

# on Trust

Ian Grigg  
WTSC19 St Kitts

## **3<sup>rd</sup> Workshop on Trusted Smart Contracts**

**In Association with Financial Cryptography 2019**

**February 22, 2019**

**St. Kitts Marriott Resort  
St. Kitts**

# *it's all about Trust*

1. The Ricardian Contract
2. Bitcoin & exceptions
3. smart contracts
4. Digital Signing
5. on Trust
6. Liability

# Ricardians...

- (early) 1990s - Digicash doing eCash as currency
- 1995 - Gary Howland and I did “every other instrument”
- MVP - bonds - as unregulated space



5 1/4% REPAYABLE 15TH NOVEMBER, 1987

COMMONWEALTH OF AUSTRALIA  
Treasury Bond

TRANSFERABLE BY  
DELIVERY

ISSUED UNDER THE COMMONWEALTH  
INSCRIBED STOCK ACT 1911-1963.

\$20

5 1/4% DEF 001067 \$20

*This Bond entitles the Bearer to the payment at the Reserve Bank of Australia at Canberra, Sydney, Melbourne, Brisbane, Adelaide, Perth, Hobart or Launceston of*  
**— TWENTY DOLLARS —** *together with interest thereon at the rate of*  
**FIVE AND ONE QUARTER** *per centum per annum in accordance with attached coupons,*  
*and such sums are secured on the Consolidated Revenue of the Commonwealth of Australia.*  
*Principal is repayable on the* **FIFTEENTH DAY OF NOVEMBER, ONE THOUSAND NINE HUNDRED AND EIGHTY SEVEN.**

*Dated this 14th day of February, 1966.*

*Roland Wilson*  
SECRETARY TO THE TREASURY.

1987

PRINTED BY THE AUTHORITY OF THE GOVERNMENT OF THE COMMONWEALTH OF AUSTRALIA

COMMONWEALTH OF AUSTRALIA TREASURY BOND  
INTEREST COUPON

5 1/4% DEF 001067 <sup>41</sup>

INTEREST FOR SIX MONTHS ON \$20 REPAYABLE 1987

15TH MAY, 1986 \$0.52

COMMONWEALTH OF AUSTRALIA TREASURY BOND  
INTEREST COUPON

5 1/4% DEF 001067 <sup>42</sup>

INTEREST FOR SIX MONTHS ON \$20 REPAYABLE 1987

15TH NOV., 1986 \$0.53

COMMONWEALTH OF AUSTRALIA TREASURY BOND  
INTEREST COUPON

5 1/4% DEF 001067 <sup>43</sup>

INTEREST FOR SIX MONTHS ON \$20 REPAYABLE 1987

15TH MAY, 1987 \$0.52

COMMONWEALTH OF AUSTRALIA TREASURY BOND  
INTEREST COUPON

5 1/4% DEF 001067 <sup>44</sup>

INTEREST FOR SIX MONTHS ON \$20 REPAYABLE 1987

15TH NOV., 1987 \$0.53



# What's a bond?

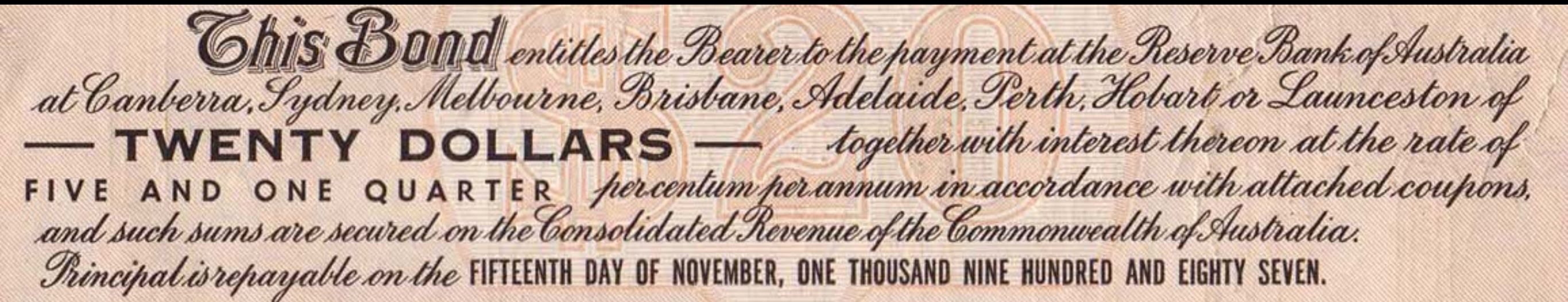
- face, periods, coupons, text...



- could put these params into a database?
  - *today: DSLs, formal models (e.g. VeriSolid)*
- but, people! kept changing the text

# But!

- legally, a bond is a *contract...* and People!



*This Bond* entitles the Bearer to the payment at the Reserve Bank of Australia at Canberra, Sydney, Melbourne, Brisbane, Adelaide, Perth, Hobart or Launceston of  
— **TWENTY DOLLARS** — together with interest thereon at the rate of  
FIVE AND ONE QUARTER per centum per annum in accordance with attached coupons,  
and such sums are secured on the Consolidated Revenue of the Commonwealth of Australia.  
*Principal is repayable on the* FIFTEENTH DAY OF NOVEMBER, ONE THOUSAND NINE HUNDRED AND EIGHTY SEVEN.

- every bond is slightly different...
- modelling and abstraction isn't sufficient

# SO...

- flip the problem upside down
- if we can't beat them, join them
- bend the tech to work for the wordsmiths
- place the programmers in 2nd tier



# prose inspired by people

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

;
; Prepaid Services Dollar, Issue A.
;
; Being, a Contract to settle USD-denominated services.
;
; Between, Systemics Inc. and Users.
;

[definitions]
definitions_dollars = *
{
  Prepaid Services Dollar ("PSD") means the electronic
  currency, denominated in United States of America dollars
  ("USD"), as facilitated by this Ricardian contract.  Other
  dollars, which may be used as exchange for PSD, are referred
  to as Account Dollars.
}

definitions_units = *
{
  The unit of the PSD is the iota, which is defined as having
  the value of PSD 0.0001.
}

definitions_purpose = *
{
  The purpose of PSD is to facilitate the payment of services
  provided by Systemics Inc.
}
```

**Explanatory Comment**

**Heading**

**Prose clauses**



# Markup inspired by HTML

```
[issue]
;
; This section identifies general aspects of this contract.
;
issue_type = currency
issue_name = Systemics Pre-paid Services Dollar

[currency]
currency_symbol = $
currency_tla = PSD

[unit]
;
; The Unit of Account is the PSD. This currency is denominated
; in PSD, with an underlying unit of contract of iota, which
; is equal to PSD 0.0001.
;
unit_power = 4
unit_mediate_power = 2
unit_major = $
unit_mediate = c
unit_minor = p
unit_major_unit = PSD
unit_mediate_unit = cent
unit_minor_unit = iota
```

**tag-value pairs,  
parseable by  
program**

**Slightly smart  
decimalisation**

- but done with INI

# PGP cleartext signature inspired:

```
- -----BEGIN PGP SIGNED MESSAGE-----
```

```
Hash: SHA1
```

```
05.02.11
```

```
'Alice' is the owner of the GPG key with fingerprint:
```

```
4F16 E4D6 BB9B D4A0 39F8 9644 DF23 CB88 2400 ACE3
```

```
'Bob' is the owner of the GPG key with fingerprint:
```

```
05CA A3B0 9322 1874 9D1A 2357 9C07 2DDC 4394 91B7
```

```
This contract is for the exchange of 20 Bitcoins at a  
rate of USD $3.25 per bitcoin, for a total of $65 USD.
```

```
Bob agrees to send $65 USD, plus any fees charged by  
Paypal, via a Paypal payment with transaction type 'Payment  
Owed' (to reduce chargeback risks) to the paypal account  
'alice@lol.com' within 24 hours of both parties  
signing this contract. Alice agrees to send 20 bitcoins  
to 1DjlSocbbH9Lbb9aTdqSHB9AAjhdXNNZha within 4 hours  
of receiving this Paypal payment.
```

```
- -----BEGIN PGP SIGNATURE-----
```

```
Version: GnuPG v1.4.11 (GNU/Linux)
```

```
iJwEAQECAAYFAk2/PKAACgkQ3yPLiCQArO0c/AP9GL0EgVQMTHZqOX5ynNVGBFb2  
6eB7QzRdNQH8Zcj6R0y7fzbpYPbgwX+G3EYtsDjs4G3M8LdlFFCcJ/JLJGle19le  
KLpXp/BWMRayn3KcFYOGogmONtxklwOVoxF+wiK9jZYFIdjI87qh8iUOCboFVqQk  
T3OG7odEKJOjNwYP+j0=
```

```
=2mDw
```

```
- -----END PGP SIGNATURE-----
```



**“A Ricardian Contract can be defined as a single document that is**

- a) a contract offered by an issuer to holders,**
- b) for a valuable right held by holders,**  
**and managed by the issuer,**
- c) easily readable by people (like a contract on paper),**
- d) readable by programs (parsable like a database),**
- e) digitally signed,**
- f) carries the keys and server information, and**
- g) allied with a unique and secure identifier..”**

*–The Ricardian Contract*

## *an early form of trust-enabling technology*

- self-evident
  - users can read what is supposed to happen
  - software gets out its special params
- hash over document is strong
  - spoofing impossible?
- *the rule of one contract*



# To our surprise...

- *Not everyone was happy!*
  - Banks
  - Bitcoin
  - ICOs

# (what is) Bitcoin (?)

- SN did not use the Ricardian Contract
  - design exercise was different
- primarily a payment system
  - gaming, e-gold, Liberty Reserve, etc
  - under the threat of regulatory and banking censure



# (what does) Bitcoin (say?)

- Bitcoin says less - no point of attack
  - Information: current accounting
  - no future offering, no contract
  - active price was sufficient info for payments
- Ricardian says more - no weakness in meaning

# 2 Debilitating exceptions

- 1/ Ricardians made your words stick
- Banks, ICOs didn't want to be committed

- 2/ as soon as another 'Bitcoin' was added, had to describe it
- Bitcoin has the ONE, no 'room' for another
- disputes mean confusion, wars, forks



# smart contracts

- term 'smart contracts' both empowering and deceptive
- small programs with properties:
  - keeps running?
  - can't be interfered with?
  - transparent?
  - legally benign?
- not really true

- Riccy not trustless
  - users believe the word of parties
- SC not trustless
  - users hope it does what they think it should do
  - it keeps running
  - no hacks, no bugs, no forks

# On the belief that...

- Users believe that...
  - a (Ricardian) issuer is good for her word
  - a (SmartContract) programmer has done a good job
- enable these beliefs, not hinder them



# Hope & Belief

- How do users ensure their desired outcome?

## **3<sup>rd</sup> Workshop on Trusted Smart Contracts**

- We don't have the answer - yet
- maybe we've been here before

# Digital Signing

- 1980s: telcos built concept of PKI - x500
- phone could receive emails, read them offline
- how would users know they were reliable?
- answer - give every household (phone) a certificate
- question: which came first, problem or solution?

# looking for a problem

- graft old 'certs' into new (DH) SSL
  - ==> SSL v2
  - convince Netscape that MITMs were bad
- could also use 'certs' to replace the pen
  - signing contracts -> courts -> laws -> lobbying

# Why DigSigs failed?

- Digital signing was not of benefit to consumers
- hardware, crypto, software is impenetrable to user
- paper does a better job in a dispute
- millions of certs means revenue
- also means: liability's



# Liability at scale

- \$1 \* all the certs == broke
- \$0 \* all the certs == business model!
- CAs employed legal defences against liability
- Dumping all risk & liability on the users

# And then Grandma loses her house

- The 'Grandma loses her house' test:
  1. Grandma has cryptographic signing capability
  2. She cryptographically signs some digital contract
  3. Grandma loses her house
- Resolve by going to court?
- Resolve the untrust of the system?

# Digital Signing failed...

- original PKI shared liabilities in b2b context
- Internet & digital signing PKI dumped liabilities
  - CAs, certs & sigs hidden from users
  - result: untrusted
- limited success where mandated/promoted by govt.

# Who did users trust?

- Users trusted the browser
- or more accurately, the *supplier* of the browser...
- (might not be warranted ...)



# but, SSL...

- SSL worked because the software made users comply
  - businesses easy victims to compliance threat
- compliance based design no barrier to phishing
  - NB phishing is an identity verification failure
  - aka Man in the Middle.

**“Those who do not remember  
the past are condemned to  
repeat it.”**

*–George Santayana*

# So what?

- digital signing is history
- are we condemned to repeat it?

	DigSigs	Smart Contracts
impenetrable to consumers	✓	✓
strong economics of zero liability	✓	✓
financial upside to providers	✓	✓
no clear benefit to consumers	✓	?
user liability is unspecified, unlimited	✓	?
mumble something trust something	✓	✓
Belief, memes, crypto, this time it's different <b>TM</b>	✓	✓



# It's all about trust

- to go mainstream, need trust
  - of *individual* users
  - of *ALL* the users
- both failed with digital signing

# on Trust

- What is Trust?
- And where does it come from?

**“Alice trusts Bob”**

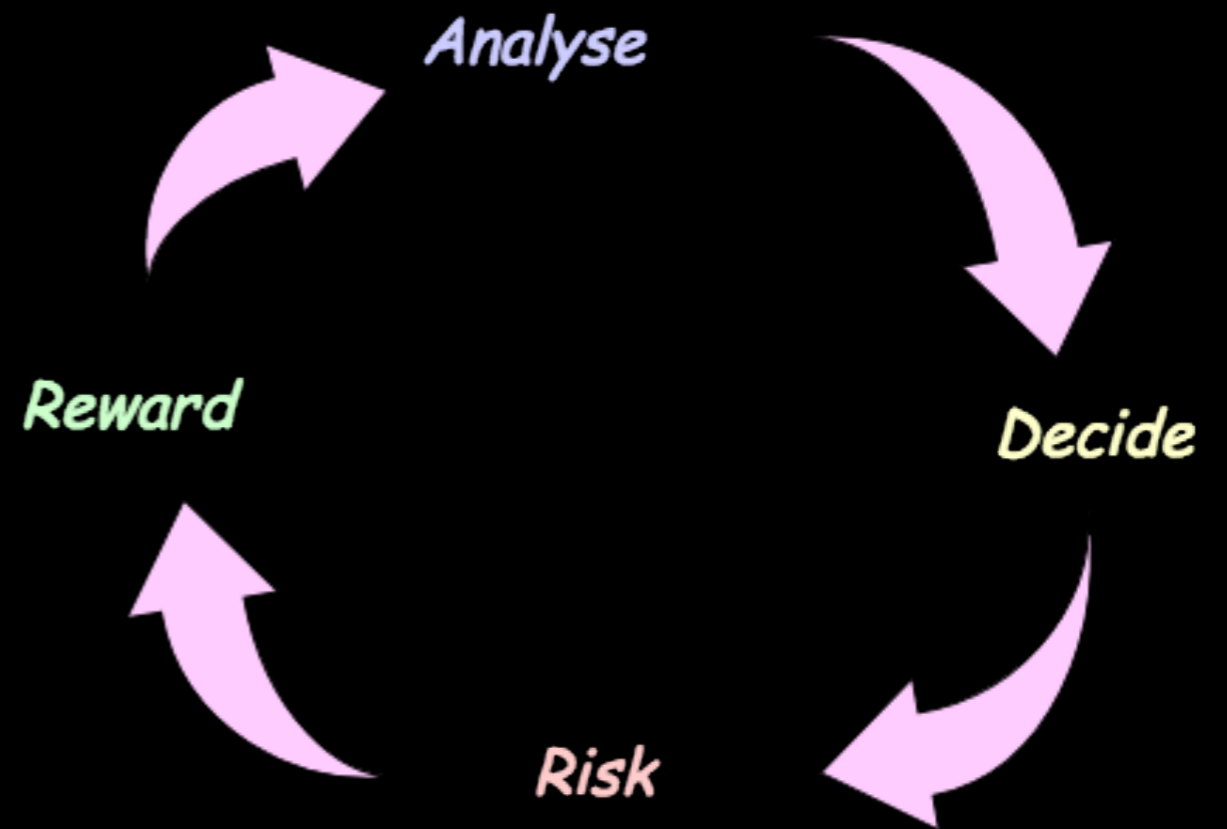
*a definition*

# no good...

- more complicated:
  - Skin in the game
  - Alice must make a decision
  - Within a context
  - From past information

**“When Alice trusts Bob,  
she chooses to take a risk  
on Bob’s actions  
in a limited context,  
based on her prior experiences,  
to gain some expected benefit”**

# getting better...



- Trust is expensive
  - every decision costs time & energy
- Trust is a repeating game
  - need to invest in risky rounds to gain future rewards



# Robots need not apply...

- Only people can trust
  - robots follow their programming
- and trust applies to people
  - people *RELY* on the machine
  - they *TRUST* the owner

# Voluntary

- Alice has to choose to make the decision
- Compliance is not trust
- Governments  $\leftrightarrow$  citizens?

# Breaking trust...

- If Bob breaks Alice's trust:
- Fight, Flee, or Follow
  - Fight: bury her trust model deeper
  - Flee: lose the deal
  - Follow: lose/merge her identity

# Heisenbergian

- If we know what Alice's trust model is, we 'own' her
- If she knows we know, she breaks her own model...
- and reforms it: deeper, harder, more guarded.
- *Trust is integral to Identity*

# Where did this come from?

- A baby is born...

“Humans first lived in small groups on the African savanna. An artifact of this life is the fact that most people can't have serious emotional relationships with more than about 12 people, depending on how you define serious. :-). Think of it as the carrying capacity of the human 'switch', and things get interesting. These small groups communicated geodesically. When you wanted to talk to someone, you went up and talked to them.”

*–Bob Hettinga, “A Geodesic Society?” 1998*



“Then we developed agriculture and its resulting food surpluses, people tended to congregate at the crossroads of trade routes, and that's where the first cities began. Civilization means, literally, 'life in cities', remember? Once we had large groups of people in a single place, we had lots of information to pass around, but we also had expensive humans 'switching' that information who were only able to trust about 12 people at any time. ....”

*–Bob Hettinga, “A Geodesic Society?” 1998*

# Trust & Relationships

- Trust evolved to manage relationships
- Relationships evolved to manage tasks & society
- this was a very expensive mechanism

# Dunbar's number

- Grooming relationships in primates
- brain size of primate
- Humans: around 150 relationships
- (which is a lot)

# getting harder...

- 150 \* Expensive == VERY expensive
- a new born baby has very large and very empty brain
- Psychology: about 16 years to fill out the identity
- Childhood: training for trust

# no light thing

- you can't turn it off
- you can't program it
- you can't feature request it
- you can't remove it, or add to it
  
- *And, you can't avoid it!*

# Trustlessness

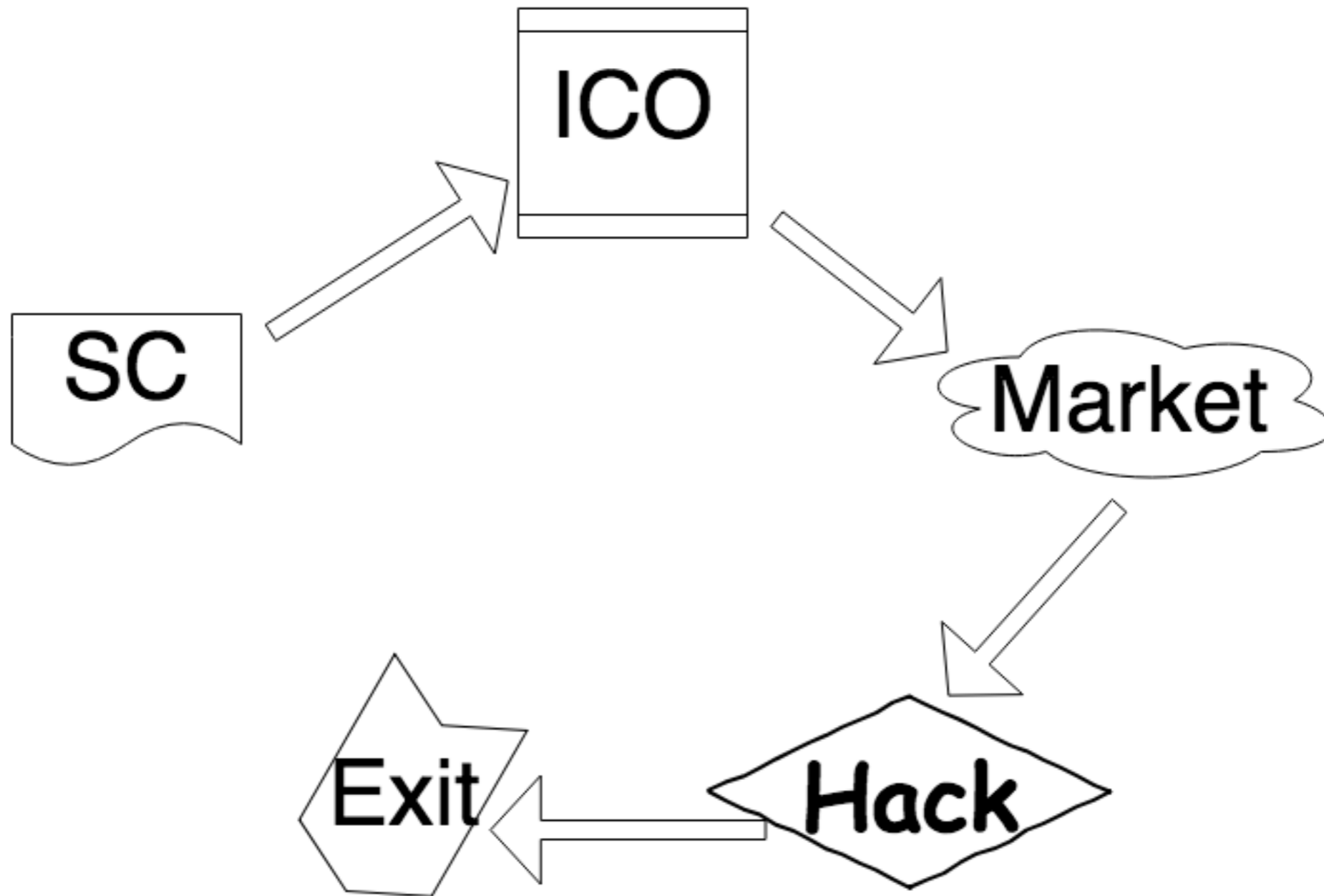
- at best, a myth
- at worst, bankruptcy in human thinking

# brains are wired

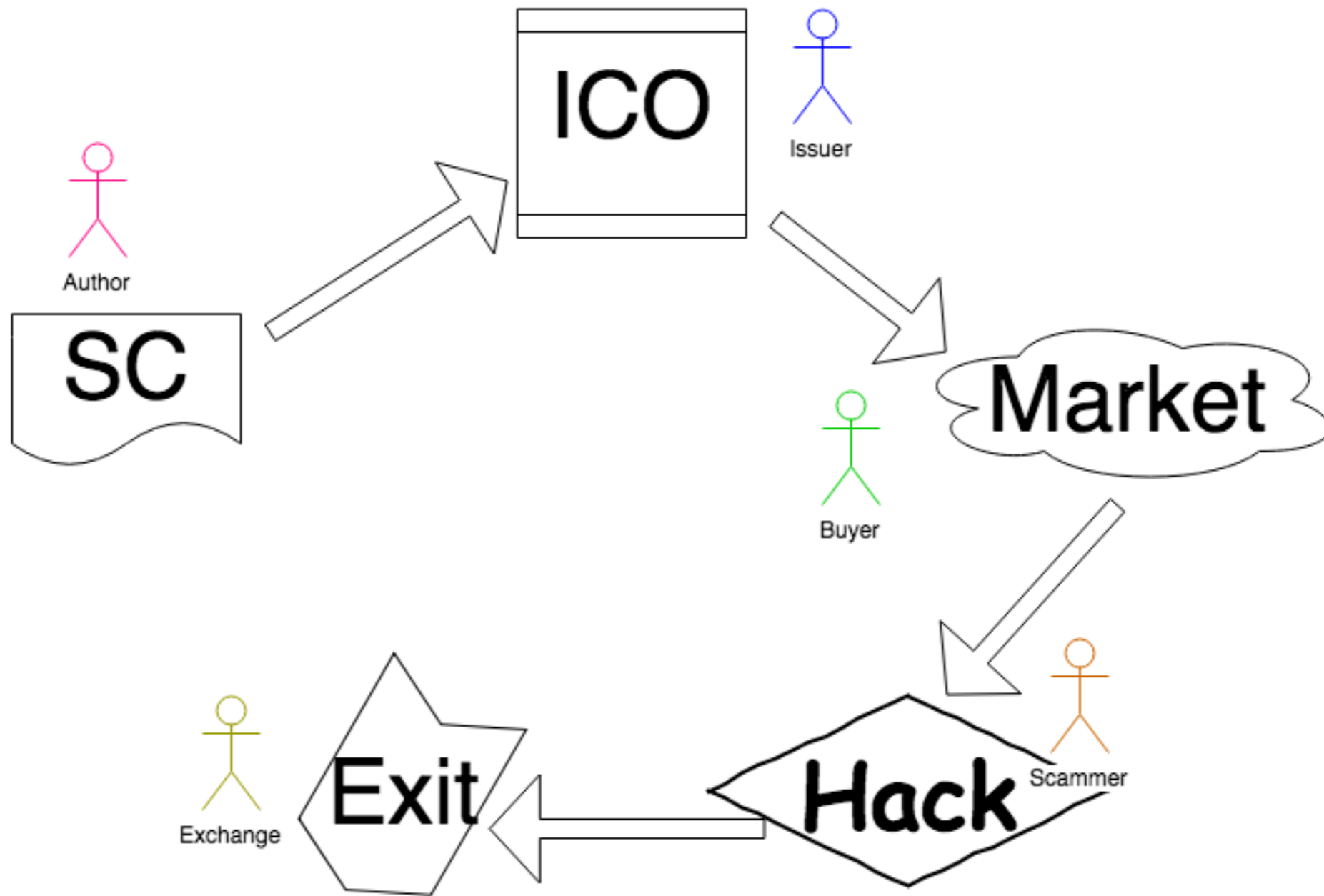
- For trust.
- Trust is more a constant than technology
- Improve the tech, move trust to a higher level
- you can no more remove trust than you can avoid the first 16 years of your life.



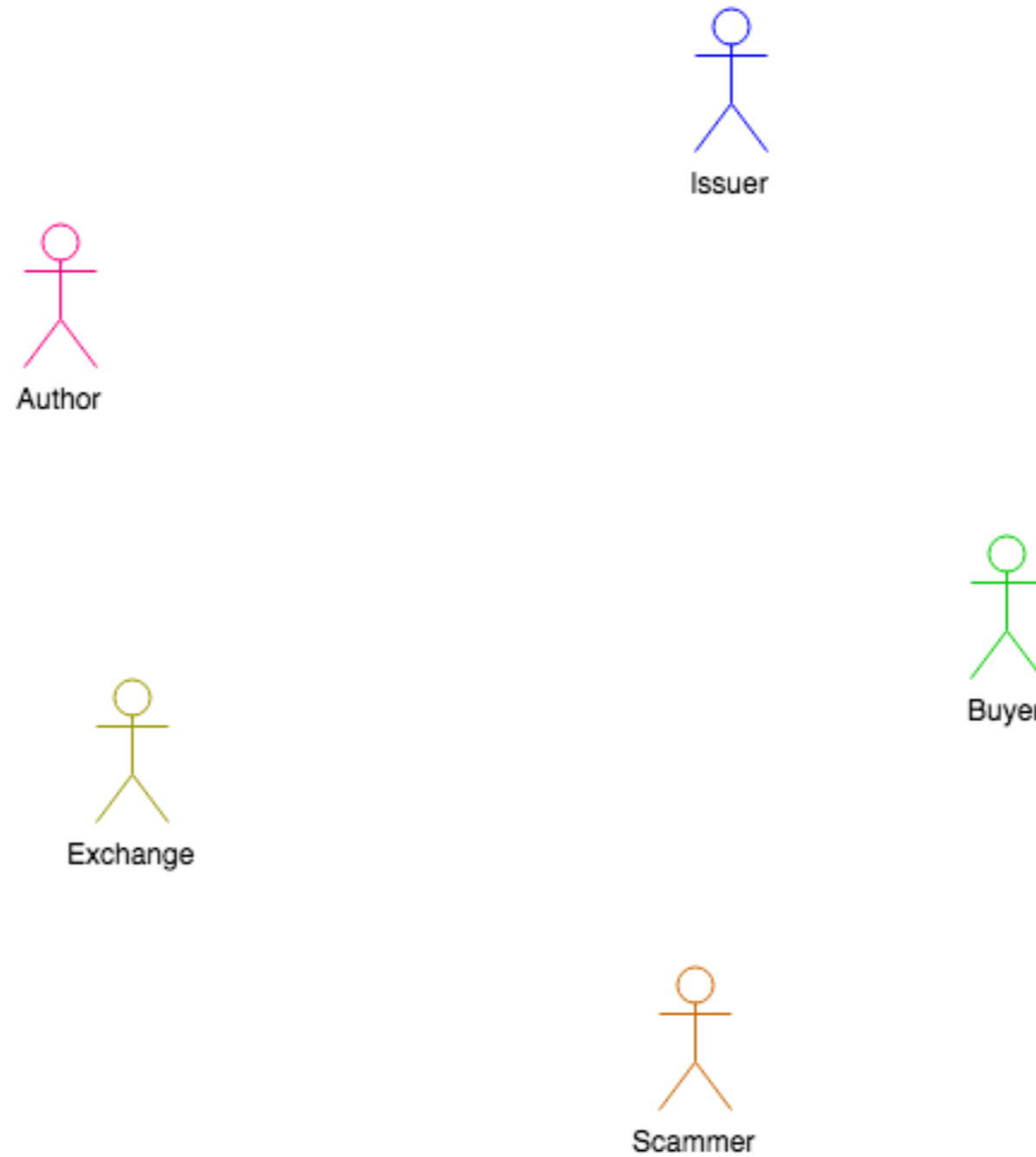
# Where did all the Trust go?



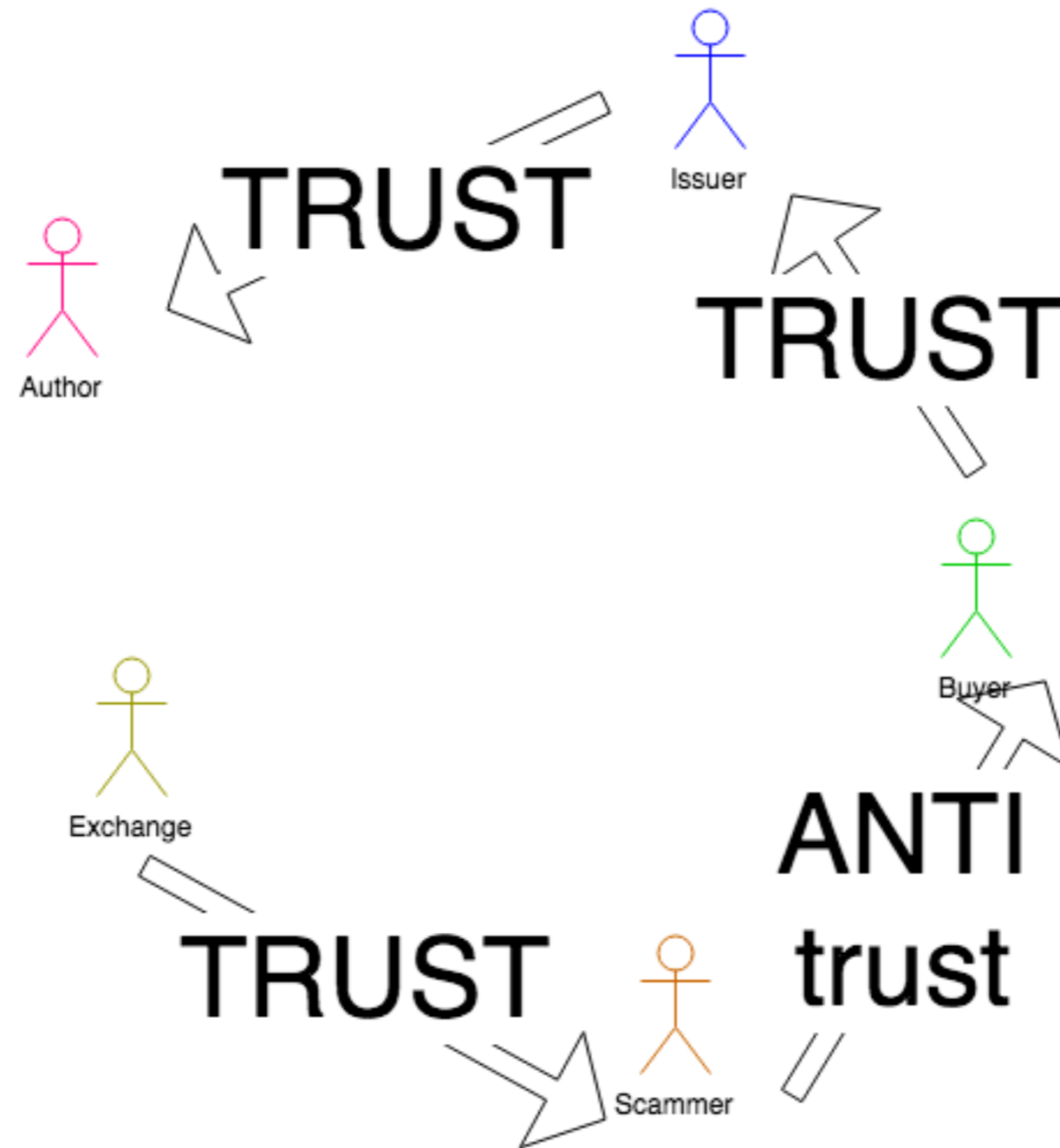
# add the people



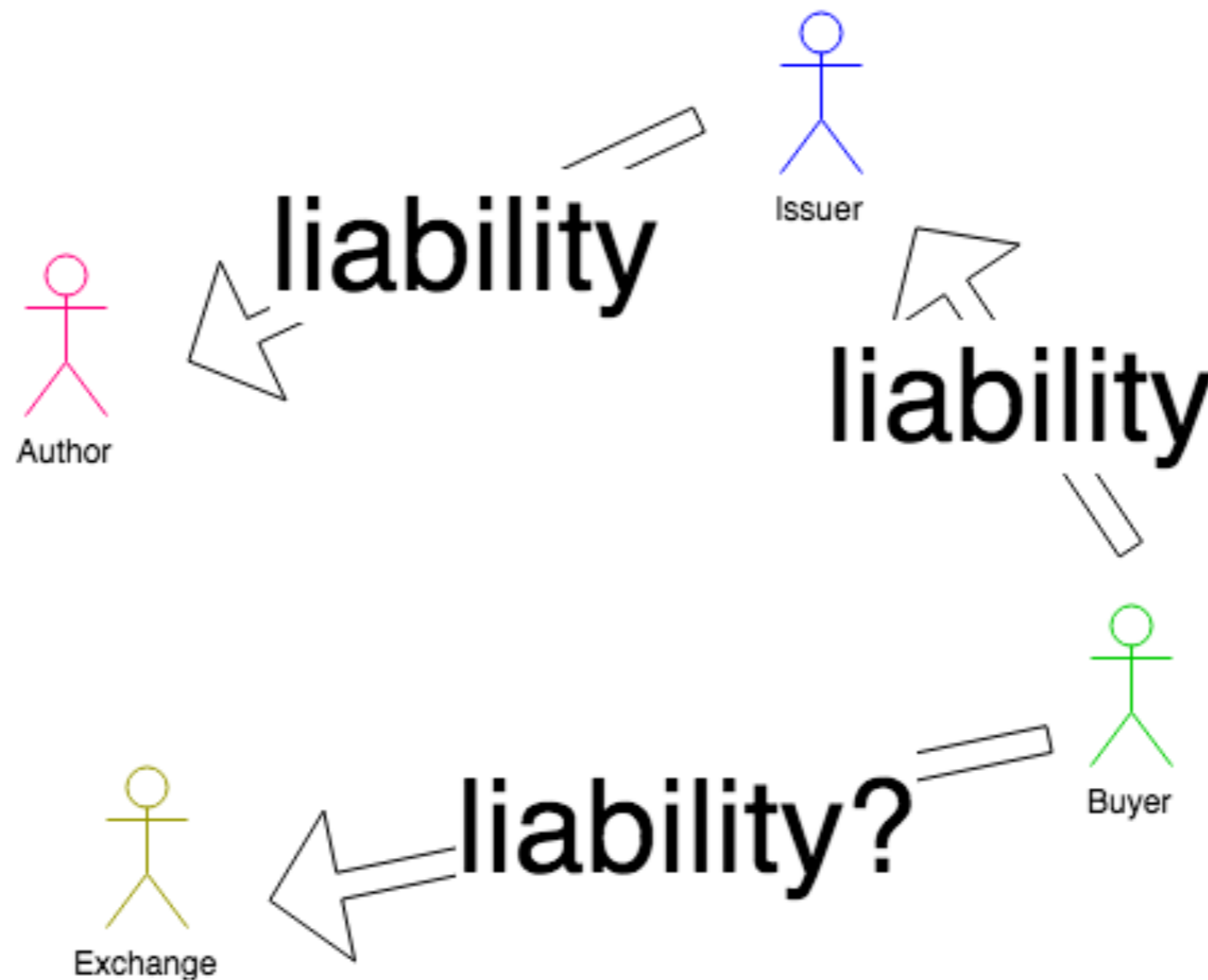
# take away the tech...



# Add the trust!



# turn Trust into Liability



# Choices in Liability

- choices
  1. zero liability
  2. some liability
  3. all the liability

# All

- \$10k per smart contract
- \$100m for a disaster
- “doesn’t scale” 😊



# Zero

- publish as open source
- issue under MIT style licence
- no benefit to author == gift not contract
- be anonymous (keynote by Neha Narula)

# Some liability

- contract for work
- Ricardian
- share the risk
- insurance
- standards
- independent verification

# Consequences of Trust

- Productive business & users need trust
- They can't turn it off
- No mainstream adoption until trusted
- Is the goal more trust or less trust?
- will be tested by regulators/courts/law

**“Trust me, I’m a financial cryptographer.”**

# Refs

- iang,
  - “An Open Audit of an Open CA,” 2008
  - “The Governed Blockchain,” 2018
  - “The Ricardian Contract,” 2004
  - “Identity Cycle,” parts 1, 2, 3, 2015-2018
- Bob Hettinga, “A Geodesic Society?” 1998
- Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008
- Nick Szabo, “The Idea of Smart Contracts,” 1997.