What did blockchain record

- What did blockchain record
- Analysis BTC,ETH,Link-Chain
- Some thinking of data sets

What did blockchain record

Perspective of blockchain

endless

Data

Data

Data

Data

Data

Data

Data sets

Time

Chain

State

S1

S2

S3

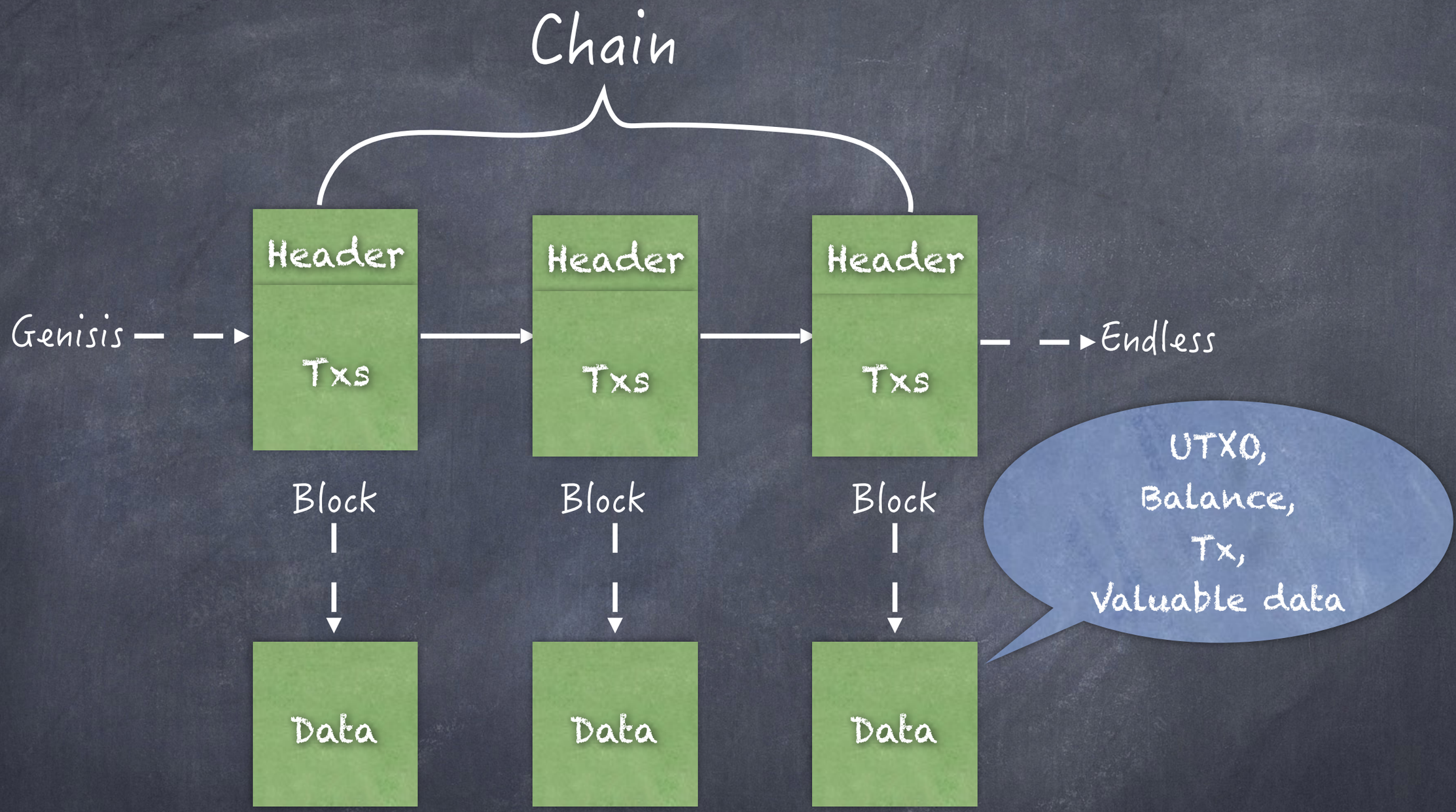
Endless

Consensus

P2P

Value:

- transparency
- Safety
- Correctness


Chain
Genisis
Header
Txs
Header
Txs
Header
Txs
Endless
Block
Block
Block
Data
Data
Data
UTXO,
Balance,
Tx,
Valuable data

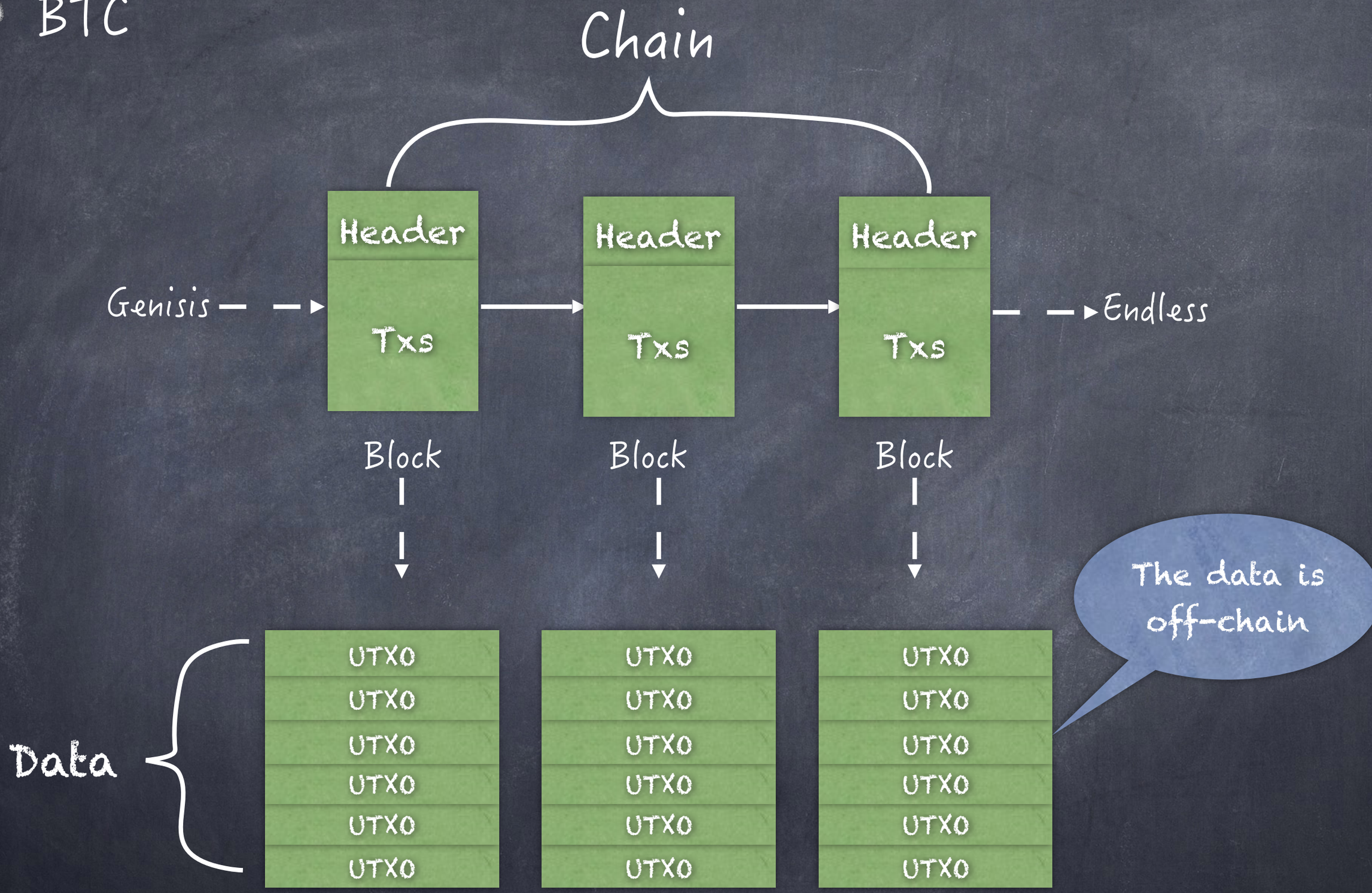
Analysis BTC,ETH,Link-Chain

BTC: Data sets store many UTXOs

UTXO: It's like cheque or coin

Data sets: It's a map

- BTC

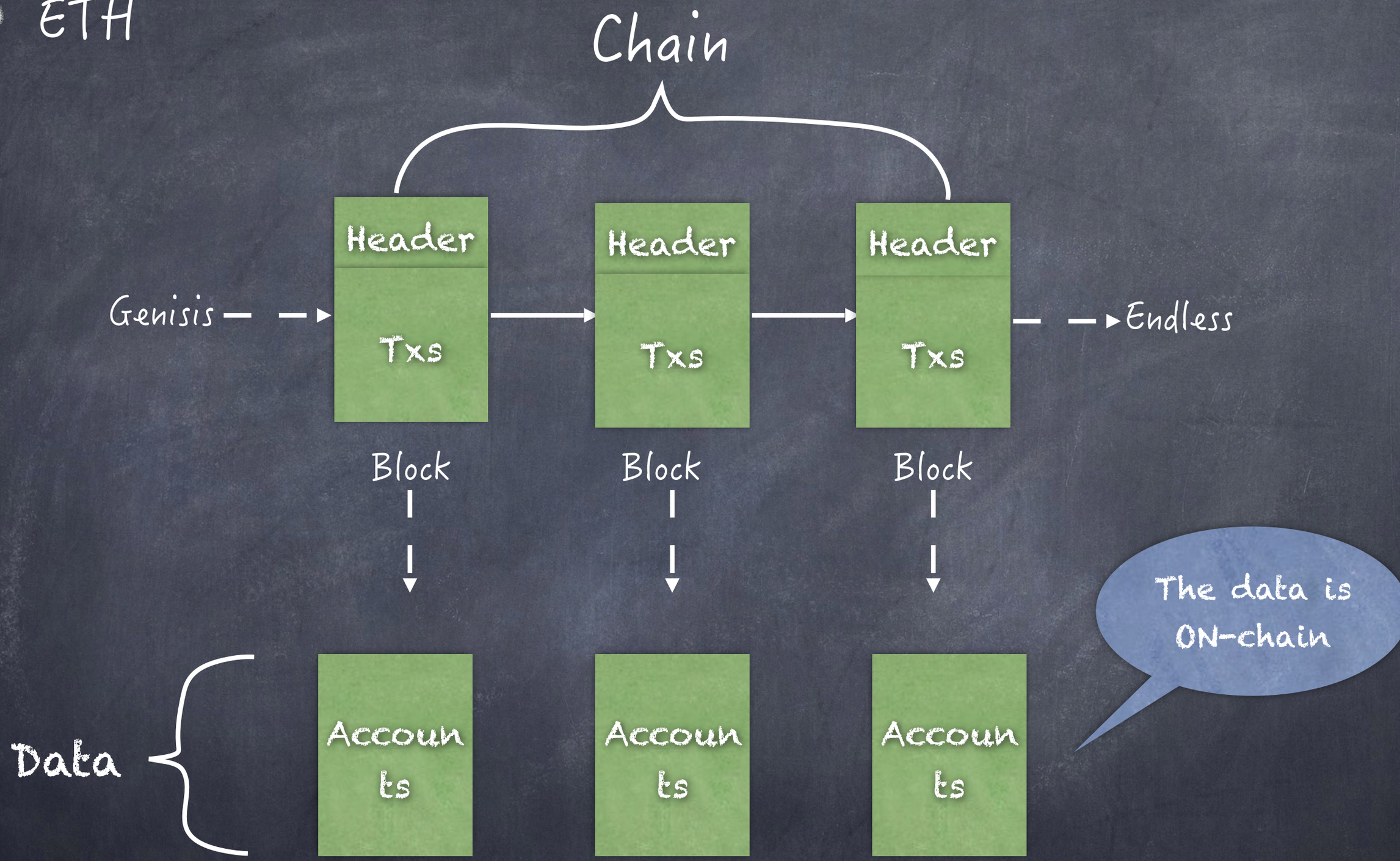

Chain
Header
Txs
Block
Genisis
Endless
UTXO
Data
The data is off-chain

ETH: Data sets store many Accounts

Account: Balance, StorageRoot, Code

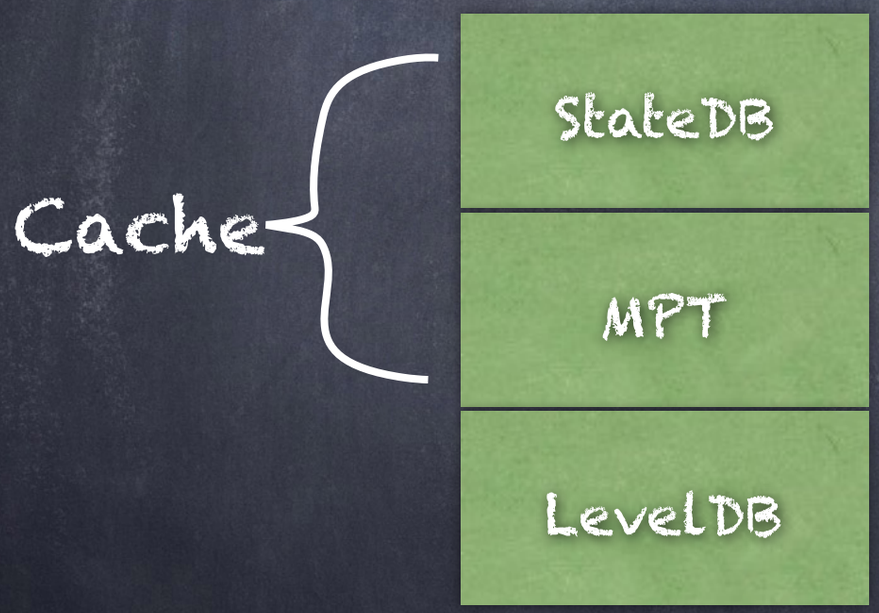
Data sets: It's a tree

- ETH


Chain
Header
Txs
Block
Genisis
Endless
Data
Accounts
The data is ON-chain

- Analysis Account Data Center

Account Storage: StateDB, MPT, LevelDB



StateDB: Preparing API

MPT:A special tree

LevelDB:K-V dataBase

- StateDB

1.It's the first cache of accounts.

2.Preparing series of API which is Reading or Writing to account.

3.Preparing a interface for managing MPT,Database.

- MPT

1.It's record account's status and record the change of account.

2.It's can calculate summary of ALL accounts.

3.Accounts be indexed for quick retri eval.

4.It's a prefix-tree and a merkle-tree

Ethereum Modified Merkle-Paricia-Trie System

An interpretation of the Ethereum Project Yellow Paper

G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", 2014.

Lee Thomas
Ver 8.0 2016-09-23

Block Header, H or B_H

stateRoot, H_r

Keccak 256-bit hash of the root node of the state trie, after all transactions are executed and finalisations applied

Hash function:

KECCAK256()

Simplified World State, σ

Keys							Values
a	7	1	1	3	5	5	45.0 ETH
a	7	7	d	3	3	7	1.00 WEI
a	7	f	9	3	6	5	1.1 ETH
a	7	7	d	3	9	7	0.12 ETH

World State Trie

ROOT: Extension Node

prefix	*shared nibble(s)*	*next node*
0	a7	

Branch Node

0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*a*	*b*	*c*	*d*	*e*	*f*	*value*

Leaf Node

prefix	*key-end*	*value*
2	1355	45.0ETH

Extension Node

prefix	*shared nibble(s)*	*next node*
0	d3	

Leaf Node

prefix	*key-end*	*value*
2	9365	1.1ETH

Prefixes

0 – Extension Node, even number of nibbles
1□ – Extension Node, odd number of nibbles,
2 – Leaf Node, even number of nibbles
3□ – Leaf Node, odd number of nibbles
□ = 1st nibble
1 nibble = 4 bits

Branch Node

0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*a*	*b*	*c*	*d*	*e*	*f*	*value*

Leaf Node

prefix	*key-end*	*value*
3□	7	1.00WEI

Leaf Node

prefix	*key-end*	*value*
3□	7	0.12ETH

Root

h00

<hash, node data>数据对保存在leveldb

node data

hash

0	a7	value

0	1	2	3	...	7	...	f	value

h10

h20

h21

h22

0	1355	value

0	d3	value

0	9365	value

45

h30

0	1	2	3	...	9	...	f	value

h31

1.1

h32

0	7	value

h40

h41

0	7	value

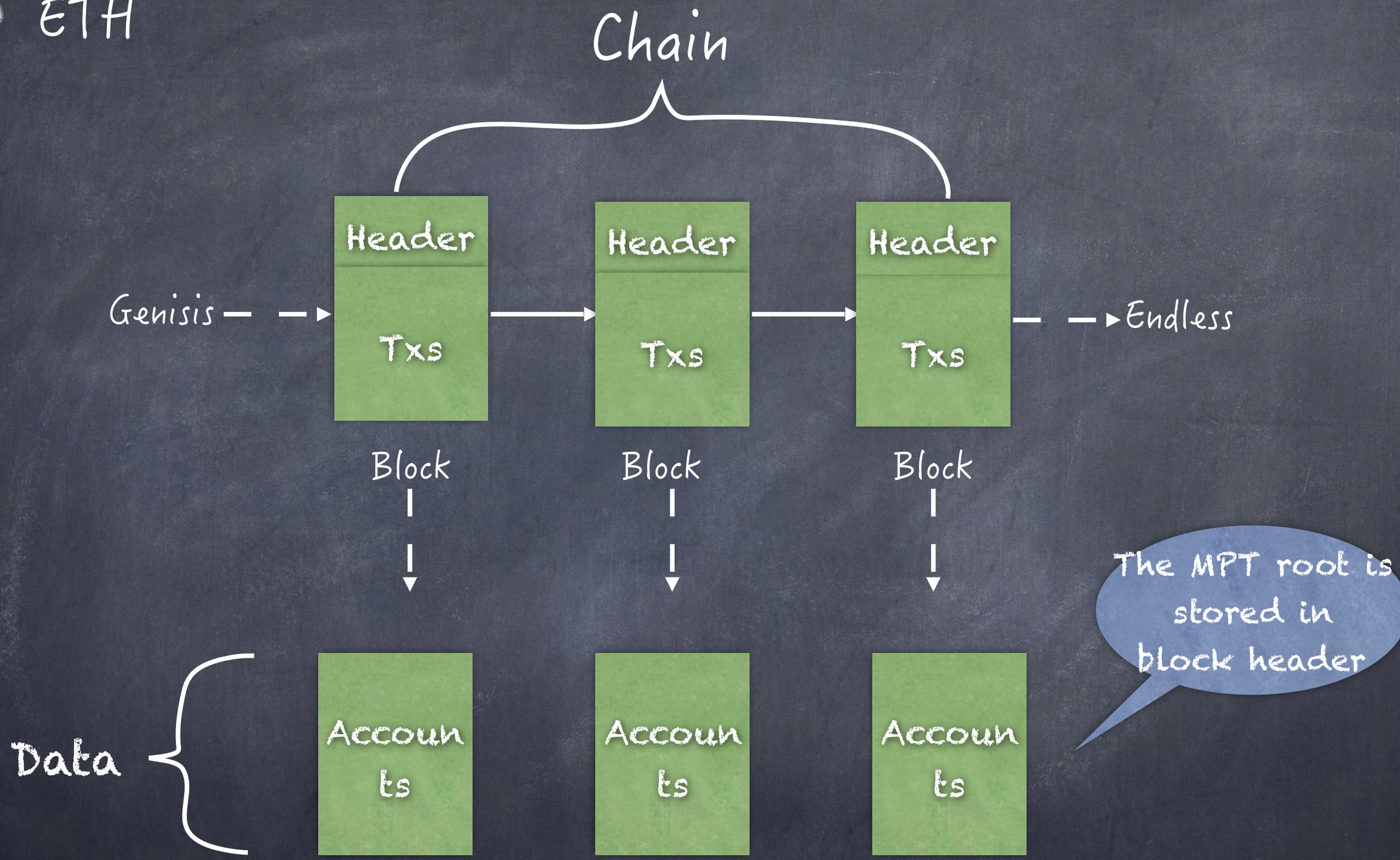
1.0

h50

0.12

h51

- ETH


Chain
Header
Txs
Block
Genisis
Endless
Data
Accounts
The MPT root is stored in block header

- Link-chain

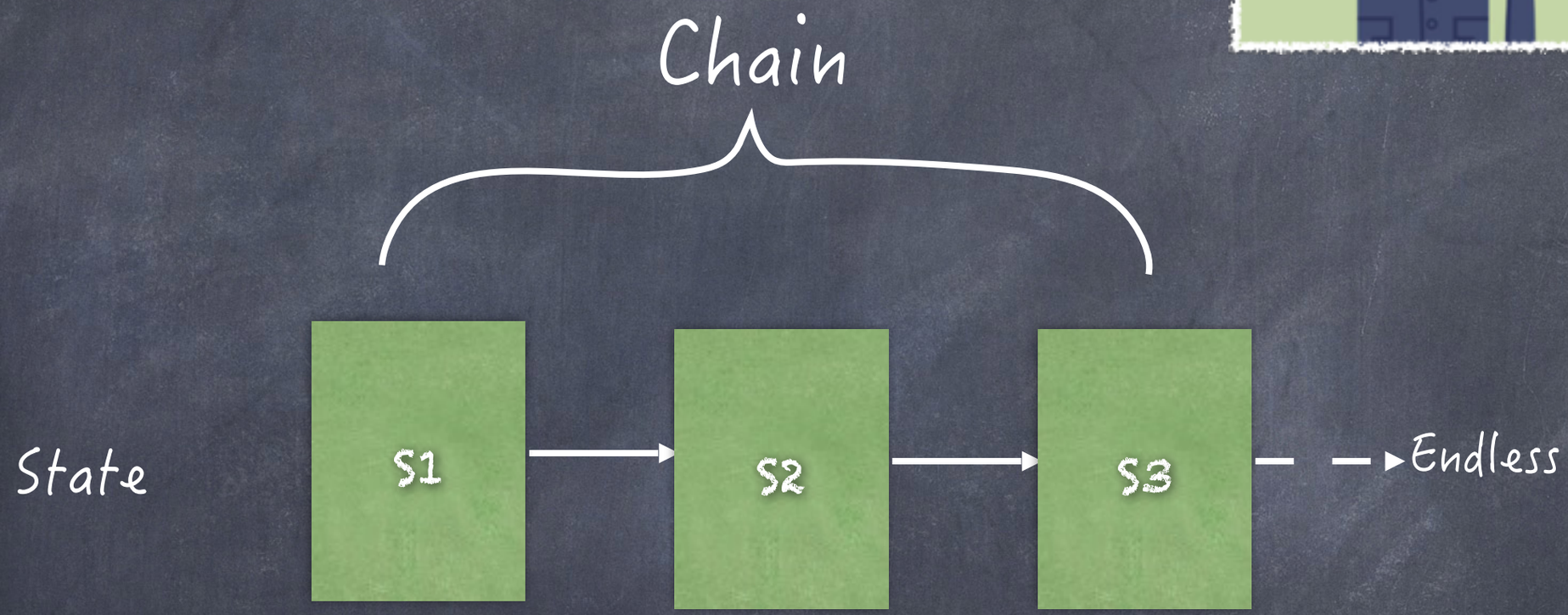
1.The Data sets of Link-chain is son of ETH.

2.Link-chain's account store UTXO and other data. ETH's account store balance.

Some thinking of Data Sets

What did blockchain record?

Chain



I think the blockchain record any valuable data

What is tx and block function??

I think the Tx is a input, which can be change the data sets.

The Block is record output and input of data sets.

Block body is input of data sets, which is a series of txs.

Block header store summary of data sets.

MPT is the best structure of data sets?

What is the structure of DAG data sets?

What valuable data can be stored?

Thank you!