Smart Contracts

Kate Sills
LAW928 - Dispute Resolution, Technology And The Digital Economy
University of Miami School of Law
03/08/24

Untangling Smart Contract Concepts

Ethereum Smart Contracts

“Systems which automatically move digital assets according to arbitrary pre-specified rules.” Code that runs on a blockchain.

Legal Contracts

A “promise or set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty”

Computable Contracts

Traditional legal contracts clearly specified enough to be written in code and executed at least in part by a computer. Generally have nothing to do with blockchains.

Ambiguity in contracts

Rule ambiguity: Bad

- We know the facts, but we don’t know what the contract says should happen
- Rule ambiguity is a bad thing, since the point of law is to “project dependable order into a set of future interactions.”

Event Ambiguity: Good?

- A vagueness about whether a particular trigger has occurred
- Sometimes a beneficial shorthand
- Sometimes used to specify events that require human judgment to resolve

“Ambiguity” in Legal Specification: Feature or Bug?
Oliver R. Goodenough, Vermont Law School & CodeX Future Law, Stanford Law

> “[C]ontract law is a remedial institution. Its aim is not to ensure performance ex ante, but to adjudicate the grievances that may arise ex post.”

—Kevin Werbach and Nicholas Cornell

Contracts Ex Machina

Why do we use contracts?

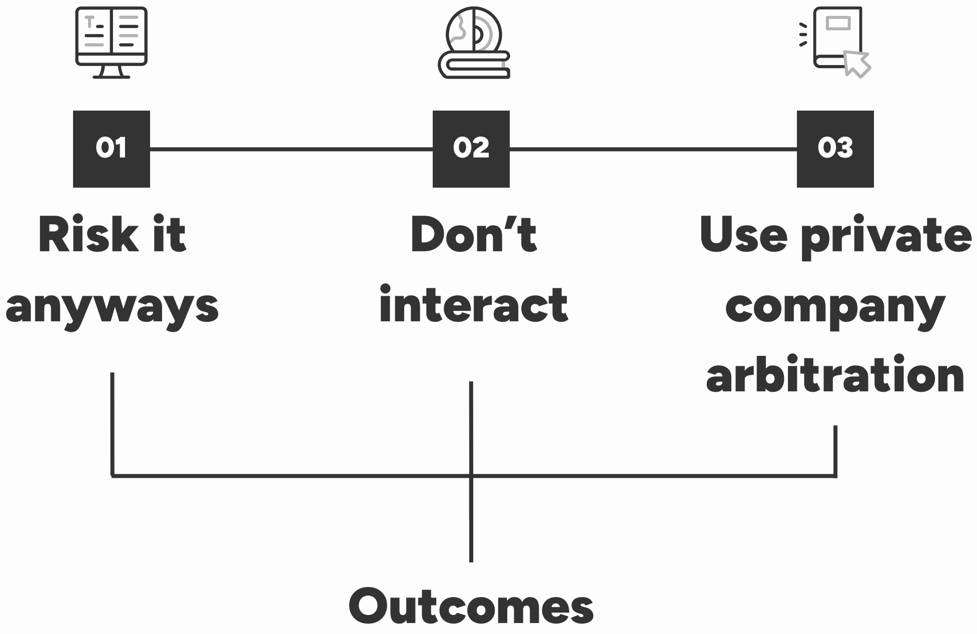
Some ideas from the subfield of law & economics

- To solve “transactional insecurity”
  - Contract Law and the State of Nature by Yale Law Prof Anthony Kronman
- To have more certainty about future events
  - Oliver Hart
- To create “credible commitments” that change other parties’ incentives and thus behavior
  - Thomas Schelling
- To signal something
  - Unenforceable clauses as an example

Transactional insecurity on the Internet

Current situation

There are eight billion people in the world, and if we choose a person at random to trade with, 96 out of every 100 times, they're not going to be in the United States. How do we trade securely?



01

Risk it anyways

02

Don't interact

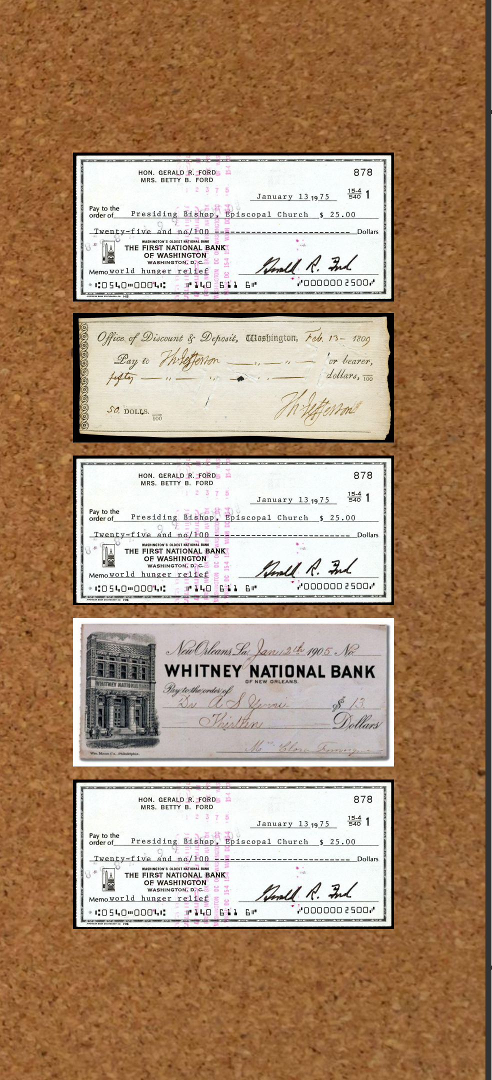
03

Use private company arbitration

Outcomes

Bitcoin and Ethereum

The reality of “smart contracts” as code on a blockchain
With examples



HON. GERALD R. FORD
MRS. BETTY B. FORD
878
January 13 1975 15-4/540 1
Pay to the order of Presiding Bishop, Episcopal Church $ 25.00
Twenty-five and no/100 Dollars
WASHINGTON'S OLDEST NATIONAL BANK
THE FIRST NATIONAL BANK OF WASHINGTON
WASHINGTON, D. C.
Memo world hunger relief
Gerald R. Ford
⑆0540⑈0004⑆ ⑈140 611 6⑈ ⑈0000002500⑈

Office of Discount & Deposit, Washington, Feb. 13 – 1809
Pay to Th: Jefferson or bearer,
fifty dollars, 100
50. DOLLS. 100
Th: Jefferson

HON. GERALD R. FORD
MRS. BETTY B. FORD
878
January 13 1975 15-4/540 1
Pay to the order of Presiding Bishop, Episcopal Church $ 25.00
Twenty-five and no/100 Dollars
WASHINGTON'S OLDEST NATIONAL BANK
THE FIRST NATIONAL BANK OF WASHINGTON
WASHINGTON, D. C.
Memo world hunger relief
Gerald R. Ford
⑆0540⑈0004⑆ ⑈140 611 6⑈ ⑈0000002500⑈

New Orleans La. Jan 2th 1905 No.
WHITNEY NATIONAL BANK
OF NEW ORLEANS.
Pay to the order of Dr. A. S. [illegible] $ 13
Thirteen Dollars

HON. GERALD R. FORD
MRS. BETTY B. FORD
878
January 13 1975 15-4/540 1
Pay to the order of Presiding Bishop, Episcopal Church $ 25.00
Twenty-five and no/100 Dollars
WASHINGTON'S OLDEST NATIONAL BANK
THE FIRST NATIONAL BANK OF WASHINGTON
WASHINGTON, D. C.
Memo world hunger relief
Gerald R. Ford
⑆0540⑈0004⑆ ⑈140 611 6⑈ ⑈0000002500⑈

Bitcoin, simplified

Analogy: like checks posted to an append-only bulletin board. But unlike real checks, the checks are never deposited - they're just reused. The payee becomes the payer and chooses a new payee.

"We define an electronic coin as a chain of digital signatures."
— Bitcoin white paper

Bitcoin Escrow with 2 of 3 multisig

Buyer signs a transaction

“To spend these bitcoin, either the seller and I must sign, or the seller and the prespecified arbitrator sign, or I and the arbitrator sign.”

Seller transfers item or performs service

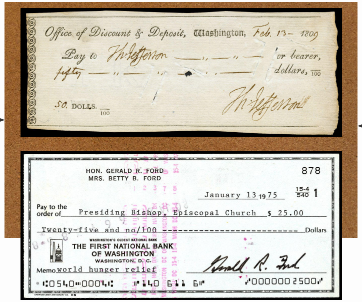
Outcomes:

- Buyer and seller are both happy and sign. Money goes to the seller. Arbitrator has zero power.
- DISPUTE: Buyer says they didn’t get the full item or service
    - Arbitrator decides & signs a transaction with either buyer or seller. Arbitrator cannot get the bitcoin for themselves at all.
- Buyer and seller both decide to undo the transaction. Money goes back to the buyer. Arbitrator has zero power.

Oracles

Humans or computers that provide information about the outside world to blockchain code through transactions.

Only input:
Transactions



Office of Discount & Deposit, Washington, Feb. 13 – 1809

Pay to Th: Jefferson or bearer,

fifty dollars, $\frac{}{100}$

50. DOLLS. $\frac{}{100}$

Th: Jefferson

HON. GERALD R. FORD
MRS. BETTY B. FORD

878

January 13 1975 $\frac{15\text{-}4}{540}$ 1

Pay to the order of Presiding Bishop, Episcopal Church $ 25.00

Twenty-five and no/100 ------------------------- Dollars

WASHINGTON'S OLDEST NATIONAL BANK
THE FIRST NATIONAL BANK
OF WASHINGTON
WASHINGTON, D. C.

Memo world hunger relief

Gerald R. Ford

⑆0540⑈0004⑆ ⑈140 611 6⑈ ⑈0000002500⑈

AMERICAN BANK STATIONERY CO. HS

Only output:
Someone reading the "board"

- Blockchain code can't query the outside world, but it can wait for input.
- Blockchain code can't control anything in the outside world, but something external can choose to listen.

Ethereum

Allow anyone to create their own tokens

Rather than trying to imbue Bitcoin transactions with additional meaning, anyone can make a “smart contract” with its own mini-database of which accounts own what

Write any kind of rules you want

But you still can’t query or control the outside world

All of this code runs on the same blockchain

Code in one “smart contract” can call another smart contract. Tokens of different types can be traded with each other atomically

Ethereum's most novel feature:
Escrow without opportunism

AKA blockchain code itself as sole owner

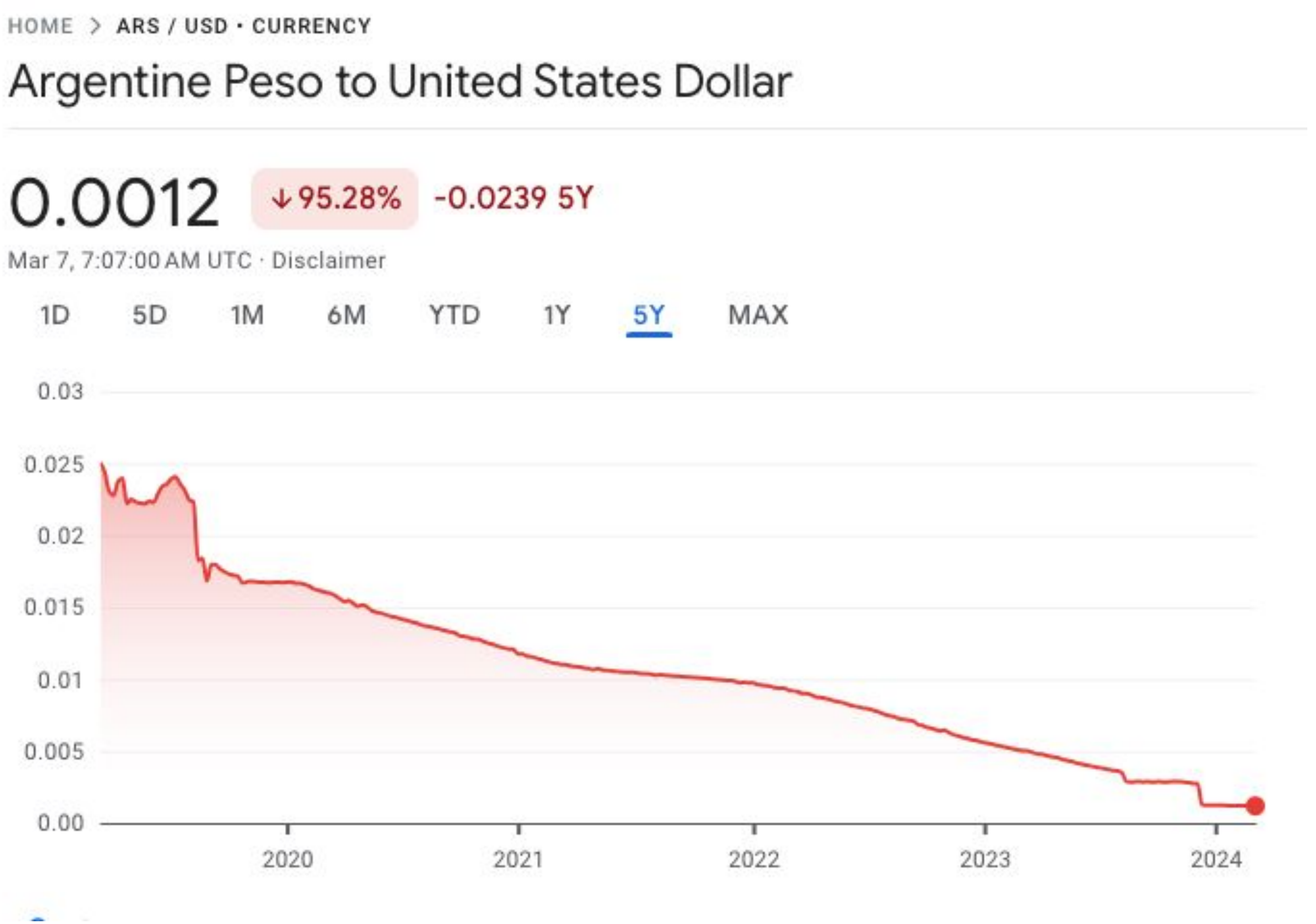
- Ethereum “smart contract” code can have sole control over particular tokens, meaning that nothing else - no human, no company - has control of the particular tokens until the code releases it

By contrast - without blockchains:

- The holder of collateral can just sell it or take it if they want, which has additional effects

“By giving me collateral that is equal in value to the performance I have been promised, you create an opportunity for bargaining that I can exploit, if I am skillful enough, to appropriate the gain you expected to realize from our transaction” – Anthony Kronman, Contract Law and the State of Nature

Example:
Maker Protocol
Vaults and Stablecoins



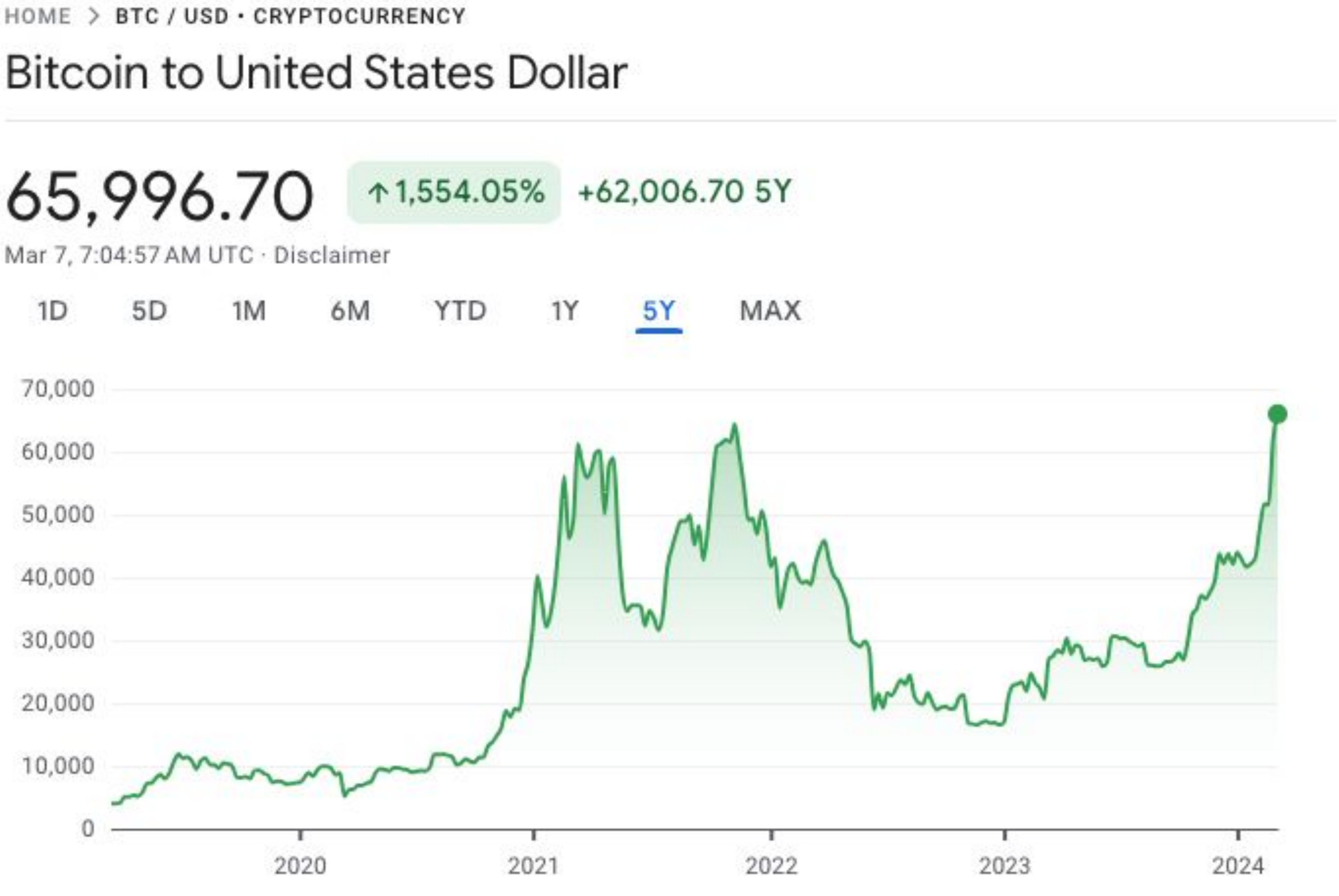
HOME > ARS / USD • CURRENCY

Argentine Peso to United States Dollar

0.0012 ↓95.28% -0.0239 5Y

Mar 7, 7:07:00 AM UTC · Disclaimer

1D 5D 1M 6M YTD 1Y 5Y MAX



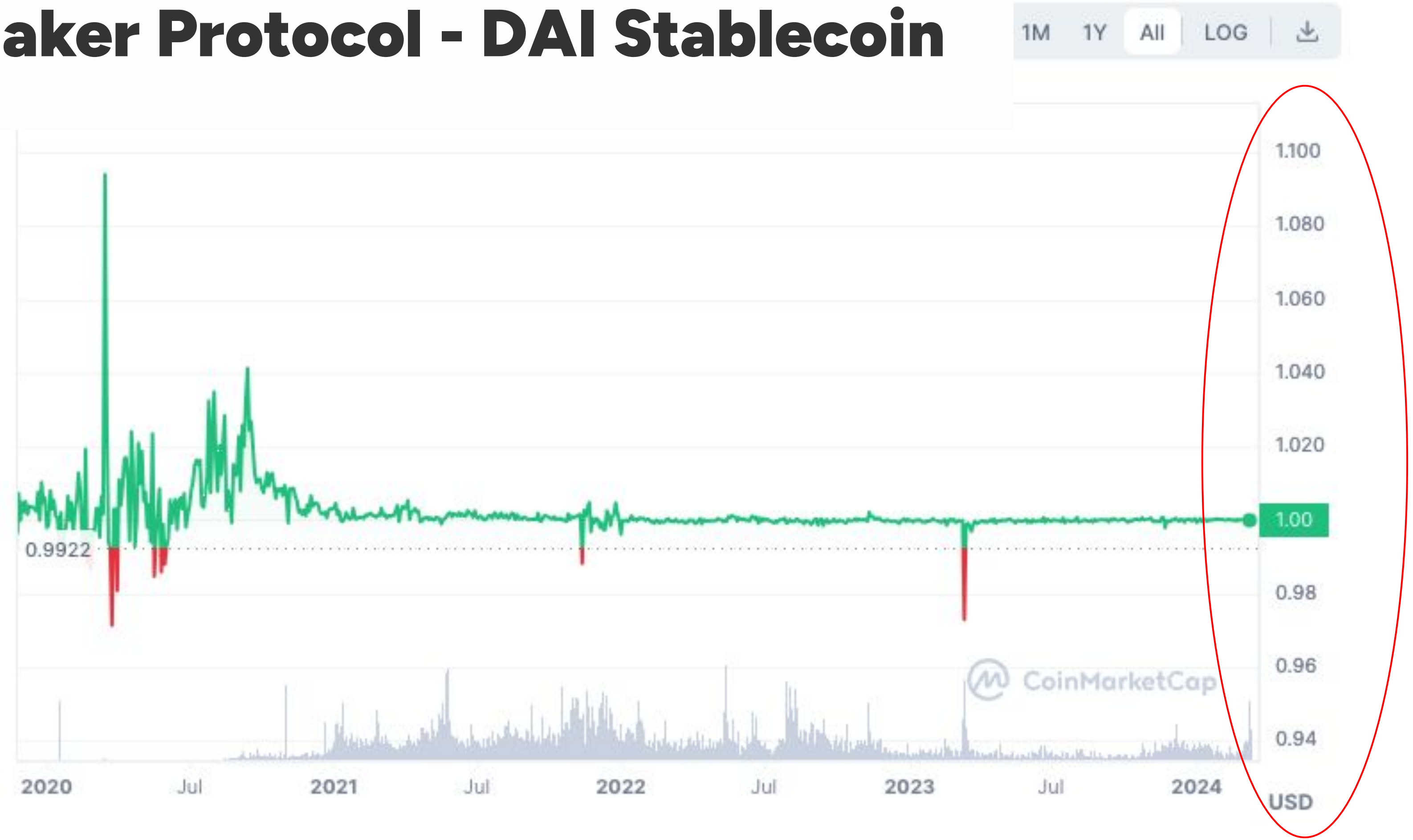
HOME > BTC / USD • CRYPTOCURRENCY

Bitcoin to United States Dollar

65,996.70 ↑1,554.05% +62,006.70 5Y

Mar 7, 7:04:57 AM UTC · Disclaimer

Maker Protocol - DAI Stablecoin



Example: Maker Protocol Vaults

- User launches a new smart contract
- User deposits some form of collateral in the form of tokens
- The “vault” contract code has sole control and ownership over the collateral.
  - MakerDAO (the company) and their investors cannot take the collateral
- User gets DAI (a stablecoin soft-pegged to the US dollar) back as a loan
  - The loan is overcollateralized: the collateral is worth more than the loan amount
- If the value of the collateral goes down, either the user:
  - Adds more collateral
  - Repays the loan (in part or in full)
  - Does nothing and the code sells the collateral automatically

Collateral is escrowed without the possibility of opportunism - for the first time in history.

Digital Assets on a Blockchain

Intrinsic Value

- E.g. a cryptocurrency like Bitcoin or Ether, where there is no external reality to match

Representative/Referential

- E.g. a shipment of coffee represented as a non-fungible token that gets transferred from account to account as the coffee goes through the supply chain from producer to consumer
- Entirely reliant on outside entities mapping between reality (the facts on the ground) vs what is represented in the token ownership

False Dichotomies... Everywhere

- Not blockchain code vs legal contracts with legal remedies in US courts

A variety of tools:

- Code on a single machine
- Code running on blockchains
- Amateur individual human arbitrators
- Expert and well-designed dispute resolution systems
- Mechanism design for creating credible commitments
- Legal enforcement and legal remedies

For any particular goal, pick the best tools for that particular job

Thanks!

katelynsills@gmail.com
@kate_sills on Twitter
@katelynsills.com on BlueSky

katelynsills.com

CREDITS: This presentation template was created by **Slidesgo,** and includes icons by **Flaticon,** and infographics & images by **Freepik**