The Project of Cryptoanarchy

By J. "smuggler" Logan

About myself

- "Cryptoanarchist" for decades
- Operator of darknet communities, anonymous communication systems, developer of anonymous communication- & digital cash systems….
- Etc.

Cryptoanarchy

Label? Brand? Sociopolitical idea?
Today: Degraded to label – no content.
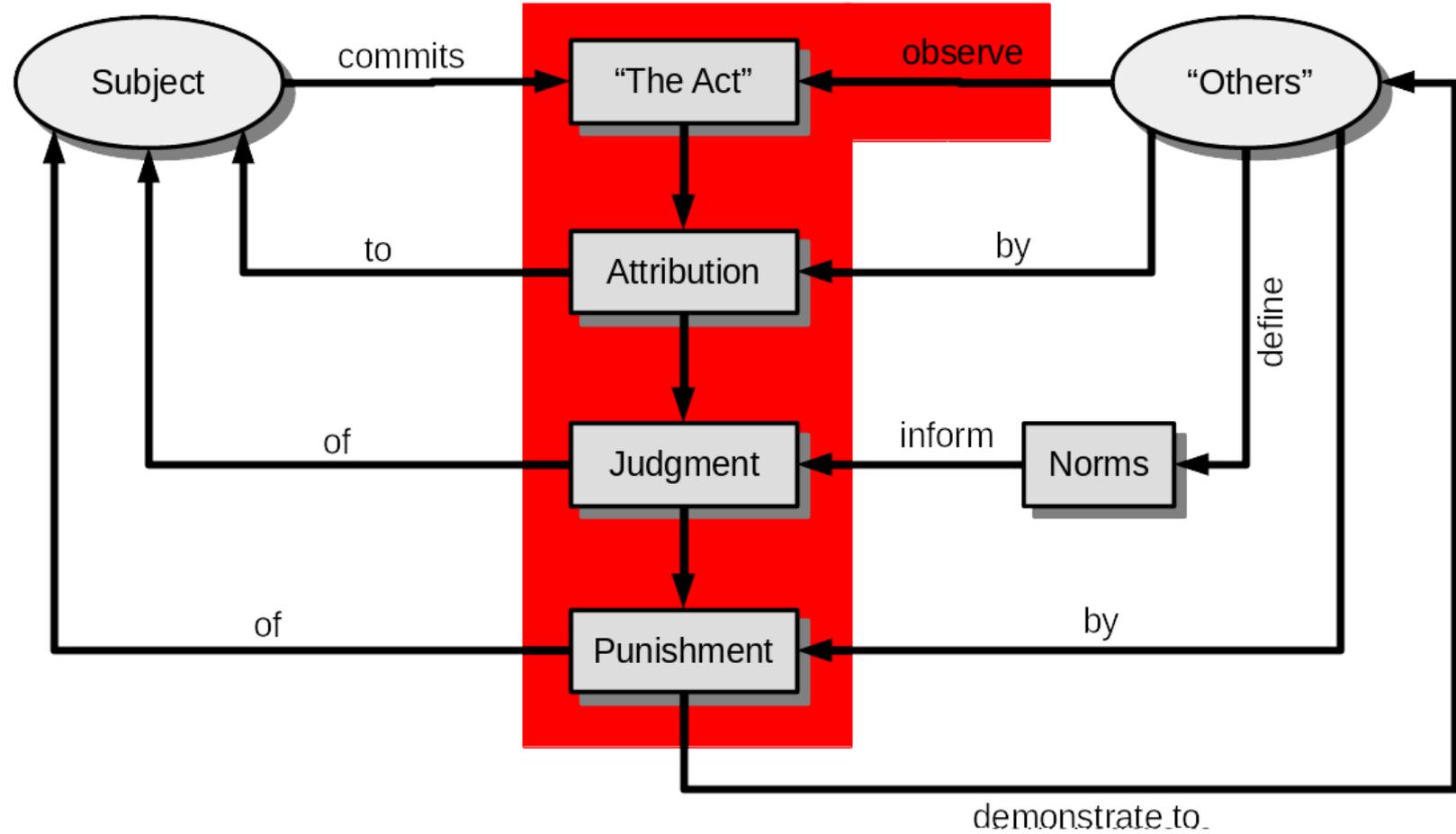But do we understand what it means?

What is Cryptoanarchy?
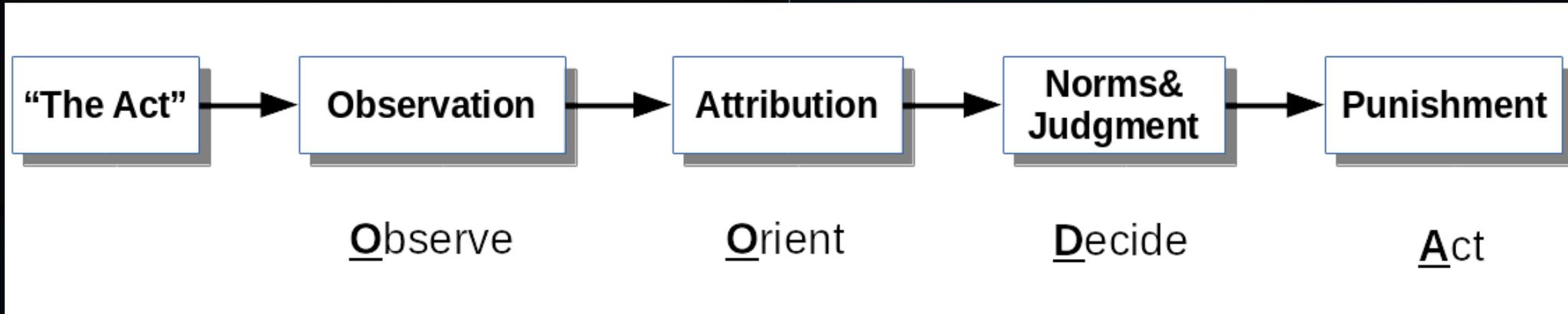
The realization of anarchy by means of **cryptography**

Anarchy???

<u>NOT</u> "archy"
Archy: Rulership, dominion, "coercion"

Understanding Rulership (101)

The OODA Loop of Rulership

Who are the others?

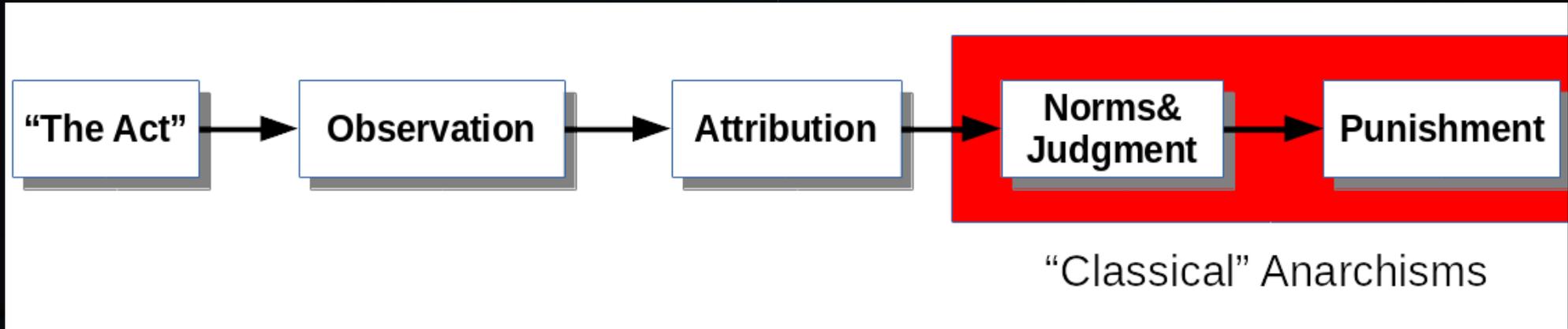|	Violent	Hierarchical	Total	Consentaneous	Voluntary	Archy?
Government	X	X	X			Yes
Organizations		X			X	
Platforms*		X	X	X		Yes
Society			X			(yes)
Contract				X	X	
Self			X			(yes)

Hierarchy: Dominance Hierarchies only

- Unequal opportunity to participate in the definition and enforcement of norms.

- Definition (normative) & Enforcement (factual) power.

Anarchy: **NOT** Archy - Classical

- No Norms: "Bomb throwing anarchist" => Anomie, not anarchism.

- No Punishment: (Diplomatic) immunity, hegemonic states, recreational nuclear weapons, Christian Anarchism

- Voluntary & non-total norms: Mutualism, Anarcho-Capitalism, Anarcho-Syndicalists

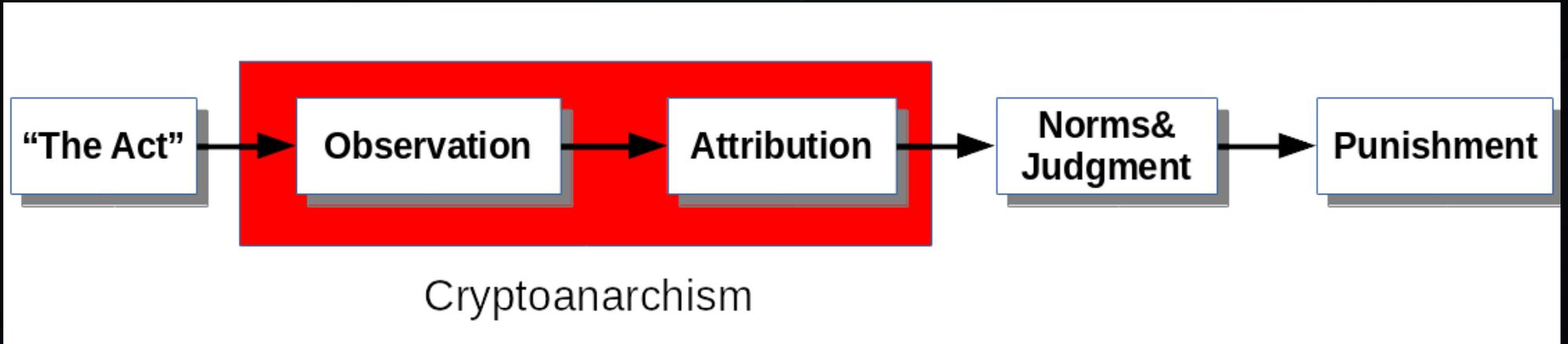Black Block "anarchism": Not anarchy but total norms, reverse hierarchy

Anarchism's attack on the Rulership OODA Loop

"The Act" → Observation → Attribution → Norms& Judgment → Punishment

"Classical" Anarchisms

Reform of norm definition and punishment. "Revolutionary"

Cryptoanarchy is **very different**

Cryptoanarchism

Cryptoanarchism undermines <u>observation and attribution</u>, and is ultimately subversive

Attack on Observation

- Opaque "Walled Gardens": Walls of Cryptography

- Access Control

- Internal "jurisdiction"

Attack on Attribution

- Untraceable & anonymous communication, ...

- ..., payments

- ..., activities

DISCONNECT THE PHYSICAL BODY FROM THE ACT

...by means of cryptography

- Encryption for confidentiality, "Masks"
- Mixes & Relays
- Blind signatures
- Zero Knowledge Proofs

Math of hiding, concealing, covering up

"Cryptography rearranges power.
This makes it an inherently political tool."
                                        - P. Rogaway

Technologies of non-attribution, untraceability, opaqueness and confidentiality are the **political** tools of Cryptoanarchy.

                                        All else is neutral or worse….

<u>NOT</u> Cryptoanarchy

<u>No cryptography of confidentiality ==> Not Cryptoanarchy</u>

- Techno-libertarianism/Techno-anarchy

- 3D Printed Guns (Techno-anarchy)

- Decentralization is no defining attribute (but technically useful)

- Bitcoin is about as cryptoanarchist as a car ("Crypto-minarchists" :))

Zcash, Monero ==> Cryptoanarchist !!!

Cryptoanarchy poses difficult questions

- Non-Attribution breaks all previous concepts of justice and punishment.

- Punishment can only apply to <u>previously</u> transferred collateral/security.

- Punishment cannot reach into the future!

==> Cryptoanarchism is **<u>NOT</u>** anarcho-capitalism.

Cryptoanarchy in Practice

- Cryptohippie AnonAuth

- Privacy VPN: No attribution!!!

- How to punish abuse???

- Untraceable blind tokens for authentication:
  - Hold, and invalidate on abuse.

- User running out of tokens loses service.

Cryptoanarchist World

- Digital Darknet

- Untraceable digital cash

- Physical Darknet: Dead Drops and Drone networks

- "Black Box" Places: TAZs, masks

- Opaque Transport: Autonomous cars, "diplomatic pouches"

- Embedded into tolerant political "host" systems

Cryptoanarchists use 'nyms, or nothing :)

Get involved!

- Cryptocurrency OTC

- All or Nothing Escrows

- Social protocols with direct apprehension or collateral/security

- Anonymous sharing economy

- Privacy Enhancing Clothing

Thank you!

- Credits: Tatjana Adamov, Frank Braun, Paul Rosenberg.

- Contact: smuggler@staff.anarplex.net

- Twitshit/mobmedia: @TheRealSmuggler

- OpenPGP FP: 0x4B975D1702FF8A29DABD40B13E11D4CBB7A7ACF8