Democracy .Earth

A 501 (c) 3 non-profit founded in 2015 building open source censorship resistant digital democracy.

Y Combinator

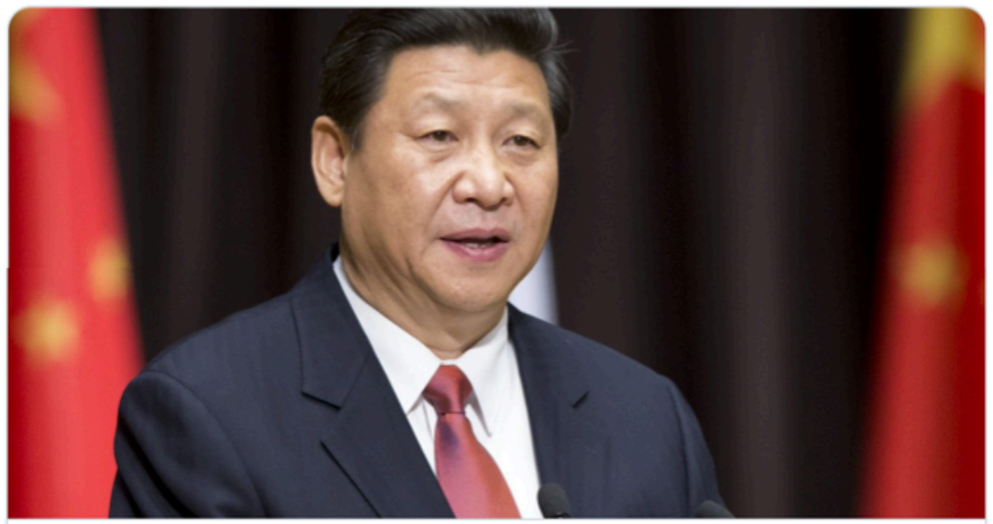
TEMPLETON WORLD
CHARITY FOUNDATION

Donald J. Trump
@realDonaldTrump

I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air. Unregulated Crypto Assets can facilitate unlawful behavior, including drug trade and other illegal activity....

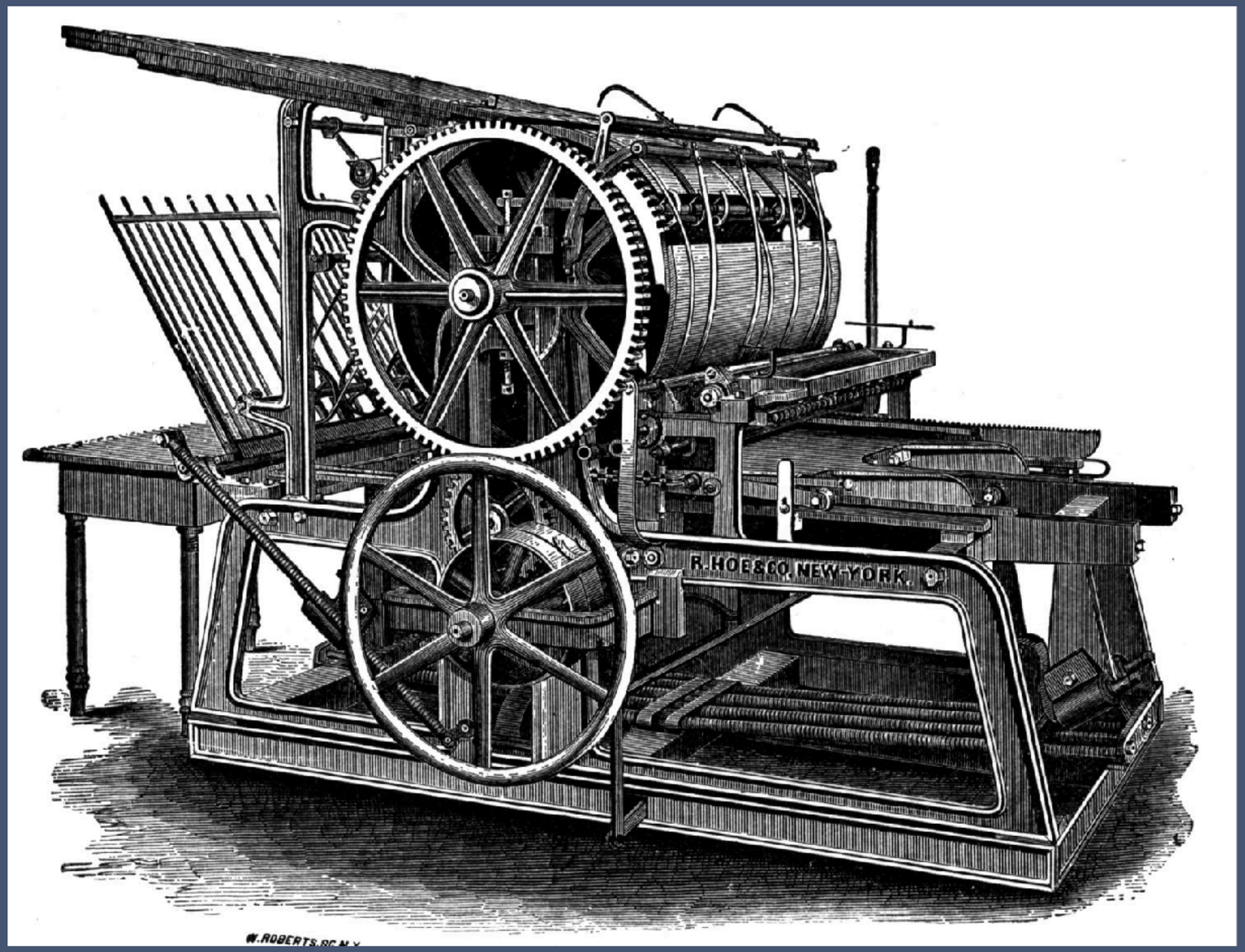
CoinDesk
@coindesk

BREAKING: In his first major comments on blockchain, Chinese President Xi Jinping said the country should implement the technology across the economy, reports @wsfoxley.

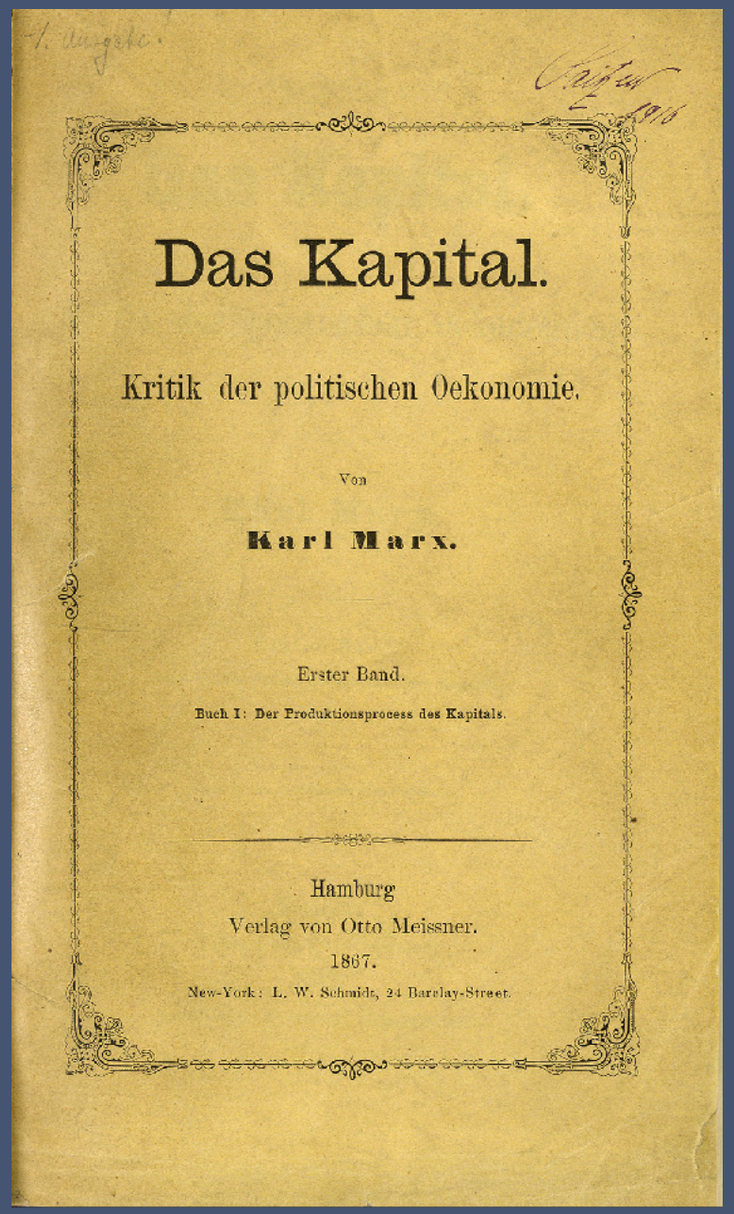


President Xi Says China Should 'Seize Opportunity' to Adopt Blockchain - Coi...
In his first major comments on blockchain, Chinese President Xi Jinping said the country should implement the technology across the economy.
coindesk.com

Censorship resistance does not necessarily translate into utopia.



Technology development always led to the emergence of new political orders.



Das Kapital.

Kritik der politischen Oekonomie.

Von

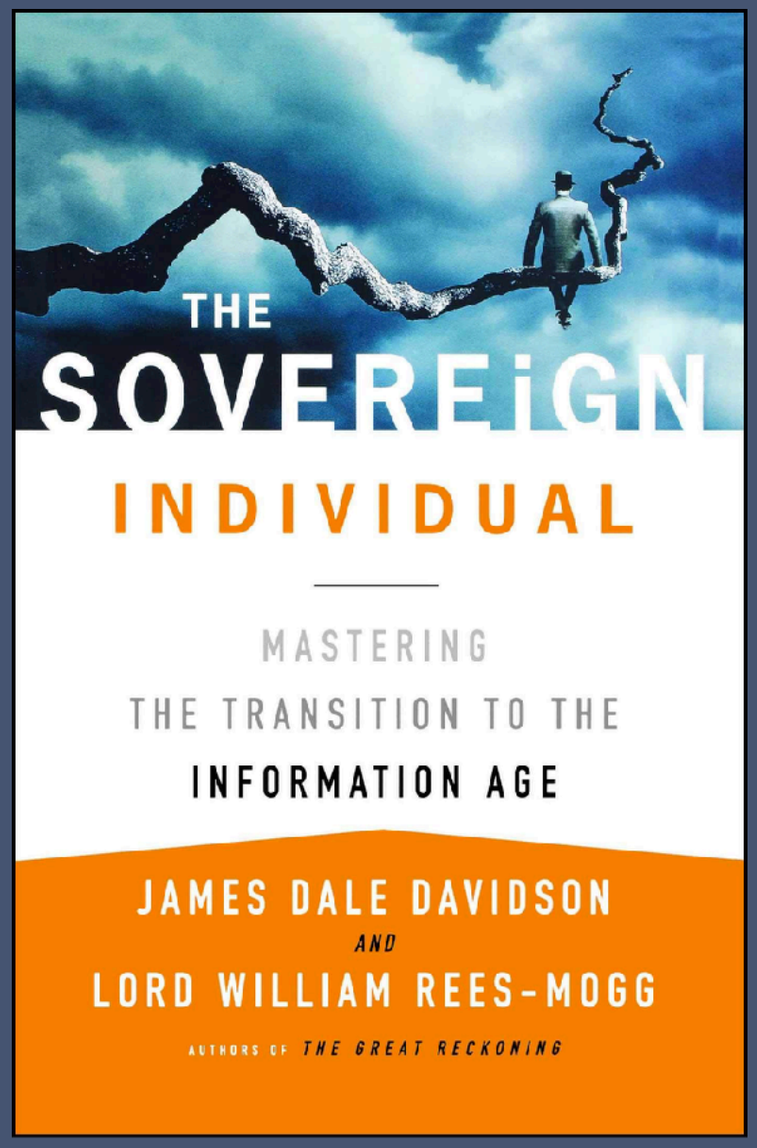
Karl Marx.

Erster Band.

Buch I: Der Produktionsprocess des Kapitals.

Hamburg
Verlag von Otto Meissner.
1867.

New-York: L. W. Schmidt, 24 Barclay-Street.



"When technology is mobile, and transactions occur in cyberspace (...) governments will no longer be able to charge more for their services"

Category XIII— Materials and Miscellaneous Articles

(a) [Reserved]

(b) Information security or information assurance systems and equipment, cryptographic devices, software, and components, as follows:

(1) Military or intelligence cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components, and software (including their cryptographic interfaces) capable of maintaining secrecy or confidentiality of information or information systems, including equipment or software for tracking, telemetry, and control (TT&C) encryption and decryption;

(2) Military or intelligence cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components, and software (including their cryptographic interfaces) capable of generating spreading or hopping codes for spread spectrum systems or equipment;

(3) Military or intelligence cryptanalytic systems, equipment, assemblies, modules, integrated circuits, components and software;

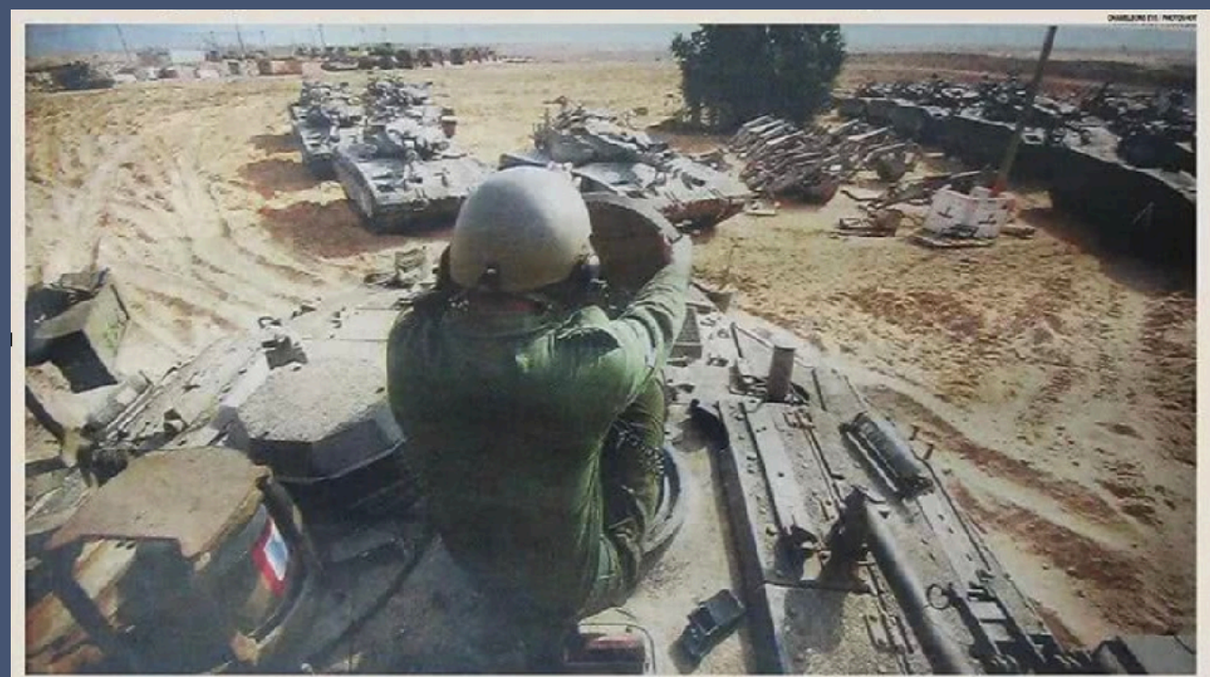
(4) Military or intelligence systems, equipment, assemblies, modules, integrated circuits, components, or software (including all previous or derived versions) authorized to control access to or transfer data between different security domains as listed on the Unified Cross Domain Management Office (UCDMO) Control List (UCL); or

(5) Ancillary equipment specially designed for the articles in paragraphs (b)(1)-(b)(4) of this category.

(c) [Reserved]

Cryptographic technology is legally considered a weapon in the United States.

WHO WATCHES THE WATCHMEN?



Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

Bitcoin is a political act.

Proof of Work (PoW) ignores society.

Nakamoto governance is centered around machines, not people.

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

Biticoin's white paper paragraph on governance (2008). Guaranteeing a right to privacy bent early blockchain design toward anonymity. While that approach helps fight financial corruption, political manipulation still exploits the internet in ways that can also be fought back with decentralized computation.

"The one vulnerability being exploited across all systems is Identity”

Edward Snowden — Web3 2019 (Berlin)

Humans on the Blockchain.

Is Proof of Human (PoH) possible?

If a PoH protocol existed, then the **social blockchain** would emerge.

Political initiatives that require Proof of Human.

Dapps pending to be built:

- *Democracy*
- *Universal Basic Income*
- *Portable Credit*
- *Alternatives to KYC*
- *Fair Airdrops*

Anything facing society, not capital.

Constraints: AI & Sybils.

Avoid recreating either Facebook or the Chinese Communist Party.

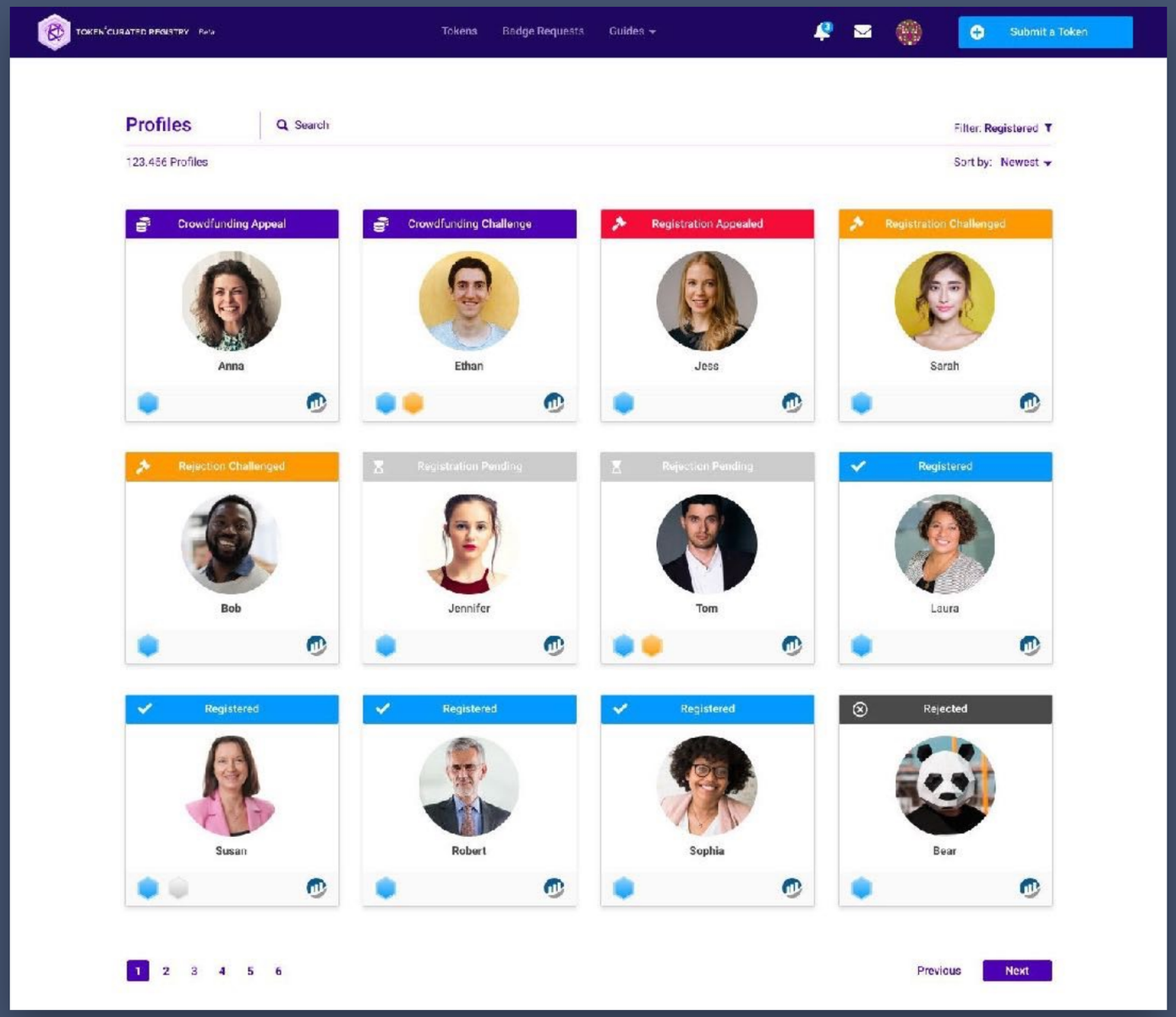
Name Spaces — The risks of a One Dimensional Identity

Human identities narrowed down to a one dimensional identifier (eg. usernames, domains, addresses) that are kept on an immutable ledger can be a recipe for disaster in the wrong hands (eg. Totalitarian governments).

Proof of Human Prototypes.

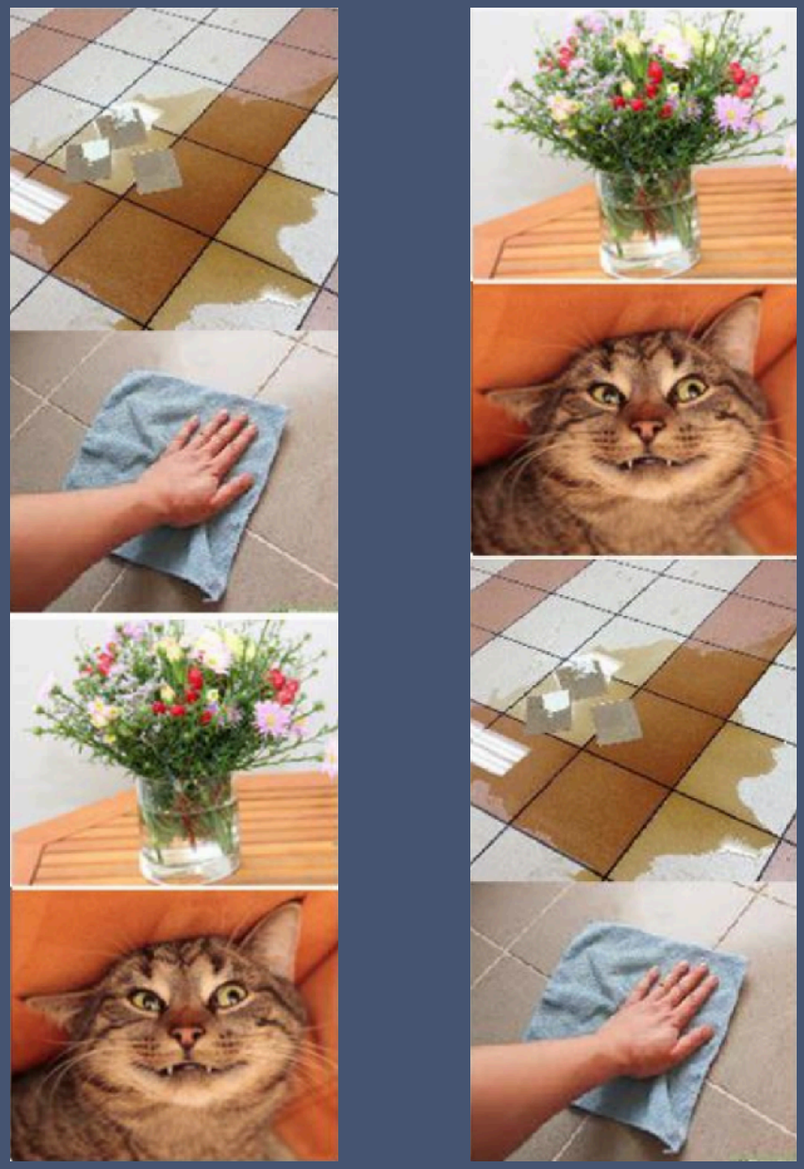
Ongoing experiments aiming to verify human participants.

Kleros — Web of Trust TCR with Video Proofs.



Use a Kleros TCR that randomly elects jurors that verify video of candidate IDs.

Idena Network — Synchronous Turing Tests.



Idena implements a synchronous event held over the entire network where participants are required to solve Turing tests that are hard for Machine Learning systems to solve.

This provides a proof of personhood assuming the tests cannot be captured by existing AI.

Which one of the two strips is the right one?

Idena Network — Synchronous Turing Tests.

Machine Learning resistant games:

Belonging to the class of AI-hard problems.

Not based on pattern recognition (and hence exploitable by neural networks) but able to interpret information using common sense reasoning or reading the *unsaid* between the lines.

Created by Humans.

Must not be created algorithmically in order to escape being a pattern recognition task, very much in reverse to how Google creates captchas.

Unpredictable and an infinity of possible captchas.

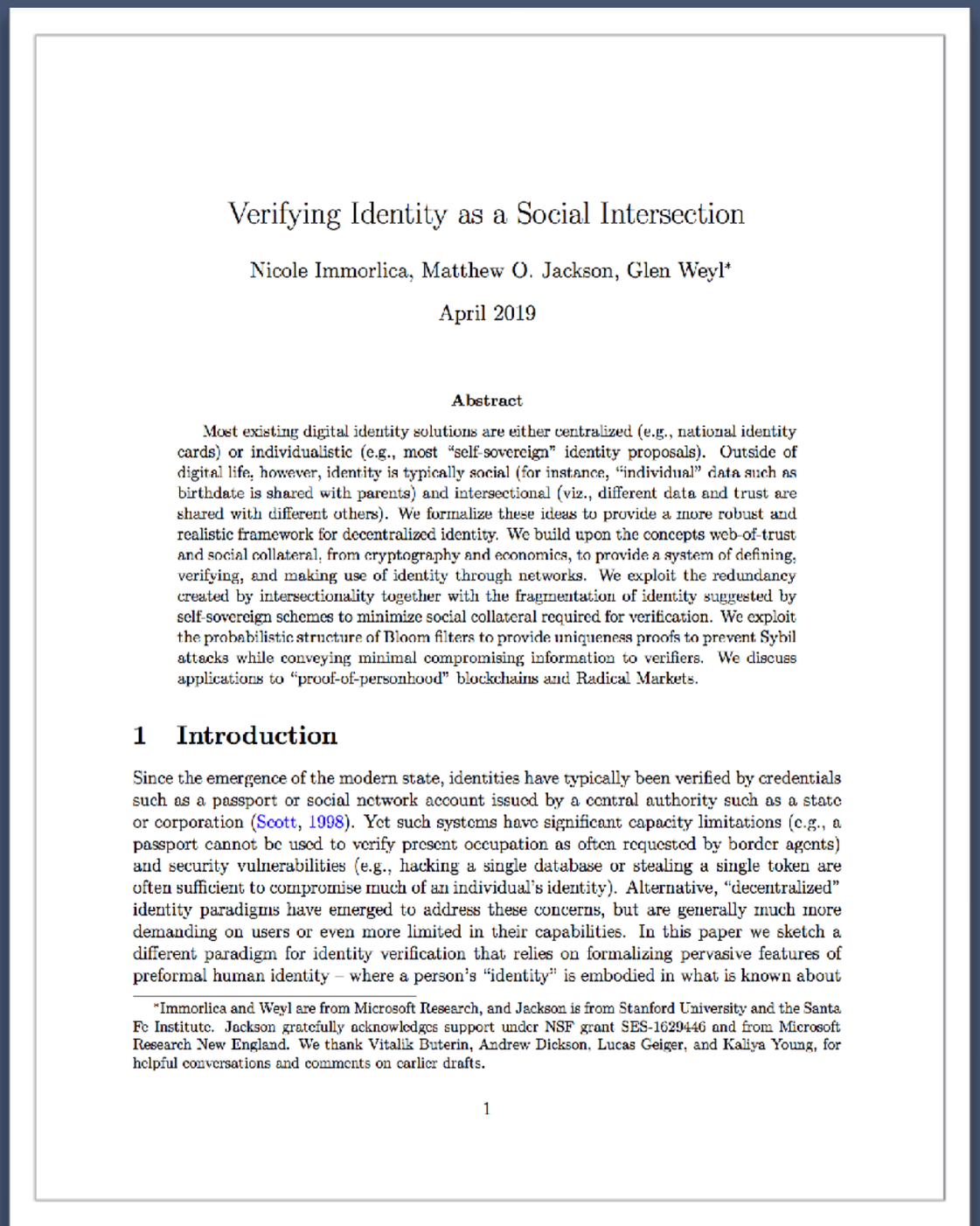
The range of possible tasks should not be limited (similarly as in the tasks of understanding the meaning of a text, where there can be an infinite range of texts and meanings).

No major systemic vulnerabilities.

We don't mean the vulnerability of one single captcha, but a systemic vulnerability, which allows the algorithmic solving of hundreds of thousands of captchas with high probability, above 80 percent.

Which one of the two strips is the right one?

Intersectional Identity — Be Your Social Graph



Verifying Identity as a Social Intersection

Nicole Immorlica, Matthew O. Jackson, Glen Weyl*

April 2019

Abstract

Most existing digital identity solutions are either centralized (e.g., national identity cards) or individualistic (e.g., most "self-sovereign" identity proposals). Outside of digital life, however, identity is typically social (for instance, "individual" data such as birthdate is shared with parents) and intersectional (viz., different data and trust are shared with different others). We formalize these ideas to provide a more robust and realistic framework for decentralized identity. We build upon the concepts web-of-trust and social collateral, from cryptography and economics, to provide a system of defining, verifying, and making use of identity through networks. We exploit the redundancy created by intersectionality together with the fragmentation of identity suggested by self-sovereign schemes to minimize social collateral required for verification. We exploit the probabilistic structure of Bloom filters to provide uniqueness proofs to prevent Sybil attacks while conveying minimal compromising information to verifiers. We discuss applications to "proof-of-personhood" blockchains and Radical Markets.

1 Introduction

Since the emergence of the modern state, identities have typically been verified by credentials such as a passport or social network account issued by a central authority such as a state or corporation (Scott, 1998). Yet such systems have significant capacity limitations (e.g., a passport cannot be used to verify present occupation as often requested by border agents) and security vulnerabilities (e.g., hacking a single database or stealing a single token are often sufficient to compromise much of an individual's identity). Alternative, "decentralized" identity paradigms have emerged to address these concerns, but are generally much more demanding on users or even more limited in their capabilities. In this paper we sketch a different paradigm for identity verification that relies on formalizing pervasive features of preformal human identity – where a person's "identity" is embodied in what is known about

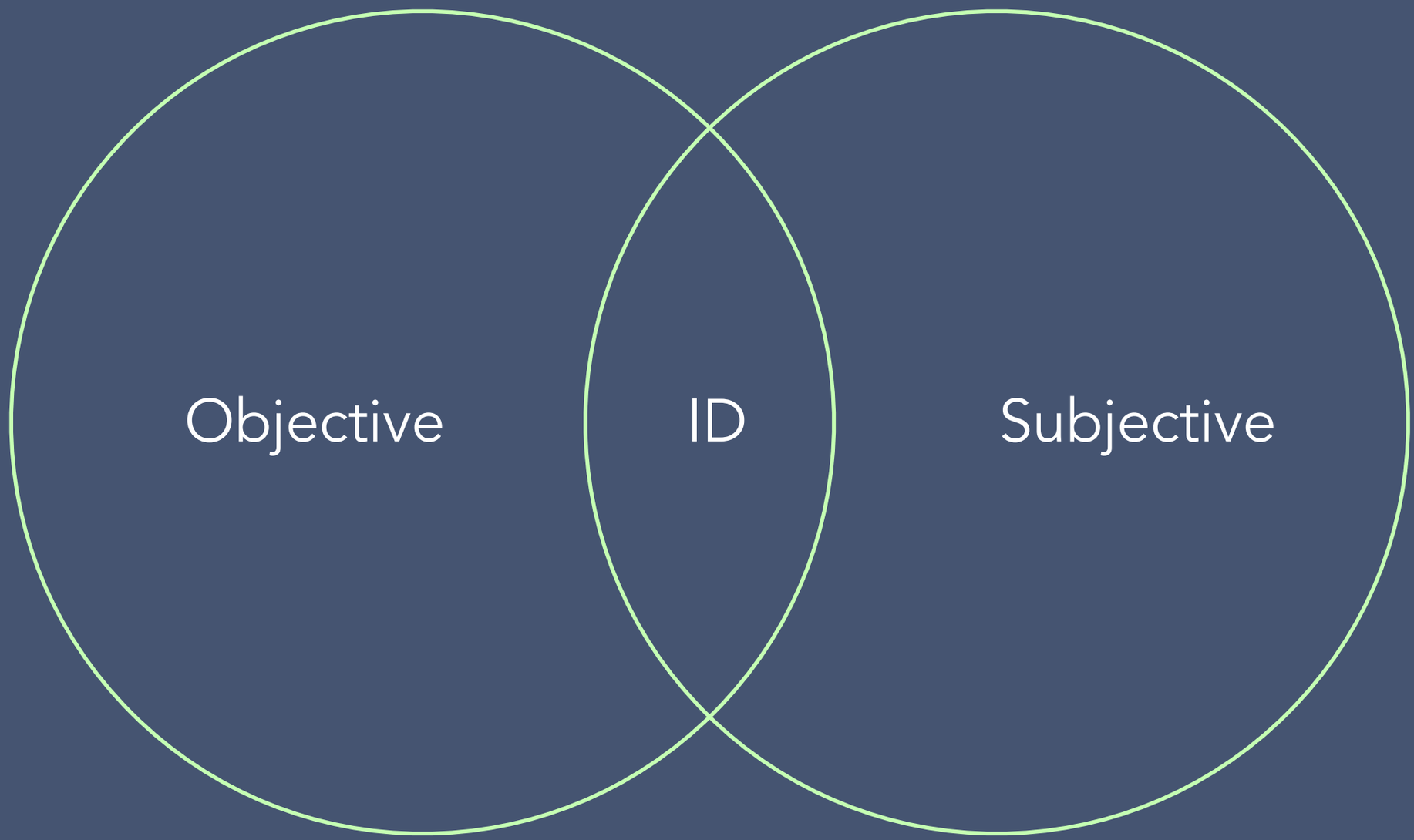
*Immorlica and Weyl are from Microsoft Research, and Jackson is from Stanford University and the Santa Fe Institute. Jackson gratefully acknowledges support under NSF grant SES-1629446 and from Microsoft Research New England. We thank Vitalik Buterin, Andrew Dickson, Lucas Geiger, and Kaliya Young, for helpful conversations and comments on earlier drafts.

The features of the pre-formal identity —intersections of social groups— are stored, in the normal course of human lives, in minds and other emergent personal records. This paper proposes a way of formalizing social intersections in order to verify identities.

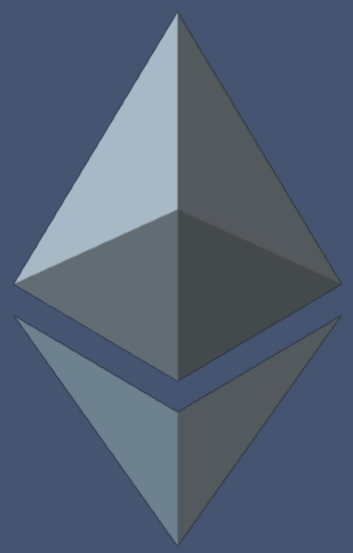
Probabilistic Identity.

Humanity as a spectrum and not a discrete value.

Why Identity is Hard.



A HumanRights( ) Algorithm.

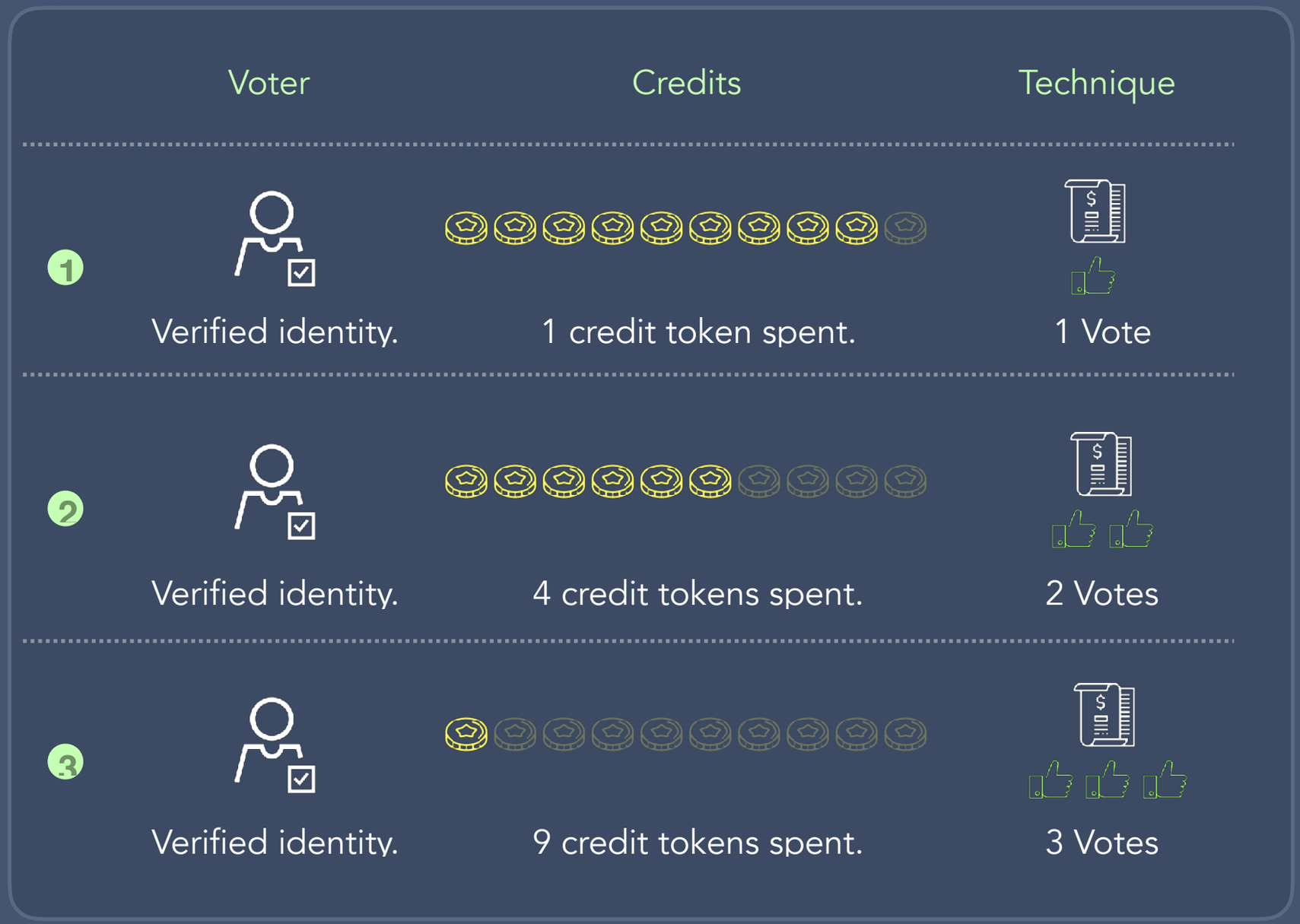


Any given
Ethereum Address

92.4% Human

A Score ranging from -100 to 100 that determines the probability of that address being a Unique Human by looking at its on-chain activity and certificates.

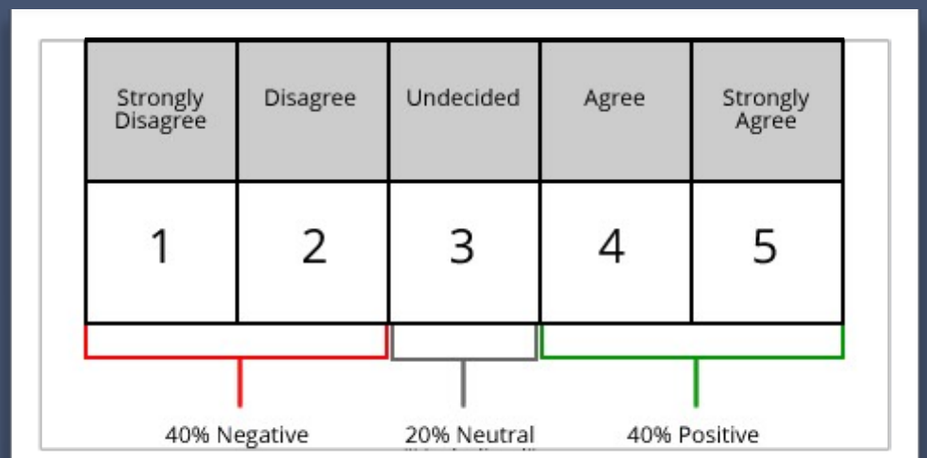
An ID scoring mechanism needs **legitimacy**.



Quadratic Voting (QV) can effectively rank a long tail of preferences.

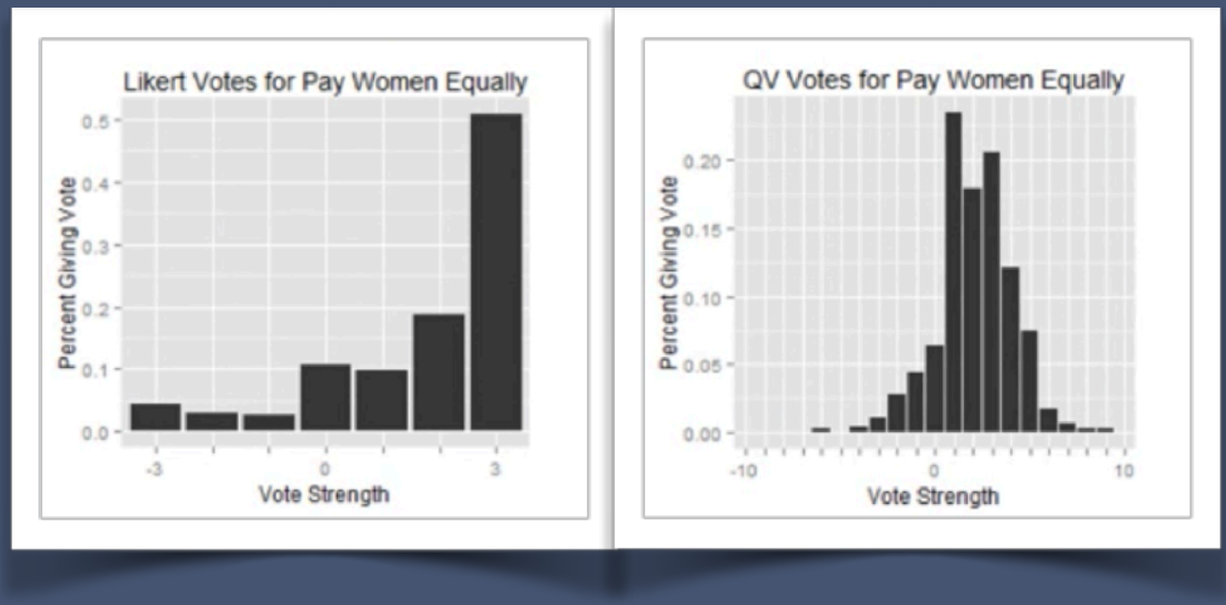
Quadratic Voting generates organic data.

Comparing votes with Likert-Scale ballots not only reduced polarization but also led to a more organic distribution of preferences.



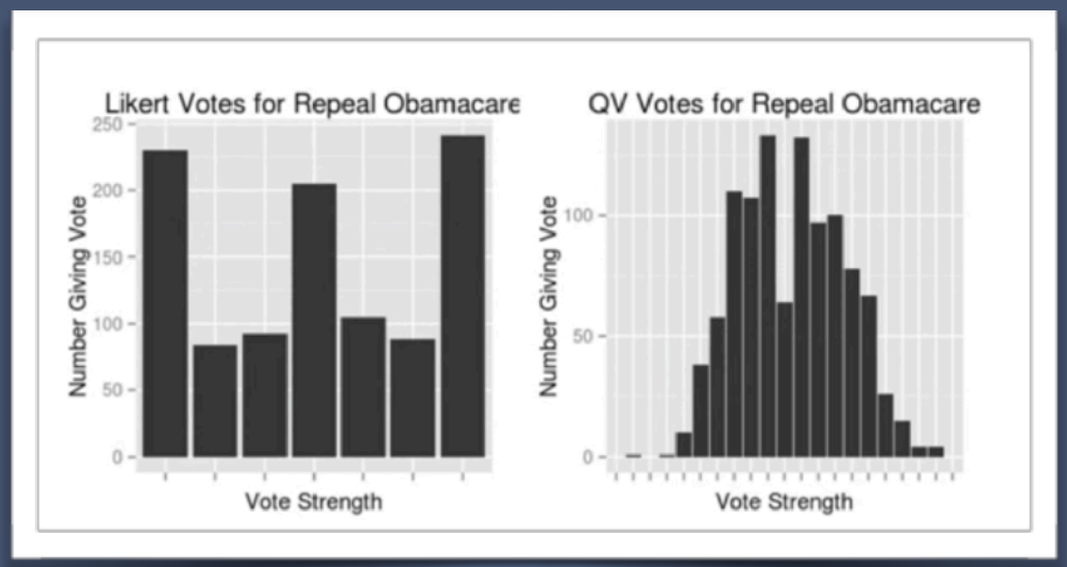
Without QV

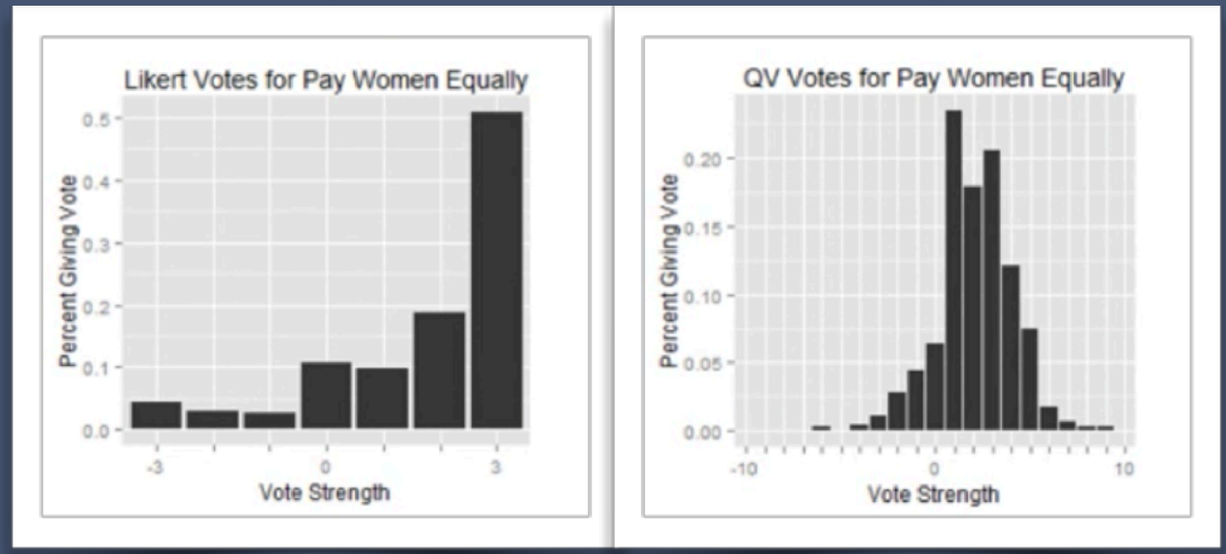
With QV



Without QV

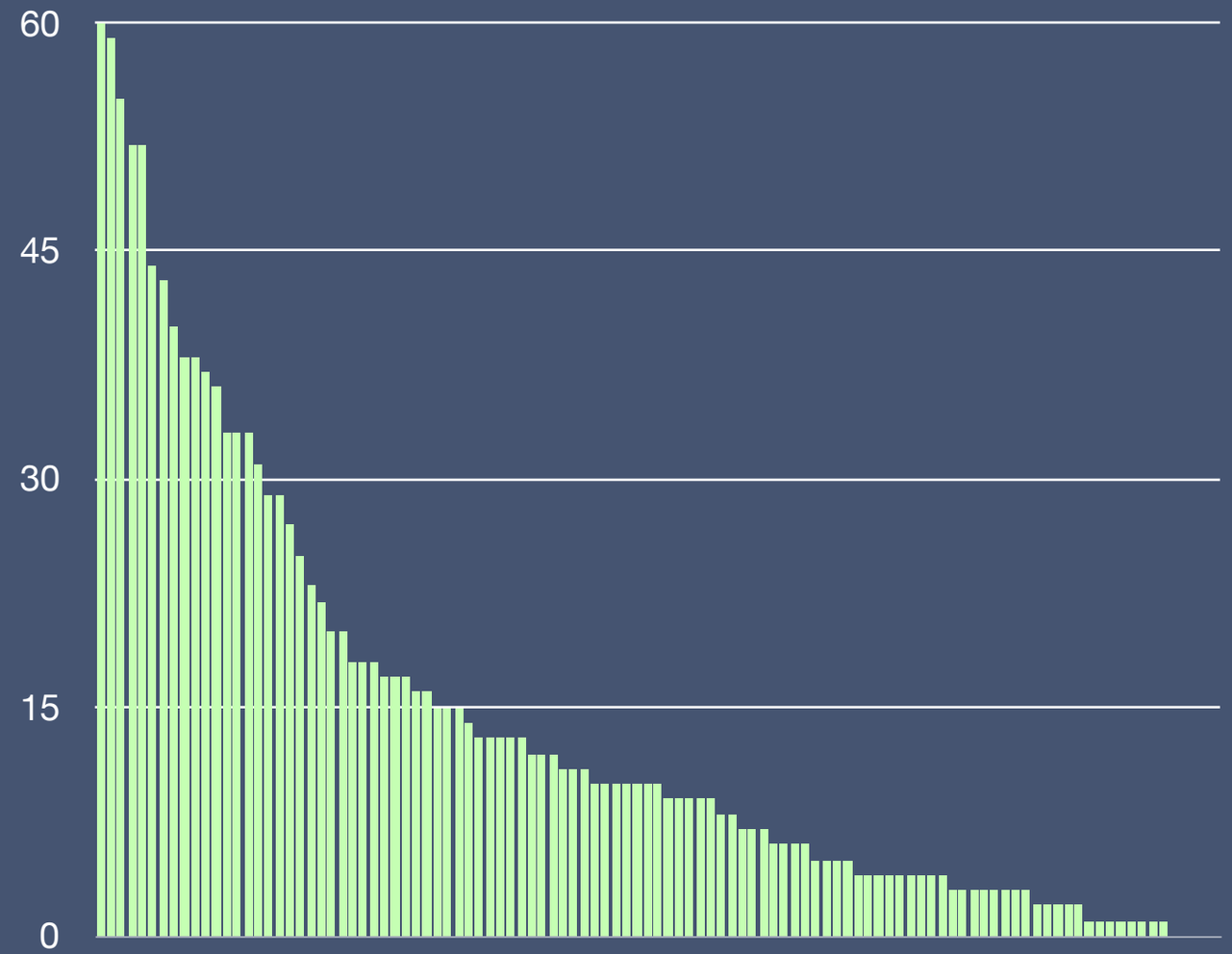
With QV





Quadratic Voting results in Colorado (USA).

Colorado 2019 Quadratic Vote distribution:



Without Quadratic Voting:

In 2018, before using QV, Rep. Hansen implemented a simpler version where each House Democrat received 15 votes to cast for the 15 bills they felt deserved funding. ***The process generated "a big blob" of bills with roughly the same number of votes and no clear preferences.***

"Colorado tried a new way to vote", Wired Magazine, March 2019

Results from first official QV implementation by a US Government (2019).

Stay in contact:

Santiago Siri — @santisiri

Founder of Democracy Earth Foundation
and leading RadxChange in Madrid.
santi@democracy.earth & linkedin.com/in/santisiri/

Democracy Earth is a 501 (c) 3 non-profit
based in California, New York and Madrid.

democracy.earth

Democracy.Earth