www.komodoplatform.com

WELCOME TO PRESENTATION

Presented By

Chris ‘Diesmaster’ van Maarseveen

Jr. Marketing Manager

Chris ‘Diesmaster’ van Maarseveen

I work on coin integration of BarterDEX, and give presentations.

© 2017 Copyright | All Rights Reserved

This presentation is about

Delayed Proof of Work

Komodo Platform

This consensus method is used throughout the Komodo Platform, not only the komodo Coin.

But before we can discuss the D, we first need to discuss the PoW

© 2017 Copyright | All Rights Reserved

INSERT YOUR GREAT SUBTITLE HERE

Proof of Work

Digital money

In 2008 Satoshi Nakamoto thought of the Proof of Work principle. There had been previous attempts to make digital money, but they had all been shut down by governments.

© 2017 Copyright | All Rights Reserved

The Evolution of PoW

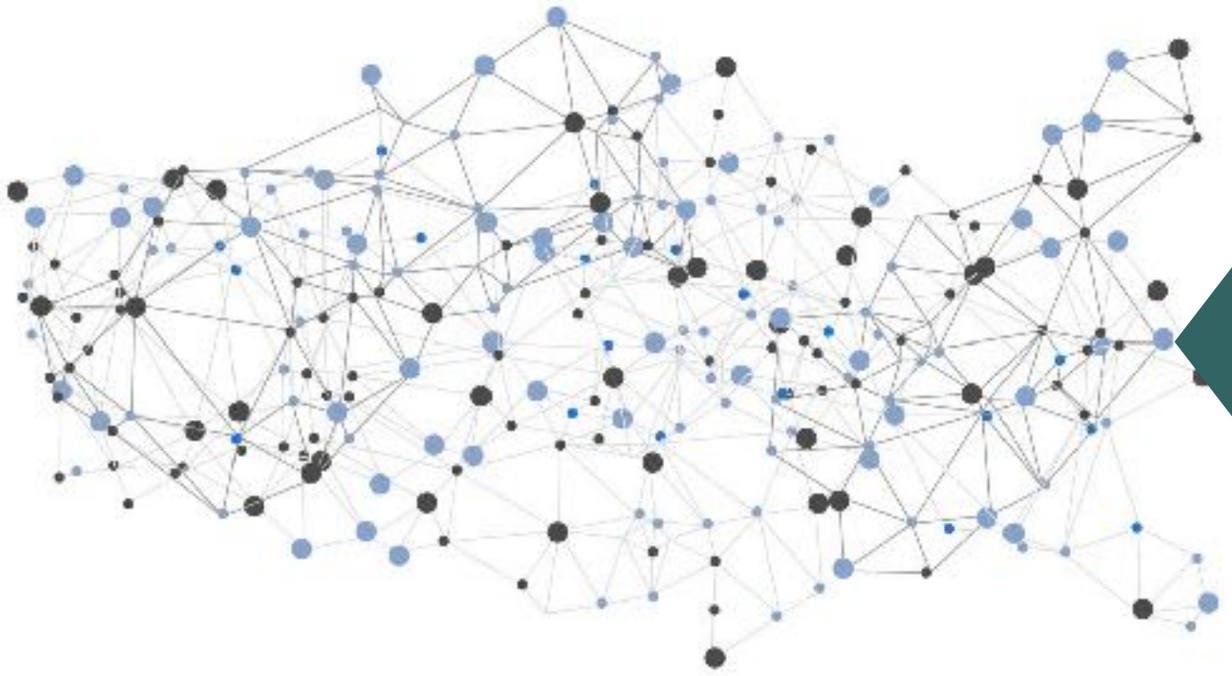
01 Digital Cash

What if I made a bunch of word documents with 1 Komodo on them? Would this work as money?

02 Problem

No, it is on a computer, so everybody can just copy past it a bunch of times and be rich.

© 2017 Copyright | All Rights Reserved



03

DLT, the solution of this is to give the spreadsheet that now banks own with a name and an amount of money to everyone. Now I can't lie that I have more money because everybody can check it

03

This technique was thought of first by the Dutch east indie company the VOC. To protect themselves against boat owners that would tell the VOC they had less cargo then they actually had. The VOC gave the cargo logs to multiple boat owners at the same time

INSERT YOUR GREAT SUBTITLE HERE

04

blocks

Now we have a log that can not be changed, but sometimes change is needed. You can submit a change in the logs Al a transaction, and then the miners can verify your change. This will be placed in a block.

© 2017 Copyright | All Rights Reserved

INSERT YOUR GREAT SUBTITLE HERE

05

=

79054025
255fb1a2
6e4bc422
aef54eb4

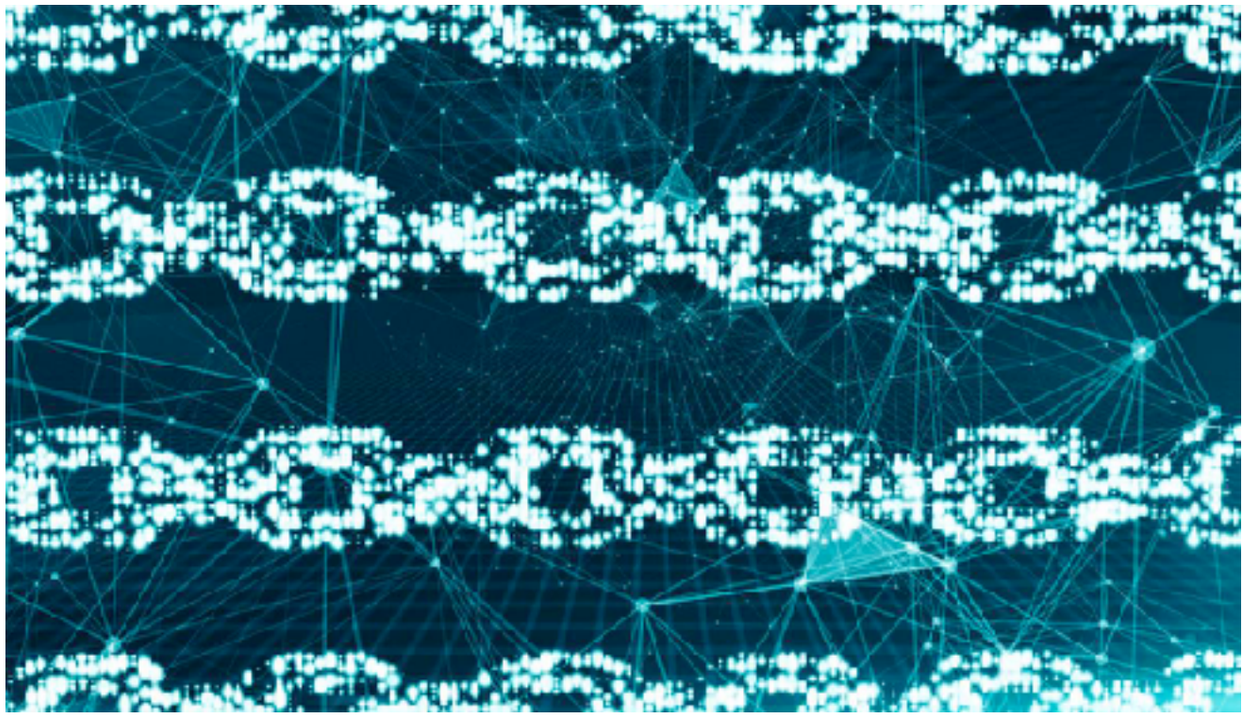
Hashing

The Chain is formed because the miners will take the blocks and hash it. The hashing is the miners that extract a code form the block that has a 1 to 1 correspondence with the information the block contains. It is like a fingerprint for a dataset.

© 2017 Copyright | All Rights Reserved

INSERT YOUR GREAT SUBTITLE HERE

06



The Chain

These hashes are placed as last line of the block that they are extracted from, and then as first line of the next block creating a chain.

Note: the previous hash is part of the information that gets hashed in the next block.

© 2017 Copyright | All Rights Reserved

INSERT YOUR GREAT SUBTITLE HERE

Attack

So what happens when an attack happens?

If a previous block is changed, its hash changes, since the information in the block is changed.

Now the hash changed and you also need to change the next block, to get the correct hash on top.

Now you changed a second block and need to repeat this until the end of the chain.

© 2017 Copyright | All Rights Reserved

How hard is this?

INSERT YOUR GREAT SUBTITLE HERE

Theoretically you need 51% of the miners to do this. This is about it has been tried 24/7 for 10 years and nobody was able to do it with one of the biggest prices for a hack in history, if you change a block to send all the bitcoins it contains to you you'll get 50+ million dollars in bitcoin.

INSERT YOUR GREAT SUBTITLE HERE

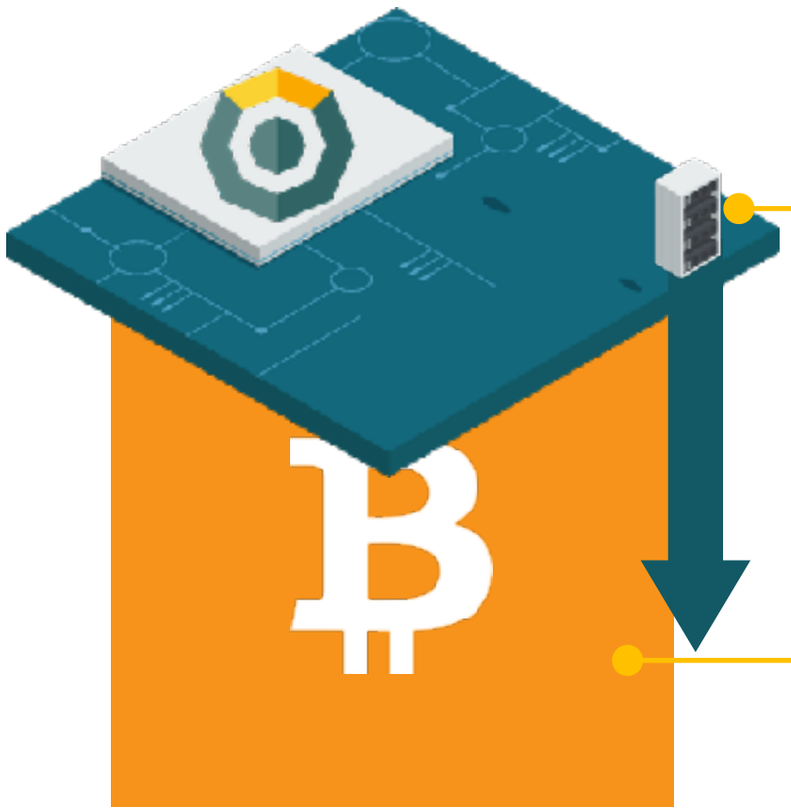
Delayed-PoW

Bitcoin has the most miners, and is therefore the most secure. Is there a way we can make the Komodo and bitcoin chains work together to ensure security for Komodo?

© 2017 Copyright | All Rights Reserved

Eliminate Risk Through Secure Automated Backups (dPoW)

Privacy Coin Origins

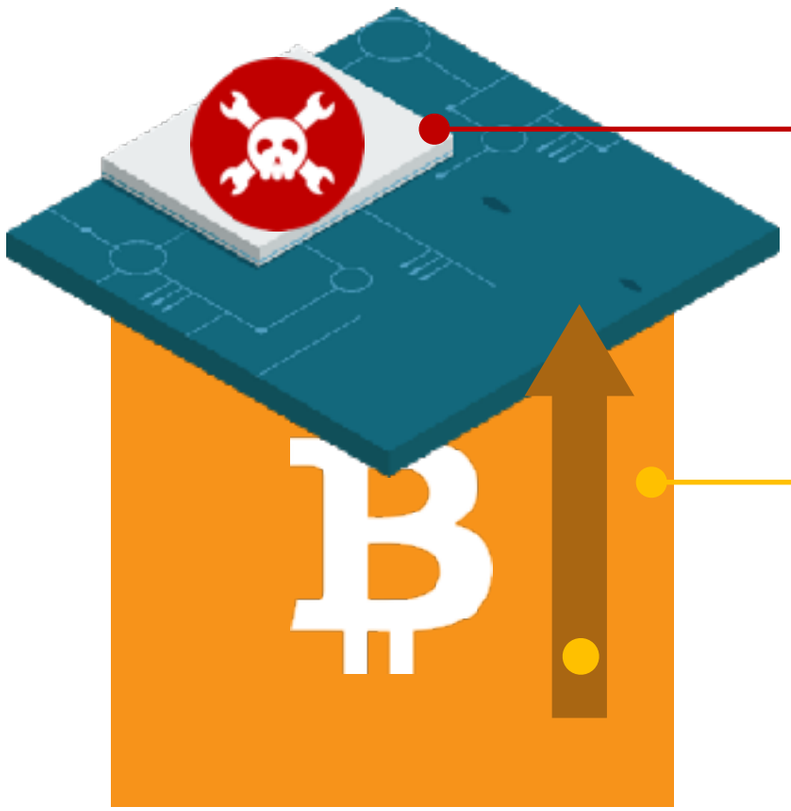


Komodo takes its hashes and then makes a small transaction on the Bitcoinchain. With this small transaction they can write a small text message, this small message are the Komodo block hashes.

Now the hashes of the Komodochain are not only stored in the Komodo blockchain, but also in the Bitcoinchain.

Eliminate Risk Through Automated Backups to Bitcoin (dPoW)

Privacy Coin Origins



In the event of a devastating attack on Komodo

The hashes in the bitcoinchain can be recovered, and the chain can easily be restored to its previous state.

Why is this so cool

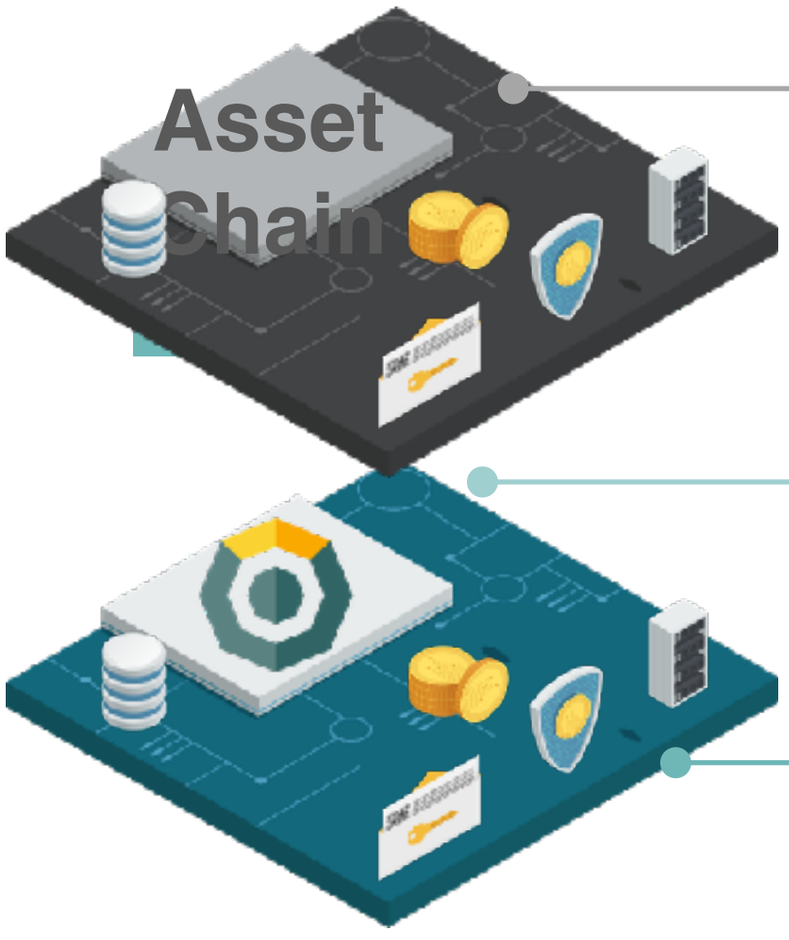
INSERT YOUR GREAT SUBTITLE HERE

01

Asset chains. Asset chains are independent parts of the Komodo platform.

Build Your Own Independent Blockchain in Minutes

Privacy Coin Origins | **Platform Evolution**



Asset Chains are fully independent blockchains. They are not impacted by any other chain in the Komodo ecosystem and they receive all of our technology updates.

You can build on our platform by creating an **Asset Chain**, which is a clone copy of Komodo's main chain.

We wanted to enable developers and businesses to build on our modular platform framework, without having to create or code their own blockchain

All the Benefits with None of the Risk

Privacy Coin Origins | **Platform Evolution**

- Fully Independent Blockchain
- 2 Megabyte Block Size
- 1 Minute Block Time
- POW Equihash Algorithm
- zKsnarks Enabled
- On Demand Blocks
- Scale on Demand

Asset Chains have our automated backup **security feature built in**, extending **bitcoin level security to anyone** building on our platform.

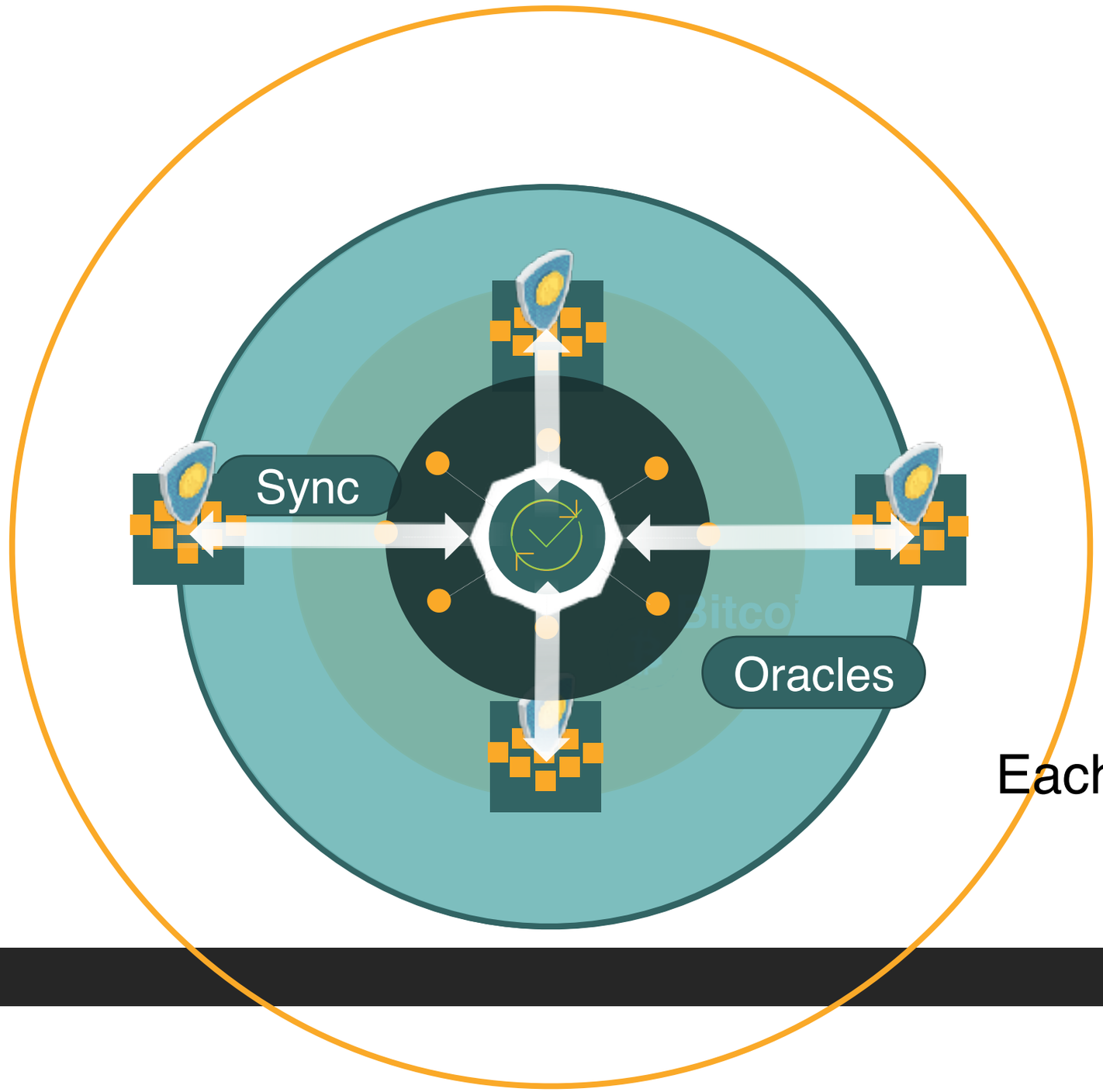
Why is this so cool

INSERT YOUR GREAT SUBTITLE HERE

02

Scaling. You might have heard about the scaling options that Etherium and Bitcoin propose. These options however are less secure.

Nested Merkle Proofs and Oracles for Multi-Chain Syncing



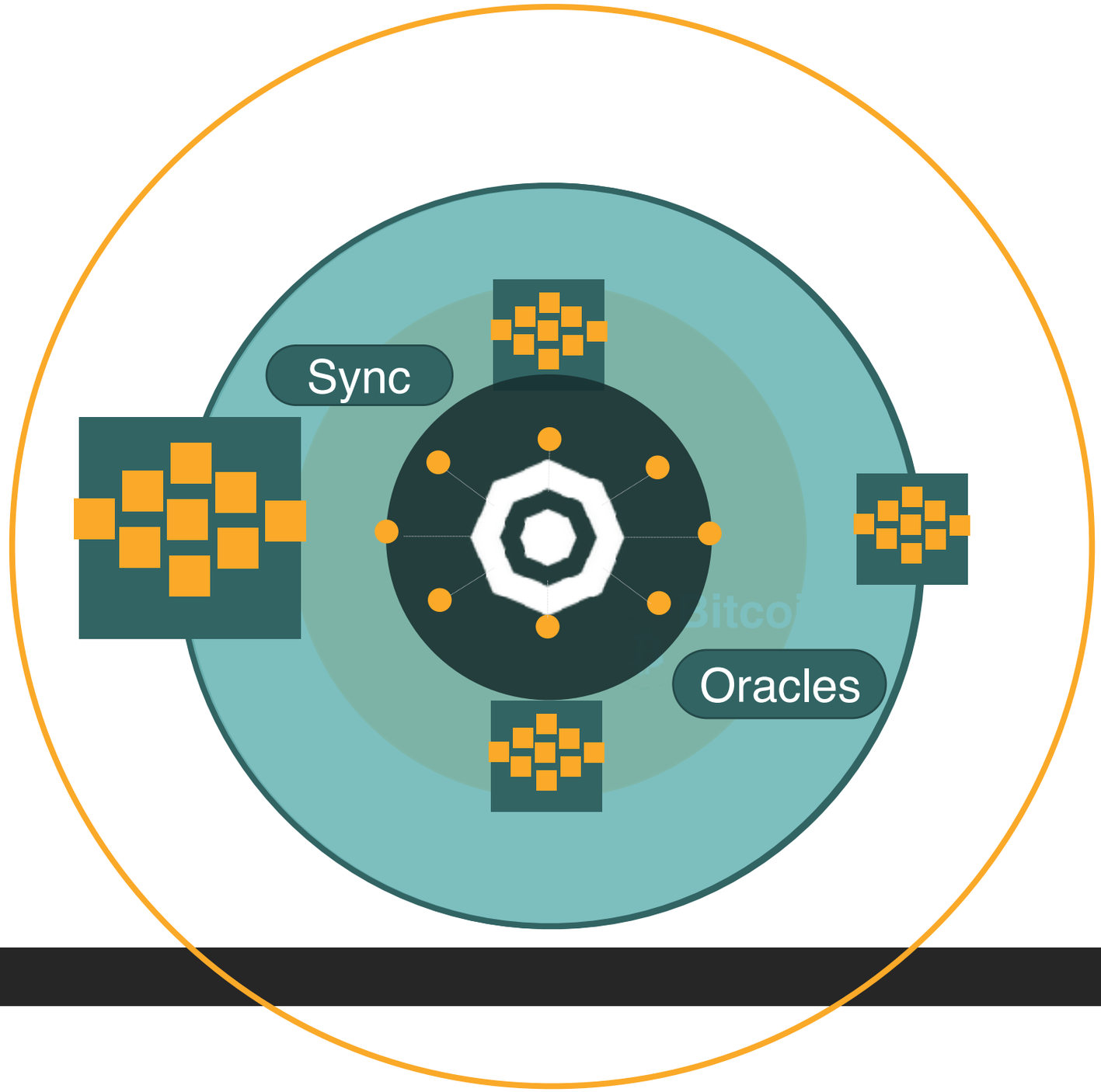
1 - All Independent blockchains send their merkle proofs to our notary nodes (oracles) for backup to Bitcoin's blockchain

2 - Merkle proofs of each chain are collected and combined into a single master merkle proof

3 - This new master merkle proof of the entire Komodo Ecosystem is sent back to each chain for syncing

Each individual chain is now synced to the Entire Ecosystem

Synced Chains Enable Inter-chain linking, allowing you to scale on demand



If you ever need to scale your independent blockchain, you can simply add another chain and link those to be recognized as one single chain cluster group

KOMODO™

Thank You!

And ask away