A gentle introduction to cryptocurrency token valuation and (mechanism) design

Crypto Monday Talk
Research Institute for
Cryptoeconomics
March 19, 2018

Dr Jamsheed Shorish

http://shorishresearch.com
http://linkedin.com/in/jshorish
jamsheed@shorishresearch.com

Valuing Tokens from Coins?

✣ Cryptocurrencies (loosely) divided into:

　✣ **coins**: associated with a blockchain (e.g. Bitcoin, Ethereum…)

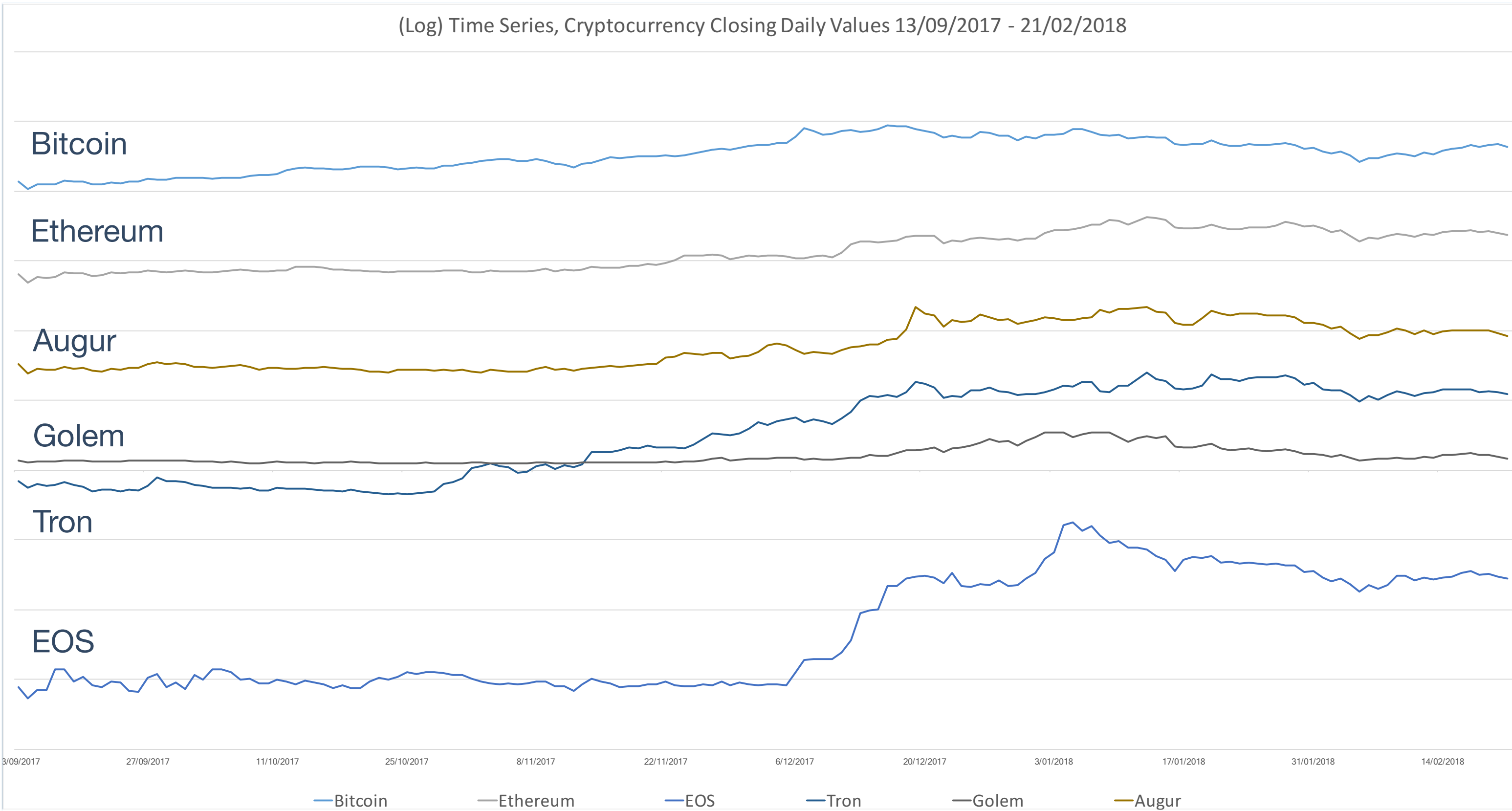　✣ (app) **tokens**: built upon a smart contract protocol (e.g. built *on* Ethereum: Tron, Golem, Augur…).

✣ Ethereum: own coin/token with value-in-use: *ether*.

✣ App tokens built on Ethereum should have an underlying (component of their) value connected to the value of ether. But *how much*?

Icon Source: github.com/cjdowner
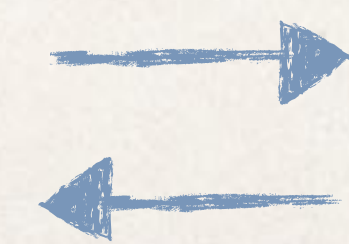
Market Value Time Series

ρ	Bitcoin	Ether.	EOS	Tron	Golem	Augur
Bitcoin	1					
Ether.	0.66797	1				
EOS	0.58785	0.82756	1			
Tron	0.72216	0.96856	0.78355	1		
Golem	0.71413	0.81487	0.86728	0.79806	1	
Augur	0.69891	0.93594	0.81040	0.94934	0.88903	1

(Log) Time Series, Cryptocurrency Closing Daily Values 13/09/2017 - 21/02/2018

Bitcoin

Ethereum

Augur

Golem

Tron

EOS

3/09/2017   27/09/2017   11/10/2017   25/10/2017   8/11/2017   22/11/2017   6/12/2017   20/12/2017   3/01/2018   17/01/2018   31/01/2018   14/02/2018

Bitcoin —— Ethereum —— EOS —— Tron —— Golem —— Augur

Source: Google/kaggle.com

Bundled Value: ICOs

✤ Initial Coin Offerings (ICOs): token offerings prior to the release of a protocol.

✤ ICO allocates tokens/token rights in return for fiat money or cryptocurrencies.

Source: https://www.coindesk.com/ico-tracker
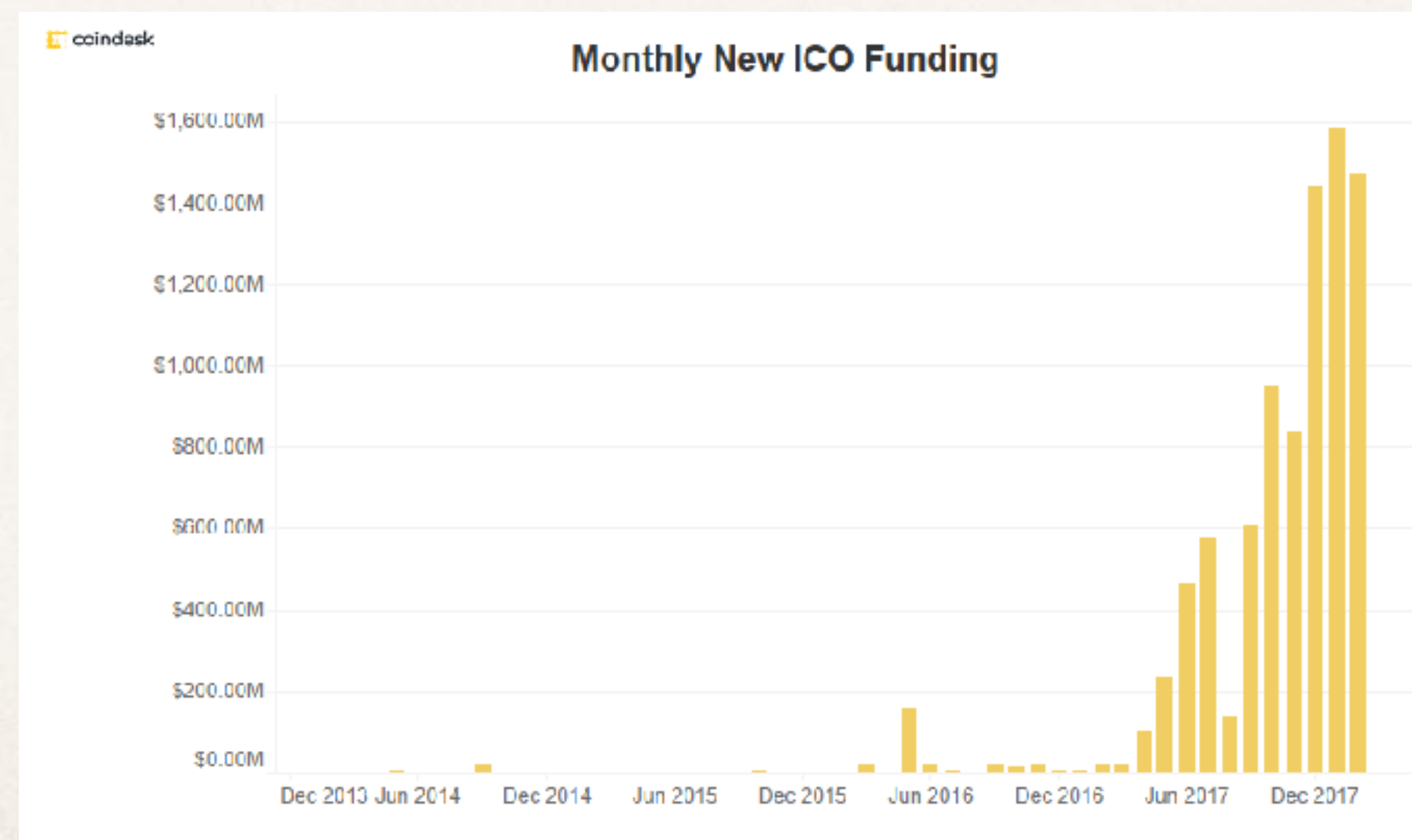
Example: Tezos ICO

- ✤ Tezos: blockchain project launches ICO in July 2017

- ✤ Goal: 'revolutionise' decentralised governance

- ✤ c. $230m raised in pre-sale coin offering

- ✤ Token = "Tez": utility/governance token

Governance token, security token, donation…?

✤ October 2017: internal control battle within the Tezos Foundation

✤ February 22, 2018: internal control dispute resolved with resignation of one party

   ✤ Increase in value of Tez pre-sale right by 10% following announcement (fortune.com)

✤ Was Tez **designed** to internalise the value of intra-foundation control?

   ✤ Tezos Foundation: pre-sale was a *donation*

   ✤ US SEC: pre-sale was a *security*

Perhaps Only A "Fundamental" Matters?

✢ Bitcoin has an underlying "fundamental" value.

✢ But: **speculative** (market) value is unoptimised/unregulated.

✢ Valuation of store-of-value, medium-of-exchange lower than they could be.

Tokens are Multivalued Instruments

✣ A cryptocurrency token is *not* single valued—it is a multivalued instrument.

✣ Token value "lives" in a *d*-dimensional space:

$$v := (v_1, v_2, \ldots, v_d) \in \mathbb{R}^d$$

✣ *Token design* requires getting each of these valuations "right".

✣ Which values a token has is a *collectively endogenous problem*.

Value Measurement

✤ Token "metric": **opportunity cost + value-added**

  ✤ **Utility**: next best protocol/incentive

  ✤ **Security**: next best investment; underlying

  ✤ **Governance**: centralisation vs. decentralisation

  ✤ **Speculation**: market

Value Sustainability: Game Theory
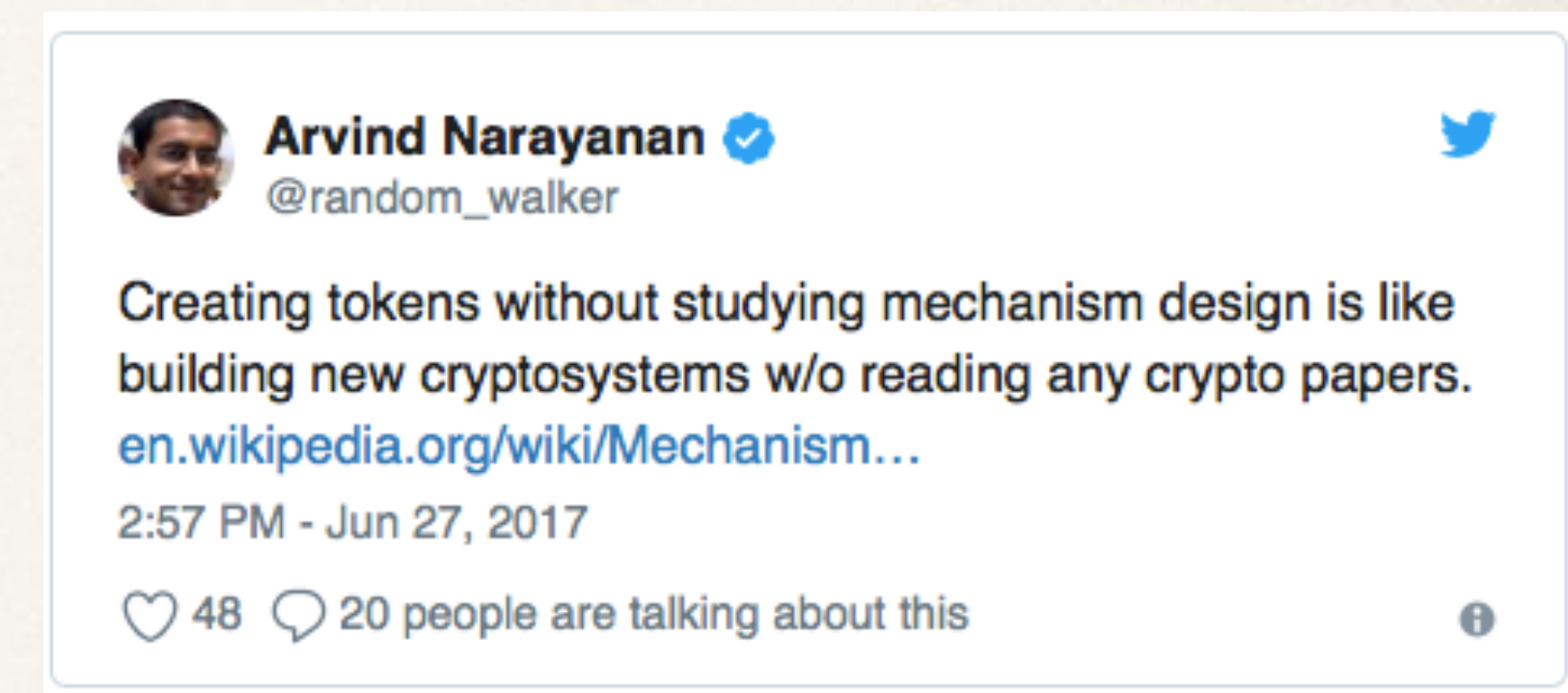

Source: Museum of Fine Arts Boston

✤ Game theory: understand <u>strategic interaction</u> between individuals and/or groups.

✤ **Nash equilibrium**: conditional optimality

✤ Actively used for consensus and governance protocols in blockchain, to:

  ✤ prevent double-spending

  ✤ prevent invalid chains

  ✤ change protocol without central authority

Incentive Compatibility: Mechanism Design

✤ If desired outcome is known => **mechanism design** problem.

✤ Given participants and private information, create <u>optimal incentives</u> to achieve a particular goal.

✤ **Revelation principle**: optimal incentives result in truthful reporting of private information (type), with no "incentive to deviate".

✤ Mechanism can be self-reinforcing, or require outside arbitration.

Arvind Narayanan ✓
@random_walker

Creating tokens without studying mechanism design is like building new cryptosystems w/o reading any crypto papers.
en.wikipedia.org/wiki/Mechanism...
2:57 PM - Jun 27, 2017

♡ 48 ◯ 20 people are talking about this

Source: twitter.com/random_walker

Mechanism Design from Economics

✤ Mechanism design addresses:

✤ What's the best way to match organ donors with recipients? [Roth & Sotomayor 1990; Roth, Sönmez & Ünver QJE 2004]

✤ How does the labour market affect human capital? [Hatfield, Kojima & Kominers, AER 2014]

✤ What's the best insurance coverage for a given health profile? [Glazer & McGuire, AER 2000]

Mechanism Design from Finance

✤ What's the best manager compensation for a given firm size (*corporate finance*)? [He, RFS 2008]

✤ What's the best legal framework for bankruptcy (*law and finance*)? [Araujo & Funchal, JFSR 2015]

✤ What's the optimal price for a firm's IPO (*entrepreneurial finance*)? [Biais, Bossaerts & Rochet RES 2002]

Mechanism Design from Political Economy

✤ What's the best voting mechanism to implement a particular policy (*political economy*)? [Maskin AER 2008]

✤ What's the optimal tax regime to generate government revenue (*law and taxation*)? [Kocherlakota Econometrica 2005]

Mechanism Design in Cryptoeconomics: Origin

✤ Satoshi Nakamoto: original Bitcoin white paper (2008).

✤ Proof-of-Work is one robust solution to the Bitcoin consensus mechanism design problem.

✤ "Quantum leap": cryptography makes deviations from desired behavior very expensive **without** a central authority.

Game Theory & Mechanism Design: Research

✤ Ongoing research: using game theory to prove that transaction verification is (or is approximately) a Nash equilibrium. [e.g. Huoy, Ledger 2016, Kiayias *et al* Adv Crypto 2017]

✤ Some research: app token mechanism design for a single valuation type. [Cerezo Sánchez 2017, BlockChannel Medium.com 2017, Kalodner *et al* WEIS 2015]

✤ No research (?) on token mechanism design when the token is multivalued.

Redux: A Token is Multivalued

✤ Token value is multi-dimensional if more than value can be attributed:
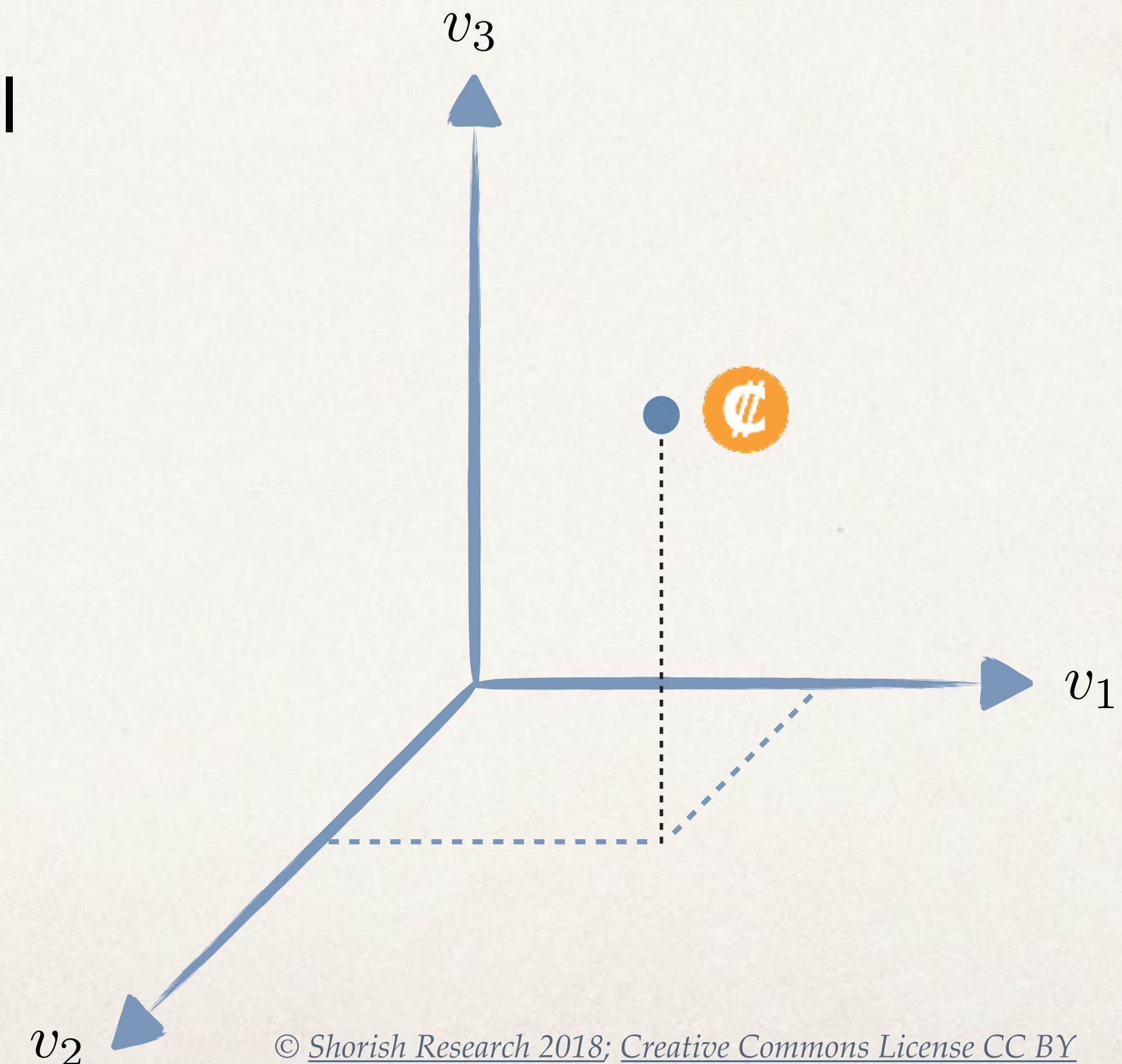
  ✤ **Utility value**: defines interaction with protocol

    ✤ Incentivise behaviour

  ✤ **Security value**: future consumption

  ✤ **Governance value**: rights management

  ✤ **Speculative value**: market

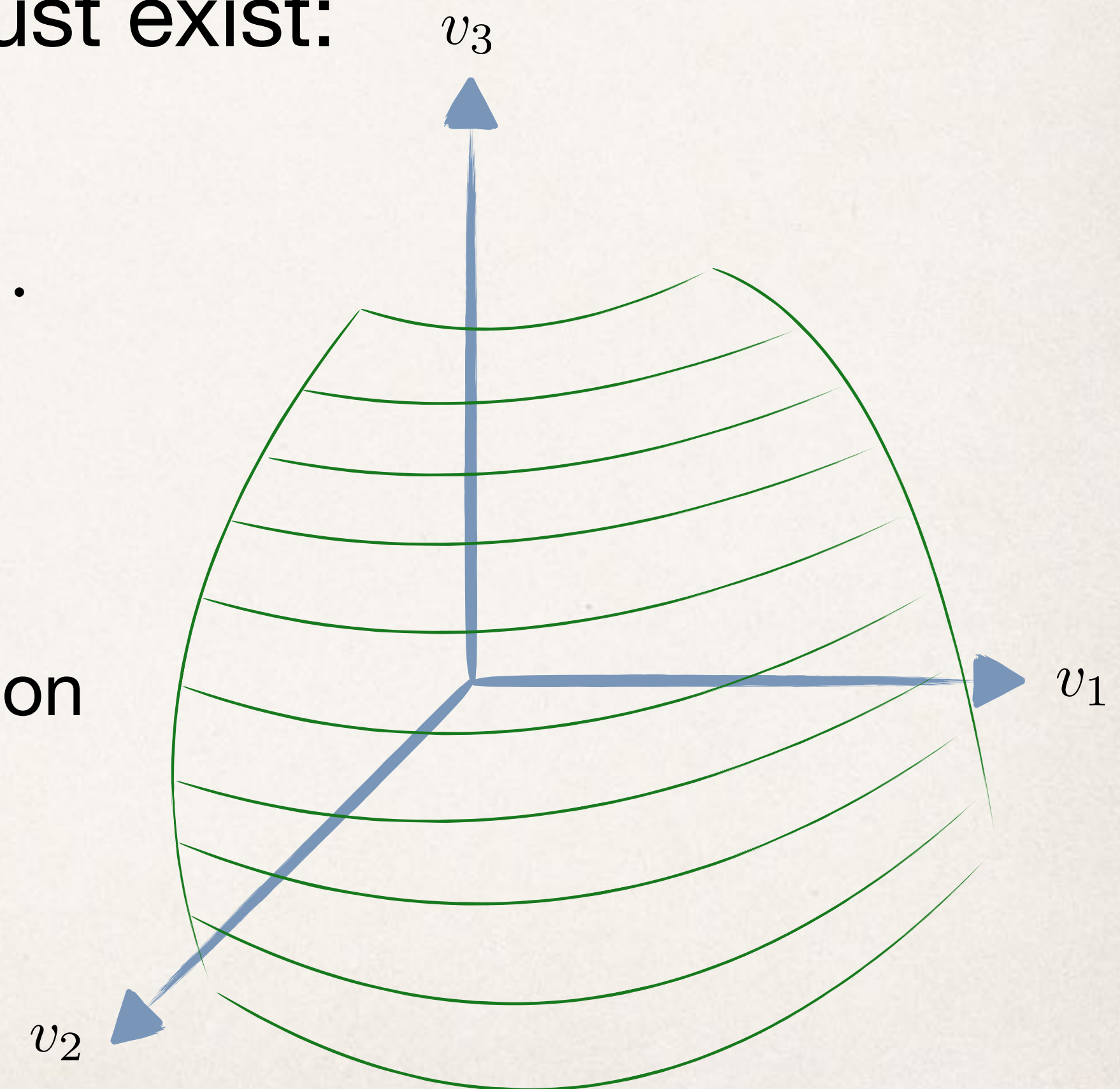 ✤ **Funding value**: ICO, pre-seed etc.

Multiobjective Optimisation

✤ For optimisation, a multiobjective function U must exist:

$$v = U(s_1, s_2, \ldots, s_N), \ s_i \in S_i, \ i = 1, 2, \ldots$$

✤ Strategy sets: S_i

✤ Select strategies to maximize v as a *Pareto optimal* solution

✤ Multicriteria decision-making

✤ Heuristic optimisation (e.g. simulated annealing)

(Mechanism) Designing Tokens

✤ Token recipients have *private information* regarding type.

✤ Type = preferences over possible values of token

✤ **Mechanism design**: select launch type (ICO, air drop, term sheet, etc.) so that

    ✤ Incentive compatibility: Recipients gain tokens according to type (revelation principle, Shorish 2018);

    ✤ Creator realises own (possibly multiobjective) goal of token distribution;

    ✤ Outcome lies on the Pareto frontier for both recipients and creator.

Designing Tokens: A Delicate Balance

✤ Once the mechanism for a token sale is created, *the token becomes a function of the mechanism*.

✤ **Regulation**: defines the "rules of the game" for the mechanism, and hence the token, **regardless** of the self-applied label of the token.

✤ Current regulatory structure is unknown: but proactive monitoring by regulatory bodies will be replaced by:

  ✤ existing legal statute;

  ✤ new KYC/AML & anti-fraud legislation.

"ICOs are highly speculative investments. ICOs, depending on how they are structured, may fall outside of the regulated space, in which case investors do not benefit from the protection that comes with regulated investments. ICOs are also vulnerable to fraud or illicit activities, owing to their anonymity and their capacity to raise large amounts of money in a short timeframe."

- European Securities and Markets Authority
13 Nov. 2017

Future Challenges and Opportunities

✣ Currently token distribution is hampered by poor valuation understanding.

✣ Mechanism design improves valuation and elicits truthful behaviour.

✣ Requires an **understanding** of: game theory, contract theory, incentives.

✣ Requires an **appreciation** of: economic engineering; securities design; regulation.

Future Challenges and Opportunities

✤ "Holy Grail" achievements:

    ✤ Given a set of desired token values, state the **optimal token sale mechanism**.

    ✤ Given a protocol/blockchain specification, state the **optimal token type**.

    ✤ Given a token type, state the **optimal regulatory structure**.

    ✤ Endgame: create a sustainable, stable cryptocurrency covering **both** fiat money and financial asset use cases, and *new*, *unique*, *revolutionary* uses!

Thank you for your attention!*

http://shorishresearch.com
http://linkedin.com/in/jshorish
jamsheed@shorishresearch.com

*Cryptocurrencies were mentioned in this presentation for illustrative purposes only, and such mention does not state or imply an endorsement or recommendation for investment.