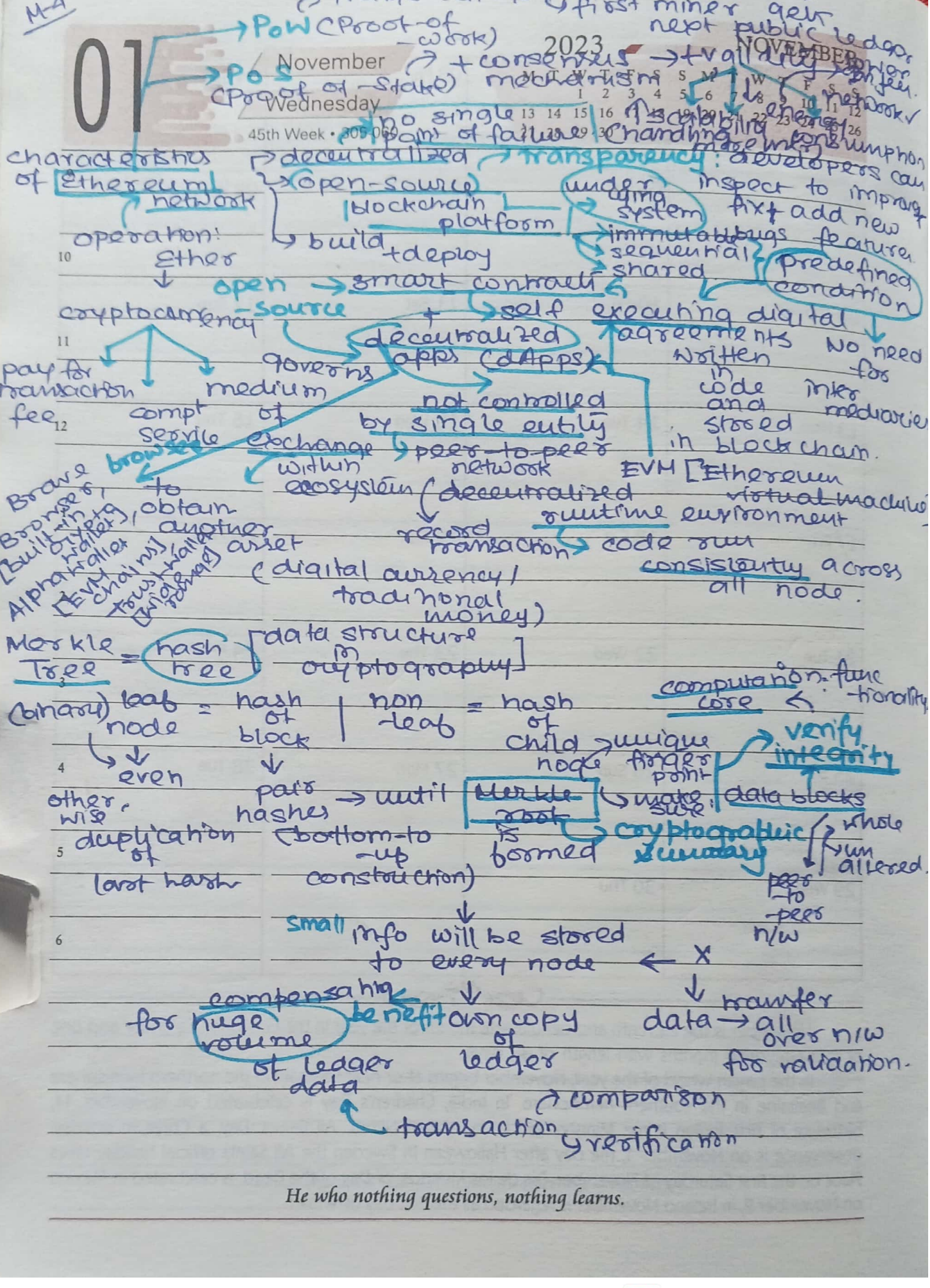
M-4

01 November 2023 Wednesday
45th Week • 305-060



He who nothing questions, nothing learns.

robustness of design + legal framework.

DECEMBER 2023 — November 02 Thursday — 45th Week • 306-059

simple

speed : faster execution

smart contracts always being beneficial → disintermediation : ✗ req for of mediators and centralized entities.

→ lower cost : no need to pay + ✗ paperwork

→ Alignment ↳ with all parties' intention

immutability — complexity ✗ + understanding

change incorporation → flows can't be rectified

↳ relatively new concept : vulnerability) — unforeseen circumstance

→ PoW = computational effort ↑ = energy intensive

Ethash ↑ modified variant algo

Dagger-Hashimoto (RAM

↳ optimal for evaluating algo)

↓ input data

block — nonce (random number for bitcoin mining)

hashing process ↓ hash value ⟺ specific target threshold.

EVM ↓ decent' computing env. → smart contract in Ethereum work → deploy blockchain appl'n

{ secure transaction validation. } ↑ ✗ central authority

→ blockchain platform

Ethereum commissioned

transactions — paid in Ether = volatile market price

vary daily → users hoping for lower ⇒ delay. Eth price

↓ change n/w state

fluctuates

comp cost fixed in 2 ↓ soln

execution — Gas unit = internal currency

predetermined < resource utilization reqd = predictable

↓ transaction ↗ stable ↳ predictable = accomplish exactly what an automobile needs fuel to drive.

Ether ↳ native crypto currency [digital asset]

supply & demand dynamics ↳ trade ↓ transaction fees ? execute smart contract

Quality only happens when we care enough to do our best.

Scanned with OKEN Scanner

03 November Friday
45th Week • 307-058

2023 NOVEMBER
M T W T F S S M T W T F S S
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 30

Smart contracts = x legal agreement
↳ execution of transaction → program ↳ protocol

1. = technological means for automation of payments → reduce costs.
2. minimise potential for human error.

ETC → opensource blockchain
[Ethereum classic] | direct continuation of Ethereum → larger developer community = market value ↑ (ongoing upgrade)

↑ hard fork ↳ ability to evolve (Ethereum) = PoW blockchain
(not backward compatible)
↗ immutable = code is law (principle) = Unaltered chain.
↳ preserving original Ethereum protocol.
↳ PoS

= x change to past transaction
↓
lower transaction fees.

Crowd funding : fund raising → peer to peer digital exchange
token ↔ capital
↓ project n/w.
smart contract → dist. : automation according to terms

mining process.
Mixhash = intermediate hash value : to find a valid block hash
↳ confirmation = PoW sufficient compt work ✓ + security
↓
hashing block header data + nonce

Code is law : → provides rule ✓
smart contract (deployed)
Justify.
ultimate governing force.
immutable ← x overrule.
public → visible transparent
→ dist. ledger = replicated to all the nodes.

investor deposit
Ether → DAO (Decentralized Autonomous Organization)
returns = contract node
↳ if flawed → hard fork
= interpretation → human judgement
ultimate enforcement

smart contract → deterministic = can only perform func. designed.
↓ self-verifying ✓
autonomy (no 3rd party) immutable

Appln
1. Real estate : ownership of apartment transferred → seller's wallet
2. vehicle ownership → enforce maintenance → failure → suspension of license
3. music royalty → owner's account credited
4. Govt. election : hard to decrypt voter's address
5. supply of raw materials, 6. → manage inventory
3. healthcare payments.

We can be happy with little and miserable with much.

2. Archive node: historical data store for query.

Full node = store + block validation → maintaining state of block. → result block chain
→ storing by smart contract execution.

(full + state) = 3. Light node — low memory access
4. Pruned node

Ethereum node (computer) — blockchain network → validating → trading data. / mining.

[PoS] → 5. Validator node: securing (consensus), earning reward for validation.
miner ← validator

Bitcoin → decentralized digital currency → replace national currency.
energy ↗
↓ transaction: keeping note

Ethereum → software platform → decentralized payment n/w.
↳ executable code.
energy ↓

Merkle Patricia Tree → data storing / verifying → key-value pair → Ethereum functionality (dynamic state of Ethereum)
↓ space optimized Trie.
↓ Transaction look-ups with common prefix
(sparse data = zero balance) combined with IoT
add layer of security
deceit → no single point

Oracle: third party service → execute off-chain data (external)
smart contract
↳ 1. weather info failure for flight delays.
↳ DeFi: realworld (decentralized finance) financial service
consensus based (market price)
↳ derive factual data
S/W — assemble online data to run on smart contract
H/W ↳ m/c readable values (sensors)
Inbound/outbound
↳ smart contract → broadcast data.
↳ bringing info from outside world.

Sunday - 05

All the heaven that ever existed is now and here.

DEC

M-3

Lower transaction per second in public blockchain
→ consensus mechanism among a large permissionless group: higher throughput
→ procedure: peers of blockchain reach a common agreement
→ higher latency (vast n/w)
→ stringent security measure: computationally intensive

× calculation
Using hard drive space rather computing power ← PoW = consensus mechanism

1. PoC (proof of capacity) → ↓ energy consumption
→ pre-computed solⁿ to cryptographic puzzle
↓ decent: ↓ mining power → cost

Public: Bitcoin, Ethereum
Example

private (restricted for internal organization): hyperledger fabric & Multichain
↓
consortium: R3 corda (multiple org with pre-selected nodes) (hybrid)
Public / Private permissioned

2. PoI (Proof of Importance): validity transactions priority → actively participation
→ cryptocurrency you hold

DAG → specified direction
→ × in finite loops in trans progression
Alt to Blockchain
→ Tangle: validate transaction + create new block
→ transaction w/o fee
→ secure commⁿ b/w IoT.

3. RAFT: distʳ system
↓
all nodes: same consistent data → log entry → replication, vote, client interaction, making decision

Byzantine general's problem: Game theory (computing problem)
↓
difficulty: decent but consensus w/o central authority? → fault tolerance → Byzantine Fault Tolerance [BFT]
→ Trust is not placed but shared among many

Blockchain
1. Consensus
1. transaction (sequence)
2. global state
message pass among precise n/w structure

2. Bitcoin
→ 1. PoW (form to valid hash)
2. h/w verifying misleading info being spread

Consensus

1. PoW (proof of work): selecting miner for next block generation : comp^t power for solving mathematical puzzle.
   ↓ × validity of every node.
2. p BFT (practical): ↓ how many times entities confirm the new block (checking malicious nodes)
3. PoS (proof of stake): investing coins at stake through an incentive mechanism.
4. PoET (Proof of Elapsed time): every validator given a fair chance → 1. random amount of time ↑ proof of wait → 2. added to block.

Challenges

1. Consortium.
   ↳ × fully decent : vulnerability, corruption.
   ↳ diff org → diff reqr : Approval
2. Hybrid: (Interconnected private-public) → new ecosystem : lacks n/w participation.
   → transparency → depends on organization.

5. PoA (Proof of Activity): PoW + PoS → random group of validators. : benefit : 51% attack ↓ zero.
   ↓ block template containing header — reward address
   ↓ Analyze block
   tran^n maintained in serial order. ⇒ * (prev contract ✓ ↳ new contract
   malicious content : DoS Attack

6. PoSA (Anonymous) → secure overlay for transaction anonymity → cloaking nodes = sender-receiver virtually untraceable. ↓ privacy ✓

M-2

Token → digital unit with value
↓ repr assets. built on blockchain infrastructure of another cryptocurrency

Fork: updating cryptocurrency protocols? participant's conflict due to consensus algo, new rules = validate transaction.

- Soft fork [backward compatible alteration in protocol]
  - ↳ new block valid by old version of S/W
  - (SegWit + Bech32 (new class of address)) Bitcoin n/w
- Hard fork [new currency existence ↳ Equivalent quantity dist → full nodes]
  - ↓ PoW → PoS [Casper Update] (Ethereum blockchain).

Need? **Bitcoin** n/w

- storing value + unit of exchange = speed in economy ↓. velocity
- peer-to-peer
- 2. ✗ central authority (intermediaries)

Altcoin → cryptocurrency other than Bitcoin

- ↳ new features
- ↳ higher returns ↗ high volatile price.
- ↳ speed ✓, security ✓

Litecoin fork of established coin.
Scrypt → diff (memory intensive) from PoW (bitcoin)
↓ processing block = 2.5 min < 10 min (bitcoin)
speed ✓

Q. 4 layers in blockchain architecture

1. H/W (infrast layer) → Client-server
   ↳ Peer-to-peer n/w (record trans) → dist^{r} db (keeps track)
   Nodes → group (block) ↓ broadcast to n/w.
2. Data layer ↳ Data structure → Linked list, Hash, Binary tree } manage str of block
   Data encryption by digital signature.
3. N/W layer → inter node comm^{n} ↓ propagate blockchain trans
4. Appl^{n} layer → Smart contracts + dApps + chain codes → comm^{n} b/w with network and users (S/W) → uphold blockchain's determinism.

Simulated env in Blockchain → allows to identify bugs (test repeated) + fix w/o real world conseq = faster development → deployment = real risk of asset
→ reduced cost for interacting with blockchain network (gas cost)
safe space for learners (controlled manner).

DApps powered by nodes × servers
Traditional apps — centralized storage — by trusted authority — s/w owned and controlled → data consistency
data consistency

decent → no single point of failure (fault tolerance)
scalability ↓
× intermediary
resistant to censorship + security.

Utility token (Filecoin) → access to product within an ecosystem ↳ Unregulated.
Security token (stocks) ↳ security regulation by ownership in an asset

Fungible Token → interchangeable → uniform value.
NFT ↳ unique category of digital assets (ownership)
↳ transfer entire token (indivisible) (×) one-to-one basis exchange

Blockchain trilemma for high performance (limitation) → trade off b/w
↓ Scalability ↓ soln layer 2-soln sharding consensus.
↓ security
↓ Decentralization ↳ Low transaction throughput ↳ high latency : time delay.

fault tolerance (known set)
pBFT (algo) → proposal + agreement of block
partially sync ↳ stream line.
→ leader node + client → leader [lamport, Shostak, Pease]
phases: pre-prepare (node no.) → prepare → commit → reply to client
less comm round ↓ ✓ consensus. speed (more realistic scenario)

Synchronous network → message to be delivered within a timeframe
Async ↓ × ↳ difficult to achieve consensus : message lost ↓ crash
Byzantine agreement: Impossible (failures are general)
traits shown → sending incorrect message or message with delay. or modifying data + colluding with faulty nodes.
↳ potentially unreliable commn channel: agreement ✓ faulty

A positive attitute overcomes the tallest obstacles.

10 November Friday 2023
46th Week • 314-051

NOVEMBER
M T W T F S S M T W T F S S
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 30

small i/p change (flip bit) → diff o/p → reveal tampering
Avalanche effect

Double Spending (risk): single unit of digital currency usage (>1)

info copy

hashes & transaction

Blockchain → transparent immutable record = DB → computational infeasible.

51% attack: gaining control of >50% of mining power ∴ prevent miners from earning rewards.

Smart contract (diff obj)

1. State var: data storage ← persistent data
2. func → modify state var, trigger events.
3. Events → notify user interface (mechanism) within contract's execution
4. Modifiers → preconditions by owners (code)

source: Block reward: mining - fixed amount of native crypto currency
Transaction fees: paid by users for including it to the block.

1. Constructor ↓ after deploy.
2. Fallback: Ether sent w/o data
3. Receive: + no fallback with payable modifier is present

Bitcoin: digital cryptocurrency
↓ decentralized
digital currency + cryptography (security)
distributed public ledger.

Gas → compt cost (fixed) ↳ resource exhaustion on n/w → prevent

Mining pool
→ individual miner: limited hash power → low probability for reward
→ compt power of many miner → predictable stream of income. ↓ variance. ↓ upfront investment

difficulty ↓ adjust n/w stability (const n/w)
1. target block creation
2. predefined algo based interval. → block creation rate → stable ✓
(fluctuate n/w hash rate)

→ web3 stack for ethereum
Swarm → storage → censorship resistant → native, BZZ cc; always available dApps (offchain)
node: chunks ↓ encryption
Whisper → secure msg protocol (anonymous) private commn

Store static, owners on Gas is expensive.

Good manners brighten the personality.

19 January Thursday 4th Week • 019-346

2023 JANUARY

M	T	W	T	F	S	S	M	T	W	T	F	S	S
						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	30	31					

Dark web
↳ least accessible ! Tor → anonymize { → user, ↳ Host } Onion Routing : difficult to trace the origin or destination of data

infected by malware by kept ...

counterfeit documents → extremist discussion

bypass govt monitoring ! → Hacking | → compromised data, Malware

Mariana's web (myth) → quantum level computing? (ultimate hidden layer)

Mediator; Gateway layer
users — sensitive info
ambiguous! (not hidden, not public)
entry under condition.
(blockchain like structure)

The Fog: (Murky) self-replicating viruses, Malicious data content

No central datapoint corrupted)

Primarch: system, sentient system (oversight all digital activity) → beyond human range
: blackbox : program
knowledge deemed to powerful or dangerous for public
who may enter: possibility
eden of technology!
digital autonomy!

Day 3

→ pseudonymity
Blockchain forensics
↳ transaction data
visible, immutable
↑ investigators can leverage

tools ↗ analyze
wallet addr ↳ clustering
trace behaviour
identify
illicit activities (money laundering)

UTXO analysis (unspent Transaction output) + Transaction timing.

Transaction graphs ↗ suspicious addr
↳ identify wallets controlled by same actor

track peel chain
↳ funds split → multiple wallets → obfuscate origin

→ AI/ML model to detect anomalie
actionable insights in cybercrime investigation

Thinking well is wise; planning well, wiser; doing well, wisest and best of all.

Theory and Applications of Blockchain

1. Blockchain Security –
   - ↳ cryptography
   - ↳ consensus mechanism
   - ↳ distributed nodes

   Threats
   - 51% attack
   - Sybil attack
   - double spending
   - smart contract vulnerabilities

2. Eclipse Attack
   - ↳ network layer attack
   - malicious node → target node : selfish mining
   - Defense : better peer selection

3. Front-running attack
   - Attackers monitor mempool (inserts transaction)
   - To buy a token, attacker buys first → sells @ higher price
   - Defense : private transaction relays

4. Tesseract
   - ↳ MIT project → cross chain atomic swaps → interoperability [no centralized exchanges]

5. Blockchain 3.0
   - ↳ scalability, interoperability, governance, sustainability
   - Polkadot

6. eCash → DigiCash [1990] → commercialized eCash (Anonymity) → Bitcoin → Cryptocurrency.
   - David Chaum [1980] → Electronic money using blind signature.

7. Byzantine Agreement in Algorand
   - ↳ Pure Proof of Stake
   - ↳ even if malicious (some)
   - ↳ speed ✓

8. Issues with Nakamoto consensus
   - ↳ High energy consumption, low throughput
   - ↳ centralization risk