What is cryptoeconomics?

Vlad Zamfir

Well, what is economics?

Economics is the social science that studies economic activity to gain an understanding of the processes that govern the production, distribution and consumption of goods and services in an economy.

- Wikipedia

Cryptoeconomics might be..

A formal discipline that studies protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy.

Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols.

Economics: theory and practice

Classically, it is difficult to conduct economic experiments because people and institutions are necessarily involved. Partly because of these empirical limitations, and partly because theory is more tractable, economics is focused on various simple economic models.

Cryptoeconomic theory vs practice

In theory cryptoeconomic experiments are easier to conduct. In practice, today, the state and centralization of software development and deployment makes it difficult.

The relationship between theory and practice is different in cryptoeconomics than in classical economics.

Weirdness: human vs software

- Humans are weird because they are mammals with culture.
- homo sapien =/= homo economicus
- Software is weird because of defaults, bugs and the nature of development.
- But there's still hope for rational software.

Pseudonymous economics actors

- A cryptoeconomy is "flat", global and digital
- Low emphases on reputation, identity, and traditional trustworthiness of nodes
- There are low barriers to entry

"coercion free"...

It's impossible to impose a cost on a node without having them first "voluntarily" expose themselves to the risk by:

- Buying a digital asset
- Placing a security deposit
- Earning a reputation

Cryptoeconomic mechanisms

- "Self-enforcing" mechanisms
- Low cost of mechanism creation
- Software quantifiable and verifiable assurances of market features

Cryptoeconomic security

- How difficult is it to change the Nash equilibrium of a system?
- Measure difficulty in dollars that must be budgeted and spent
- Collusion difficulty
- Or in trust

Consensus mechanisms

- A cryptoeconomic mechanism with distributed consensus as a Nash equilibrium
- The mechanism earns transaction fees
- Lets a number of participants agree on a sequence of transactions
- Lets us quantify the security of the consensus

Cryptoeconomic security as information security

- Mechanisms are really programs.
- They can distribute payoffs
- The programs have a certain behaviour in the Nash equilibrium case
- The NE has a cryptoeconomic security
- We can be assured that a program will run a particular way

Economics for cryptography

- Economic mechanisms can give guarantees that a program will run in a particular way that cryptography alone can't provide.
- Incentives are forward facing, cryptography is a function of already-existing information
- How do we provide custom cryptoeconomic guarantees?

Information security

- Availability
- Authenticity
- Confidentiality

But now we can be assured that programs run in a particular way into the future!

Information security

- We can guarantee the availability and authenticity of information into the future
- As long as we specify the program that processes the (yet unknown) future inputs
- Confidentiality is hard, and it is unclear if there are efficient general purpose cryptoeconomic mechanisms for privacy

So why is cryptoeconomics special?

- The digital, programmable nature of the economy and the participants
- The close relationship with cryptography and information security.
- Economics for cryptographers or cryptography for economists?