

Identifying Bitcoin Users by Transaction Behavior

SPIE DSS 2015

John V. Monaco

Pace University, NY

April 22, 2015

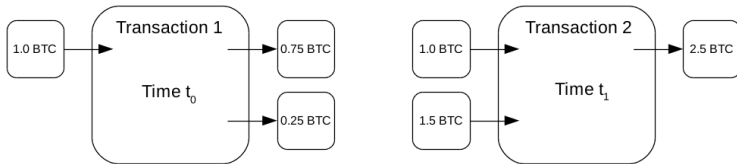
Outline

- 1 Introduction
- 2 Methodology
- 3 Experimental results
- 4 Hypothesis testing
- 5 Conclusions

Bitcoin.



Bitcoin transaction.



Transaction features.

- Inter-event time (time between transactions)
- Hour of day
- Time of day
- Time of hour
- Coin flow (BTC value lost or gained by the user)
- Input/output balance (no. outputs - no. inputs)

Why timestamps?

Timestamped events as a behavioral biometric

- Timestamps are truly ubiquitous
- Timestamps are persistent
- They're resilient to encryption and masking
- They can be incorporated into domain-specific models

Empirical data.

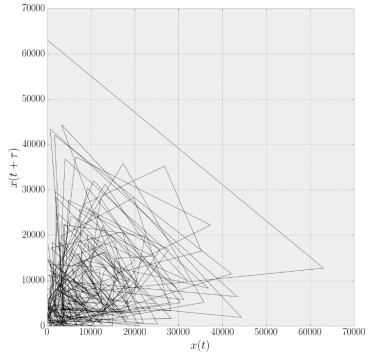
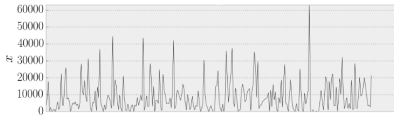
- Blockchain 230686 (transactions through April 7, 2013)
 - 6.3M vertices, 37.4M edges
- Subset for this work
 - Month-long samples that contain between 100 and 1000 outgoing transactions
 - 61 users, 6 samples each

Preprocessing.

- Collapse the transaction network into a user network through proof of ownership
- For each sample, get a time series for each feature

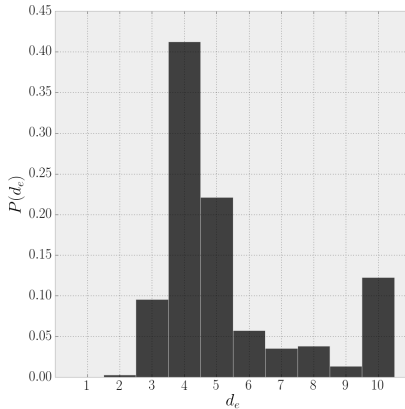
Phase space reconstruction.

- Takens' Theorem

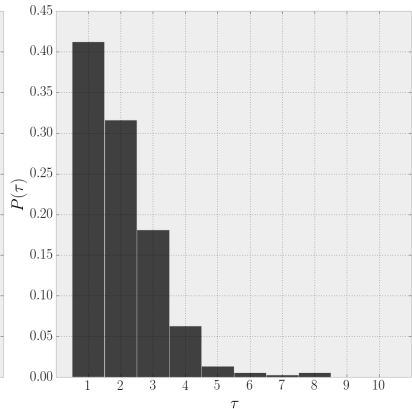


Embedding parameters.

Embedding dimension

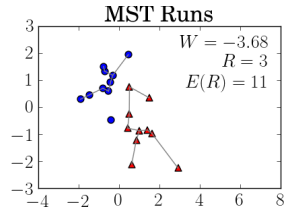
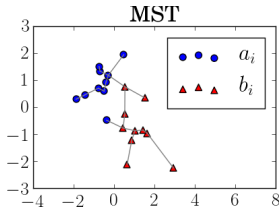
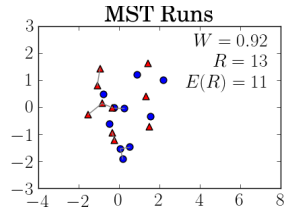
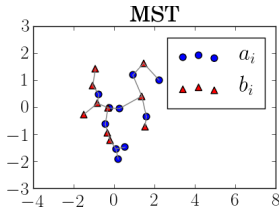


Time lag



Classification.

Multivariate Wald-Wolfowitz Test as a similarity measure in a linear-weighted kNN



Timing information only.

	ACC1(%)	EER(%)
Inter-event time	30.3	22.6
Hour of day	25.1	24.8
Time of hour	4.4	48.8
Time of day	21.0	27.5

Multiple features.

Outgoing transactions

- inter-event time
- hour of day

Outgoing/incoming transactions

- coin flow
- input output balance

76% ACC1

6.8% EER

Testing procedure.

- Surrogate data testing, Monte Carlo method
- Generate samples under a null hypothesis
 - (e.g. the data is random)
- Compare the observed test statistic to surrogate test statistics
- For each H_0 , perform 3 tests per sample using 3 different test statistics
 - Nonlinear prediction error
 - Mutual information
 - Proportion of false nearest neighbors

Is the data random?

- Generate surrogates by shuffling the data
 - Random permutations destroy any structure
- 85% samples rejected at least one test
- 43% samples rejected all 3 tests
- Conclusion: some transaction histories are random

Is the data linear?

- Generate surrogates by the Amplitude Adjusted Truncated Fourier Transform (AATFT)
 - The AATFT destroys any non-linear correlation and preserves the empirical amplitude distribution
- 78% samples rejected at least one test
- 31% samples rejected all 3 tests
- Conclusion: some transaction histories can be described by a linear stochastic process

Summary.

- Identification and verification by financial transaction behavior?
 - Maybe
- Worth exploring further?
 - Yes
- Next steps?
 - Generative model

Thank you.

Thank you