Distributed Ledgers

- A digital ledger is a digital record of **who** owns **what**
- A **distributed** digital ledger is a ledger that is replicated among many nodes
  - The main innovation is the underlying **distributed consensus** mechanism

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>+2</td>
</tr>
<tr>
<td>-5</td>
<td>+5</td>
</tr>
<tr>
<td>+3</td>
<td>-3</td>
</tr>
</tbody>
</table>

Alice sent $2 to me
Alice sent $5 to me
I sent $3 to Alice

I owe Bob $4

Alice

Bob

Alice sent $2 to me
Alice sent $5 to me
I sent $3 to Alice

Alice owes me $4
Distributed Ledgers

- There have been other good algorithms that have been used for distributed consensus
  - Paxos, PBFT
- However, besides distributed consensus, blockchains also:
  - **Scale** relatively better than existing consensus algorithms
  - **Compensate** for the costs of verifying and generating consensus
  - **Disincentivise** attacks
- Blockchains work in practice, not theory.
Transaction structure

- A transaction is a record that contains **inputs** and **outputs**
- An input has to reference a previous transaction’s output
  - In order to do this successfully, the correct key has to be provided

- Exception: the very first transaction in a block has no inputs and simply generates a set number of bitcoins for the miner (i.e. miner’s reward)
Transaction structure
Blockchain structure

- Blocks exist on top of the complex network of transactions
- They ensure that:
  - transactions are formatted and ordered correctly
  - transactions do not try to double spend
Ethereum Name Service
What is ENS?

- Map human-readable names to resources
What is ENS?

- Map human-readable names to resources
  - Ethereum accounts and contracts
  - Swarm & IPFS records
  - Public keys
What is ENS?

- Map human-readable names to resources
  - Ethereum accounts and contracts
  - Swarm & IPFS records
  - Public keys

- Distributed lookup service
  - Resistant to DDoS attacks
  - Transparent transactions
  - Upgradeable
ENS Architecture

ENS Registry

- eth
  - owner: 0x1234...

- inigomontoya.eth
  - owner: 0x34567...
  - resolver: 0x45678...

- metamask.eth
  - owner: 0x56789...
  - resolver: 0x67890...

- alice.metamask.eth
  - owner: 0x7890A...
  - resolver: 0x890AB...
Name resolution in ENS

User → resolver('foo.eth') → Registry

Registry → 0x1234... → Resolver
Name resolution in ENS

User

resolver('foo.eth')
0x1234...

daddr('foo.eth')
0x2345...

Registry

Resolver
ENS Soft Launch
As of 2017-07-31

180,822 Names auctioned

Ξ168,595 Ether deposited
First ENS Workshop
August 2017

- 27 participants
- 3 days of discussion, covering:
  - Dispute resolution
  - Permanent registrar design
  - Securing subdomains
  - DNS integration
DNS integration via DNSSEC

#. DS SHA256

#. DNSKEY RSA

#. xyz. DS SHA256

#. ethlab.xyz. DS SHA256

#. ethlab.xyz. DNSKEY RSA

#. ens.ethlab.xyz. TXT a=0x...
DNSSEC Oracle

User → Registrar: proof

User → Oracle: claim

Registrar → Oracle: query

Oracle → Registrar: answer
DNSSEC Oracle

User — Registrar — Oracle — ENS

proof — claim

query — answer

setSubnodeOwner
Thank you, and stay tuned...