universität
innsbruck

Privacy and Economics

The Swiss Blockchain Winter School, Interlaken, 2019

Rainer Böhme

This is **not** Interlaken. (Picture taken last week.)

Privacy in Blockchain-based Systems

Fundamental conflict between:

- public blockchain data, required for distributed verification,

and

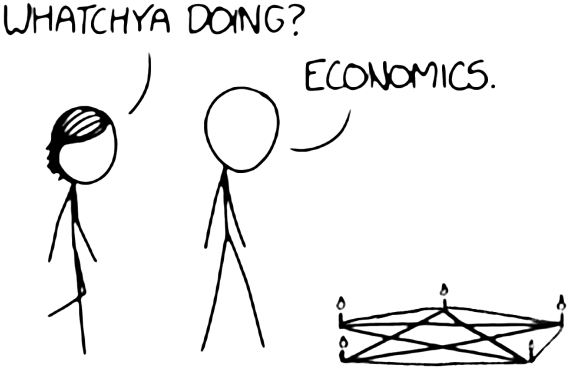
- users’ right of personality, because the information contained in (financial) transactions reveals personal preferences and circumstances of life.

Hope of mitigation:

- Pseudonyms are not directly linkable to natural persons.

Nevertheless, EU lawyers consider blockchain data as **personal data** because:

1. the link to natural persons can often be established with **additional information** (e. g. known by intermediaries, such as exchanges or network relays);
2. the persistence of blockchain data increases the probability that this will happen some time in the future.



Source: xkcd.com

Outline

1. **How to Plug Privacy into Economic Equations**
2. Observing a Market for Anonymity
3. How to Price Anonymity

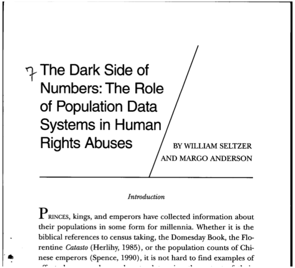
Acknowledgement: Part of the material in this talk is joint work with Malte Möser and Daniel G. Arce.

Challenge

Worst case: the system operator is the attacker.

A Startling View of Life in 1984
Forbidden Love . . . . Fear . . . . Betrayal
SIGNET
1984
A Novel by
GEORGE ORWELL
BIG BROTHER IS WATCHING YOU
SIGNET BOOKS
Complete and Unabridged

fiction



7 The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses

BY WILLIAM SELTZER AND MARGO ANDERSON

Introduction

PRINCES, kings, and emperors have collected information about their populations in some form for millennia. Whether it is the biblical references to census taking, the Domesday Book, the Florentine *Catasto* (Herlihy, 1985), or the population counts of Chinese emperors (Spence, 1990), it is not hard to find examples of

Seltzer, W. & Anderson, M. in *Social Research* **68** (2), 2001

reality

Bad, but almost unavoidable case: the system operator makes mistakes.

→ **Dead end: Quantifying the disutility of personal data abuse**

Schools of Thought

Classical economic theory

Efficient markets, perfect information, . . .

Why does advertising exist ?

New institutional economics

Information matters, asymmetry causes misallocation, . . .

Adverse selection: privacy protects bad risks

Asset pricing

Present value of expected future benefit of (re)identification

Berthold & Böhme 2009

Behavioral economics

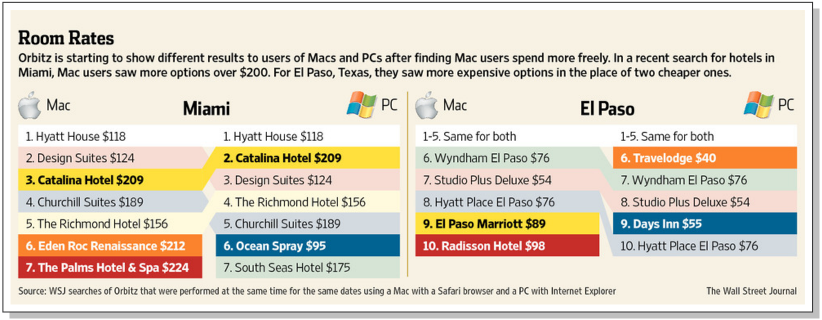
Bounded rationality, human-subject experiments

Find price tags for personal data

→ **No general theory of information distribution between economic agents**

Economics Value of Personal Data

Price discrimination by HTTP User-Agent string:



Room Rates

Orbitz is starting to show different results to users of Macs and PCs after finding Mac users spend more freely. In a recent search for hotels in Miami, Mac users saw more options over $200. For El Paso, Texas, they saw more expensive options in the place of two cheaper ones.

Miami

Mac	PC
1. Hyatt House $118	1. Hyatt House $118
2. Design Suites $124	**2. Catalina Hotel $209**
3. Catalina Hotel $209	3. Design Suites $124
4. Churchill Suites $189	4. The Richmond Hotel $156
5. The Richmond Hotel $156	5. Churchill Suites $189
6. Eden Roc Renaissance $212	**6. Ocean Spray $95**
7. The Palms Hotel & Spa $224	7. South Seas Hotel $175

El Paso

Mac	PC
1-5. Same for both	1-5. Same for both
6. Wyndham El Paso $76	**6. Travelodge $40**
7. Studio Plus Deluxe $54	7. Wyndham El Paso $76
8. Hyatt Place El Paso $76	8. Studio Plus Deluxe $54
9. El Paso Marriott $89	**9. Days Inn $55**
10. Radisson Hotel $98	10. Hyatt Place El Paso $76

Source: WSJ searches of Orbitz that were performed at the same time for the same dates using a Mac with a Safari browser and a PC with Internet Explorer

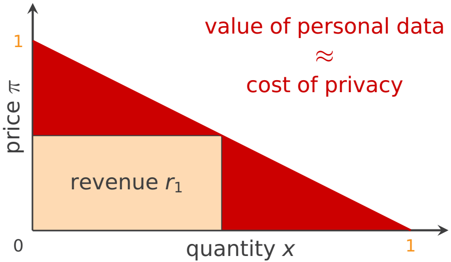
The Wall Street Journal

Source: The Wall Street Journal 2012

Privacy and Price Discrimination

Demand function $D : \pi \mapsto x$

Case 2: Seller knows each buyers’ willingness to pay



value of personal data
≈
cost of privacy

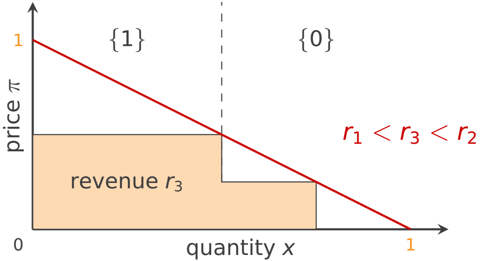
Odlyzko 2003

Assumptions: monopolistic seller, no arbitrage, zero marginal cost

Privacy and Price Discrimination

Demand function $D : \pi \mapsto x$

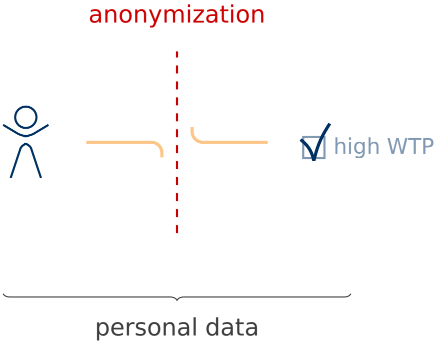
Case 3: Seller knows one bit about each buyers' WTP



Odlyzko 2003

Assumptions: monopolistic seller, no arbitrage, zero marginal cost

Technical Approach



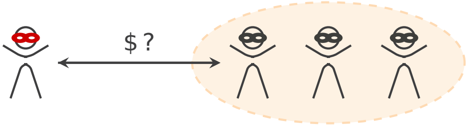
anonymization

☑ high WTP

personal data

Economics of Anonymity

"Anonymity is the state of not being identifiable within a set of subjects, the anonymity set."

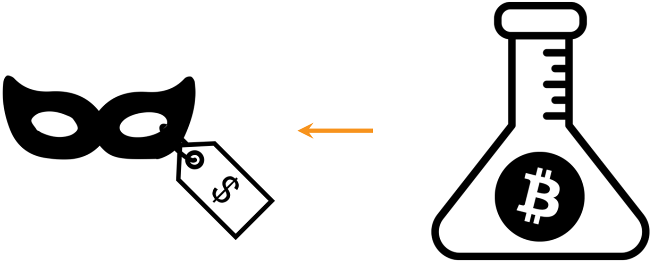


"anonymity loves company"

Dingledine & Mathewson 2006

Pfitzmann & Köhntopp 2001

Opportunity



The price of anonymity

Bitcoin as a
social science lab

Icons based on
Flask by Andrew Was from the Noun Project

Tag and Eye Mask by Creative Stall from the Noun Project

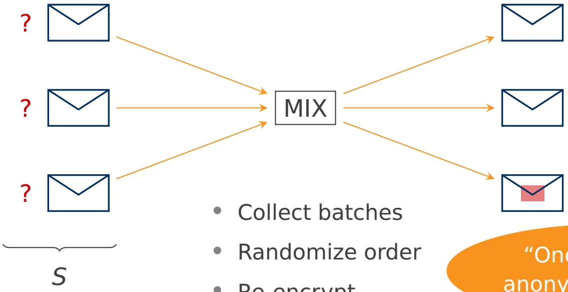
Outline

1. How to Plug Privacy into Economic Equations
2. **Observing a Market for Anonymity**
3. How to Price Anonymity

Acknowledgement: Part of the material in this talk is joint work with Malte Möser and Daniel G. Arce.

The Mixing Principle

Establish **unlinkability** of messages in communication systems.



- Collect batches
- Randomize order
- Re-encrypt

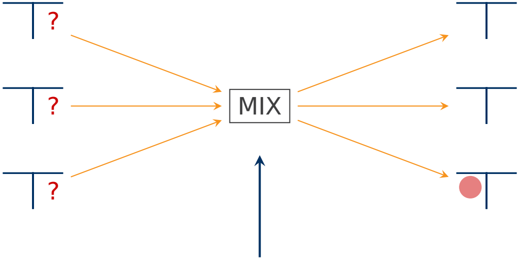
“One cannot be anonymous alone.”

The size of the **anonymity set** $|S|$ is a measure of privacy.

Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *CACM*, 24 (2), 1981, pp. 84–88.

Application of the Mixing Principle to Bitcoin

Establish unlinkability of flows in **transaction systems**.

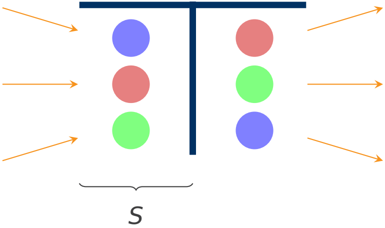


belongs to the ecosystem

Requires substantial **trust** in mix operator.

“CoinJoin” Transactions

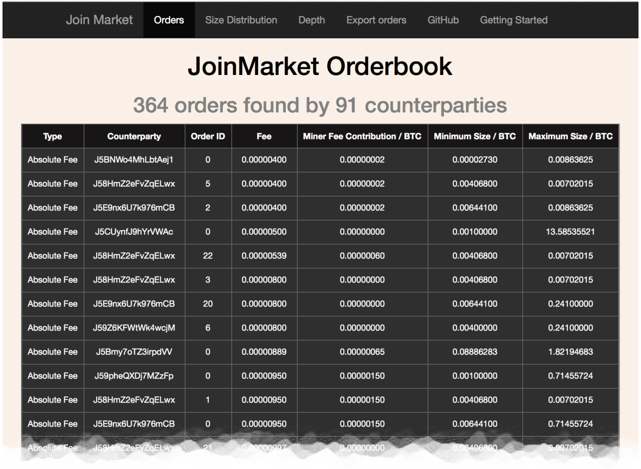
Bitcoin’s **transaction logic** allows multiple inputs and outputs.



More secure alternative: all participants must sign the transaction.

Maxwell 2013

Matchmaking for CoinJoins



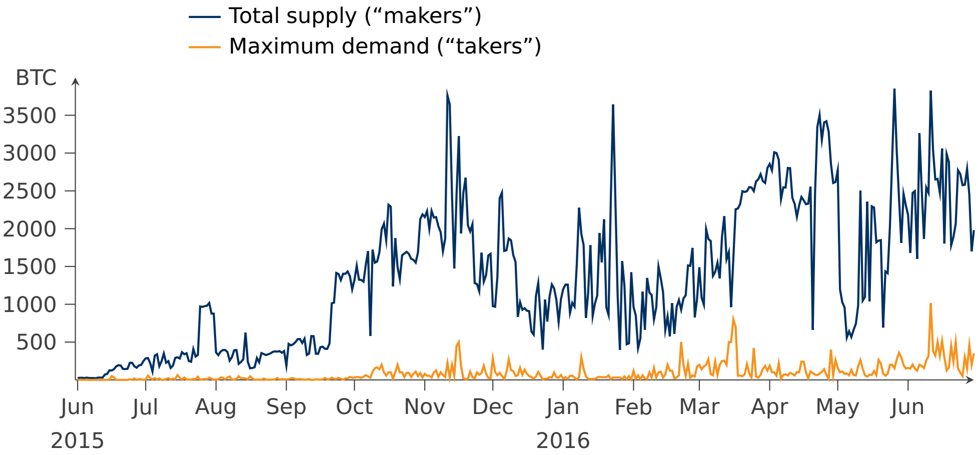
JoinMarket Orderbook

364 orders found by 91 counterparties

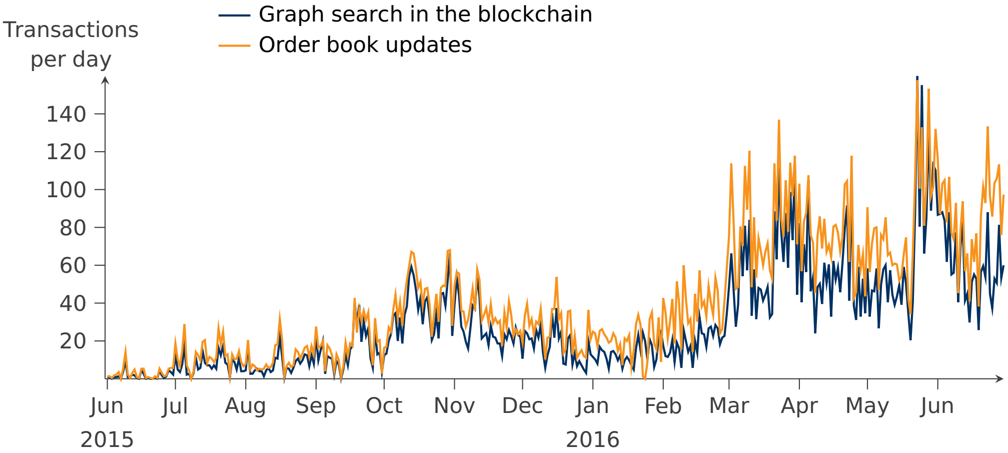
Type	Counterparty	Order ID	Fee	Miner Fee Contribution / BTC	Minimum Size / BTC	Maximum Size / BTC
Absolute Fee	J5BNWo4MhLbtAej1	0	0.00000400	0.00000002	0.00002730	0.00863625
Absolute Fee	J58HmZ2eFvZqELwx	5	0.00000400	0.00000002	0.00406800	0.00702015
Absolute Fee	J5E9nx6U7k976mCB	2	0.00000400	0.00000002	0.00644100	0.00863625
Absolute Fee	J5CUynfJ9hYrVWAc	0	0.00000500	0.00000000	0.00100000	13.58535521
Absolute Fee	J58HmZ2eFvZqELwx	22	0.00000539	0.00000060	0.00406800	0.00702015
Absolute Fee	J58HmZ2eFvZqELwx	3	0.00000800	0.00000000	0.00406800	0.00702015
Absolute Fee	J5E9nx6U7k976mCB	20	0.00000800	0.00000000	0.00644100	0.24100000
Absolute Fee	J59Z6KFWtWk4wcjM	6	0.00000800	0.00000000	0.00400000	0.24100000
Absolute Fee	J5Bmy7oTZ3irpdVV	0	0.00000889	0.00000065	0.08886283	1.82194683
Absolute Fee	J59pheQXDj7MZzFp	0	0.00000950	0.00000150	0.00100000	0.71455724
Absolute Fee	J58HmZ2eFvZqELwx	1	0.00000950	0.00000150	0.00406800	0.00702015
Absolute Fee	J5E9nx6U7k976mCB	0	0.00000950	0.00000150	0.00644100	0.71455724
Absolute Fee	J58HmZ2eFvZqELwx	21	0.00000997	0.00000000	0.00406800	0.00702015

http://joinmarket.io, last access: February 25th, 2018

Supply and Demand

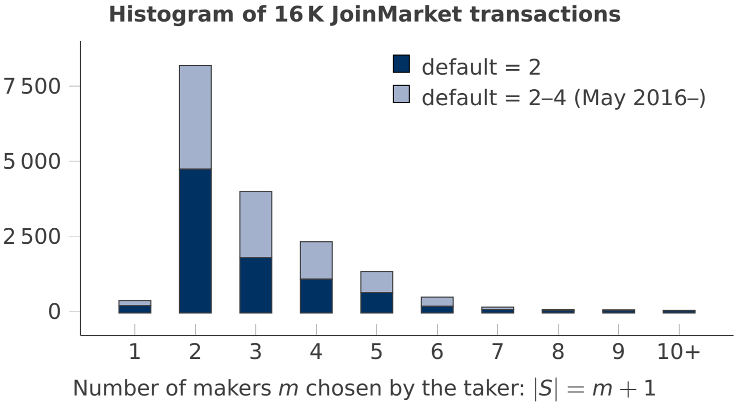


Identifying JoinMarket Transactions

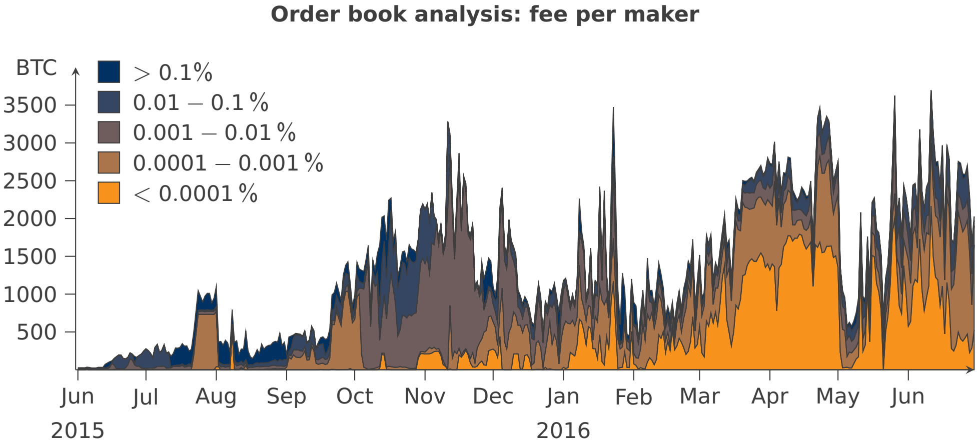


Size of the Anonymity Set

S is composed of exactly one **“taker”** and $m \geq 1$ **“makers”**.



Empirical Prices of Anonymity



For comparison: mix operators charge 1–3 %.

Möser et al. 2013

Outline

1. How to Plug Privacy into Economic Equations
2. Observing a Market for Anonymity
3. **How to Price Anonymity**

Acknowledgement: Part of the material in this talk is joint work with Malte Möser and Daniel G. Arce.

Anonymity Market

“One cannot be anonymous alone.”

Cooperative game theory to model the co-creation of anonymity.

Model

- 1 “taker” and $m \geq 1$ “makers”
- **Only the taker pays** for anonymity: fee f to each maker.
- The taker **and all makers benefit** from anonymity set, $|S| = m + 1$.
- Taker has an outside option, e. g., a mix charging fee $F \gg f$.
- Solve for f endogenously.

$\rightarrow$ **Shapley value as solution concept.**

Utility of Anonymity

Assumption: the attacker guesses within the anonymity set (i. e., GPA)

Case 1: coalition with makers

Taker expects: $D \cdot \frac{m}{m+1}$

Maker expects: $d \cdot \frac{m}{m+1}$

$D \gg d$

Case 2: outside option

Taker expects: $\delta \cdot D$

Maker receives: 0

$\delta \in (0, 1)$

Solution for $m = 2$ Makers (sketch)

Characteristic function V

$$V(\{t\}) = \{x_t \mid x_t \leq \delta D - F\} \tag{1}$$

$$V(\{i\}) = \{x_i \mid x_i \leq 0 : i = 1, 2\} \tag{2}$$

$$V(\{t, 1\}) = \{(x_t, x_1) \mid x_t \leq {}^{D}\!/_{2} - f, x_1 \leq {}^{d}\!/_{2} + f\} \tag{3}$$

$$V(\{t, 2\}) = \{(x_t, x_2) \mid x_t \leq {}^{D}\!/_{2} - f, x_2 \leq {}^{d}\!/_{2} + f\} \tag{4}$$

$$V(\{1, 2\}) = \{(x_1, x_2) \mid x_1 \leq 0, x_2 \leq 0\} \tag{5}$$

$$V(\{t, 1, 2\}) = \{(x_t, x_1, x_2) \mid x_t \leq {}^{2}\!/_{3}D - 2f, x_{1,2} \leq {}^{2}\!/_{3}d + f\} \tag{6}$$

D, d: value of anonymity for taker/maker; f: fee per maker; δ, F: quality/fee of outside option

Solution for $m = 2$ Makers (sketch, cont'd)

Worth function ω

$$\omega(\{t\}) = \delta D - F \tag{7}$$

$$\omega(\{1\}) = \omega(\{2\}) = 0 \tag{8}$$

$$\omega(\{t,1\}) = {}^{D}\!/_{2} + {}^{d}\!/_{2} \tag{9}$$

$$\omega(\{t,2\}) = {}^{D}\!/_{2} + {}^{d}\!/_{2} \tag{10}$$

$$\omega(\{1,2\}) = 0 \tag{11}$$

$$\omega(\{t,1,2\}) = {}^{2}\!/_{3}D + {}^{4}\!/_{3}d \tag{12}$$

D, d: value of anonymity for taker/maker; δ, F: quality/fee of outside option

Shapley Value and Associated Fee f

Shapley value φ

$$\varphi_t = \frac{14}{36}D + \frac{22}{36}d + \frac{1}{3}(\delta D - F) \tag{13}$$

$$\varphi_1 = \varphi_2 = \frac{5}{36}D + \frac{13}{36}d - \frac{1}{6}(\delta D - F) \tag{14}$$

“The Price of Anonymity”

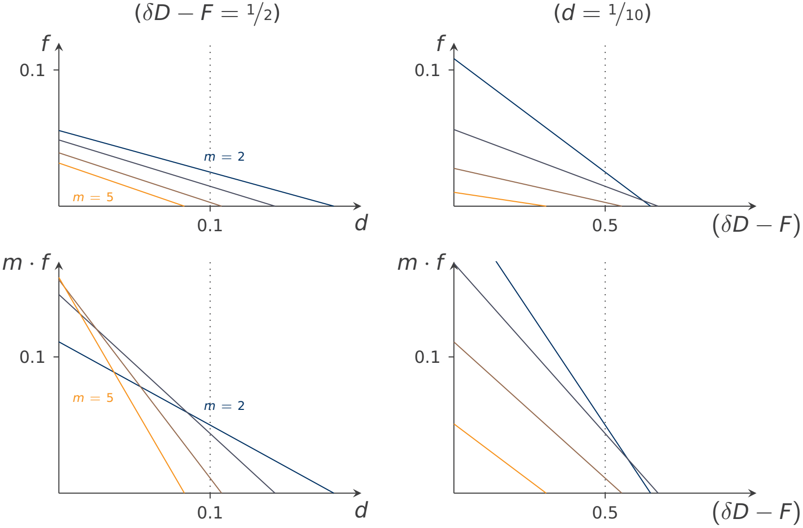
$$f = \frac{5}{36}D - \frac{11}{36}d - \frac{1}{6}(\delta D - F) \tag{15}$$

$\rightarrow$ **General solution** for $m > 2$ is efficiently computable.

D, d: value of anonymity for taker/maker; f: fee per maker; δ, F: quality/fee of outside option

Visualization

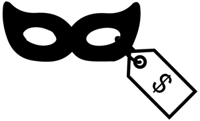
Normalization: $D = 1$



$(\delta D - F = 1/2)$

$(d = 1/10)$

Upshot



We have introduced an NTU cooperative game-theoretic model of a CoinJoin anonymity market that is consistent with:

1. The prevalent measure of anonymity: the **anonymity set**.
2. The **peculiar nature** of anonymity markets:

   One demand-side participant (the ‘taker’) pays for anonymity but all suppliers (the ‘makers’) **also** receive the good in demand (anonymity).

Take-Home Messages

1. Blockchain data is (almost always) personal data.
2. It is possible (but not trivial) to plug privacy into a utility function.
3. Forgotten objective in protocol design: incentivize privacy-enhancing behavior.
4. Blockchain systems are crystal balls for studying the economics of privacy.

universität
innsbruck

Privacy and Economics

The Swiss Blockchain Winter School, Interlaken, 2019

Thank you for your attention.

Talk, research visit, post-doc ? rainer.boehme @ uibk.ac.at

Further Reading

1. Möser, M. and Böhme, R. The Price of Anonymity: Empirical Evidence from a Market for Bitcoin Anonymization. *Journal of Cybersecurity*, 3, 2 (2017), 127–135.
2. Arce, D. G. and Böhme, R. Pricing Anonymity. In S. Meiklejohn and K. Sako, eds., *Financial Cryptography and Data Security*. 2018.
3. Abramova, S., Schöttle, P., and Böhme, R. Mixing Coins of Different Quality: A Game-Theoretic Approach. In *Financial Cryptography (4th Workshop on Bitcoin and Blockchain Research)*. Malta, 2017.
4. Acquisti, A., Taylor, C., and Wagman, L. The Economics of Privacy. *Journal of Economics Literature*, 54, 6 (2016), 442–292.
5. Böhme, R., Christin, N., Edelman, B., and Moore, T. Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29, 2 (2015), 213–238.

The Shapley Value Solution for *m* Makers

After overcoming some technical hurdles, e. g., specifying $\omega : V(\hat{S}) \to \mathbb{R}$, the **fees** of the Shapley value solution for *m* makers are:

$$f = \frac{1}{(m+1)}D - \frac{D}{m\,(m+1)}\sum_{n=1}^{m}\frac{n}{n+1} - \frac{d}{m\,(m+1)}\sum_{n=1}^{m}\frac{n^2}{n+1} + \frac{F - \delta D}{m\,(m+1)}$$

(A formula replacing the finite sums with harmonic numbers is given in the paper.)

- Increasing in *D*.
- Increasing in *F*.
- Decreasing in *d*.
- Theoretical lower bound for identifying dishonest makers.
- Experimentally/behaviorally testable by endowing subjects with *D*, *d*, δ and *F* values.