it... **CatVM**!*

Satoshi: *What is this? You have found a solution to the Isle of Chain's plight???*

Satoshi emerges in the clouds above.

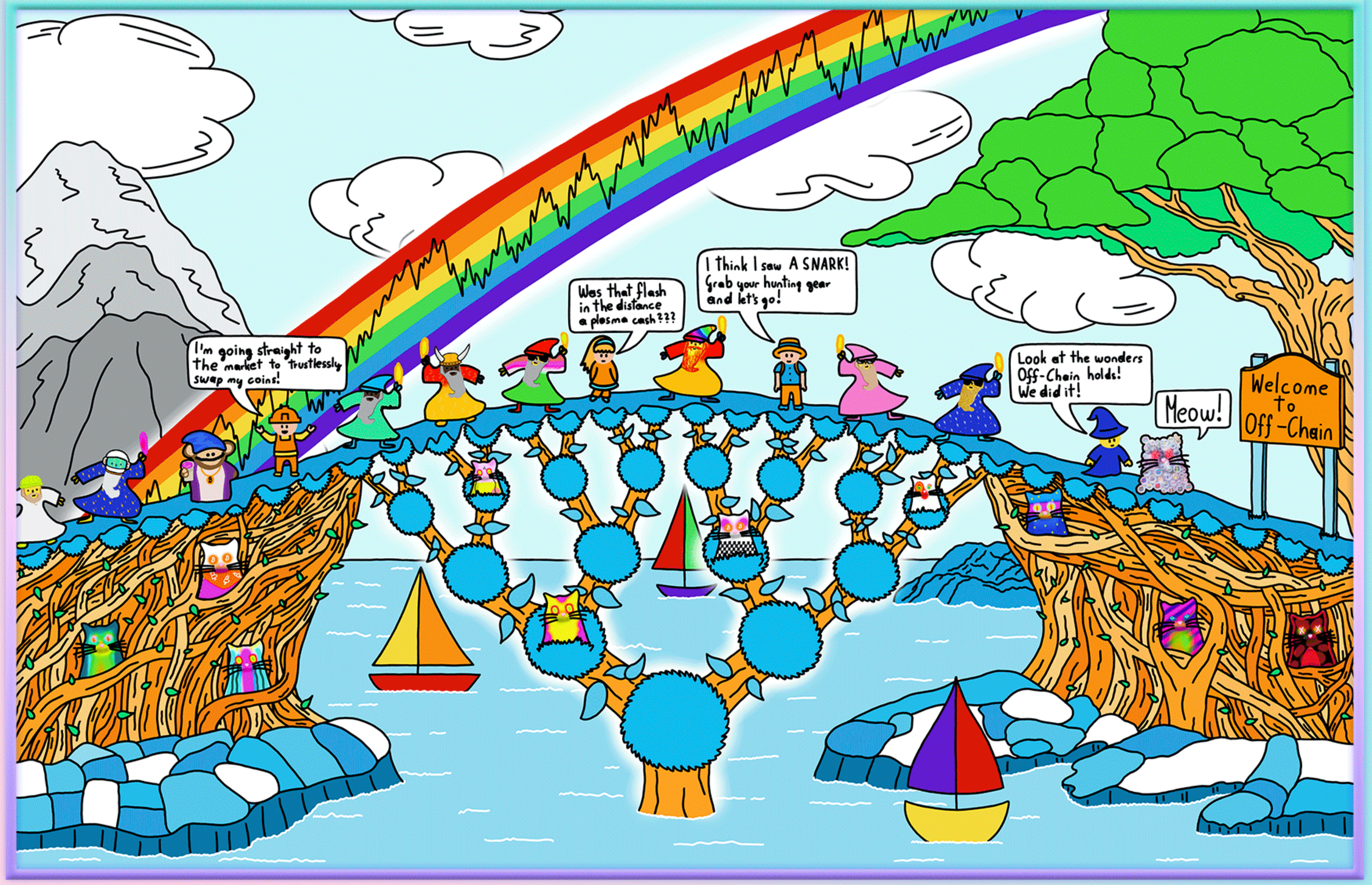
Young Rijndael: *Yes! This bridge has all the characteristics any islander could want!*
ANYONE will be able to cross back and forth - not just the most daring.
The structure is sound and simple.
The costs to create and utilize the bridge will be minimal.
And it will lead directly to the riches of Off-Chain!

Satoshi: *This is truly incredible Young Rijndael! You must begin construction at once!*

Young Rijndael: *I have everything I need except one thing...*
The power of the Quantum Cat!

Satoshi: *I once feared the Quantum Cat's power was too great.*
But the Isle of Chain has grown since that age. I believe it is time...
QUANTUM CAT, I RELEASE YOU!

Young Rijndael thanks **Satoshi** for seeing reason, and sets out to construct **CatVM** with the **Quantum Cat** off of **Permissionless Point.**


I'm going straight to the market to trustlessly swap my coins!
Was that flash in the distance a plasma cash???
I think I saw A SNARK! Grab your hunting gear and let's go!
Look at the wonders Off-Chain holds! We did it!
Meow!
Welcome to Off-Chain

The **Great Spirit Satoshi** floats above with the **Quantum Cat**. Along with **Young Rijndael**, they reflect on the marvel they achieved with the **CatVM bridge**.

Satoshi: *CatVM has safely linked the Isles of Chain and Off-Chain.*

Your work for the citizens of Chain is complete.
I will now return you to your world, Young Rijndael.
But take with you this token of our undying gratitude.

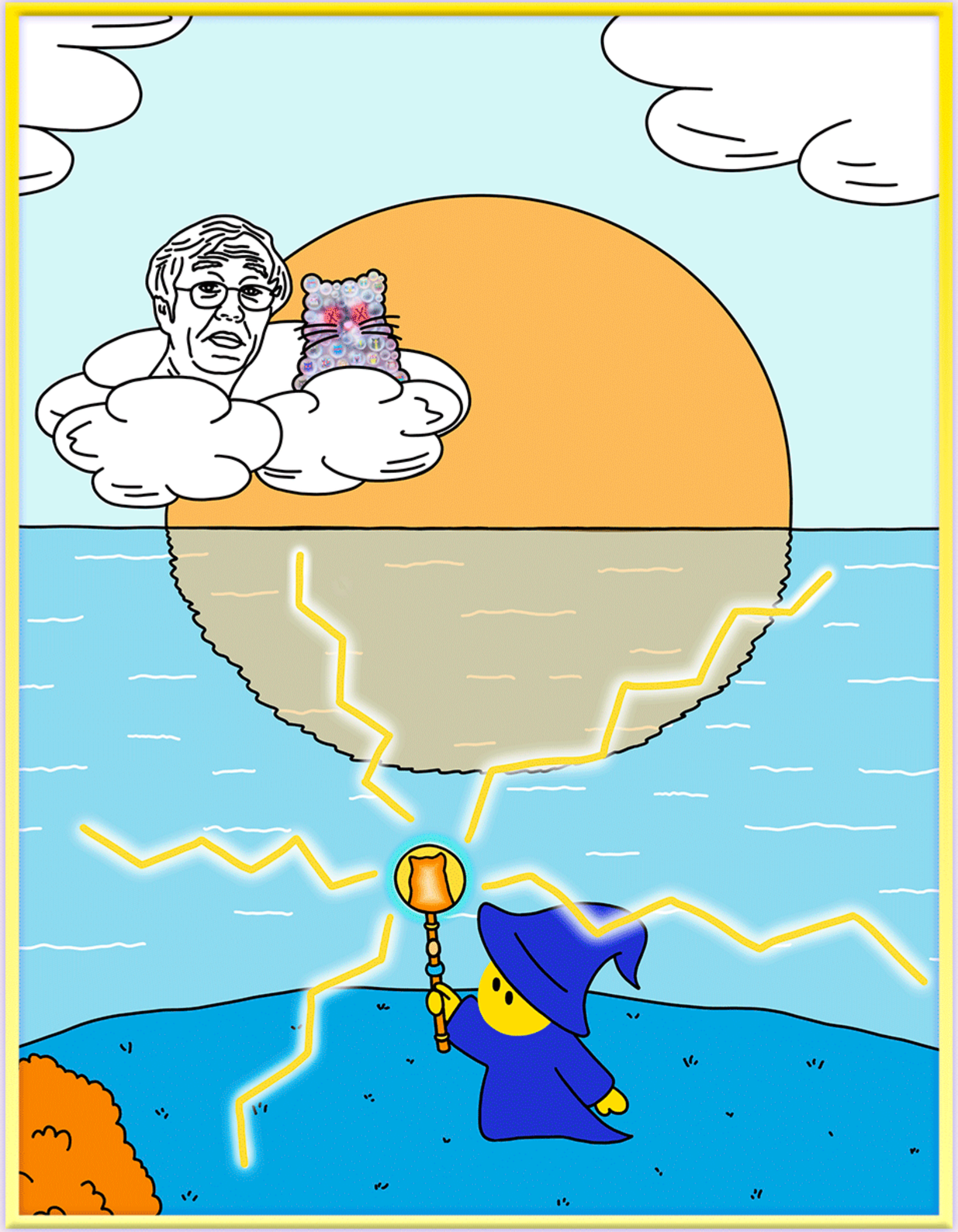
As **Young Rijndael** begins to fade, a shining wand appears in Rijndael's hand with the **Quantum Cat** intricately etched onto it.

Satoshi: *This wand is a covenant that will link you to the Isle of Chain forever.*

Whenever you wish to return to us, merely wave your wand and speak the words "meow meow meow". Farewell for now, Young Rijndael. Perhaps one day we shall meet again...

As **Young Rijndael** fades back into a dream, **Satoshi** and the **Quantum Cat** walk off into the sunset.

FIN



CatVM: There and Back Again

by Taproot Wizards

Art by Theresa (@theresalieb)

Join us: https://discord.gg/taprootwizards