

Crypto and Exchanges

A technical briefing on blockchains, validators, and staking

Jeffrey M. Glazer

Clinical Professor

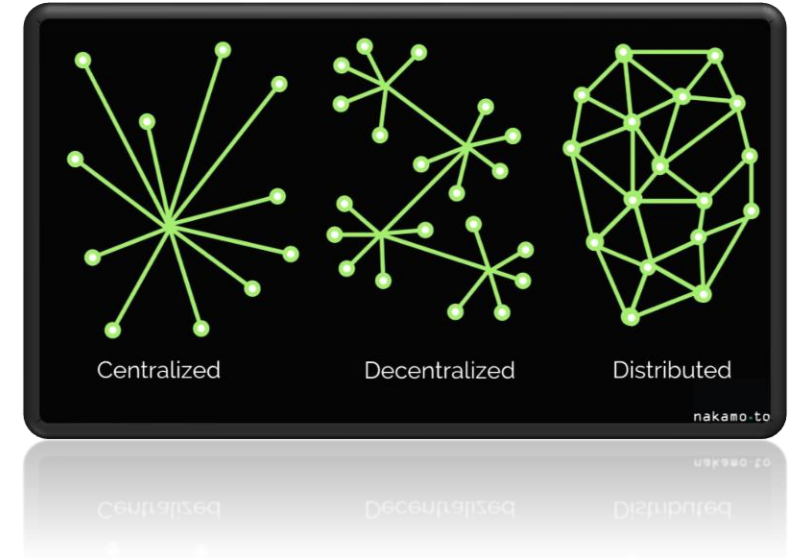
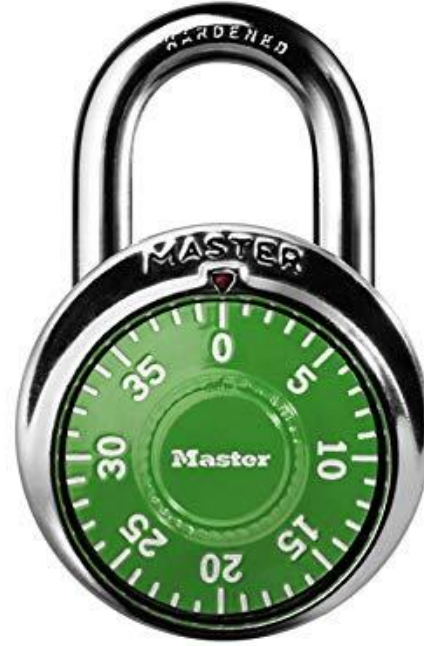
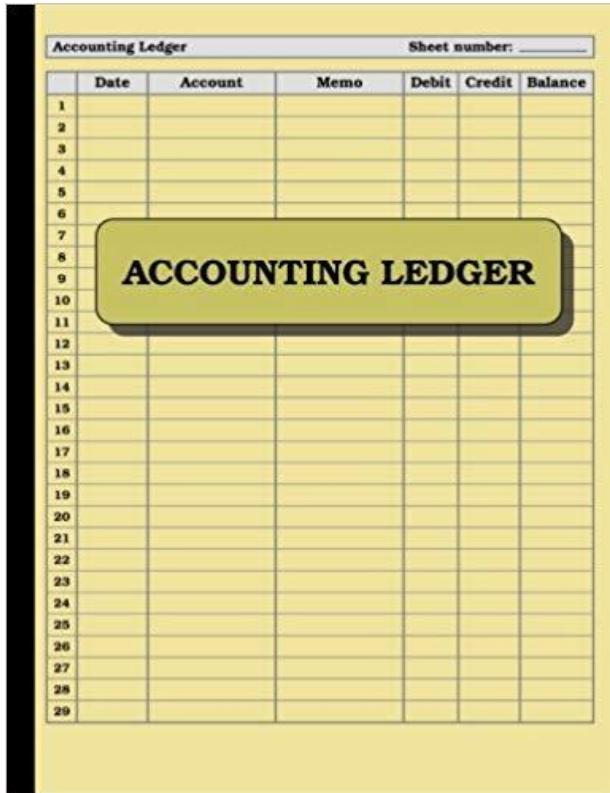
jmglazer@wisc.edu

A “Wallet” is a Key, Not a Container

Part I – The What: Basic Infrastructure and Definitions

Part II – The How: Creating and Securing the Ledger

Part III – The Why: The Economics of Validating and Staking



Part I

Wherein I Attempt To Describe a Blockchain Using Oversimplified Analogies

Protocols

Bitcoin: BTC (Proof-of-Work)

Ethereum: ETH (Proof-of-Stake)

Protocol: Running code plus a social process for changing it

A “node” runs the software does the work of the network

Changes to protocol require regular maintenance

NODE

A computer that stores and checks the ledger

Gossips with peers. Verifies what it hears. Needs no keys at all.
keys at all.

WALLET

A key manager, not a container

Holds a private key: the sole capacity to author a valid instruction moving a balance.

Coins and Tokens

COIN

The native asset of its own chain

Lives at the protocol layer. The only thing that can be staked.

TOKEN

An entry in a contract on top of a chain chain

An application's database running on someone else's computer.

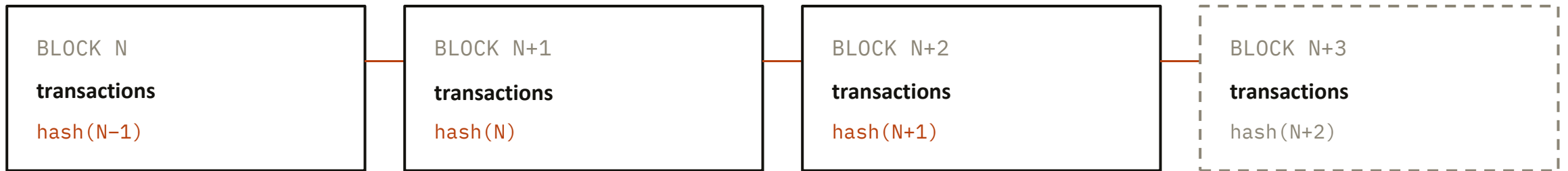
Exchange Accounts

Account v. Wallet

Wallet: holds own key on-chain

Account: Exchange holds key(s) on-chain in “omnibus wallet”, user/customer holds a contractual claim to amount in account

What is this Ledger You Speak of?



And A “Node”?



Dappnode

Dappnode Home 32/2

A cost-effective model using the latest hardware. Ideal for all use cases except Ethereum validation.

2,190.00€ Taxes not included

- ASUS NUC U7 S14
- 32 GB DDR5 RAM
- 2TB NVMe

Buy it now



Dappnode

Dappnode Home 64/4

The most powerful Dappnode Home perfect for Ethereum Validation

3,150.00€ Taxes not included

- ASUS NUC U7 S14
- 64 GB DDR5 RAM
- 4TB NVMe

Buy it now



Dappnode

Dappnode Home 64/8

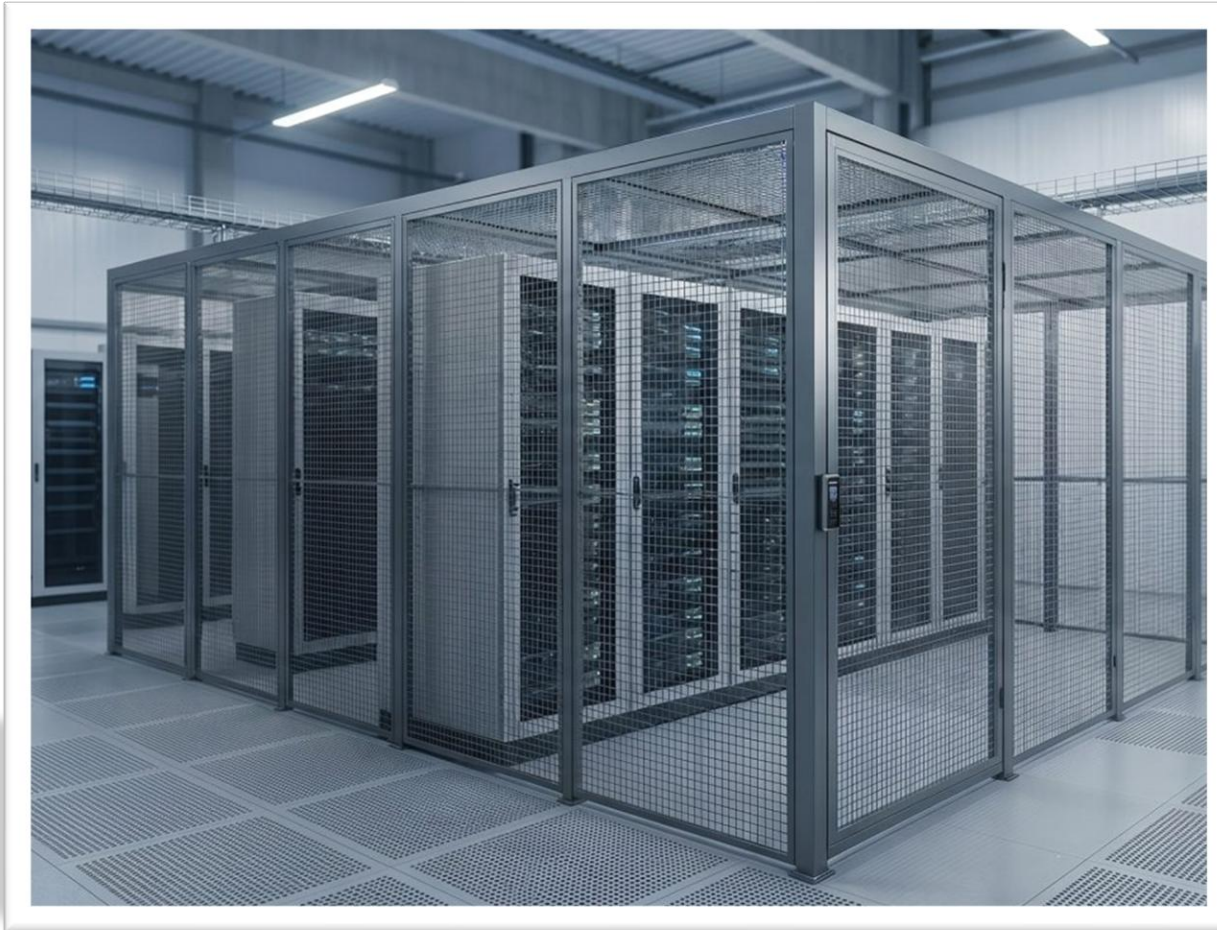
Dappnode Home 64/8 is our most powerful device, ideal for running Ethereum validators and multiple nodes with maximum reliability and performance. Product available on demand.

4,290.00€ Taxes not included

- ASUS NUC U7 S14
- 64 GB DDR5 RAM
- 8 TB NVMe

Buy it now

Also a “Node”

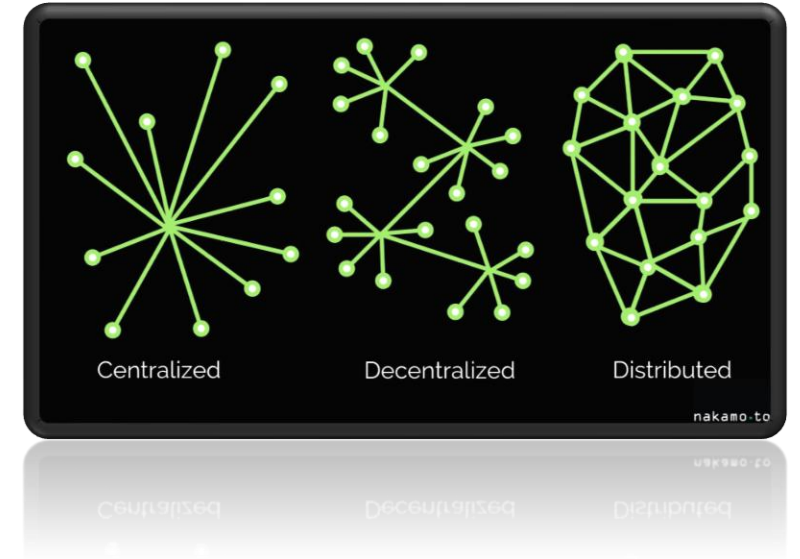
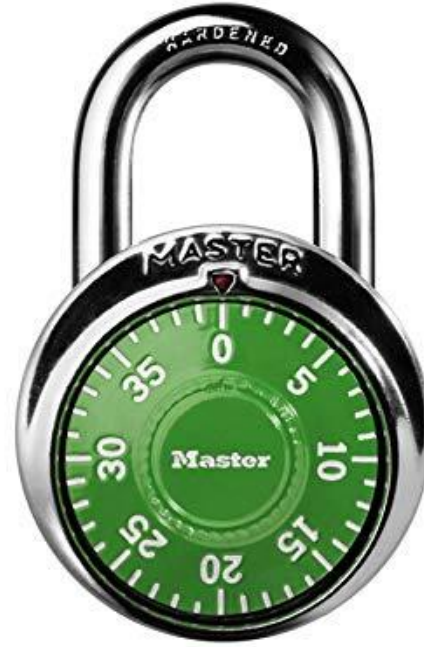


Accounting Ledger

Sheet number: _____

	Date	Account	Memo	Debit	Credit	Balance
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						

ACCOUNTING LEDGER



Part II

How Does This Thing Work?

What Does a “Node” Do?

Proof of Work Only

- Miner
- Routing
- Watchtower

Proof of Stake (and some PoW)

- Full (Validator)
 - Builder + Relay + Proposer
- Sequencer
- Prover
- Challenger
- Light Client

What Does a “Validator” Do?

Attest + Propose

- Attest: once every 6.4 minutes (“Epoch”); 82k/yr/ea
- Propose: min. 2/yr

Settlement

- Every 12 seconds “confirms” transaction
- Every 12.8 minutes (2 “Epochs”) confirmed transactions are “finalized”
- ~\$26B: the stake an attacker must destroy to unwind a finalized transaction

Sealing

Slashing?

Operator signs two contradictory things

- 1 ETH taken immediately
- 36 days to force node off network

Operating a Node

2 concepts: funding + operating

Funding (Withdrawal Credential/Key)

- 32 ETH + Pubkey + Withdrawal Credential
- Until May 2025 (Pectra Upgrade) only Operator received rewards; Pectra allowed separating operator from funder

Operating (Signing Key)

- Attest + Propose (cause rewards for funder)
- Cause Slash to Occur (cause penalties for funder)

So ... If the Operator Doesn't Touch Money...

Funder: Only supplies capital

Operator: Does all of the risk and reward activity

Solo, done cleanly

The customer holds the withdrawal credential. Principal is theirs to recall.

Exchange staking

The exchange holds both keys. The customer holds a book entry.

Liquid staking

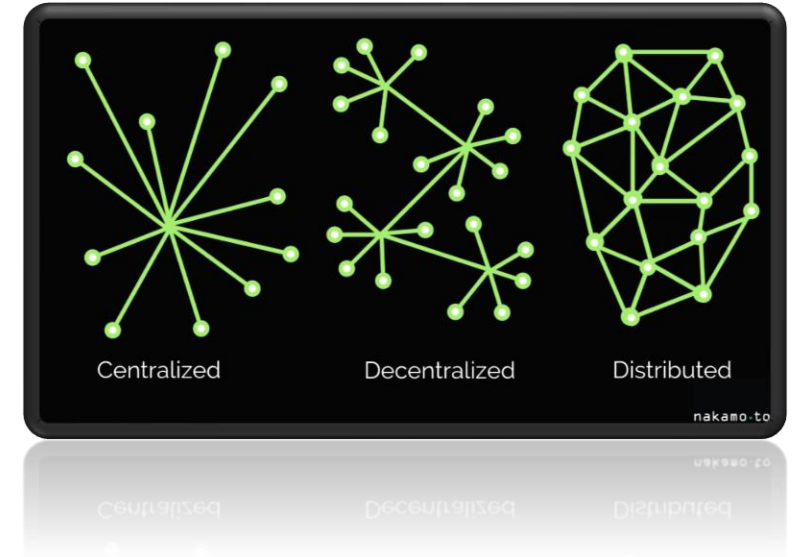
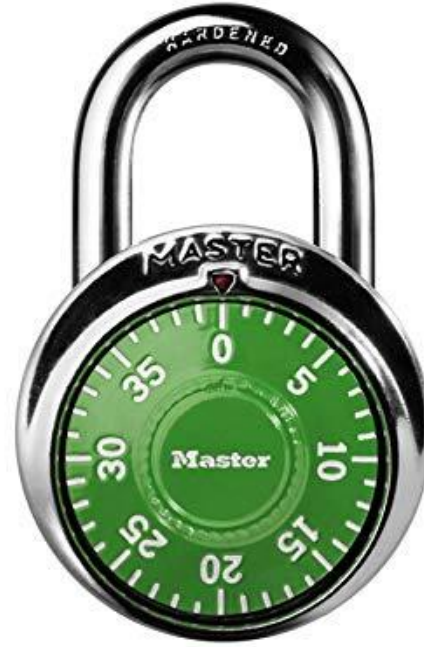
The credential points at the protocol's own contract. The customer holds a token.

Accounting Ledger

Sheet number: _____

	Date	Account	Memo	Debit	Credit	Balance
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						

ACCOUNTING LEDGER



Part III

The Economics of Staking

Eligible Population

00.06%

of Ethereum addresses with a balance hold at least the 32 ETH it takes to run one validator.

~120,000 ADDRESSES AT OR ABOVE 32 ETH

~200,000,000 WITH A BALANCE

Break-Even for a Service

Operating Expenses: \$122,000 a year before it earns a dollar.

Capital Expense: \$17,000 - \$29,000

Equipment + Maintenance: 150 – 300 hours

COMMISSION	ETH NEEDED	IN DOLLARS
10% — the liquid-staking rate	21,631	\$40.7M
15% — a mid-tier exchange rate	14,421	\$27.1M
25% — the highest retail rate	8,652	\$16.3M

A Concise Review

- The Operator Holds No Property (only the withdrawal key)
- Customer/User's Return Based on Operator Capability
- Break-even at a 10% Commission = ~21,600 ETH (\$40M) under management