UNIVERSITY OF STIRLING

Decentralised Computing

Trust in a trustless world?

Andrea Bracciali
abb@cs.stir.ac.uk

Distributed Ledger Technology Workshop *Perugia, 1 2 2018*

UNIVERSITY OF STIRLING

Decentralisation: interesting new idea

Implemented in Blockchain technologies
(technical, social, economical, … and political aspects)

Some open questions deserve research

2015 IEEE Symposium on Security and Privacy

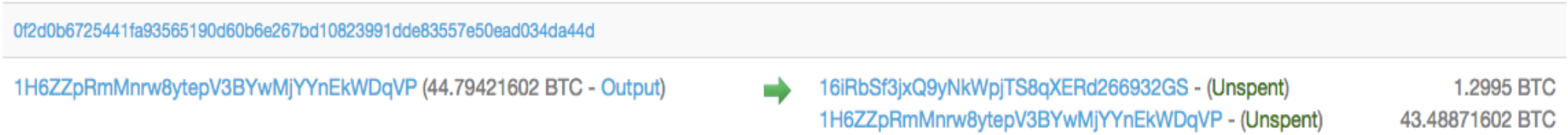
SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies

Joseph Bonneau*†‡, Andrew Miller§, Jeremy Clark¶, Arvind Narayanan*, Joshua A. Kroll*, Edward W. Felten*
*Princeton University, †Stanford University, ‡Electronic Frontier Foundation, §University of Maryland, ¶Concordia University

UNIVERSITY OF STIRLING

Bitcoin: a currency without a (central) bank
A football match without a referee?

Decentralised trust implemented by a distributed consensus mechanism (*proof of work*) and validated by computation:



DUP HASH160 PUSHDATA(20)[3eae3697975ae35c475e52307f26b8db0d554dcb] EQUALVERIFY CHECKSIG

DUP HASH160 PUSHDATA(20)[b08f46e4d21cd0547a8a1e2e43e5440284f710a4] EQUALVERIFY CHECKSIG

TECHNICAL LEGAL SOCIAL

Bitcoin: a currency without a (central) bank
A football match without a referee?

But*

- what in case of a theft?
  A stolen password

- what is a theft?
  A “stealing transaction” is indistinguishable from a genuine one

- which police?
  No authority, no recovery, back-ups, back-tracks …

- who is the thief?
  No people, no identities

UNIVERSITY OF STIRLING

Bitcoin: a currency without a (central) bank
A football match without a referee?

Decentralised trust relying on

1. a complex and sensitive *crypto-economics* framework, e.g. ,

When cryptocurrencies mine their own business*

Jason Teutsch, Sanjay Jain, and Prateek Saxena

which models ?

Rational agents, stochastic behaviour, preferences …

Socio-economic …

CRYPTO-ECONOMICS TECHNICAL ECONOMICAL SOCIAL

UNIVERSITY OF STIRLING

Bitcoin: a currency without a (central) bank
A football match without a referee?

Decentralised trust relying on

2. suitable design of monetary policy,

e.g. 21M BTC limit, deflationary?

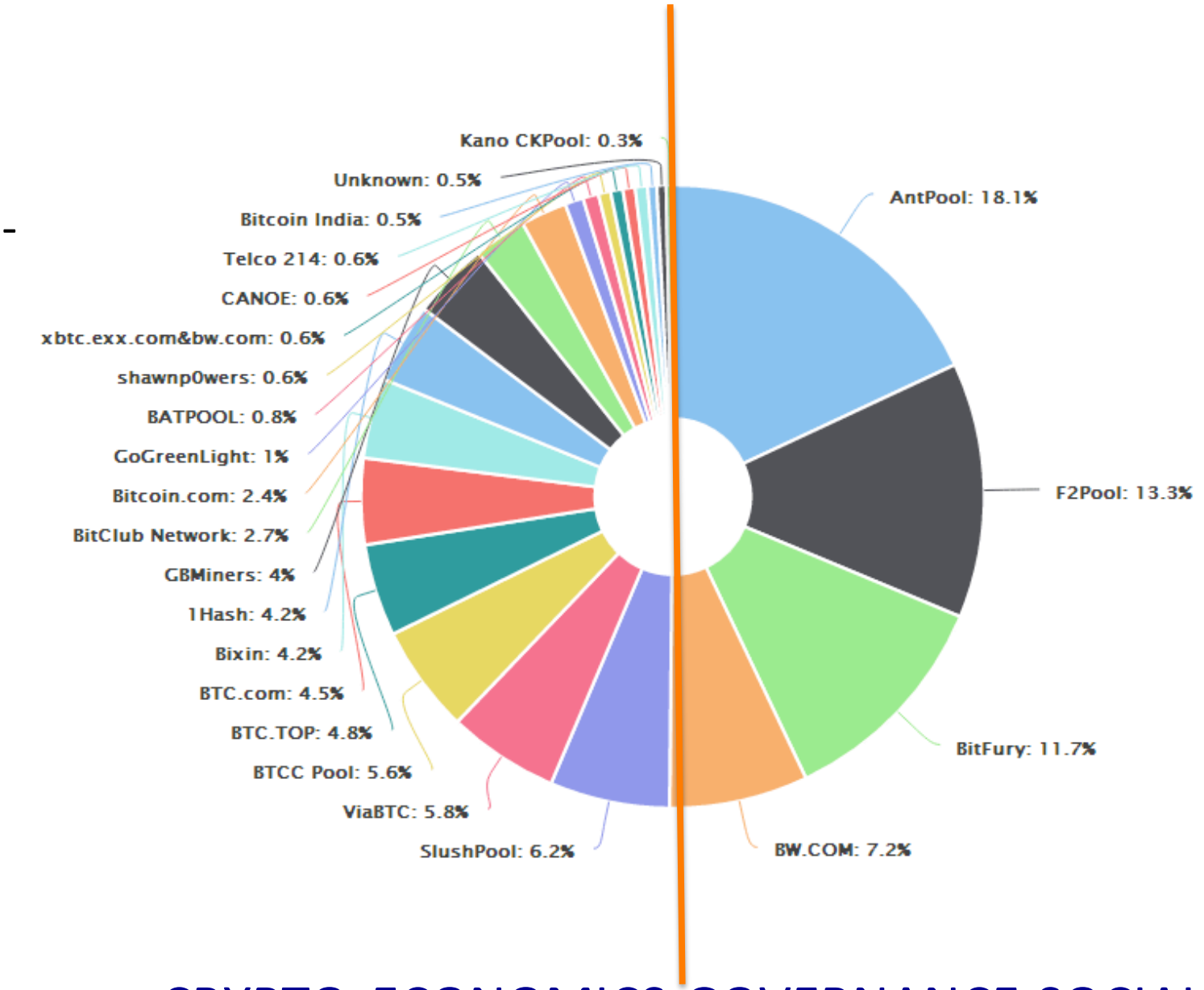
non-adaptive (so far), store of value, new gold.

3. support by fiat currencies, measure of value (so far).

CRYPTO-ECONOMICS TECHNICAL ECONOMICAL SOCIAL

UNIVERSITY OF STIRLING

Really decentralised governance?



50%
Four groups

CRYPTO-ECONOMICS GOVERNANCE SOCIAL POLITICAL

UNIVERSITY OF STIRLING

Decentralised governance: disputes and forks

Scalability

#transactions 5 - 20 vs 2 000 (VISA)

Recent dispute (2017) off-chain transactions (side chains) vs larger blocks

A scalable verification solution for blockchains

Jason Teutsch
TrueBit Establishment
jt@truebit.io

Christian Reitwießner
Ethereum Foundation
chris@ethereum.org

Ended up in a split of the *community* and of the currency BCH

Was also a problem of governance: larger blocks, larger computers, less decentralisation (but … see previous slide).

GOVERNANCE TECHNICAL ECONOMICAL SOCIAL

UNIVERSITY OF STIRLING

Decentralised governance and external control

Patrolling the borders:

- exchanges

(e.g. recent correlation South Korea presumed norming vs BTC volatility)

Decentralisation fades away when crossing virtual and real boundaries,

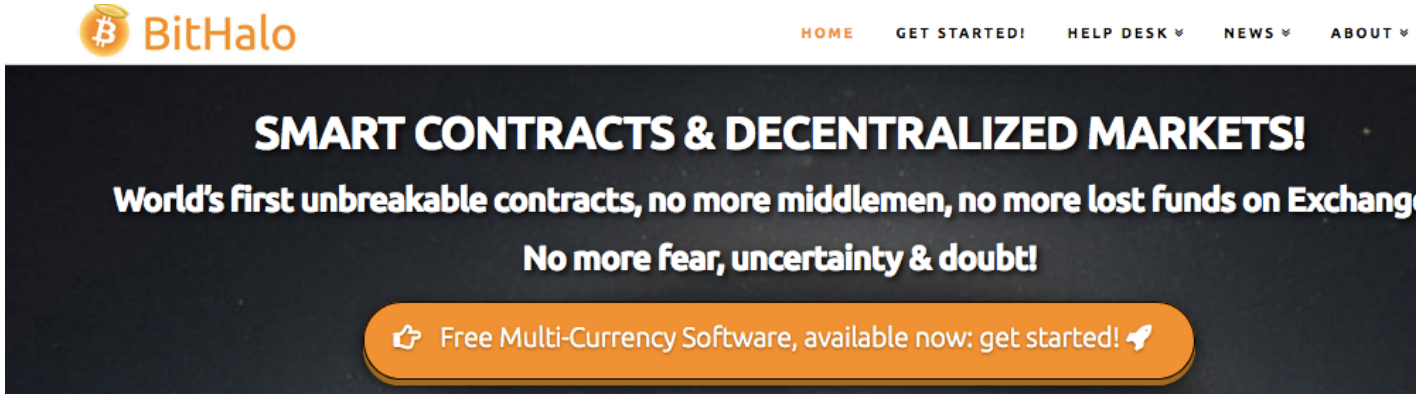
- exchanges
- regulatory bodies (US SEC and local govs, UK FCA, …)
- taxes

- tracking identities (iwannacry, pseudo-anonymity)
- Monero, zero-knowledge protocols, homomorphic encryption

LEGAL ECONOMICAL SOCIAL

UNIVERSITY OF STIRLING

dapp I: Bithalo (BAY): decentralised ebay (trust in escrows)



Two untrusting partners save a deposit in an escrow.
The smart contract returns the deposit, if both are happy about a given transaction.

No central authority intervention or previous trust between parties.

Which models?

LEGAL ECONOMICAL SOCIAL

UNIVERSITY OF STIRLING

dapp I: Bithalo (BAY): decentralised ebay (trust in escrows)

- GAME THEORY: exploring and defining strategies
- FORMAL METHODS: automated quantitative analysis of a probabilistic model

- QUANTITATIVE CHARACTERISATION OF THE PROTOCOL'S FEATURES

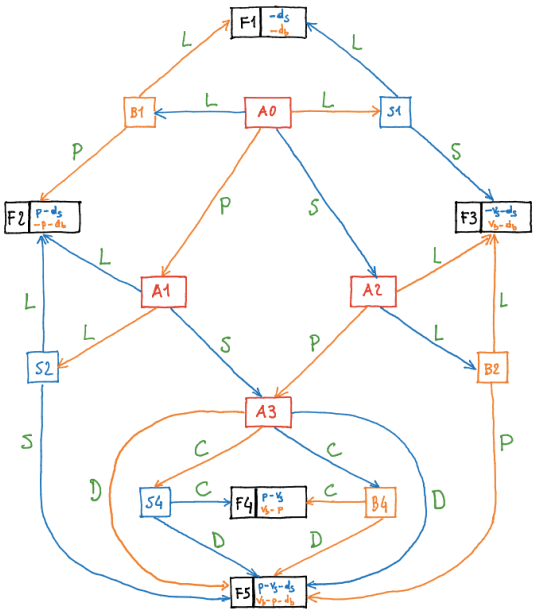
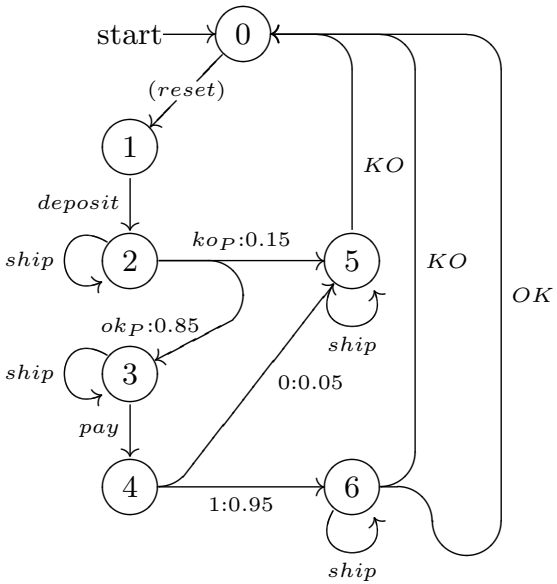


Fig. 1. The graph of the transaction protocol.

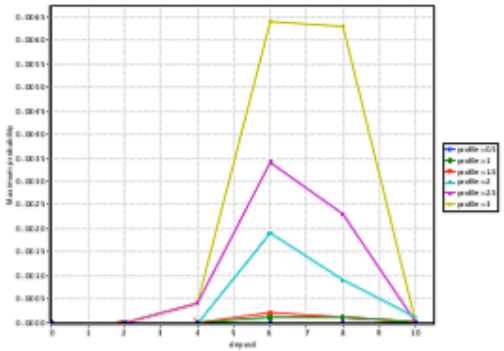


(a) Buyer's automata

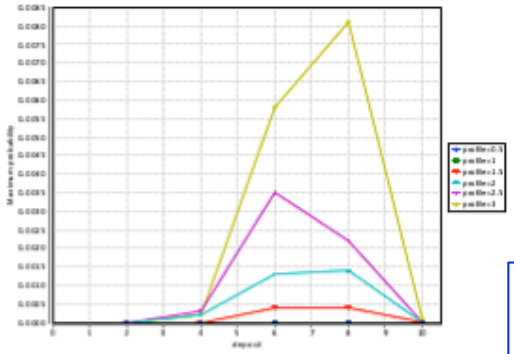
TECHNICAL CRYPTO-ECONOMICS

UNIVERSITY OF STIRLING

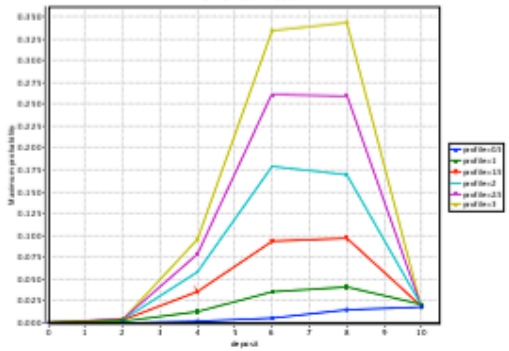
dapp I: Bithalo (BAY): decentralised ebay (trust in escrows)



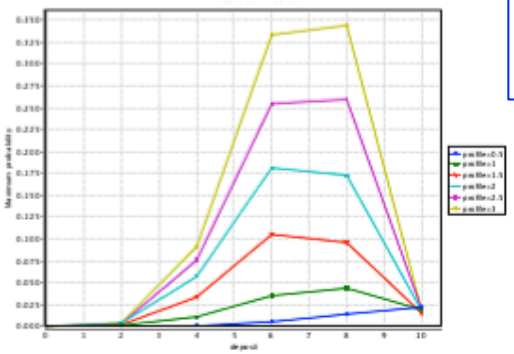
(a) Seller profiles, loss ∼ 40%



(b) Buyer profiles, loss ∼ 40%



(c) Seller profiles, loss ∼ 30%



(d) Buyer profiles, loss ∼ 30%

Validation of Decentralised Smart Contracts Through Game Theory and Formal Methods

Giancarlo Bigi[1], Andrea Bracciali[2(✉)], Giovanni Meacci[3,4], and Emilio Tuosto[5]

TECHNICAL CRYPTO-ECONOMICS

UNIVERSITY OF STIRLING

dapp II: Decentralised (quality) information (empowering citizens' *data ownership* – *GDPR, H2020, …*)

The NEW ENGLAND JOURNAL of MEDICINE

CORRESPONDENCE

An Unconscious Patient with a DNR Tattoo

N Engl J Med 2017; 377:2192-2193 | November 30, 2017 | DOI: 10.1056/NEJMc1713344

Gregory E. Holt, M.D., Ph.D.
Bianca Sarmento, M.D.
Daniel Kett, M.D.
Kenneth W. Goodman, Ph.D.
University of Miami, Miami, FL
gholt@miami.edu

LEGAL ECONOMICAL SOCIAL POLITICAL

dapp III: Lending crypto-currencies in a decentralised world

Difficult ! (not there yet)

1. Volatility
2. Counter-party risk

Should be managed by code!

Proposed solutions inch towards centralisation, e.g. for 1.:

linking the debt to a fiat currency:

I will return the equivalent of 100USD in BTC.

Who does provide the exact amount?

Relaxing decentralisation (back to business as usual?)

From non-permissioned to permissioned (and double-permissioned) blockchains, e.g.

- Hyperledger (IBM++)
- Stellar

The Stellar Consensus Protocol:
A Federated Model for Internet-level Consensus

DAVID MAZIÈRES, Stellar Development Foundation

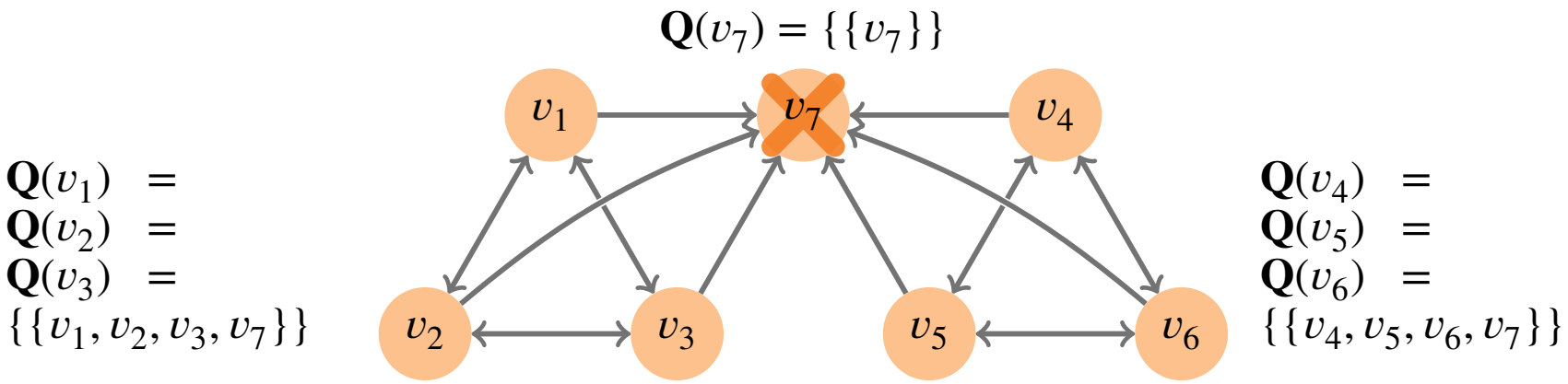


Fig. 7. Ill-behaved node v_7 can undermine quorum intersection.

LEGAL TECHNICAL SOCIAL

UNIVERSITY OF STIRLING

Ethereum: the consensus computer

ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER
EIP-150 REVISION

DR. GAVIN WOOD
FOUNDER, ETHEREUM & ETHCORE
GAVIN@ETHCORE.IO

Decentralised computation:

- state and computation enter the blockchain,
- each node deterministically reproduce the “agreed” computation
- new software engineering paradigm

Which models? Need to be crypto-economics enabled
Which governance?

TECHNICAL

UNIVERSITY OF STIRLING

TEZOS decentralised governance

.

Tezos: A Self-Amending Crypto-Ledger
Position Paper

L.M Goodman

Decentralisation embeds governance, besides trust.

Consensus on how to change rules, also those that rule consensus.

Which (meta-?)models ?

TECHNICAL

UNIVERSITY OF STIRLING

TEZOS decentralised governance

> **Indeed. Tezos has an official goal of eliminating the need for extra-protocol governance; I personally disagree with this direction.**
>
> **— Vitalik Buterin (@VitalikButerin) July 10, 2017**

> **To be clear: eliminate the need yes, the possibility, no. Hard-forks are valuable failsafes and you make a great case for it.**
>
> **— Tezos (@tezos) July 10, 2017**

… more at WTSC18@FC – 26/02 02/03 March 2018

TECHNICAL

YAP
[from wikipedia]