Improving Privacy of Blockchains

Emily Schaefer

Computer Science Senior Seminar
Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

November 18th, 2017

Introduction

Blockchains were proposed by Satoshi Nakamoto in 2008

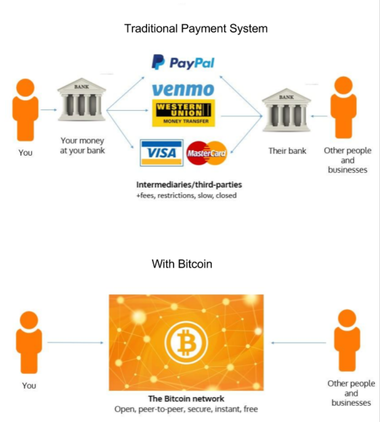
Founded Bitcoin in 2009

Bitcoin is a currency and an electronic cash system without the use of third parties using blockchains

Increasing in popularity

Introduction

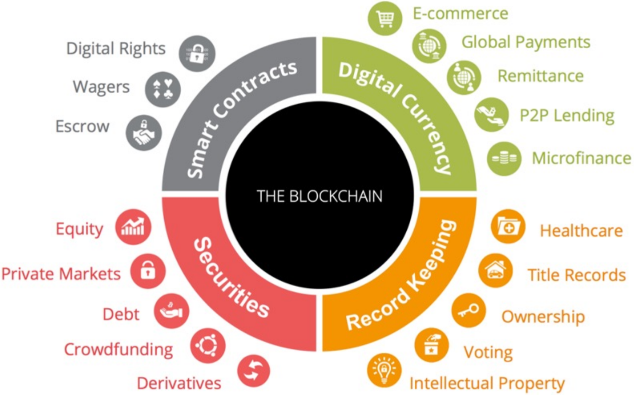
Decentralized



Modified from http://cryptorials.io/real-power-bitcoin-lie-purchasing-power-vs-remittance/

Introduction

There are many variations and applications for blockchains!



https://datafloq.com/read/what-is-the-blockchain-and-why-is-it-so-important/2270

Outline

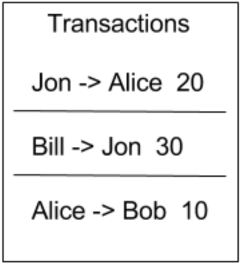
1. Overview of Blockchains
2. Cryptography Background
3. Bitcoin's Blockchain Protocol
4. Improving Privacy of Blockchains

Outline

1. Overview of Blockchains
   - What are Blockchains?
   - Blockchain Characteristics
2. Cryptography Background
3. Bitcoin's Blockchain Protocol
4. Improving Privacy of Blockchains

What are Blockchains?

A blockchain is a record of financial transactions that is made up of a chain of blocks. Each block contains transactions and is in chronological order.



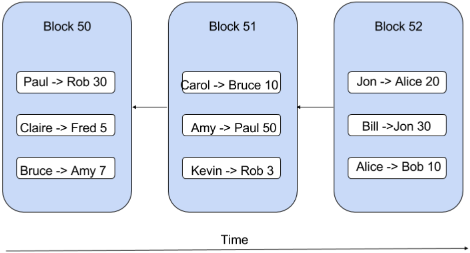
Transactions

Jon -> Alice 20

Bill -> Jon 30

Alice -> Bob 10

Based on https://www.linkedin.com/pulse/blockchain-breathes-mastermind-group-computers-ajitesh-kumar



Block 50

Paul -> Rob 30

Claire -> Fred 5

Bruce -> Amy 7

Block 51

Carol -> Bruce 10

Amy -> Paul 50

Kevin -> Rob 3

Block 52

Jon -> Alice 20

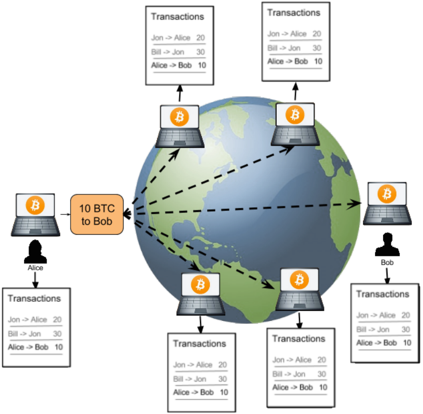
Bill ->Jon 30

Alice -> Bob 10

Time

Blockchain Characteristics

- Public
- Pseudonymous
- Distributed
- Peer-to-Peer



Modified from https://www.linkedin.com/pulse/blockchain-breathes-mastermind-group-computers-ajitesh-kumar

Outline

1. Overview of Blockchains
2. Cryptography Background
   - Public-Key Cryptography
   - Hash Function
   - Digital Signature
3. Bitcoin's Blockchain Protocol
4. Improving Privacy of Blockchains

Public-Key Cryptography

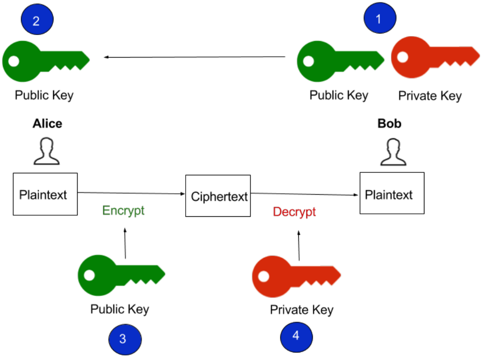
Cryptography is the study of secure communication of messages between two parties to prevent third parties from viewing the message.

- Encryption means converting a message in plaintext to ciphertext
- Decryption means decoding the ciphertext back to plaintext
- Involves public key and private key pair
- Public key is used for encryption and private key is used for decryption

Public-Key Cryptography

1. Bob generates a public and private key pair
2. Bob's public key is published
3. Alice encrypts her message with Bob's public key
4. Bob decrypts Alice's message with his private key to get Alice's original message

Example of Alice sending Bob a message



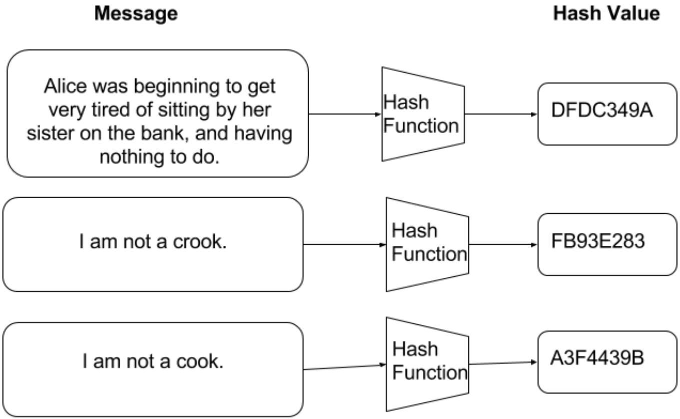
Hash Function

A hash function takes an arbitrary sized input and produces a string of a fixed length called a hash value.

Features:

1. It is easy to compute the hash value of a message
2. Given the hash value, it is impossible to find the original message
3. Two identical messages result in the same hash value
4. Two different messages do not result in the same hash value

Hash Function



Based off of Christof Paar et al, "Understanding Cryptography" (2010)

Digital Signature

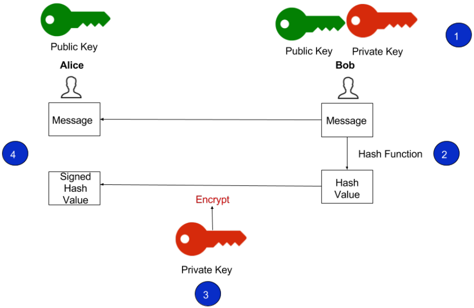
- What is a digital signature?
  It is similar to a handwritten signature to show approval of a transaction.
- General Overview: a sender signs the message by encrypting it with their private key and the receiver verifies the signature by decrypting with the corresponding public key.
- 2 Parts:
  - Signing
  - Verification

Digital Signature

Signing

1. Bob has a public and private key pair
2. A hash value is generated from Bob's message
3. Bob signs the hash value by encrypting it with his private key
4. The message and Bob's digital signature of the hash value are sent to Alice

Bob digitally signing a message to Alice

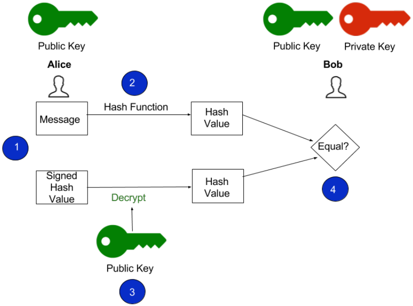


Digital Signature

Verification

1. Alice has Bob's message, signed hash value, and public key
2. Alice computes the hash value of Bob's message
3. Alice decrypts the signed hash value using Bob's public key
4. If the hash values are equal the signature is validated

Bob digitally signing a message to Alice

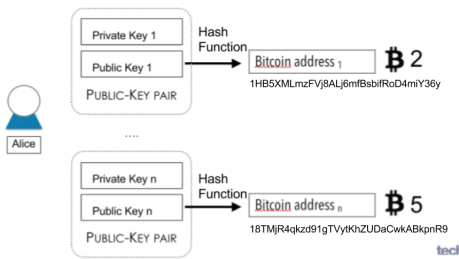


Outline

1. Overview of Blockchains
2. Cryptography Background
3. Bitcoin's Blockchain Protocol
    - Addresses
    - Transactions
    - Bitcoin Mining
4. Improving Privacy of Blockchains

Addresses

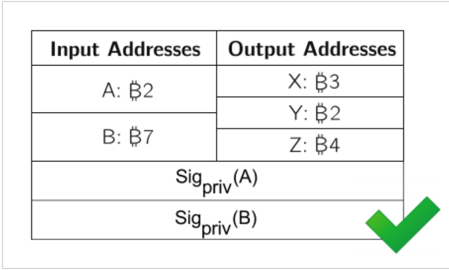
- Users perform transactions with public and private keys
- The address is the hash value of the users public key and is used to send and receive payments
- Users have several addresses with each having a Bitcoin amount associated with them
- A user's private key is used to sign transactions



Modified from http://tech.eu/features/808/bitcoin-part-one/

Transactions

- Transactions are from the sender's address to the receiver's address
- The input address is the sender's address
- The output address is the receiver's address
- The input addresses are digitally signed



Input Addresses	Output Addresses
A: ₿2	X: ₿3
	Y: ₿2
B: ₿7	Z: ₿4
$\text{Sig}_{\text{priv}}(\text{A})$	
$\text{Sig}_{\text{priv}}(\text{B})$	✓

Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

Bitcoin Mining

Mining is the process of adding blocks containing unconfirmed transactions to the blockchain.

Proof-of-work: Adding blocks to the blockchain should be difficult but verifying blocks should be easy.

Users called miners complete a resource-intensive task in proof-of-work.

2 parts:

- Resource-intensive task
- Verifying resource-intensive task to add a block to the blockchain

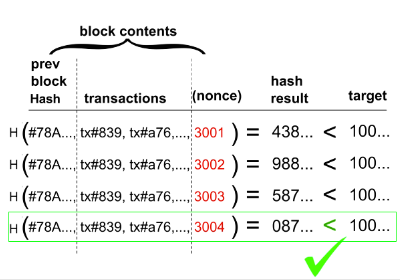
Bitcoin Mining

Resource-intensive task

Nonce: a random number

Resource-intensive task: find a nonce value that when hashed with the previous block hash value and the unconfirmed transactions results in a hash result less than a target number

Strategy: Brute force



	block contents						
	prev block Hash	transactions	(nonce)		hash result		target
H (	#78A...,	tx#839, tx#a76,...,	3001	) =	438...	<	100...
H (	#78A...,	tx#839, tx#a76,...,	3002	) =	988...	<	100...
H (	#78A...,	tx#839, tx#a76,...,	3003	) =	587...	<	100...
H (	#78A...,	tx#839, tx#a76,...,	3004	) =	087...	<	100... ✓

Modified from
http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

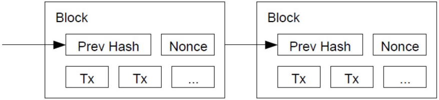
Bitcoin Mining

Verifying and Adding block

Block is broadcasted to all nodes in the Bitcoin Network

Nodes check the validity of the block by checking the hash computation of the block

If the nodes come to the consensus that it is valid, the block is added to the growing blockchain on each node.



Modified from https://promarket.org/expect-within-next-10-years-probably-half-banks-will-gone/

Outline

1. Overview of Blockchains
2. Cryptography Background
3. Bitcoin's Blockchain Protocol
4. Improving Privacy of Blockchains
   - Privacy Overview
   - Bitcoin Mixing
   - CoinShuffle Protocol
   - CoinShuffle Privacy Analysis

Privacy Overview

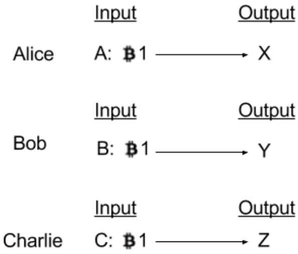
Blockchains are public and therefore transactions are public

Current Privacy: The use of pseudonymous addresses

Privacy Concerns: Once addresses are used, all transactions associated with them can be traced.

Bitcoin Mixing

Combines multiple transactions into one transaction by mixing Bitcoins with other users to make input and output addresses unlinkable.



Input Output

Alice A: ₿1 → X

Input Output

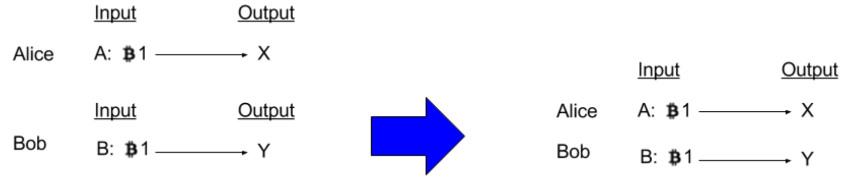
Bob B: ₿1 → Y

Input Output

Charlie C: ₿1 → Z

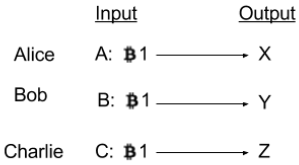
Bitcoin Mixing

Combines multiple transactions into one transaction by mixing Bitcoins with other users to make input and output addresses unlinkable.



Bitcoin Mixing

Combines multiple transactions into one transaction by mixing Bitcoins with other users to make input and output addresses unlinkable.



Input Output

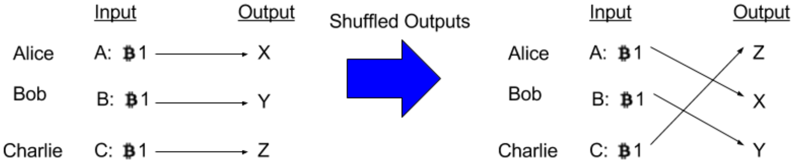
Alice A: ฿1 → X

Bob B: ฿1 → Y

Charlie C: ฿1 → Z

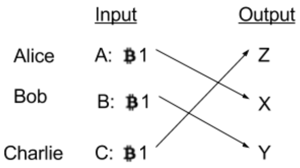
Bitcoin Mixing

Combines multiple transactions into one transaction by mixing Bitcoins with other users to make input and output addresses unlinkable.



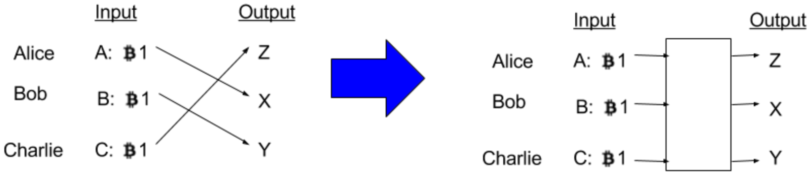
Bitcoin Mixing

Combines multiple transactions into one transaction by mixing Bitcoins with other users to make input and output addresses unlinkable.



Bitcoin Mixing

Combines multiple transactions into one transaction by mixing Bitcoins with other users to make input and output addresses unlinkable.



CoinShuffle Protocol

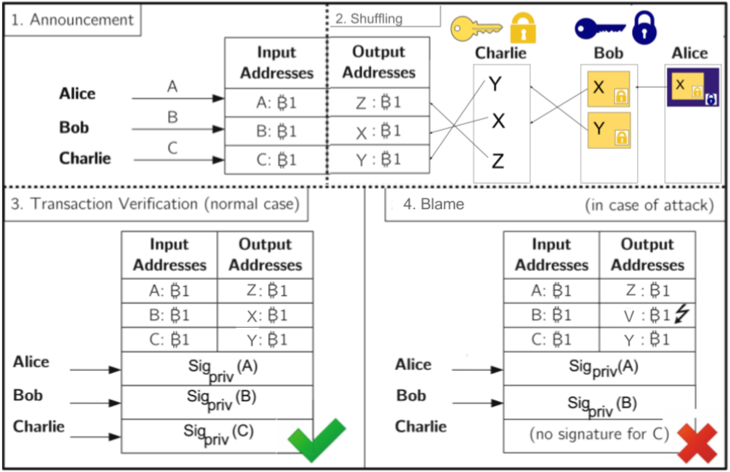
CoinShuffle Protocol

- Announcement
- Shuffling
- Transaction Verification
- Blame

Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

CoinShuffle Protocol

Protocol



1. Announcement

Input Addresses	Output Addresses
A: ₿1	Z : ₿1
B: ₿1	X : ₿1
C: ₿1	Y : ₿1

3. Transaction Verification (normal case)

Input Addresses	Output Addresses
A: ₿1	Z: ₿1
B: ₿1	X: ₿1
C: ₿1	Y: ₿1
Sig_{priv} (A)	
Sig_{priv} (B)	
Sig_{priv} (C)	

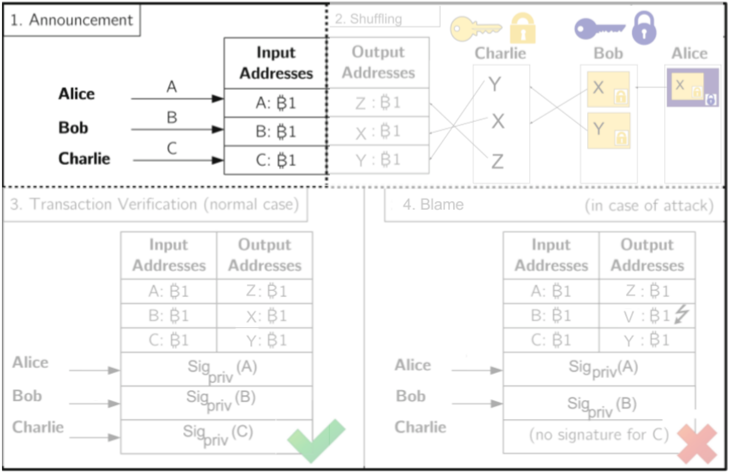
4. Blame (in case of attack)

Input Addresses	Output Addresses
A: ₿1	Z : ₿1
B: ₿1	V : ₿1 ⚡
C: ₿1	Y : ₿1
Sig_{priv}(A)	
Sig_{priv} (B)	
(no signature for C)	

Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

CoinShuffle Protocol

Announcement



Input Addresses	Output Addresses
A: ₿1	Z : ₿1
B: ₿1	X : ₿1
C: ₿1	Y : ₿1

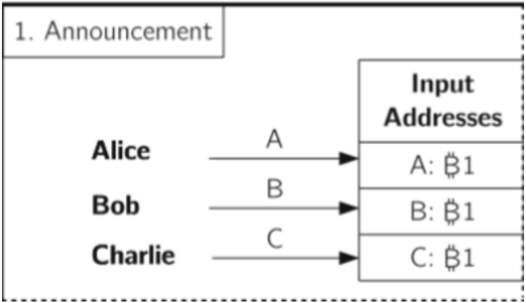
Input Addresses	Output Addresses
A: ₿1	Z: ₿1
B: ₿1	X: ₿1
C: ₿1	Y: ₿1
Sig$_{priv}$ (A)	
Sig$_{priv}$ (B)	
Sig$_{priv}$ (C)	

Input Addresses	Output Addresses
A: ₿1	Z : ₿1
B: ₿1	V : ₿1 ⚡
C: ₿1	Y : ₿1
Sig$_{priv}$(A)	
Sig$_{priv}$ (B)	
(no signature for C)	

Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

CoinShuffle Protocol

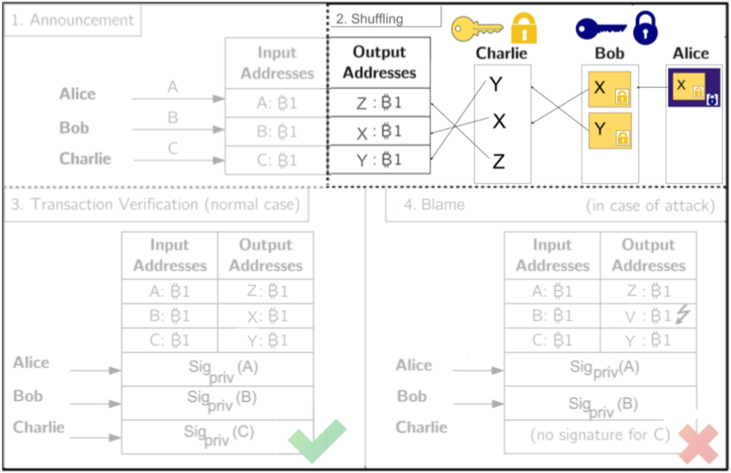
Announcement



Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

CoinShuffle Protocol

Announcement



Input Addresses	Output Addresses
A: ₿1	Z : ₿1
B: ₿1	X : ₿1
C: ₿1	Y : ₿1

Input Addresses	Output Addresses
A: ₿1	Z: ₿1
B: ₿1	X: ₿1
C: ₿1	Y: ₿1
$\mathrm{Sig}_{\mathrm{priv}}$ (A)	
$\mathrm{Sig}_{\mathrm{priv}}$ (B)	
$\mathrm{Sig}_{\mathrm{priv}}$ (C)	

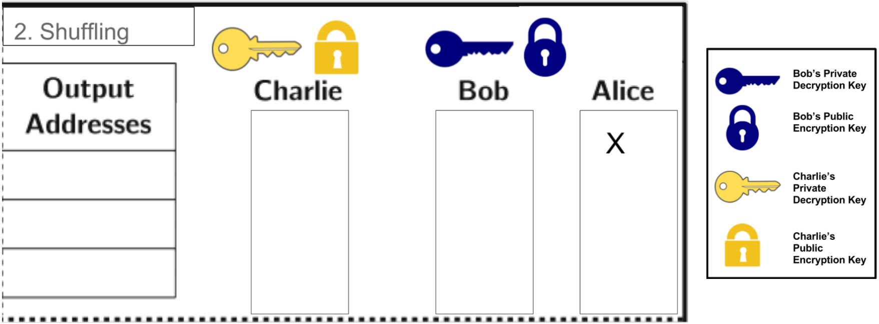
Input Addresses	Output Addresses
A: ₿1	Z : ₿1
B: ₿1	V : ₿1 ⚡
C: ₿1	Y : ₿1
$\mathrm{Sig}_{\mathrm{priv}}$(A)	
$\mathrm{Sig}_{\mathrm{priv}}$ (B)	
(no signature for C)	

Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

CoinShuffle Protocol

Shuffling

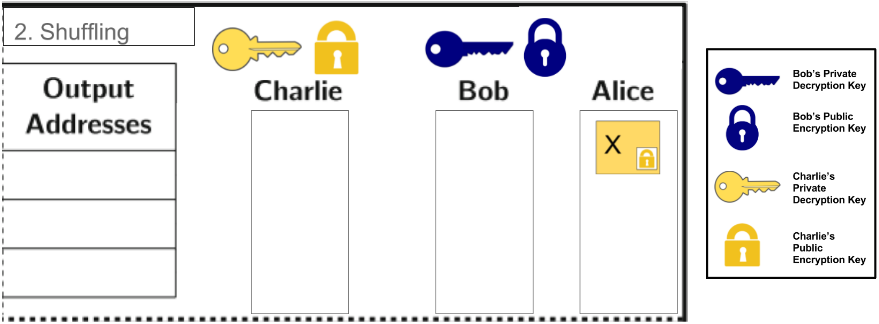
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

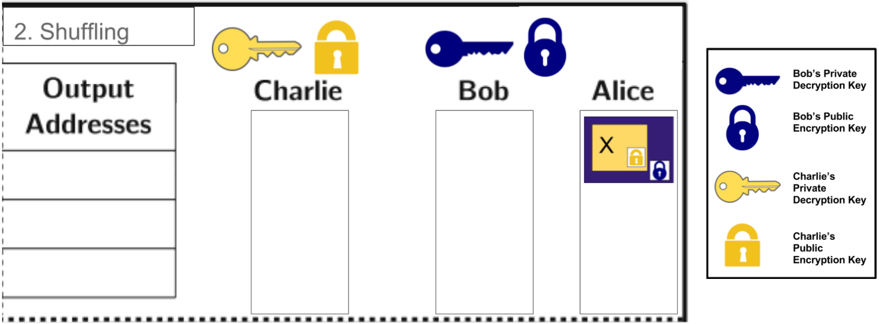
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

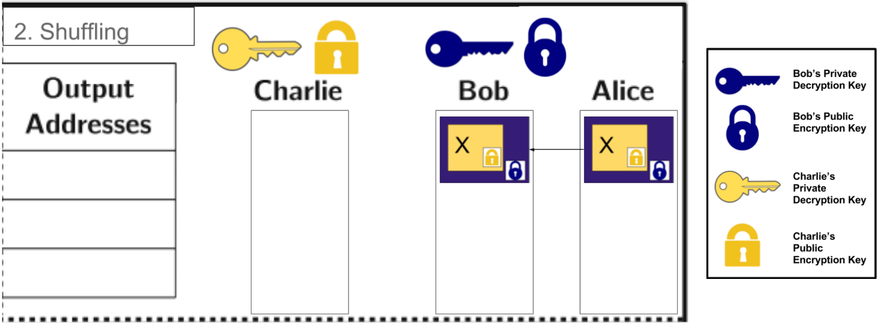
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

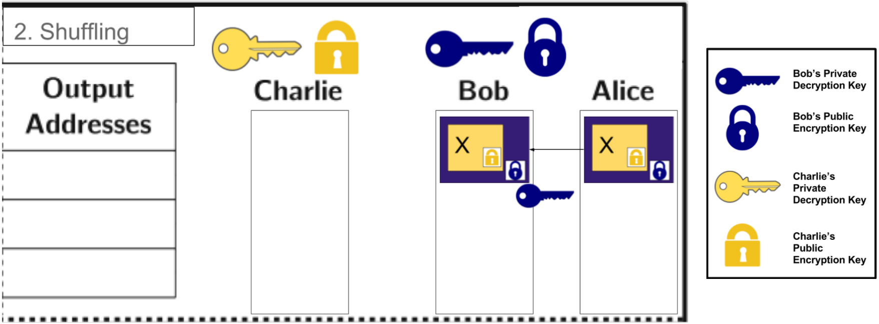
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
X
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

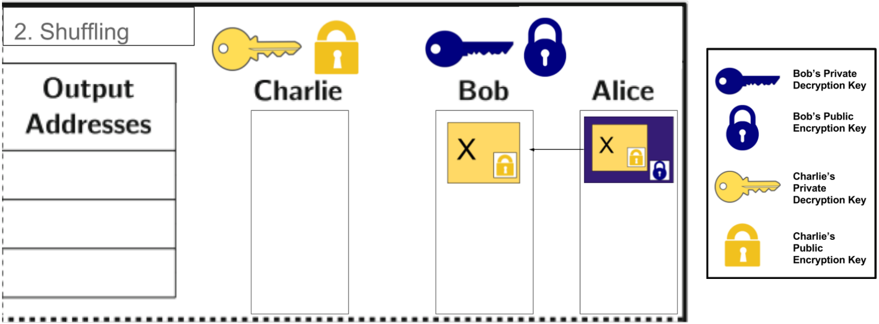
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
X
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

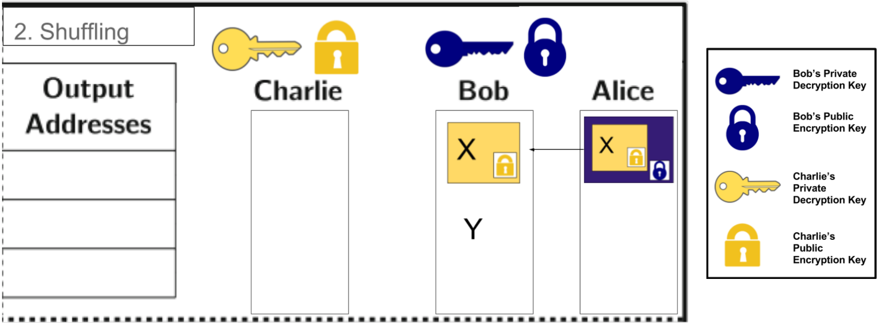
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
X
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

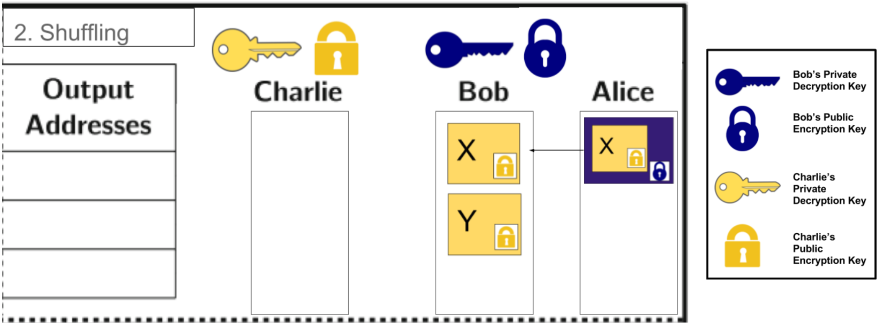
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
X
Y
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

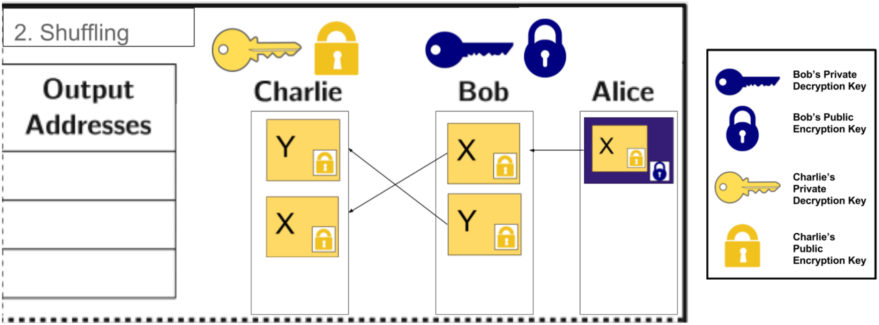
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
X
Y
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

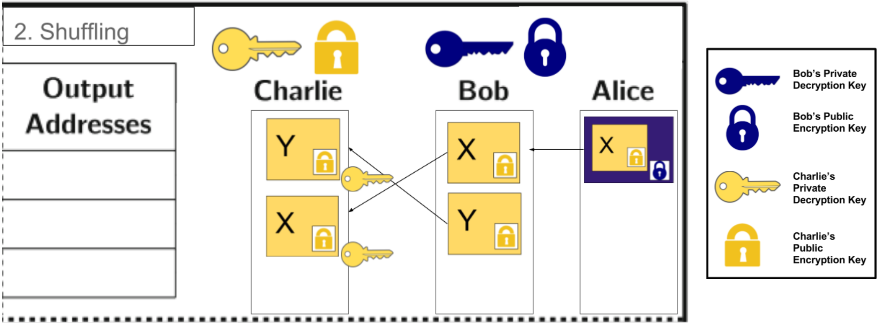
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
Y
X
X
Y
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

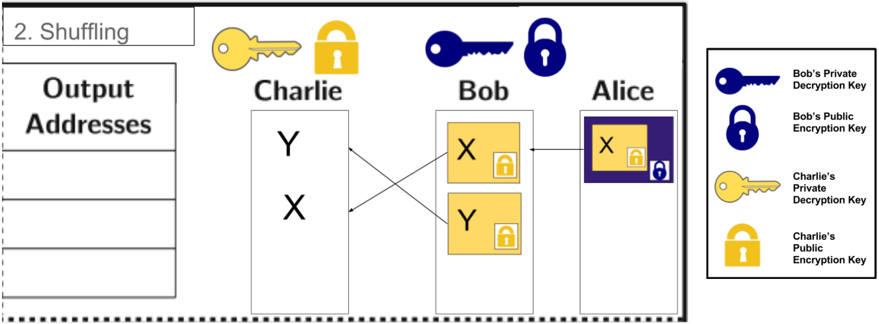
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
Y
X
X
Y
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

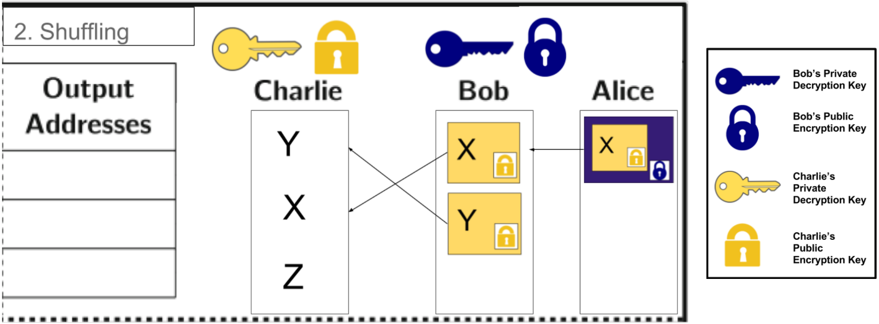
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
Y
X
X
Y
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

Shuffling

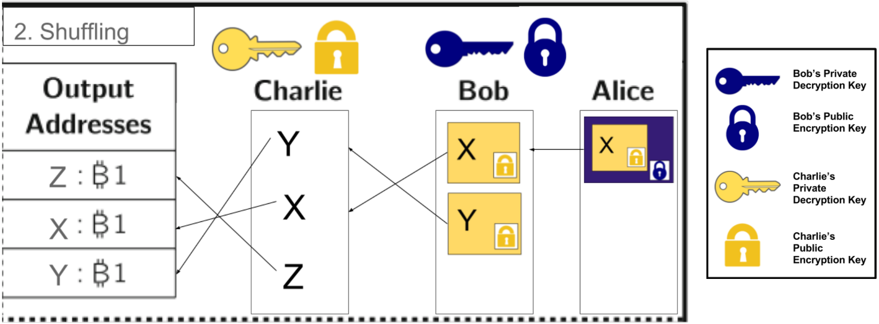
Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Charlie
Bob
Alice
Y
X
Z
X
Y
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

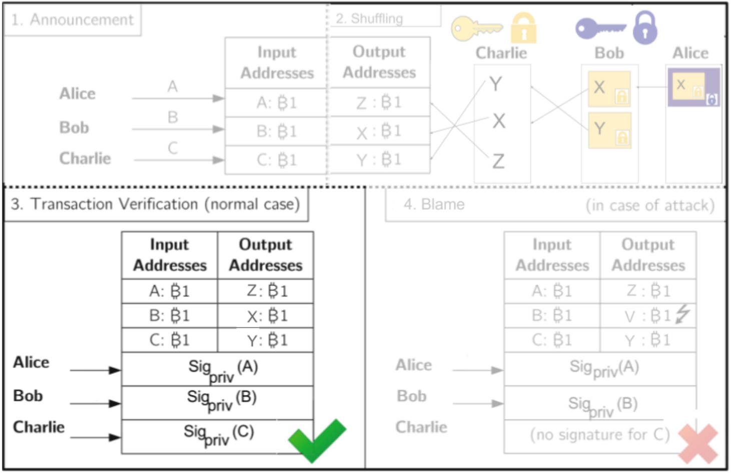
Shuffling

Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)


2. Shuffling
Output Addresses
Z : ₿1
X : ₿1
Y : ₿1
Charlie
Y
X
Z
Bob
X
Y
Alice
X
Bob's Private Decryption Key
Bob's Public Encryption Key
Charlie's Private Decryption Key
Charlie's Public Encryption Key

CoinShuffle Protocol

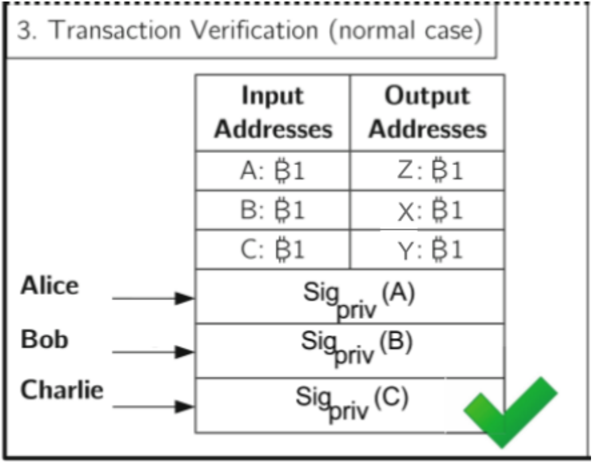
Transaction Verification



Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

CoinShuffle Protocol

Transaction Verification



3. Transaction Verification (normal case)

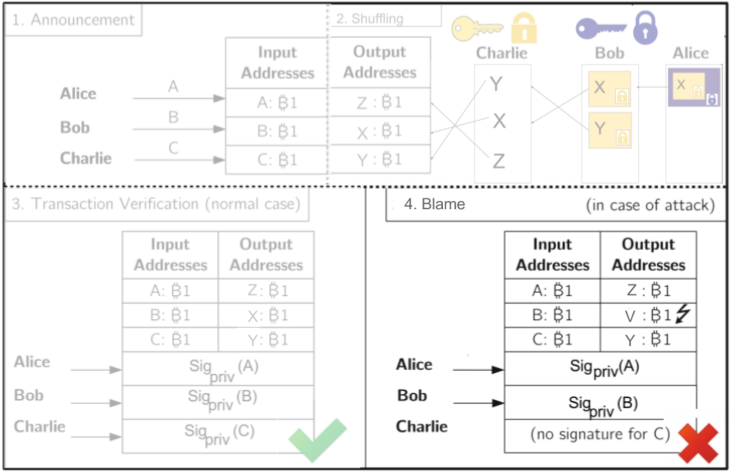
Input Addresses	Output Addresses
A: ₿1	Z: ₿1
B: ₿1	X: ₿1
C: ₿1	Y: ₿1

Alice
Bob
Charlie
Sig_{priv} (A)
Sig_{priv} (B)
Sig_{priv} (C)

Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

CoinShuffle Protocol

Blame



Input Addresses	Output Addresses
A: ₿1	Z : ₿1
B: ₿1	X : ₿1
C: ₿1	Y : ₿1

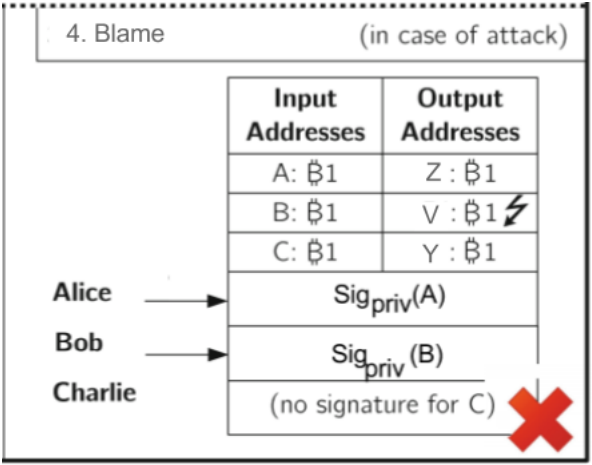
Input Addresses	Output Addresses
A: ₿1	Z: ₿1
B: ₿1	X: ₿1
C: ₿1	Y: ₿1
Alice → Sig$_{priv}$(A)	
Bob → Sig$_{priv}$(B)	
Charlie → Sig$_{priv}$(C)	

Input Addresses	Output Addresses
A: ₿1	Z : ₿1
B: ₿1	V : ₿1 ⚡
C: ₿1	Y : ₿1
Alice → Sig$_{priv}$(A)	
Bob → Sig$_{priv}$(B)	
Charlie → (no signature for C)	

Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

CoinShuffle Protocol

Blame



4. Blame (in case of attack)

Input Addresses	Output Addresses
A: ฿1	Z : ฿1
B: ฿1	V : ฿1 ϟ
C: ฿1	Y : ฿1
Sig$_{priv}$(A)	
Sig$_{priv}$ (B)	
(no signature for C) ✗	

Modified from Tim Ruffing et al, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" (2014)

CoinShuffle Privacy Analysis

The shuffling participants don't learn the relationship between an input address to its corresponding output address.

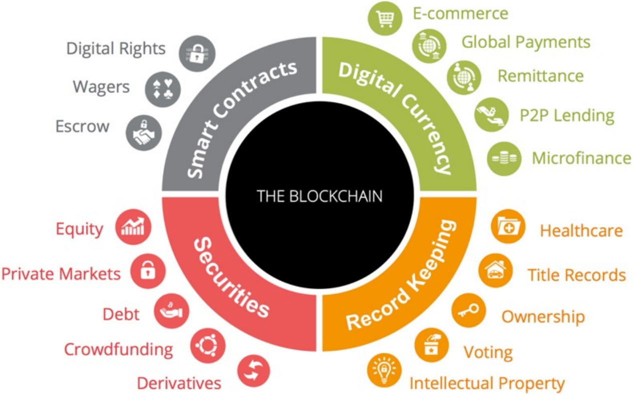
The only information that is shared among participants are:

- Input addresses
- Amount of Bitcoins
- Public encryption key (lock)
- List of shuffled output addresses

Overall: CoinShuffle allows users to combine transactions to mix Bitcoins to decrease the correlation between input and output addresses without giving any additional information to other participants.

Conclusions

Privacy is important in all blockchain uses!



https://datafloq.com/read/what-is-the-blockchain-and-why-is-it-so-important/2270

References I

[1] Elli Androulaki et al. "Evaluating User Privacy in Bitcoin". In: 2015.

[2] Joseph Bonneau et al. "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies". In: 2015.

[3] Damiano Di Francesco Maesa, Andrea Marino, and Laura Ricci. "Uncovering the Bitcoin Blockchain: An Analysis of the Full Users Graph". In: 2016.

[4] Ujan Mukhopadhyay et al. "A brief survey of Cryptocurrency systems". In: 2016.

[5] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system". In: 2008.

[6] Christof Paar and Jan Pelzl. *Understanding Cryptography*. Springer, 2010. ISBN: 978-3-642-04100-6.

[7] Tim RuffingPedro, Moreno-Sanchez, and Aniket Kate. "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin". In: 2014.

References II

[8] Zibin Zheng et al. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends". In: 2017.

Acknowledgements

Thank you for your time and attention!

Special thanks to Elena Machkasova, and K.K. Lamberty for their guidance and feedback.