Blockchains as Infrastructure and Semicommons

A. Jason Windawi
James Grimmelmann

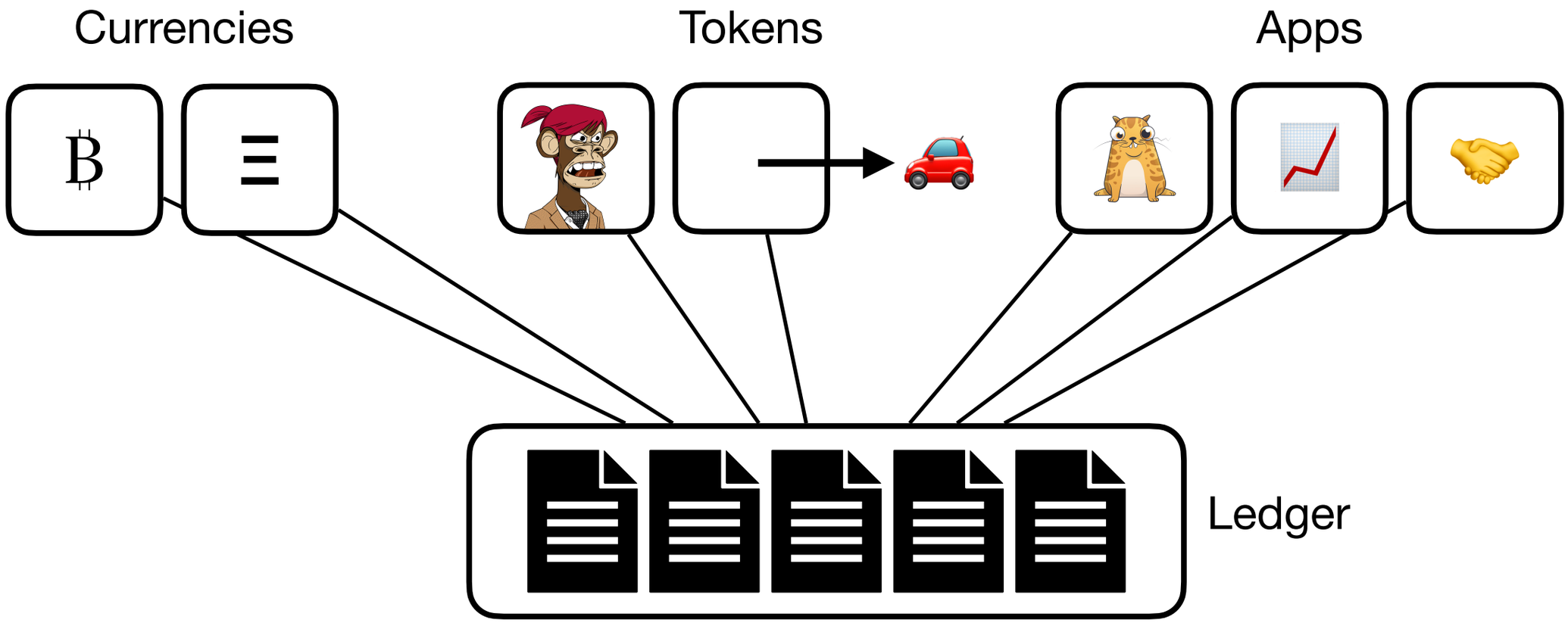
William and Mary Law Review Cryptocurrency Symposium February 11, 2022

Infrastructure

Infrastructure

- Brett Frischmann's definition of ***infrastructure***:
  - ***nonrival***: "may be consumed nonrivalrously for some appreciable range of demand"
  - ***input***: "[demand] is driven primarily by downstream productive activities that require the resource as an input"
  - ***generic***: "may be used as an input into a wide range of goods and services, which may include private goods, public goods, and social goods"
- Examples: roads, telecommunications networks, the natural environment, ideas, and languages

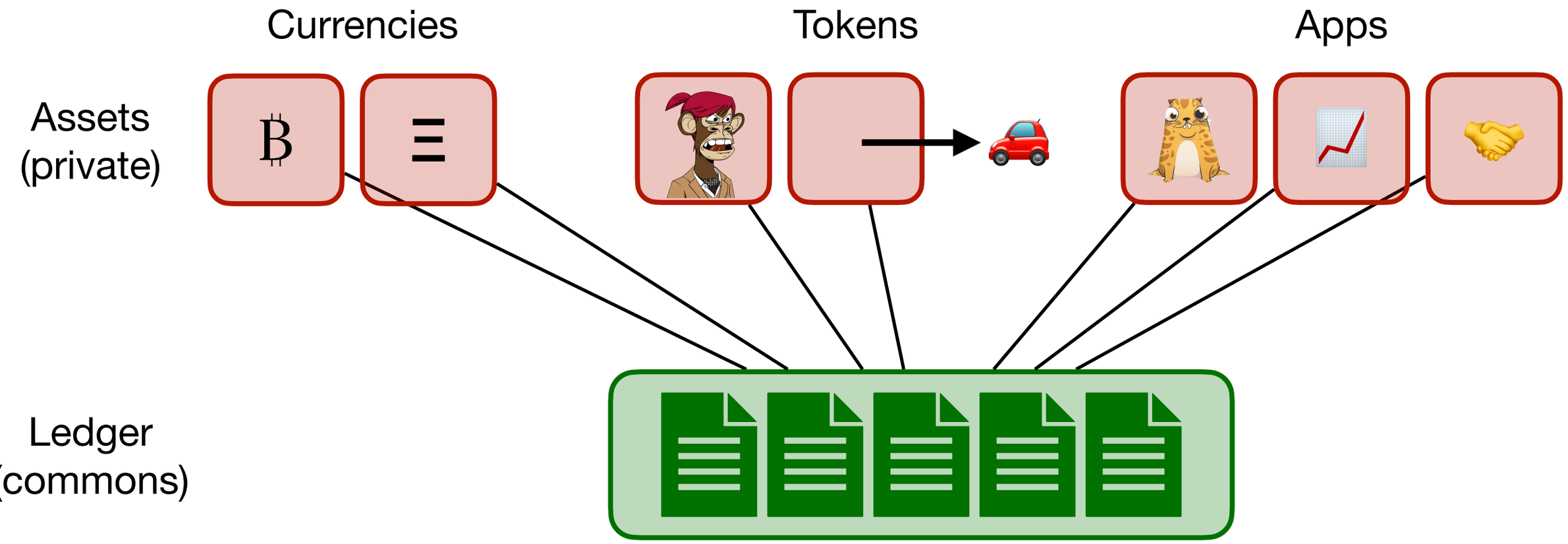
Ledgers are *infrastructure*



The dilemma of infrastructure

- Downstream uses create positive ***spillovers*** that have social benefit exceeding their private value to the user
    - Network effects benefit *other* users
    - Public goods benefit *everyone*
- Thus, users will not and cannot pay for all the value they create
    - Treating infrastructure as a private good, with a price based on willingness to pay, causes overpricing and underuse
- Frischmann's solution: ***commons management***, in which the infrastructure is shared among users on nondiscriminatory terms

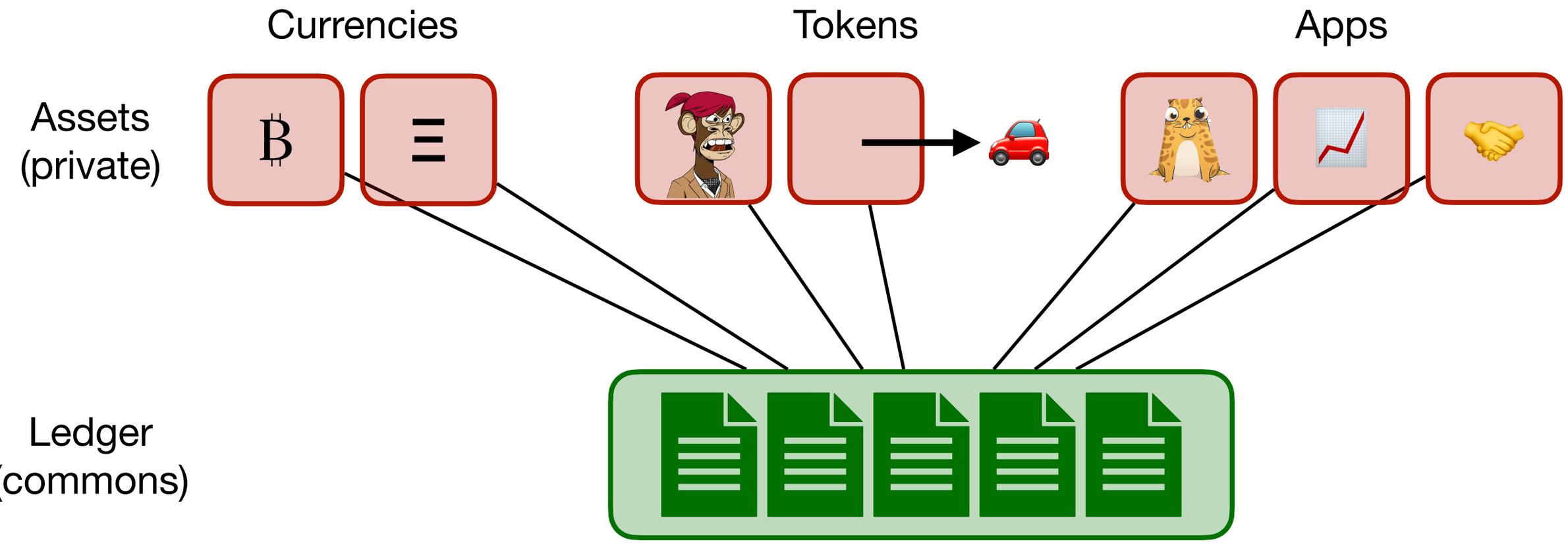
Ledgers as commons



Blockchains as commons

- A (public) blockchain is a commons in this sense
  - No restrictions on who can record or read transactions
  - Transaction fees are nondiscriminatory
- Three related resources:
  - The *ledger itself*: infrastructure managed as a commons
  - The *information on the ledger:* pure (common) information goods
  - The *assets tracked on the ledger*: private goods, because cryptographic signatures prevent unauthorized transactions

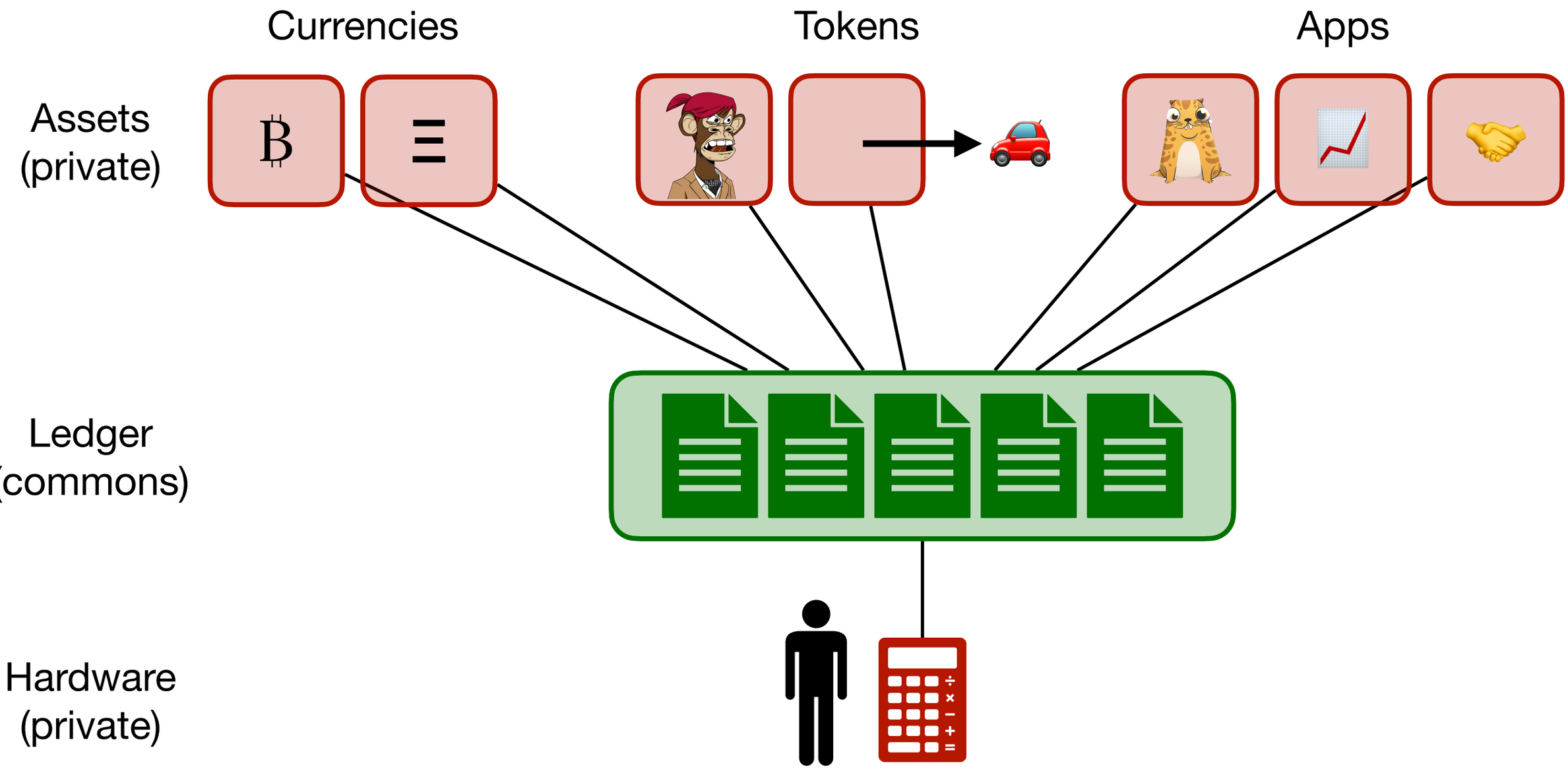
Ledgers as commons



Centralization

- Commons governance of infrastructure faces two challenges:
  - Demand-side: preventing ***congestion*** due to overuse
  - Supply-side: creating incentives for resource ***provision***
- Traditional solutions: direct public provisioning (e.g. roads) or public utility regulation (e.g. telephone network)
  - Free (local roads) or regulated (telephone) pricing
- Publicly provisioned ledgers include land and IP records
  - The ledger database itself is not especially costly

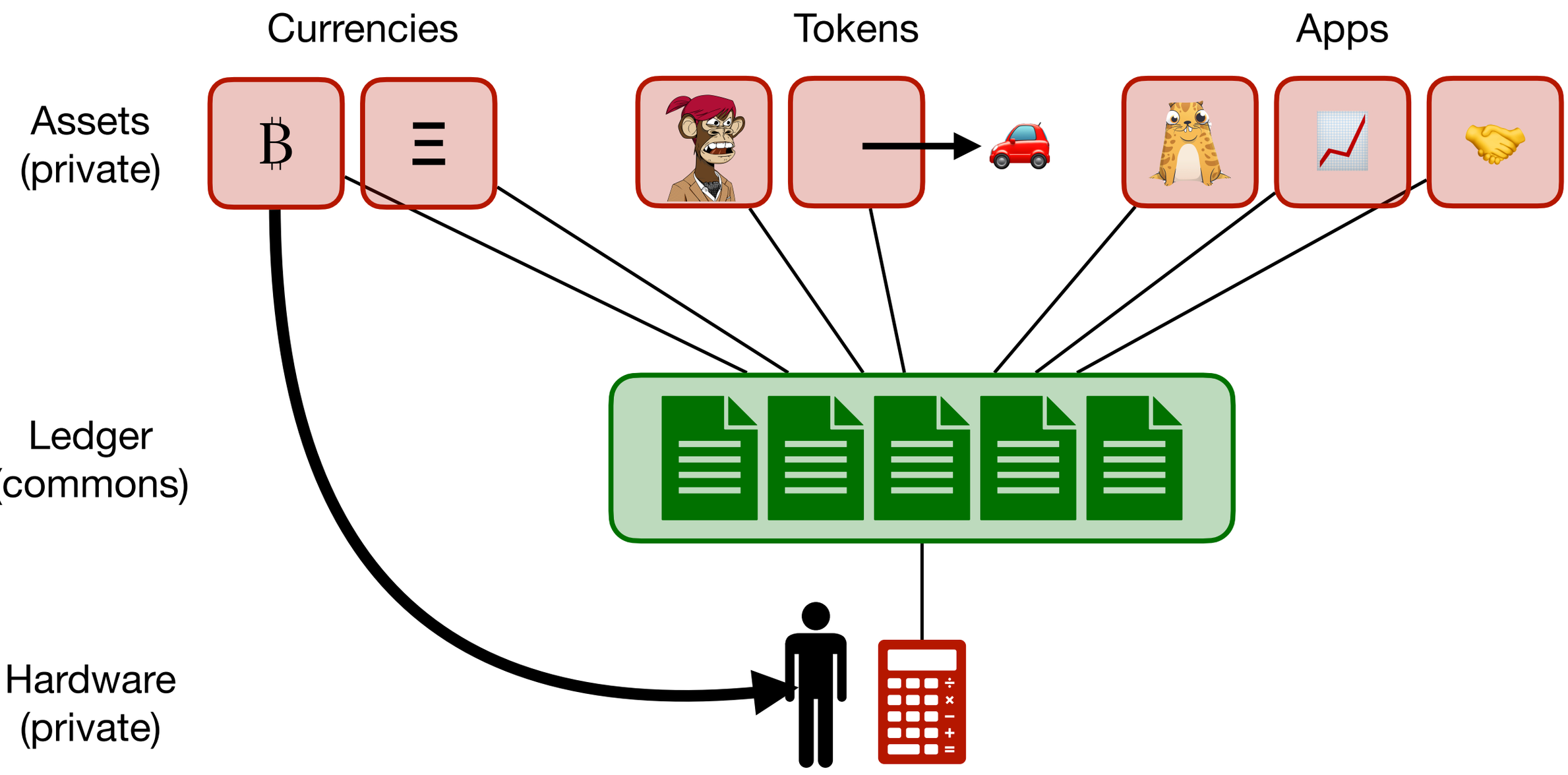
Centralized ledger



The downside of centralization

- But centralization has its own serious problems
  - A centralized administrator can discriminate among users
  - Or manipulate the resource corruptly for their own benefit
  - A ledger administrator could *lie* about the ledger's contents

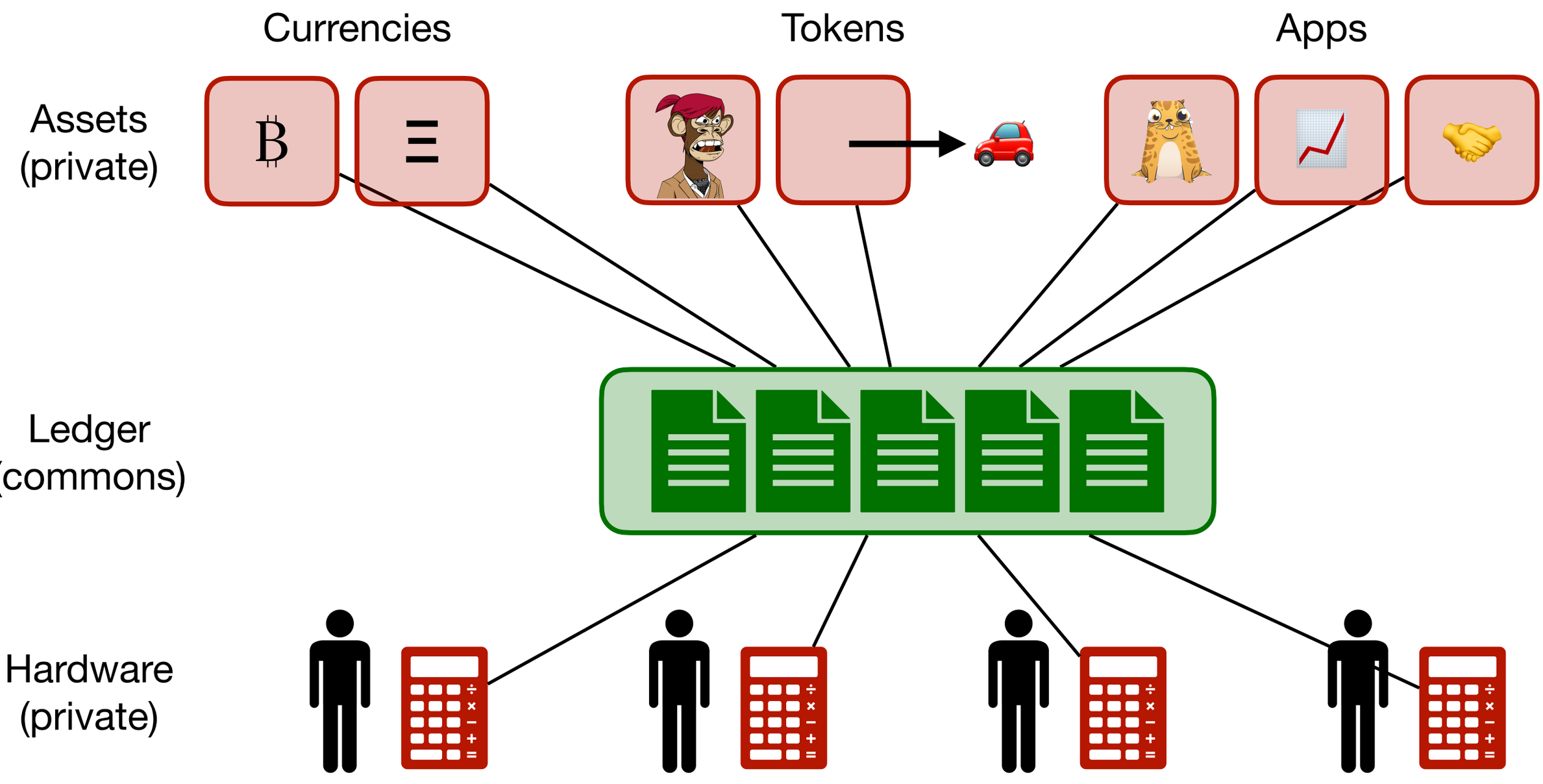
Corruption


Currencies
Tokens
Apps
Assets
(private)
Ledger
(commons)
Hardware
(private)

Decentralization

- This is the impetus for ***distributed*** ledger technology
- I.e., numerous participants *collectively* maintain the ledger
- Each of them contributes its own (private) hardware and effort

Distributed ledger

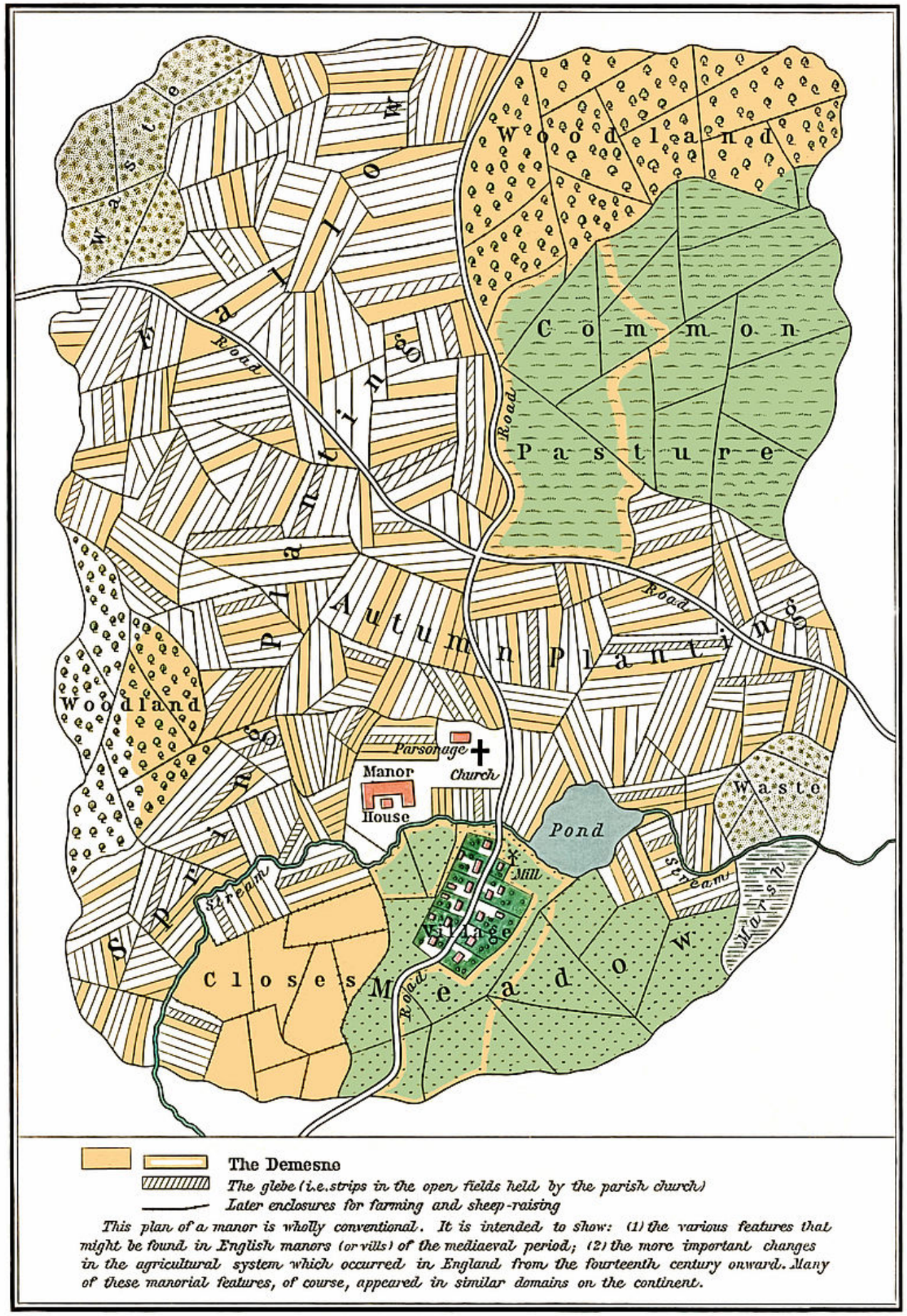


Semicommons

New solutions, new problems

- Decentralization raises its own new challenges:
  - ***Incentives***: Why should a participant contribute its resources?
  - ***Governance***: What if participants disagree?
- Building a sustainable commons on top of privately-contributed resources is a hard problem
  - But it turns out that it's a problem that's been solved before!

Plan of a Mediaeval Manor.



This plan of a manor is wholly conventional. It is intended to show: (1) the various features that might be found in English manors (or vills) of the mediaeval period; (2) the more important changes in the agricultural system which occurred in England from the fourteenth century onward. Many of these manorial features, of course, appeared in similar domains on the continent.

Semicommons

- In the medieval “open-field” system …
  - … farmers worked individual strips of land privately
  - … but livestock were grazed on the whole field in common
- Henry Smith’s definition of a ***semicommons***:
  - ***Privately owned*** with respect to some substantial uses
  - ***Held in common*** with respect to other substantial uses
  - Private and common uses substantially ***affect each other***

Semicommons challenges

- At first, semicommons look strictly *worse* than pure commons
    - You still have the challenges of overuse (by common users) and underprovisioning (by private users)
- But you *also* now have the challenge of ***targeting*** by common users who choose which private users their use affects
    - Shepherd picks where the sheep trample (bad) or poop (good)
- And even functioning semicommons are vulnerable to changes in prices or production technology
    - Landlords ultimately enclosed the open-field semicommons

Why a semicommons?

- The semicommons form is valuable when the gains from participating in the common use outweigh all these costs
  - E.g., wool + manure > trampling
  - E.g., games + shopping + memes > price of a computer
- The question is whether and how these costs can be kept sufficiently small that it’s > and not <

Semicommons mechanisms

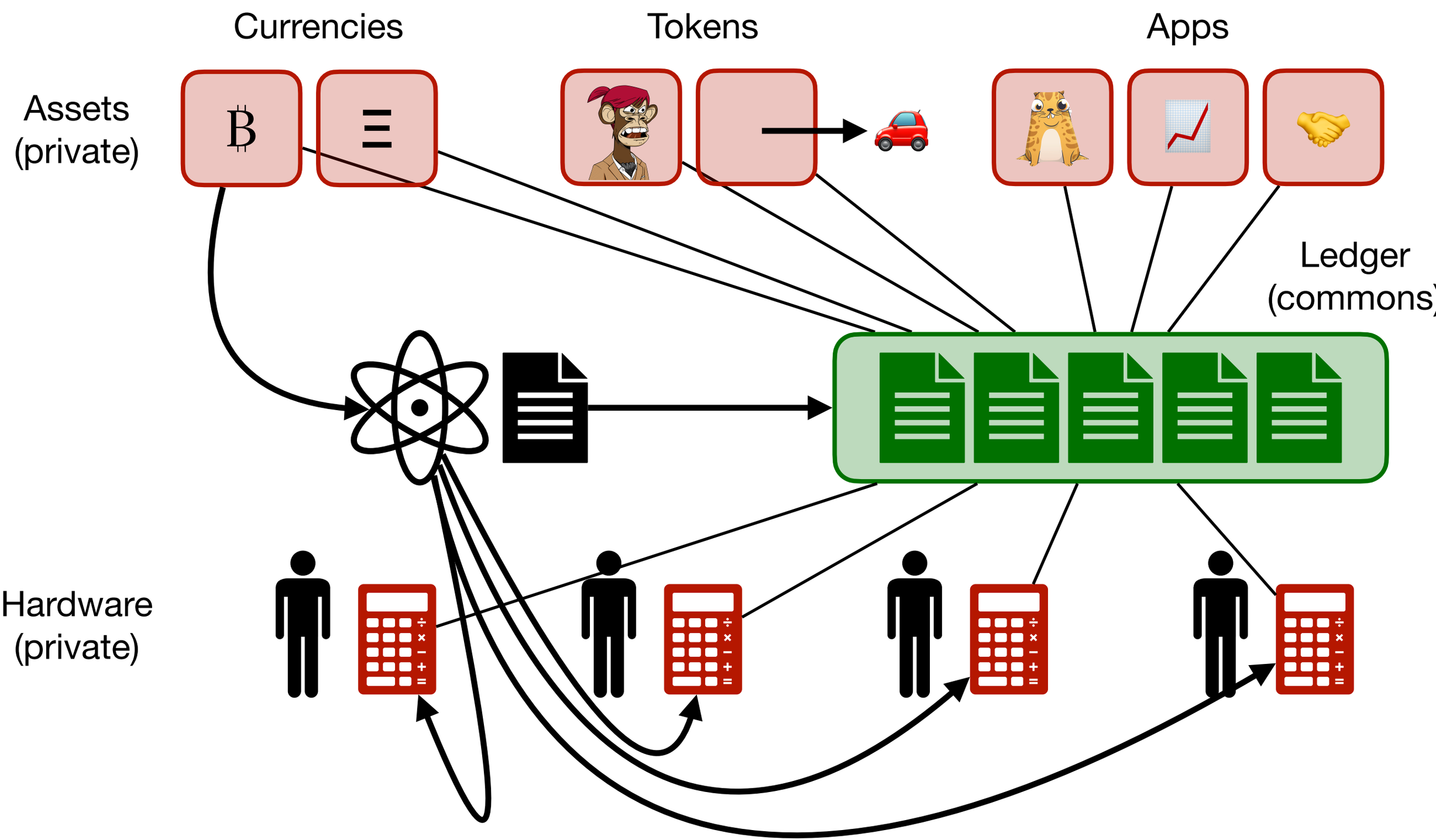
- ***Compensation*** (explicit or implicit) to reward private users for participating in provisioning the common uses

- ***Boundary-setting*** so that private users can defend themselves against targeted overuse and abuse

- ***Scattering*** so that commons users cannot target the costs and benefits of their uses to particular private users

- ***Governance*** institutions to resolve disputes and adjust in light of experience in a way that is acceptable to participants

Mining rewards



The blockchain balance

- Transaction fees (+mining rewards) create necessary incentives:
  - They give miners an incentive to provide (private) resources
  - They limit (common) congestion/overuse by pricing access
  - They are nondiscriminatory
- Proof-of-work block rewards are a form of scattering
  - They divide the benefits of the common use among private users in proportion to the computational resources those users contribute
  - Note the tight link between the private assets *on top of* the common ledger and the private resources that *maintain* it

Consensus as governance

- The longest-chain convention establishes consensus
  - It gives participants a strong incentive to agree with each other
    - Dissenting about the state of the ledger means losing your on-chain assets, because no one else will accept them from you
- This is a governance institution!

Complications

Protocols and software

- A blockchain's ***protocol*** and ***software*** are both public goods
  - They are pure commons, so there is no risk of overuse
  - (Indeed, they are typically open-sourced to induce greater adoption)
  - But as pure information, they are at risk being underprovided
- Common solution: add private incentives
  - A new blockchain's developers reserve some on-chain assets for themselves, or for the investors who fund the development (e.g., ICOs)
  - This creates its own governance issues, so it's also common for a foundation to steward these assets and coordinate development for the benefit of the blockchain community

It’s turtles all the way up, too

- On-chain assets (e.g. smart contracts) can be infrastructure, too!
- These raise very similar provisioning and governance issues
  - E.g., who pays for the coding and debugging?
  - E.g., should the code be free for reuse by competitors?
  - E.g., can participants trust the creators?
- Note the reuse of familiar consensus mechanisms here

Resource consumption

- Subtle but massive inefficiency in proof-of-work consensus
  - *Miners* will enter until the expected net reward drops to zero
    - But if *users* highly value the ledger, fees and rewards are high
    - Result: immense inefficient *over*-provisioning of redundancy
    - With catastrophic environmental consequences
- Problem: *some* redundancy is essential to trustworthiness
  - Thus, lots of work on developing proof-of-stake mechanisms (Who does this work? See the previous slide.)

Tyranny of the majority

- 51% attack: a majority of compute power hijacks a blockchain
  - The game theory here gets very complicated very quickly
    - And so does the political maneuvering
- Why? The protocol's anti-targeting guarantees break down!
  - *Cf.* miner-extractable-value attacks (e.g. front-running)
- This is a governance problem that no protocol can fully resolve
  - A different consensus mechanism (e.g. proof of stake) creates its own opportunities for strategic behavior

Consensus breakdown

- Blockchain protocols aren’t natural laws of the universe
  - A nation can always scrap its constitution and write a new one
  - A blockchain community can always modify its protocol
- Thus, the longest-chain consensus is not inviolate
  - Sometimes an influential participant intervenes (e.g. Vitalik after the DAO hack, or OpenSea after ape thefts)
  - Sometimes the community collectively decides
  - A few truly contentious disputes lead to forks

Inherent instability

- No large software project is ever finished or free of bugs
- Using tokens as incentives creates complex reward systems that depend on social behavior and have massive price volatility
- Constant technological change means that incentives, threats, and design alternatives are always shifting
- Collective community governance decisions…
  - … are routine, not exceptions
  - … are a feature, not a bug
  - … *make blockchains work*

Conclusion

You can’t hide from governance

- Blockchains are a new way of providing ledger infrastructure
  - Decentralization avoids some familiar corruption problems
  - And semicommons mechanisms address some familiar incentive problems of decentralization
- But they have governance and incentive problems of their own
  - The temptation is to add more epicycles to the protocol: new staking mechanisms, new abuse mitigations, etc.
  - But no protocol can solve all governance problems for all time

The moral

- There is something new, interesting, and possibly useful here
  - Blockchains aren’t just scams, hype, and carbon emissions
- But most descriptions of blockchains cannot be taken at face value
  - Blockchains are technosocial systems, not just technologies
  - On-chain stability is possible only because participants engage in extensive off-chain governance work
- Pay attention to *actual* blockchain governance mechanisms
  - Not just the ones formally instantiated in protocols and code

Discussion