blockchain-based voting

potential & limitations

Jeremy Clark (@PulpSpy)
Concordia Institute for Information Systems Engineering

Time Stamping

Prediction Markets

Anonymity

Solvency

Usability

History & SoK

Part 1:
Scaling Bitcoin in terms of users

Part 2:
Blockchain-based voting

A First Look at the Usability of Bitcoin Key Management

Shayan Eskandari*, David Barrera†, Elizabeth Stobert‡, and Jeremy Clark*
*Concordia University, †ETH Zürich, ‡Carleton University

The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy*

Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl

Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users

Xianyi Gao, Gradeigh D. Clark, Janne Lindqvist
Rutgers University

15:25 - 15:50	Sia	David Vorick	
15:50 - 16:20	Fidelity: Bitcoin usability & scaling	Dave Weissburg	Raghav Chawla
16:20 - 16:45	Identity	Christian Lundkvist	

Who are the Bitcoin non-users & what do they think

Average Bitcoin User

- male (95%)
- 32 (average age)
- american (44%)
- libertarian (47%)

Non-users: residual humans

Non-users think Bitcoin is:

- speculative
- for black market sales
- difficult to use
- complicated

Non-users don’t use Bitcoin b/c:

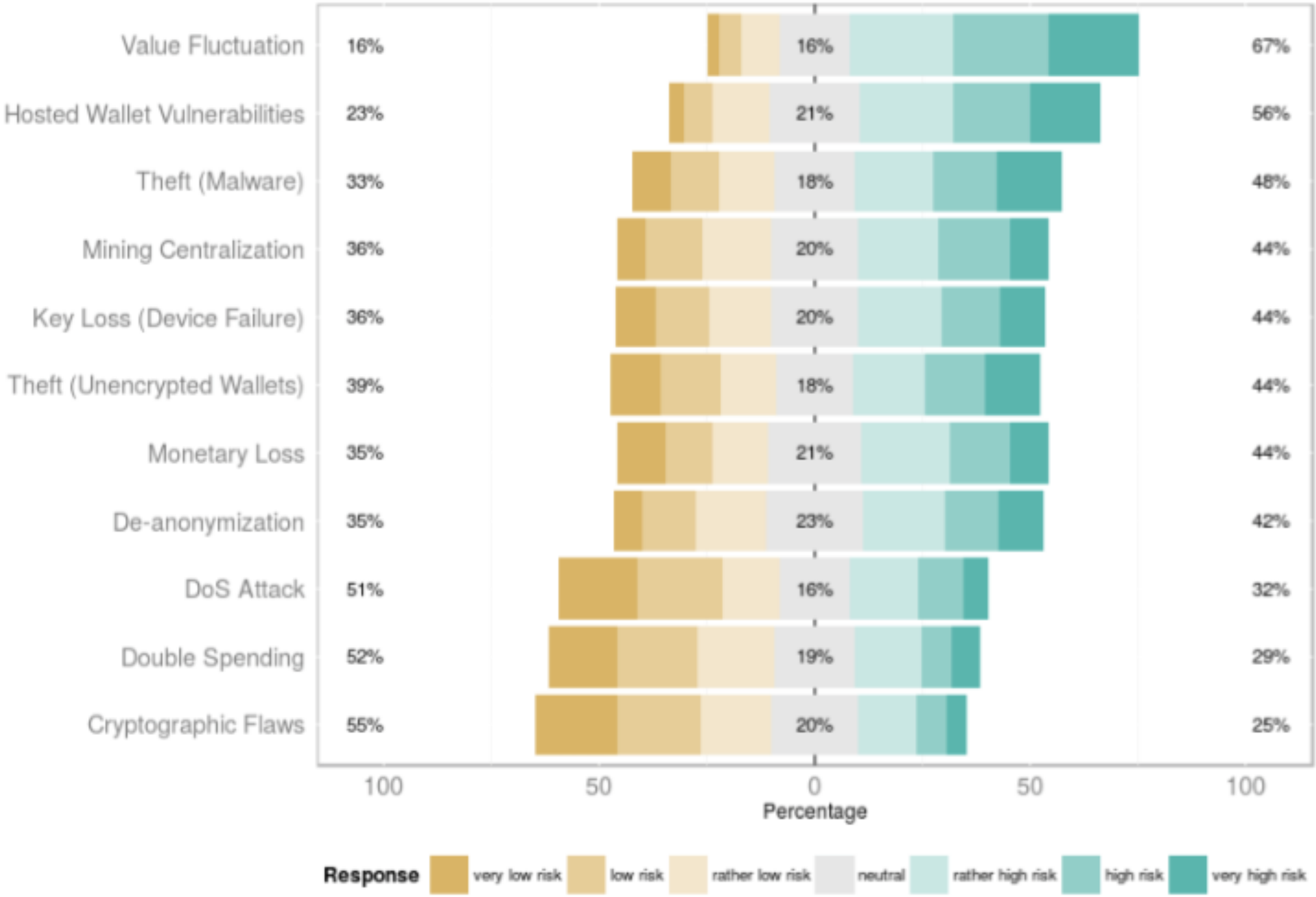
- don’t understand it
- no need for it
- have to mine to get it
- don’t know any accepting merchants

Non-users think a better financial system would be:

- faster transactions
- error-prevention/recovery
- lower fees
- cross-device portability

When non-users turn into users, they meet new concerns:

- price volatility
- security
- et cetera


Value Fluctuation
16%
16%
67%
Hosted Wallet Vulnerabilities
23%
21%
56%
Theft (Malware)
33%
18%
48%
Mining Centralization
36%
20%
44%
Key Loss (Device Failure)
36%
20%
44%
Theft (Unencrypted Wallets)
39%
18%
44%
Monetary Loss
35%
21%
44%
De-anonymization
35%
23%
42%
DoS Attack
51%
16%
32%
Double Spending
52%
19%
29%
Cryptographic Flaws
55%
20%
25%
100
50
0
50
100
Percentage
Response
very low risk
low risk
rather low risk
neutral
rather high risk
high risk
very high risk

On security

- 46% (/1000) use a hosted wallet
- Coinbase has most users
- Bitcoin Core & Armory has most value however
- 0% use an air-gap device
- 22% have lost money
  - Hardware failure (eg hard-drive)
  - Software failure (eg wallet.dat)
  - Malware

What is wrong with keys?

1) Lost — user didn’t memorize, no resets
2) Stolen — user is fully liable, no protection
3) Use — protection & availability trade-off

Category	*Example*	Malware Resistant	Key(s) Kept Offline	No Trusted Third Party	Resistant to Physical Theft	Resistant to Physical Observation	Resilient to Password Loss	Resilient to Key Churn	Immediate Access to Funds	No New User Software	Cross-device Portability
Keys in Local Storage	Bitcoin Core		●		●	●	●	●			
Password-protected Wallets	MultiBit		○	●	○	●		●	●		
Offline Storage	Bitaddress	○	●	●			●				●
Air-gapped Storage	Armory	○	●	●		●	●	●			
Password-derived Keys	Brainwallet		●	●	○			●	●	●	●
Hosted Wallet (Hot)	`Coinbase.com`						●	●	●	●	●
Hosted Wallet (Cold)		○	●				●	●		●	●
Hosted Wallet (Hybrid)	Blockchain.info		○	○			●	●	●	●	●
Cash		●	●	●		●	●	●	●	●	●
Online Banking							●	●	●	●	●

No solutions, only trade-offs

Hosted Wallet Manifesto

- Security people hate hosted wallets
- They are arguably against Bitcoin's principles
- BUT they offer the best shot at user scalability
- Idea: stop shaming people for using online wallets or keeping their BTC on exchanges
- Instead work at making these as secure as possible

Improving Hosted Wallets

1) Proof of Solvencies — snapshot in time

Give users privacy-preserving proof

Provisions: Privacy-preserving Proofs of Solvency for Bitcoin Exchanges

Gaby G. Dagher
Concordia University

Benedikt Bünz
Stanford University

Joseph Bonneau (✉)*
Stanford University

Jeremy Clark
Concordia University

Dan Boneh
Stanford University

Improving Hosted Wallets

1) Proof of Solvencies — snapshot in time

Give users privacy-preserving proof

2) Bitcoin covenants — slow theft down

Composed with solvency

Bitcoin Covenants

Malte Möser[1], Ittay Eyal[2], and Emin Gün Sirer[2]

[1] Department of Information Systems, University of Münster, Germany
[2] Department of Computer Science, Cornell University, USA

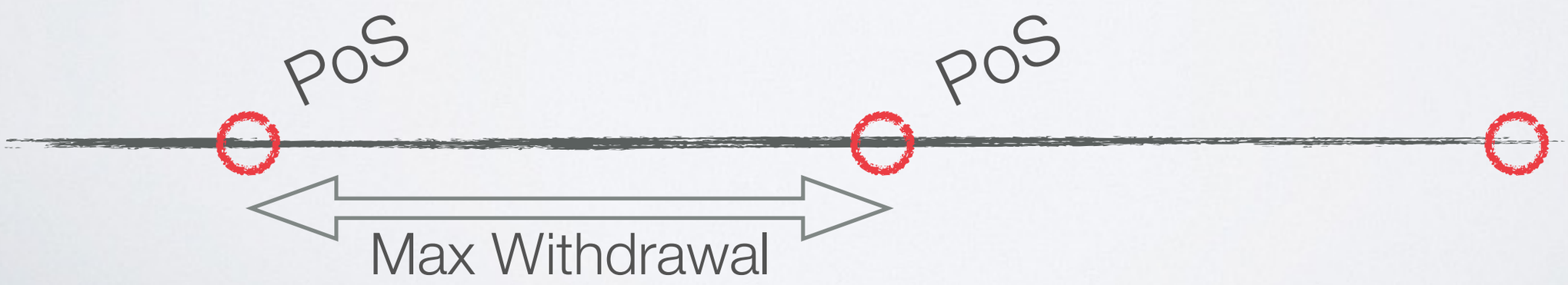
Improving Hosted Wallets

1) Proof of Solvencies — snapshot in time

Give users privacy-preserving proof

2) Bitcoin covenants — slow theft down

Composed with solvency: limited liability



Improving Hosted Wallets

1) Proof of Solvencies — snapshot in time

Give users privacy-preserving proof

2) Bitcoin covenants — slow theft down

Composed with solvency: limited liability

3) Divert liability to company — eliminate impact

Established & diversified banks; insurance

</part1>

Voting

Cryptographic voting systems prove your ballot is included and unmodified

The hard questions for any new blockchain proposal:

1) Eligibility
2) Ballot secrecy
3) Integrity

Eligibility

One vote per:

1) Unrestricted — no issue
2) Voter — requires an external roster (TTP)
3) Mined block (work) — novel for Bitcoin+
4) BTC unit (stake) — Provisions can do this
5) Algorithmic description - novel for Ethereum+

Ballot Secrecy

For public votes, no problem (shareholder votes, etc)

For work, stake, & algorithmic eligibility: anonymity of underlying crypto-currency

For roster-based w/ secrecy, you have a real challenge

- You can build an external cryptographic structure to link IDs to addresses [JCJ, Civitas, Selections, etc]
- You can even prevent coercion with indistinguishable fake addresses, however heavy lifting is external

Integrity

All cryptographic voting systems use a “bulletin board:” an append-only broadcast channel (sometimes anonymous)

Conventional elections typically ban “running tallies”

Blockchains are the best bulletin boards we have ever seen, better than purpose-build ones (esp. on equivocation)

Blockchains offer lightweight time-stamping (via network consensus) and strong “carbon-dating”: backdating a message = forking and catching up to the work

scantegrity

Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy

Richard Carback
UMBC CDL

David Chaum

Jeremy Clark
University of Waterloo

John Conway
UMBC CDL

Aleksander Essex
University of Waterloo

Paul S. Herrnson
UMCP CAPC

Travis Mayberry
UMBC CDL

Stefan Popoveniuc

Ronald L. Rivest
MIT CSAIL

Emily Shen
MIT CSAIL

Alan T. Sherman
UMBC CDL

Poorvi L. Vora
GW

scantegrity

Summary

Size	258 (bytes)
Received Time	Oct 18, 2011 1:26:00 PM
Mined Time	Oct 18, 2011 1:26:00 PM
Included in Block	0000000000000b304a21bd0e83769f0065a0d291cbe5296af52590fb8...

Details

3789397fc352e93e7f1e7be3b770a04bff251ae36fa601125372336c626cb743 mined Oct 18, 2011 1:26:00 PM

1AH7CvhTQ9XJ9He8NEtNwX5Go2FaE6qYFh 1.0682 BTC

15WFXD7HRandc72WAPRh9gBWKn9FRTEhiH 1.0582 BTC (S)

1PTAZ9wMZ2Ff9RgLt4UMXMh7vbBNdTDVbs 0.01 BTC (U)

FEE: 0 BTC

251652 CONFIRMATIONS

1.0682 BTC

Take-away

Play to Bitcoin+’s comparative advantages

Don’t try and replace conventional voting with blockchain solutions

Don’t be a solution looking for a problem

Find interesting new areas that can be democratized with novel definitions of eligibility enabled by Bitcoin+

Questions

@PulpSpy

j.clark@concordia.ca