How Bitcoin 2.0 Will Shape the Future of Business

Chris Clark

Bitcoin 1.0 - electronic payments

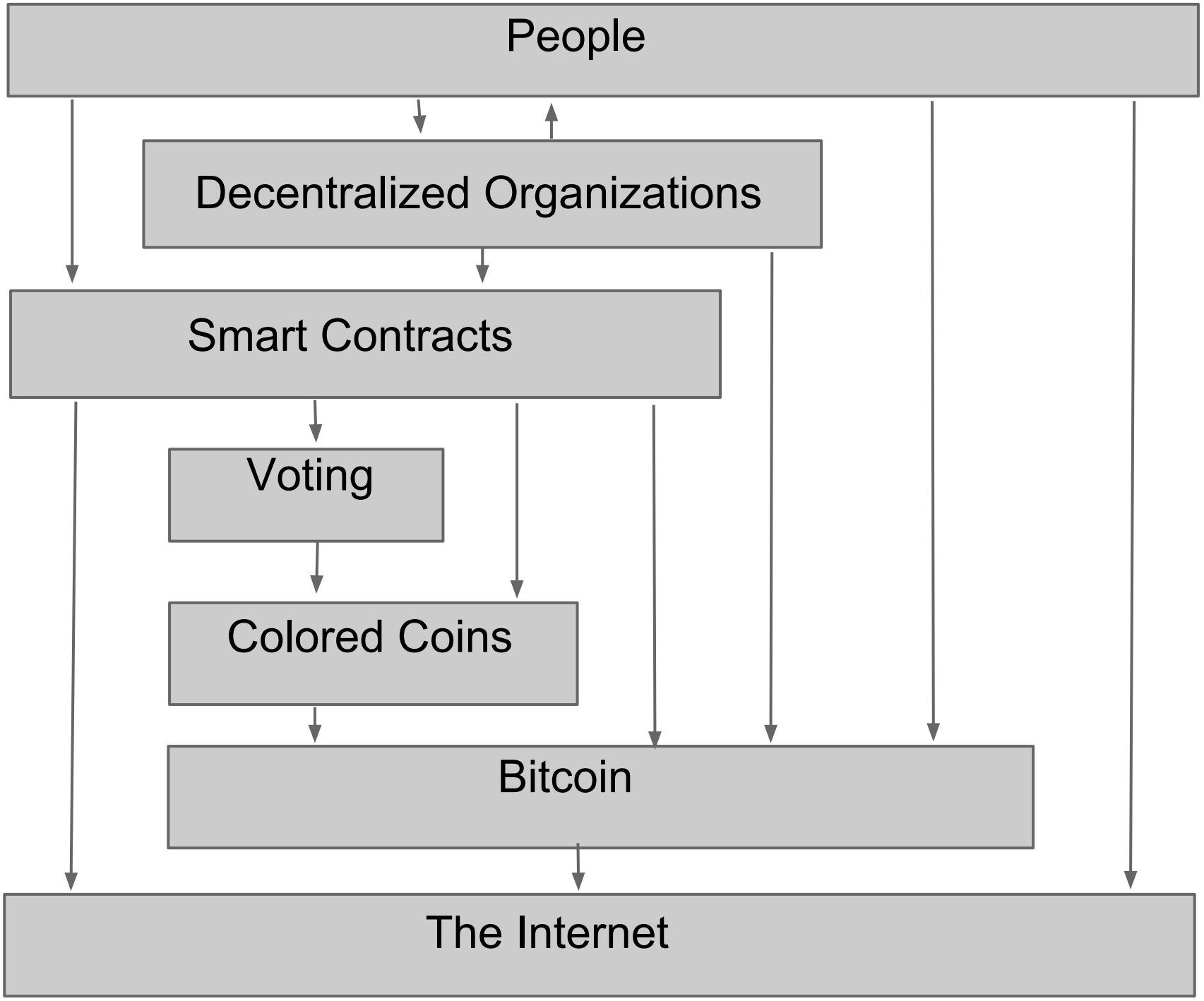
- Is Bitcoin better than a credit card?
  - Takes 1 hour to confirm a payment (for now…)
  - You lose all your money if you lose your digital wallet
  - No built-in theft insurance
- The benefits may seem minor in comparison
  - Much lower transaction fees
  - Not inflationary
  - Better privacy (if you are careful)
  - You control how much gets sent to merchant

Why Bitcoin is such a big deal

1. Bitcoin is the first electronic method of settling payments that doesn't have a choke point for regulation
2. Bitcoin is the first system that enables smart contracts

It’s hard to regulate Bitcoin

- Regulate exchanges
  - No effect on transactions in the Bitcoin system
- Regulate miners
  - No effect unless all countries in the world shut them down or internet censorship is used (like China’s Great Firewall)
- Regulate businesses accepting Bitcoin
  - Gives unfair advantage to foreign businesses
  - Most feasible option, but still very difficult to enforce


People
Decentralized Organizations
Smart Contracts
Voting
Colored Coins
Bitcoin
The Internet

Colored Coins

- An organization arbitrarily chooses some bitcoins and declares that ownership of those coins implies ownership of some real-world asset (probaby coins they own)
  - Could represent stock in a company
  - Could represent land ownership or car ownership
- Ownership is tracked as they are transacted
  - Issuer makes special rules for mixed-color inputs

Secure Voting

- A colored coin owner can prove that they own the colored coins by publishing their public key and a message signed with that public key
  - A hash of the public key is stored in the Bitcoin blockchain as the address that owns the coin
- Secure voting
  - Sign a message that contains the vote to cast

Crypto-equity

- A company sells colored coins instead of doing a traditional IPO
- The company promises to pay dividends in Bitcoin to each address that owns its colored coins
- Colored coin owners may also have votes
- Must trust the company to fulfill promises
  - Unless the company is a smart contract...

Smart Contracts

- Contracts that are enforced automatically using algorithmic transactions (a program)
  - Eliminates counterparty risk and associated costs
- Vending machine is a simple example (Nick Szabo)
- Bitcoin supports some types of smart contracts natively with it’s built-in scripting language

Multi-signature Transactions

- Payment is only made if 2 out of 3 (or m out of n) people sign
  - Useful for escrow and dispute mediation
  - Don’t have to trust the mediator because they never possess the money, it’s locked algorithmically
  - Just have to trust that the mediator won’t collude with counterparty
- To reduce risk of collusion with counterparty, use 15 mediators and require 8 signatures

Multi-signature Transaction Example

- Escrow for automobile purchase
  - The buyer creates public key K1 collects public keys from seller and mediator, K2 and K3 respectively
  - The buyer locks funds with scriptPubKey:
    - 2 <K1> <K2> <K3> 3 CHECKMUTLISIGVERIFY
  - The buyer shows this transaction to the seller
  - The seller verifies that K3 belongs to mediator by requesting that mediator sign a random nonce
  - The seller verifies that funds are locked in blockchain and hands over the keys

Multi-Signature Transaction Example

- Automobile escrow resolution
  - If all goes well, the mediator does nothing, buyer and seller both sign a transaction sending funds from escrow to seller
  - If there is a dispute, mediator reviews documents and DMV records, then creates and signs a transaction that sends money to either the buyer or seller, and whoever is receiving the money provides the second signature

Oracles

- Third party in multi-signature transaction can also be an oracle that automatically signs the transaction contingent upon information available on the internet
  - Can create financial derivatives by observing exchange rates
  - Can be used for betting by observing the news

Smart Contract Architectures

- Ethereum
  - All code runs on every node in the network
  - Contracts have “gas” that pays for their execution
  - If the gas runs out, the contract is terminated
  - Contracts have memory and can send messages like function calls
  - Contracts cannot reach out to the internet, but computers on the internet can send messages into the Ethereum network

Smart Contract Architectures (cont)

- Codius
  - Generic platform for deploying smart contracts
    - Like Amazon Web Services or OpenStack
  - Contract creator can choose how many hosts to use
    - Much more scalable than Ethereum
  - Minimize trust in hosts by using m of n consensus
  - Each Codius host can have its own billing policy
  - Contracts can be written in any language
  - Contracts can directly reach out to the internet

Decentralized Organizations

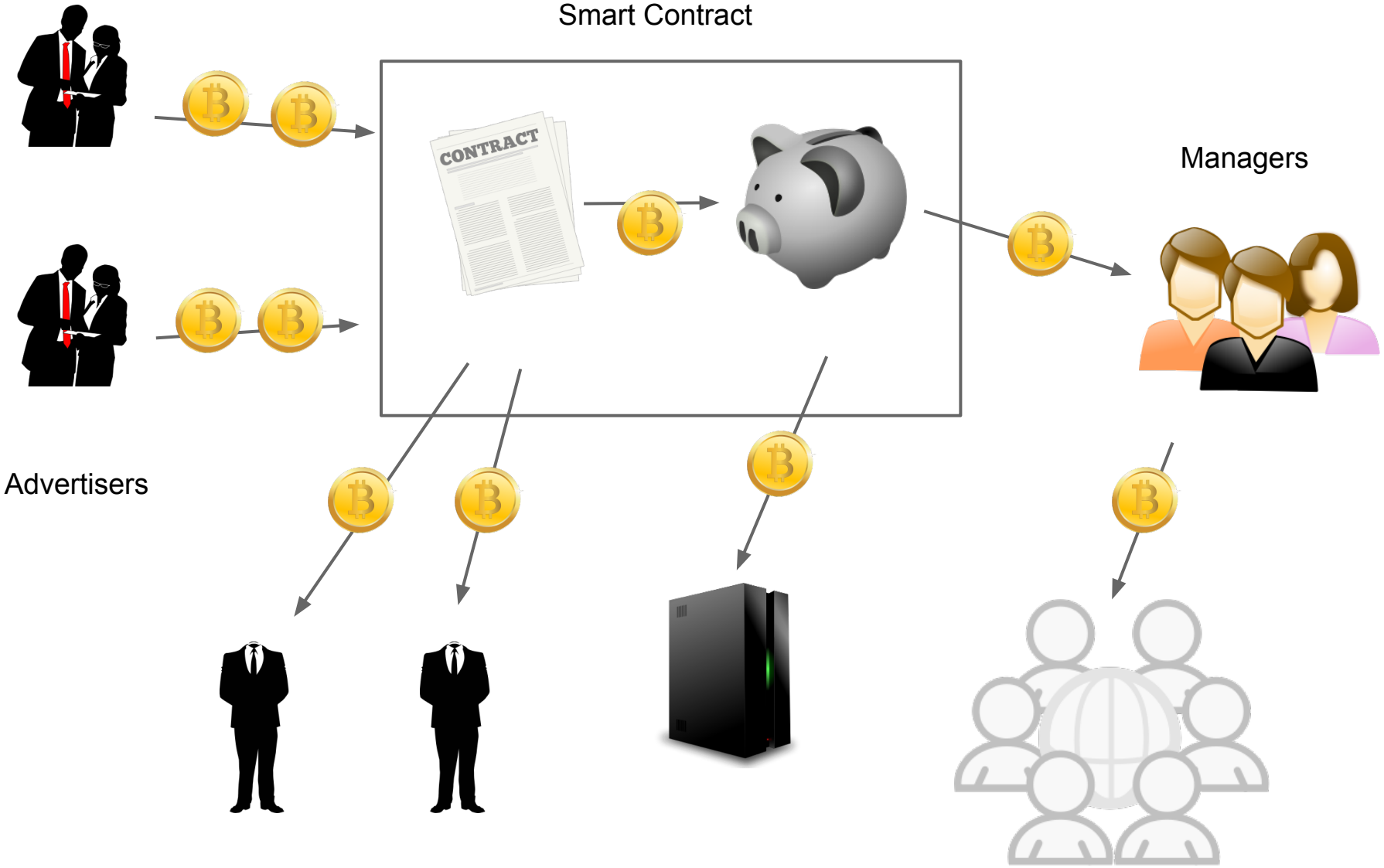
- A smart contract tied to a crypto-equity (colored coin) containing corporate by-laws and accounting logic, with real employees!
- All corporate revenues enter the smart contract through bitcoin payments and get disbursed according to budgeting rules and dividend policy
  - No more counterparty risk in crypto-equities

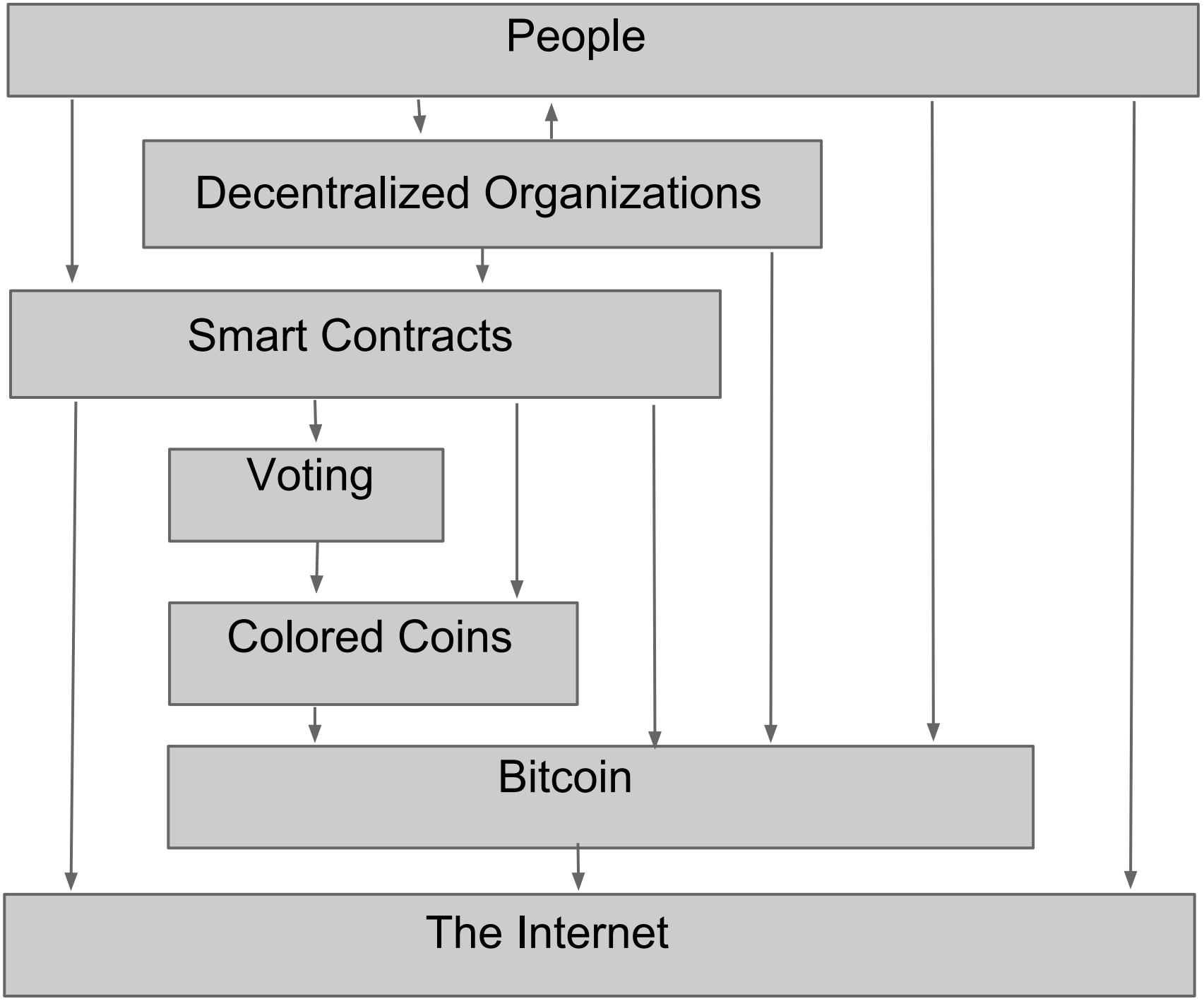
Decentralized Organizations (cont)

- DO smart contract contains bitcoin addresses and payment amounts for C-suite salaries and departmental budgets
  - Crypto-equity owners can vote to change these addresses, effectively firing the CEO or defunding a department
- Owners may also vote to change the dividend ratio

Decentralized Organization Example

- Online news site
  - All advertisers are asked to send payments to addresses in a deterministic wallet that is controlled by the smart contract (no human has access to it)
  - Smart contract sends a percentage of revenues to owners as dividends (less game-able than profits)
  - Remainder of revenues gets added to a pool of funds from which expenses are paid
    - Pool -> Managers -> Reporters & Designers etc.


Smart Contract
CONTRACT
Managers
Advertisers
Anonymous
Stockholders
Website
Hosting
Provider
Worldwide Staff


People
Decentralized Organizations
Smart Contracts
Voting
Colored Coins
Bitcoin
The Internet

Decentralized Organizations (cont)

- Why do people make corporations?
  - They allow a group of people to enter a business together, ensuring that the intended ownership of the business and dividend payments are enforced
  - They limit the liability of the owners
  - They allow ownership to be transferred at will or after death of an owner
- All of this can be handled by smart contracts
  - Liability limitation through anonymity

Decentralized Organizations (cont)

- A decentralized organization lives in the blockchain, distributed around the world
- Imagine such a company with employees in dozens of countries, doing business internationally through the internet…. which country would try to claim it's income taxes?
  - Ex: an online news site
  - Ex: a software development company

Income Taxes

- There is no feasible way to divide up corporate income between countries
- DOs (like foreign employers) have no incentive to withhold income taxes from their employees
- Employees can easily hide their bitcoin income (this is already happening)

Will companies transition to DOs?

- Most companies don’t want to change unless they have to
- Employees will accept lower wages in bitcoin if they know they can get away with tax evasion
- Traditional corporations will have to compete against DOs with 20-30% cheaper workforce
  - And they will eventually go out of business

Physical Presence

- Many companies require a physical presence (such as hosting providers)
- This can be used as a point of taxation
- But tracking income is still infeasible
- Move to resource-based government funding
  - Property taxes
  - Power consumption fees
  - Pollution fines (gas taxes)

Other Government Funding Options

- Contract signing service
  - Submit your smart contracts to a government server that charges a fee to digitally sign the contract
  - If the contract is signed, the government will help you enforce it in the real world using the court system and police, otherwise you have to pay for private arbitration (idea from Ayn Rand)
  - Fee is based on a percentage of the value bound by the contract

Definition of Tax

1. “a compulsory contribution to state revenue, levied by the government on workers' income and business profits or added to the cost of some goods, services, and transactions.” - Google
2. “A tax is a financial charge or other levy imposed upon a taxpayer (an individual or legal entity) by a state or the functional equivalent of a state such that failure to pay, or evasion of or resistance to collection, is punishable by law.” - Wikipedia

- Contract enforcement fees are **not taxes** because the government will never compel you to pay them; they are completely voluntary
- Like postage fees, they are a payment for services

Property “Taxes”

- Technically speaking, nobody owns land in the US because there is no allodial title
- Make a small change: you are not evicted from your property for not paying property taxes, you are evicted for trespassing after you stop and someone else starts paying
- Now property “taxes” are no longer taxes because they are voluntary

Is this what we want?

- Nobel prize winning economist Milton Friedman said land value tax is the least bad tax (most economically efficient)
- Ethically preferable to avoid violent compulsion
- Still generates a massive amount of revenue
  - Don’t have to eliminate social safety nets

The Invisible Hand

It is economically possible to:

1. Eliminate *ALL* taxes
2. While still funding the government/military
3. And providing a basic income to all citizens, making employment optional
    a. Just in time to address technological unemployment

- Tech is guiding policy like an invisible hand, just as capitalism guides economic activity

DAOs

- Decentralized Autonomous Organizations
  - A decentralized organization that runs itself
  - May hire programmers to improve its own code
- May be impossible to shut down
  - Each host has a different cryptographic key pair
    - Generated locally as part of deployment protocol
  - Decisions are made by consensus of 70/100 hosts
  - If you disable a host, it automatically buys another

Sidechains

- It’s possible that a better coin will be created
  - Faster settlement, more anonymous, less power consumption from mining
- But it’s hard to beat the network effect
  - Ex: Craigslist is still most popular classifieds site despite it’s primitive and inefficient user interface
- Sidechains create a two-way currency peg
  - Allow new currencies to be backed by bitcoins just like how US dollars used to be backed by gold

Instant Payment Confirmation

- BIP 65 suggests a new script op-code: OP_CHECKLOCKTIMEVERIFY
  - Compares parameter to lock time of the transaction that is trying to spend the transaction the script is in
- Can lock funds so it requires 2 signatures until some point in future, then only one
  - IF (<notary pubkey> CHECKSIG) {} // empty if block ELSE {<expiry time> CHECKLOCKTIMEVERIFY DROP} <user pubkey> CHECKSIGVERIFY

Instant Payment Confirmation (cont)

- Merchant sees that you can only spend with cooperation of notary (at least today)
- Merchant trusts notary not to collude with you to double-spend
- Merchant accepts a transaction signed by you and the notary with zero confirmations
- If notary is malicious or shuts down, you still get all your money back at expiration

Difficulty of Value Capture

- Usually monumental change provides massive opportunities for profit
- Decentralization is so impactful *precisely because* it eliminates the drain caused by middlemen
- Blockstream (company driving sidechain development) doesn’t seem to have a business model