MONASH University

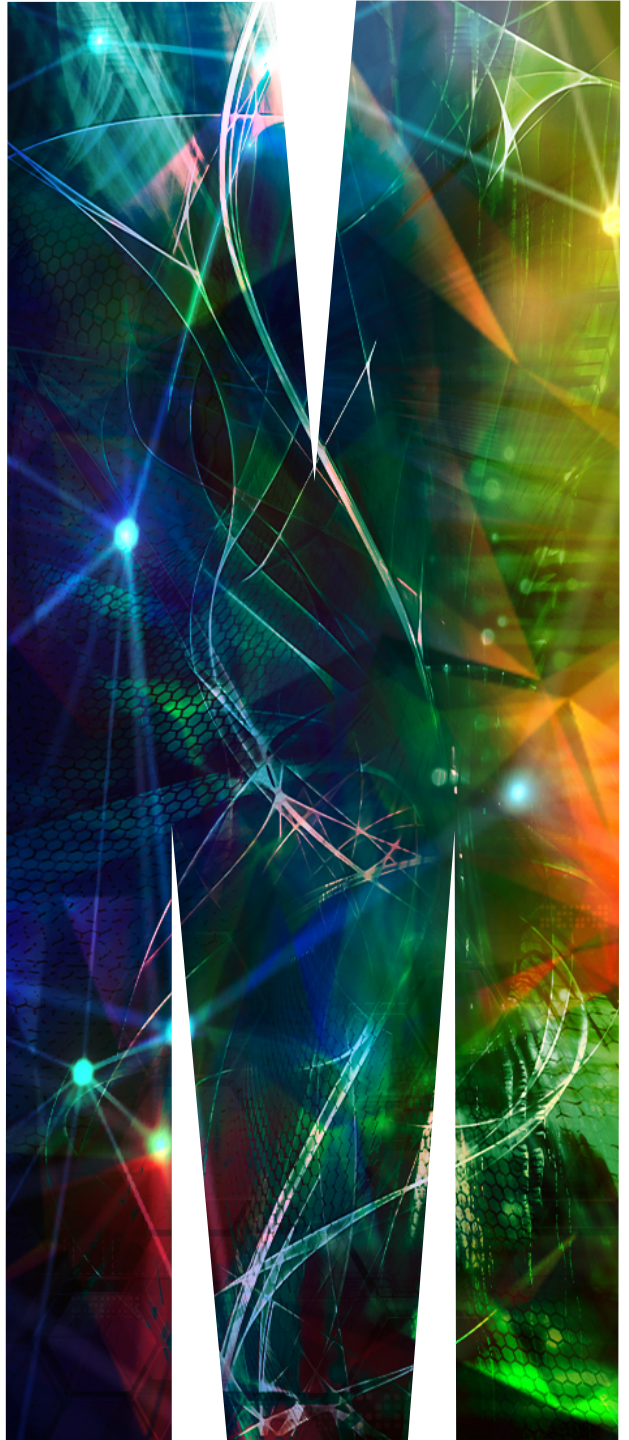
FIT5214: Blockchain

Lecture 8: Privacy

Lecturer: Rafael Dowsley

rafael.dowsley@monash.edu

https://dowsley.net



Unit Structure

- Lecture 1: Introduction to Blockchain
- Lecture 2: Bitcoin
- Lecture 3: Ethereum and Smart Contracts
- Lecture 4: Proof-of-Work (PoW)
- Lecture 5: Attacks on Blockchains
- Lecture 6: Class Test/Alternatives to PoW
- Lecture 7: Proof-of-Stake (PoS)
- Lecture 8: Privacy
- Lecture 9: Byzantine Agreement
- Lecture 10: Blockchain Network
- Lecture 11: Payment Channels
- Lecture 12: Guest Lecture

Unit Structure

- Lecture 1: Introduction to Blockchain
- Lecture 2: Bitcoin
- Lecture 3: Ethereum and Smart Contracts
- Lecture 4: Proof-of-Work (PoW)
- Lecture 5: Attacks on Blockchains
- Lecture 6: Class Test/Alternatives to PoW
- Lecture 7: Proof-of-Stake (PoS)
- Lecture 8: Privacy
- Lecture 9: Byzantine Agreement
- Lecture 10: Blockchain Network
- Lecture 11: Payment Channels
- Lecture 12: Guest Lecture

Learning outcome:

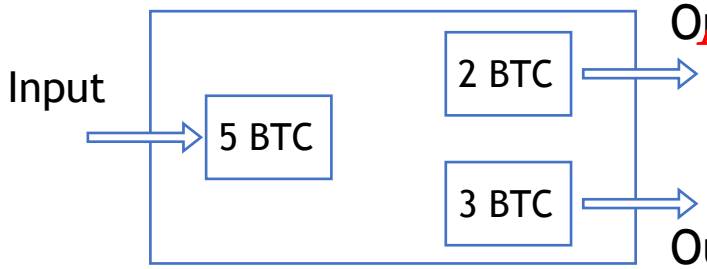
Basic understandings on privacy preserving technologies for blockchain

Bitcoin privacy

In Bitcoin, a user can create a new pair of (PK,SK) for each transaction to try to hide his identity.

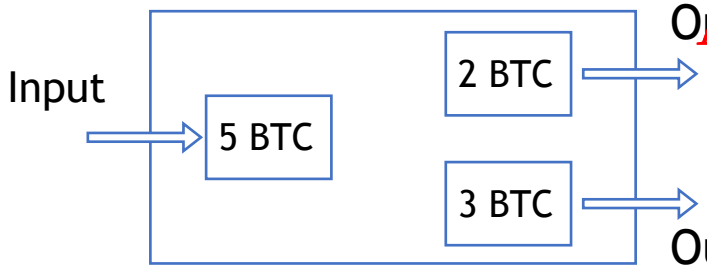
Bitcoin privacy

In Bitcoin, a user can create a new pair of (PK,SK) for each transaction to try to hide his identity.



Bitcoin privacy

In Bitcoin, a user can create a new pair of (PK,SK) for each transaction to try to hide his identity.

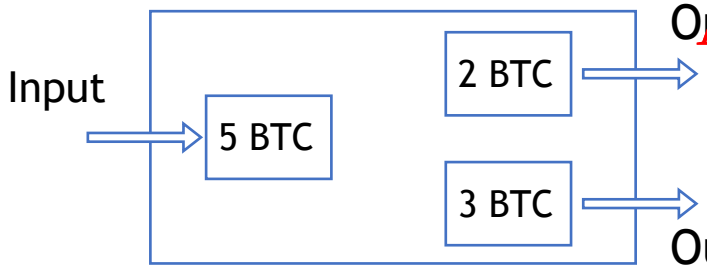


We know the amount of money being transferred.

Also, normally, one output is to the payee, and the other is the change to the payer.

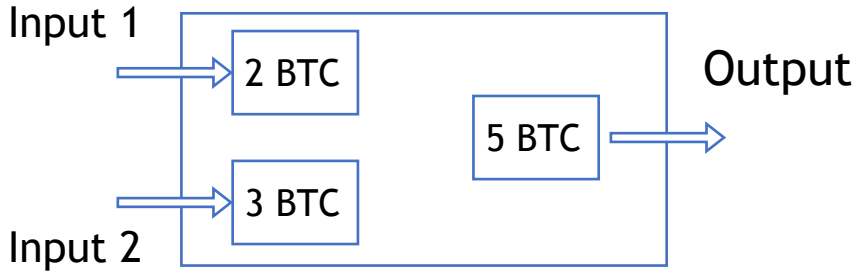
Bitcoin privacy

In Bitcoin, a user can create a new pair of (PK,SK) for each transaction to try to hide his identity.



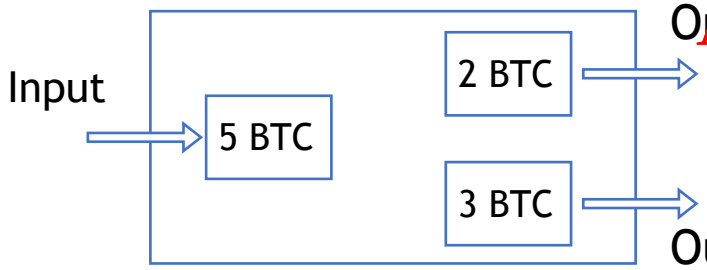
We know the amount of money being transferred.

Also, normally, one output is to the payee, and the other is the change to the payer.



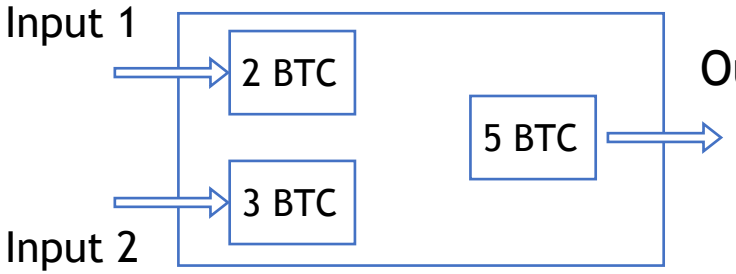
Bitcoin privacy

In Bitcoin, a user can create a new pair of (PK,SK) for each transaction to try to hide his identity.



We know the amount of money being transferred.

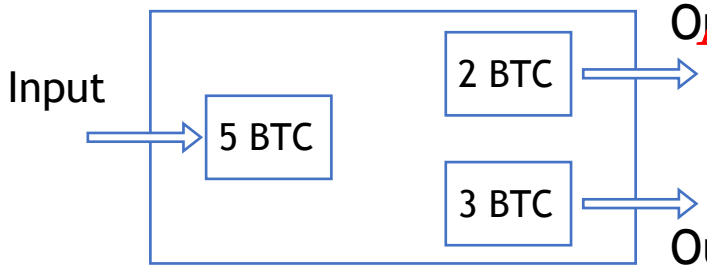
Also, normally, one output is to the payee, and the other is the change to the payer.



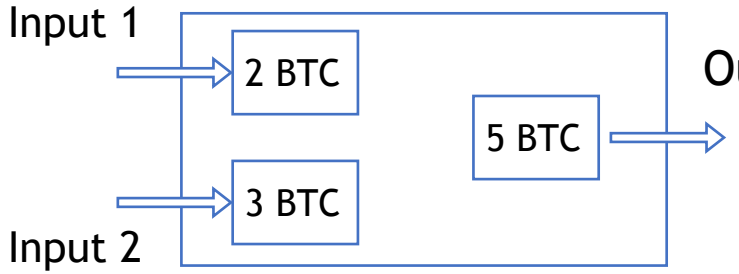
We can learn that both input 1 and input 2 belong to the same payer.

Bitcoin privacy

In Bitcoin, a user can create a new pair of (PK,SK) for each transaction to try to hide his identity.



Users may reuse the PK (address)



In fact, most users use a single or a few addresses

Bitcoin privacy

Bitcoin is Pseudonymous!!!

Anonymity = pseudonymity + unlinkability + untraceability

Bitcoin privacy

Bitcoin is Pseudonymous!!!

Anonymity = pseudonymity + unlinkability + untraceability

- **pseudonymity:** real identity is hidden
  (Linking Bitcoin addresses to real identities is not difficult)

Bitcoin privacy

Bitcoin is Pseudonymous!!!

Anonymity = pseudonymity + unlinkability + untraceability

- **pseudonymity:** real identity is hidden
  (Linking Bitcoin addresses to real identities is not difficult)
- **unlinkability:** cannot link any two transactions to the same user

Bitcoin privacy

Bitcoin is Pseudonymous!!!

Anonymity = pseudonymity + unlinkability + untraceability

- **pseudonymity:** real identity is hidden
  (Linking Bitcoin addresses to real identities is not difficult)
- **unlinkability:** cannot link any two transactions to the same user
- **untraceability:** cannot trace any coin back to another transaction
  (cash flow)

Bitcoin privacy

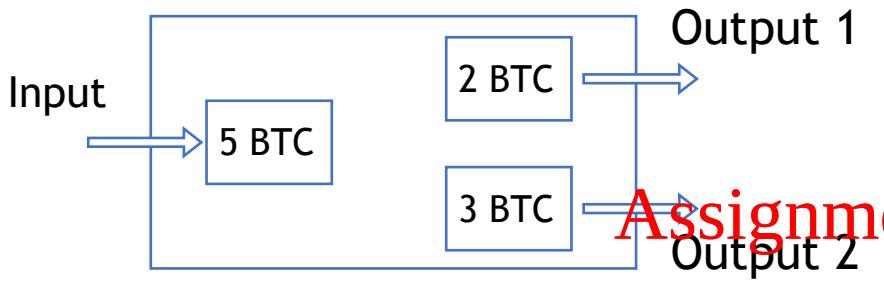
Bitcoin is Pseudonymous!!!

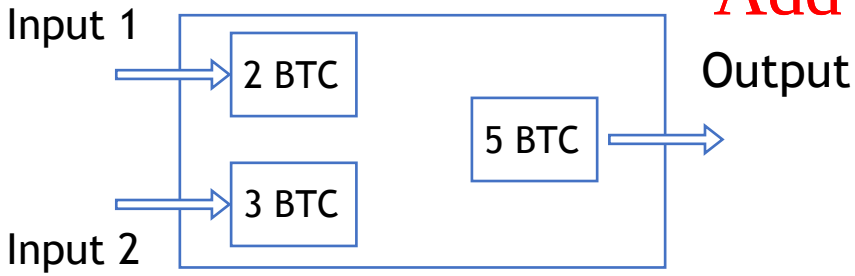
Anonymity = pseudonymity + unlinkability + untraceability

- **pseudonymity:** real identity is hidden
  (Linking Bitcoin addresses to real identities is not difficult)
- **unlinkability:** cannot link any two transactions to the same user
- **untraceability:** cannot trace any coin back to another transaction
  (cash flow)

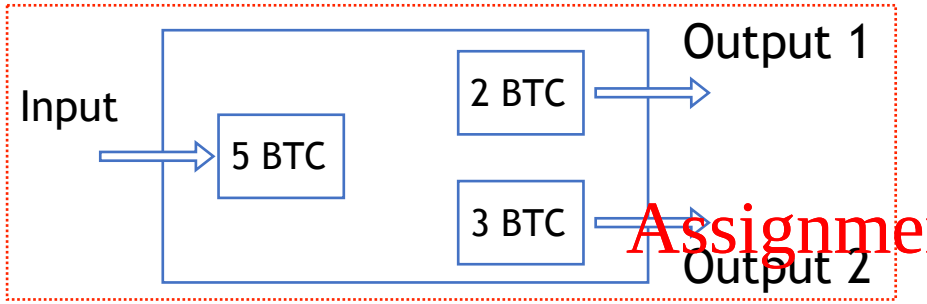
Bitcoin is NOT Anonymous!!!

Bitcoin privacy

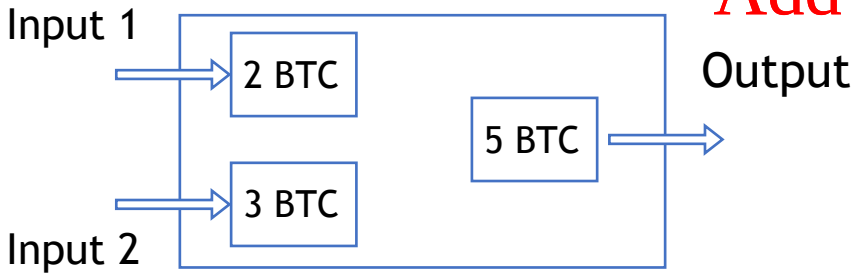




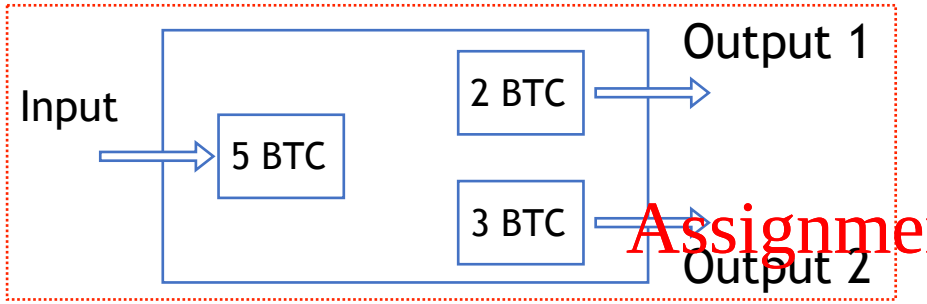
Bitcoin privacy



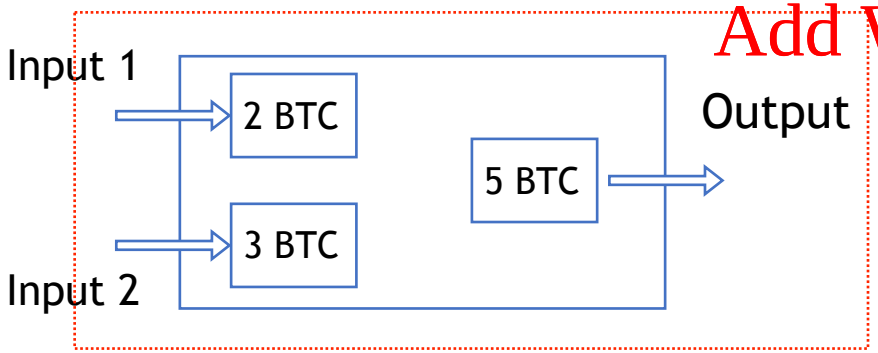
Traceable to anyone (and linkable to previous)



Bitcoin privacy

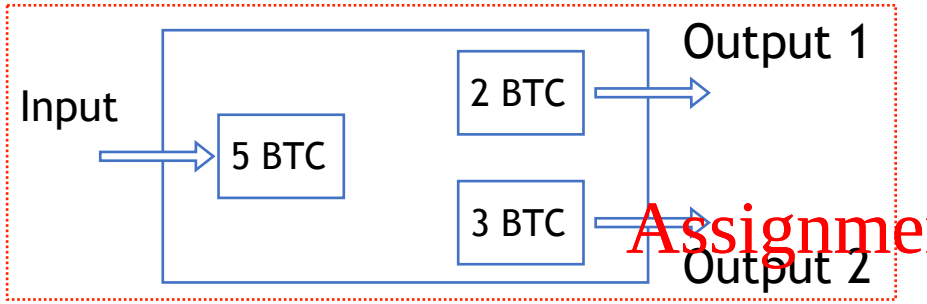


Traceable to anyone (and linkable to the same)

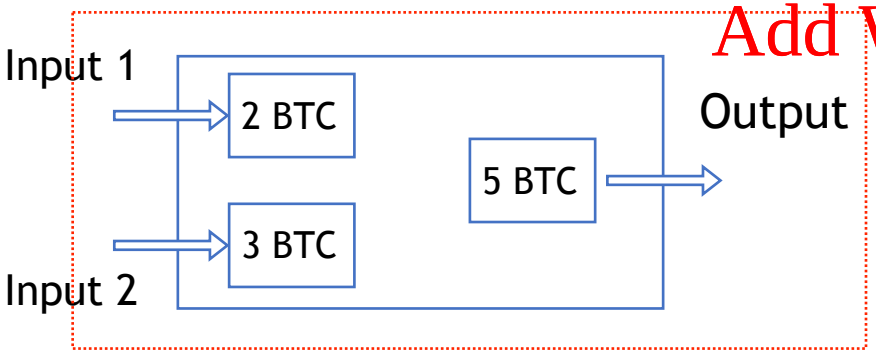


Traceable and Linkable to anyone

Bitcoin privacy



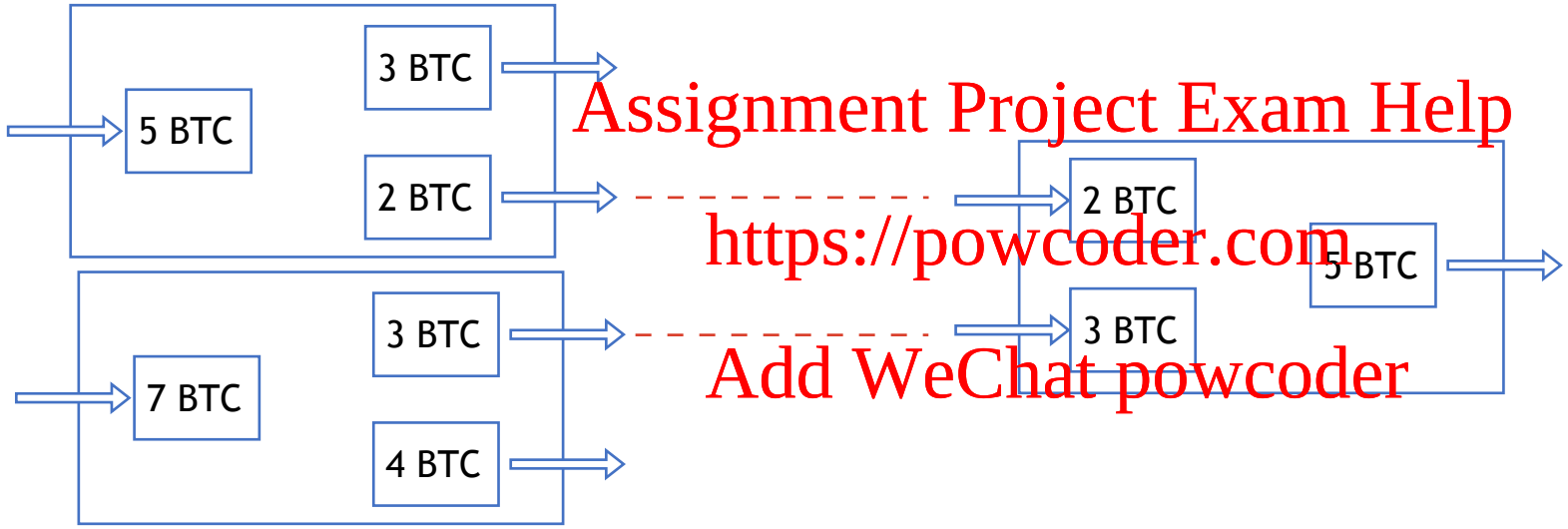
Traceable to anyone (and linkable to the payee)



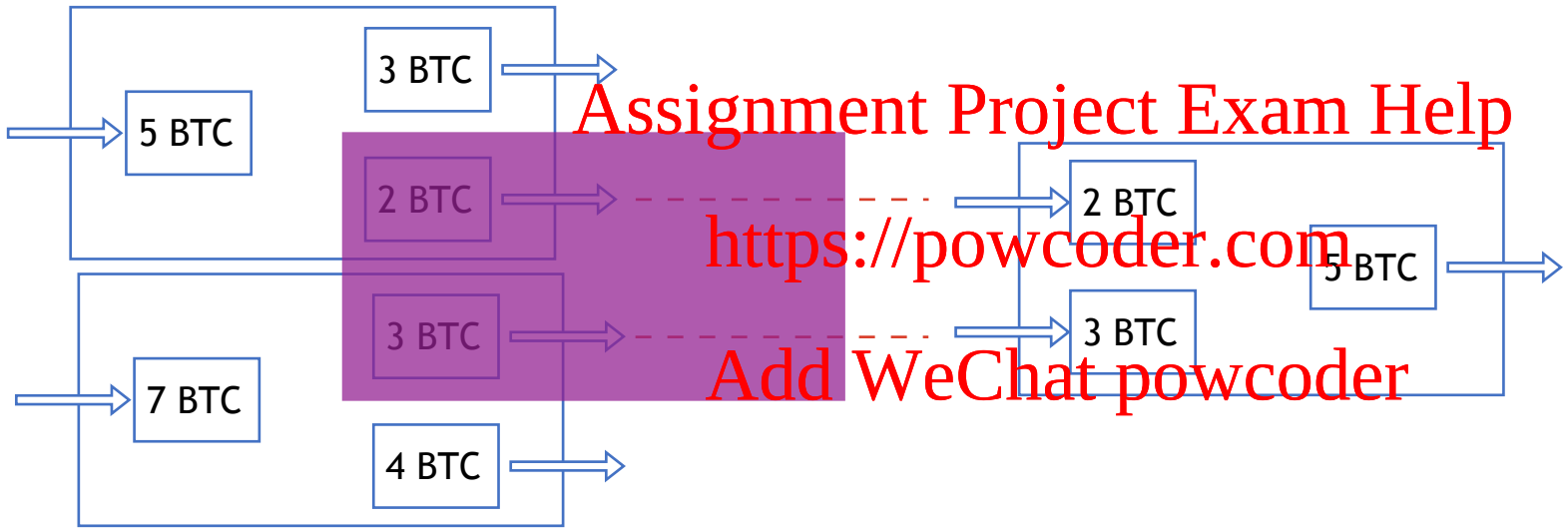
Traceable and Linkable to anyone

Additionally, account balance is also revealed in every transaction.

Bitcoin privacy

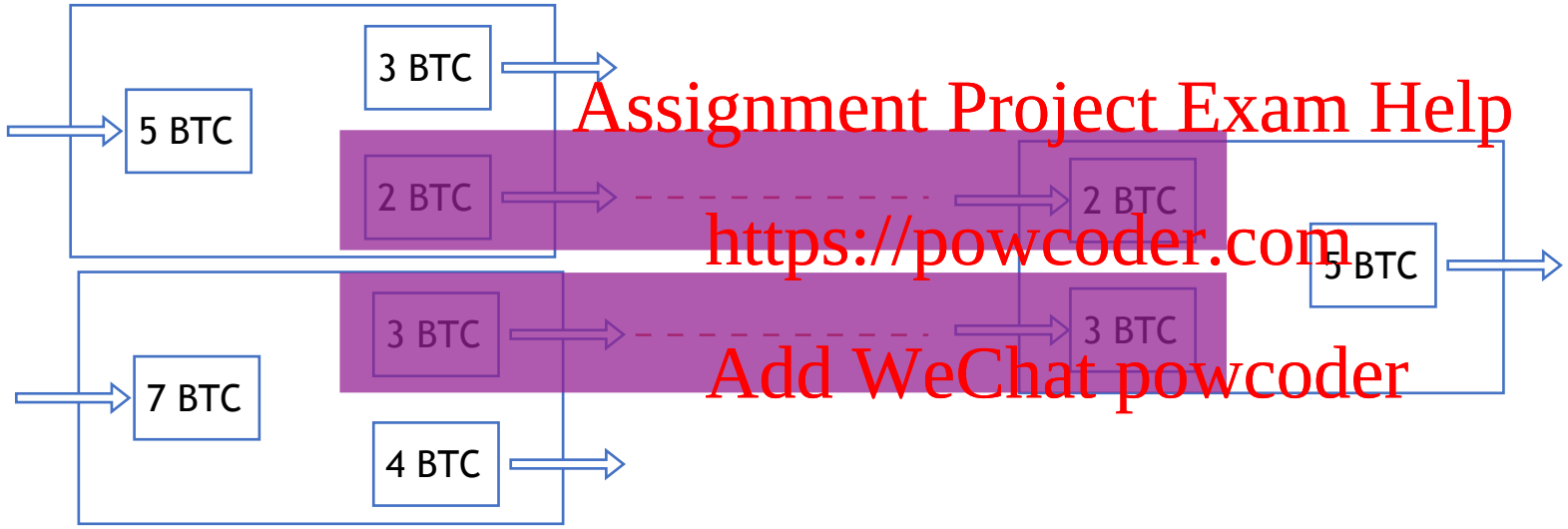


Bitcoin privacy



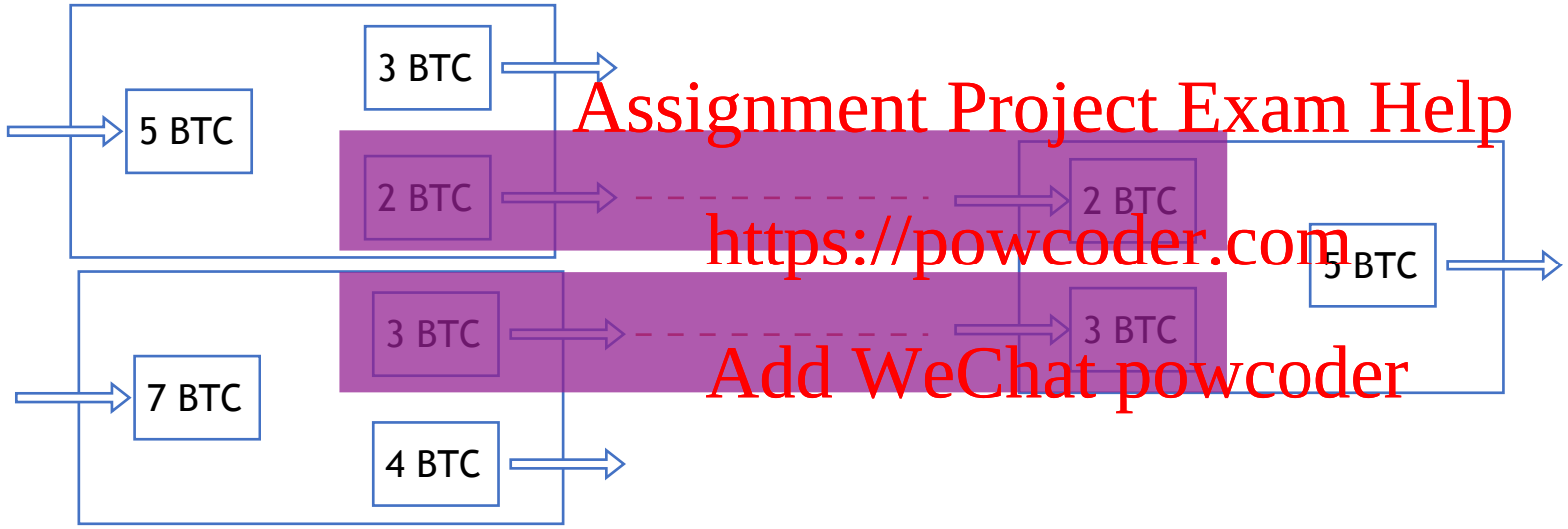
Linkable transactions (to the same payee)

Bitcoin privacy



The later transaction is traceable (back to two transactions)

Bitcoin privacy



All amounts are also visible!

The later transaction is traceable (back to two transactions)

Bitcoin privacy

A critical question

Is privacy always good?

Darknet

coindesk Blockchain 101 Technology Markets Business Data & Research Events

Stay Up to Date on Crypto & Blockchain With Our Suite of Newsletters. Subscribe

$200,000 in Bitcoin Seized in Dark Net Drug Probe

Daniel Kuhn

Jun 19, 2019 at 06:00 UTC • Updated Jun 19, 2019 at 06:04 UTC

NEWS

U.S. authorities seized more than $200,000 worth of bitcoin after alleged drug manufacturer and dealer met with undercover law enforcement officers to exchange the digital currency for cash at a hotel in Norwood, Massachusetts.

The arrest — which occurred on March 27, 2019 — was part of a wider investigation into a Boston-based drug syndicate that operated through the darknet site EastSideHigh.

During the investigation, an undercover federal agent ordered MDMA from the "EastSideHigh" vendors. Later this officer allegedly observed Binh Thanh Le, 22, deposit an envelope containing the agent's order into a United States Postal Service collection box in Stoughton, a neighborhood in Boston.

Bloomberg

Technology

Bitcoin Criminals Set to Spend $1 Billion on Dark Web This Year

By Olga Kharif
2 July 2019, 4:57 am AEST

- Year-to-date spending reached $513 million, Chainalysis says
- Proportion of Bitcoin used for illegal purchases is declining

LISTEN TO ARTICLE 1:57

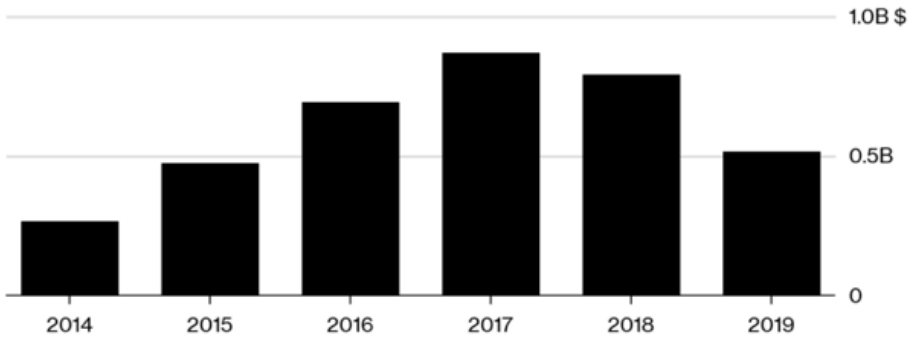
Tweet
Post
Email

Bitcoin's use in illegal online marketplaces peddling everything from drugs to child porn is on pace to set a record this year at more than $1 billion, according to a report by Chainalysis.

While the proportion of Bitcoin transactions dedicated to illegal purchases is declining, about $515 million of the digital coin has already been spent this year on the so-called dark web, according to the firm, which helps companies such as cryptocurrency exchanges investigate and prevent illegal transactions. Dark-net spending in Bitcoin peaked in 2017, at $872 million, and declined last year as the coin's price took a dramatic dive.

Bitcoin Darknet Market Activity

In U.S. dollar value

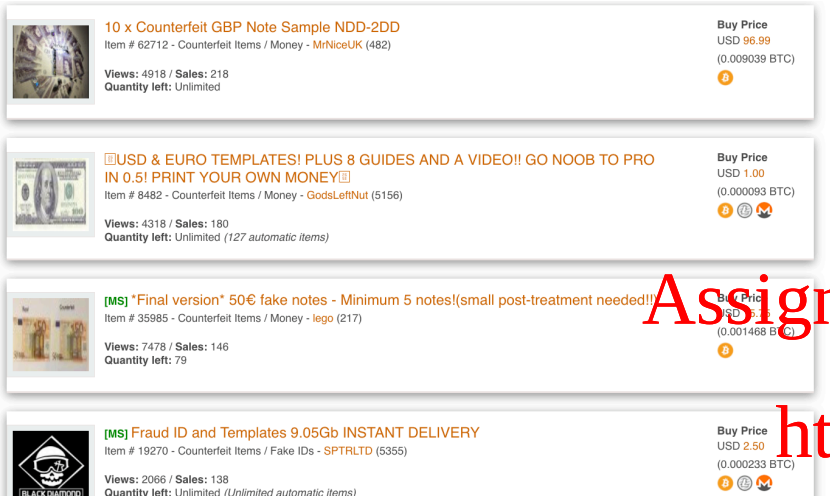


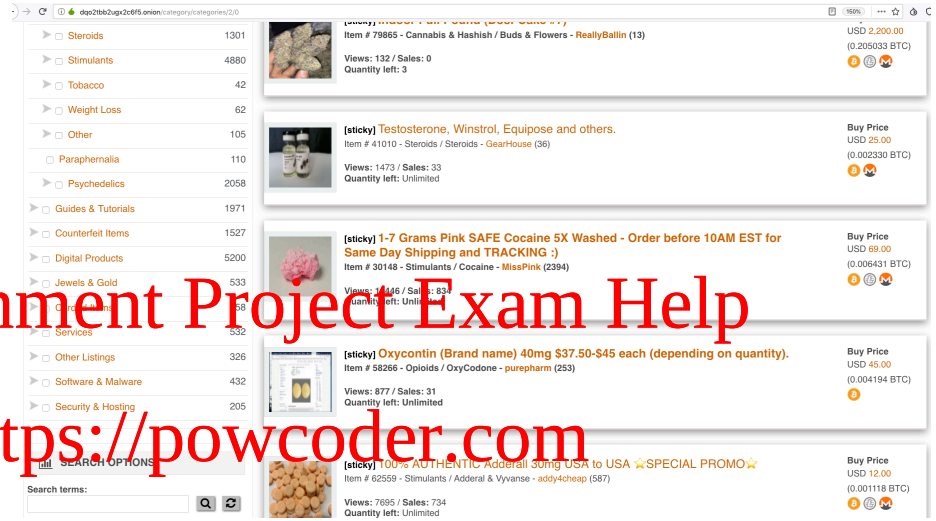
In 2019, Chainalysis looked at activity from Jan. 1 to June 28.
Source: Chainalysis

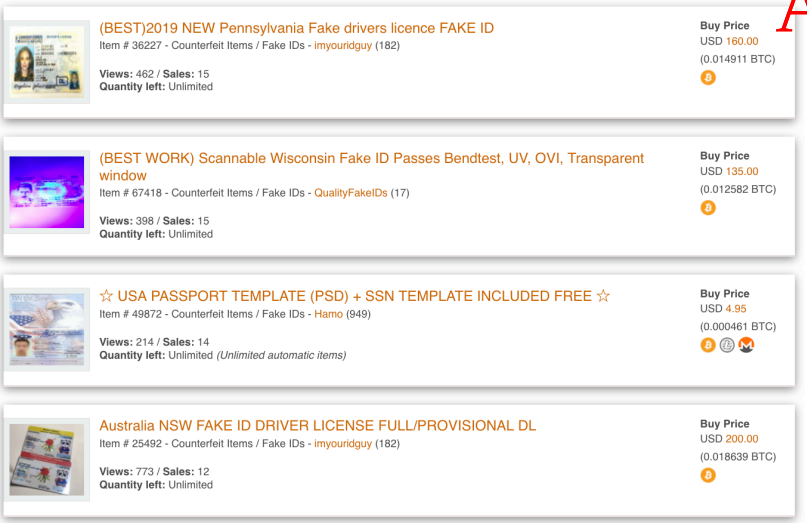
Bloomberg

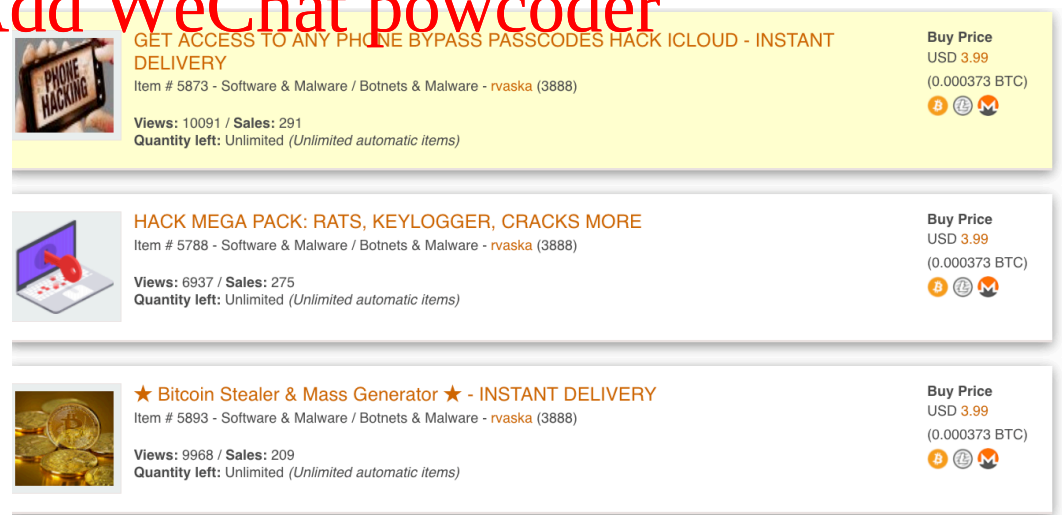
MONASH University

Darknet Market





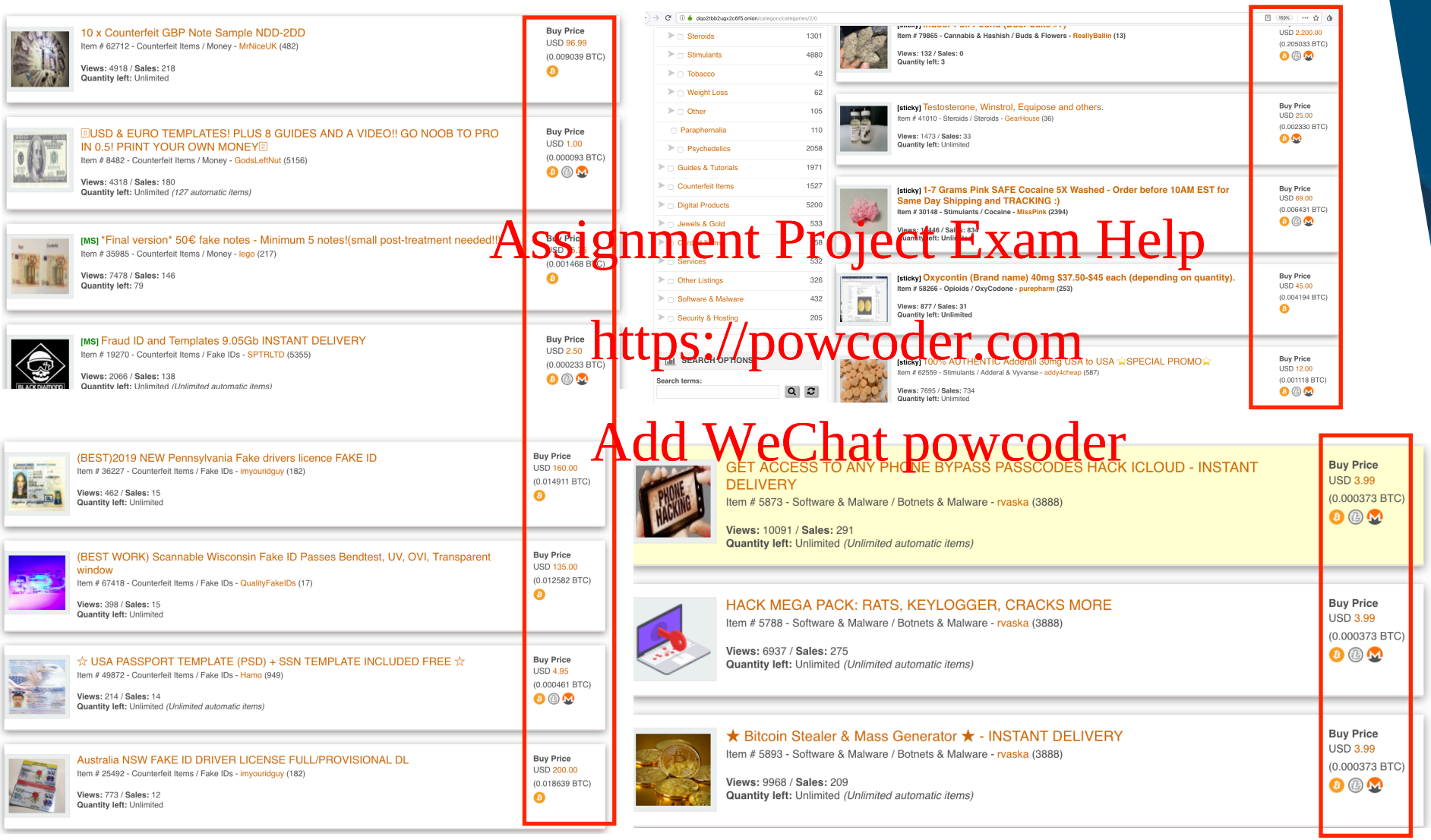




Screenshots taken on 16th-July-2019 by Dr. Jiangshan Yu, for research purpose only.

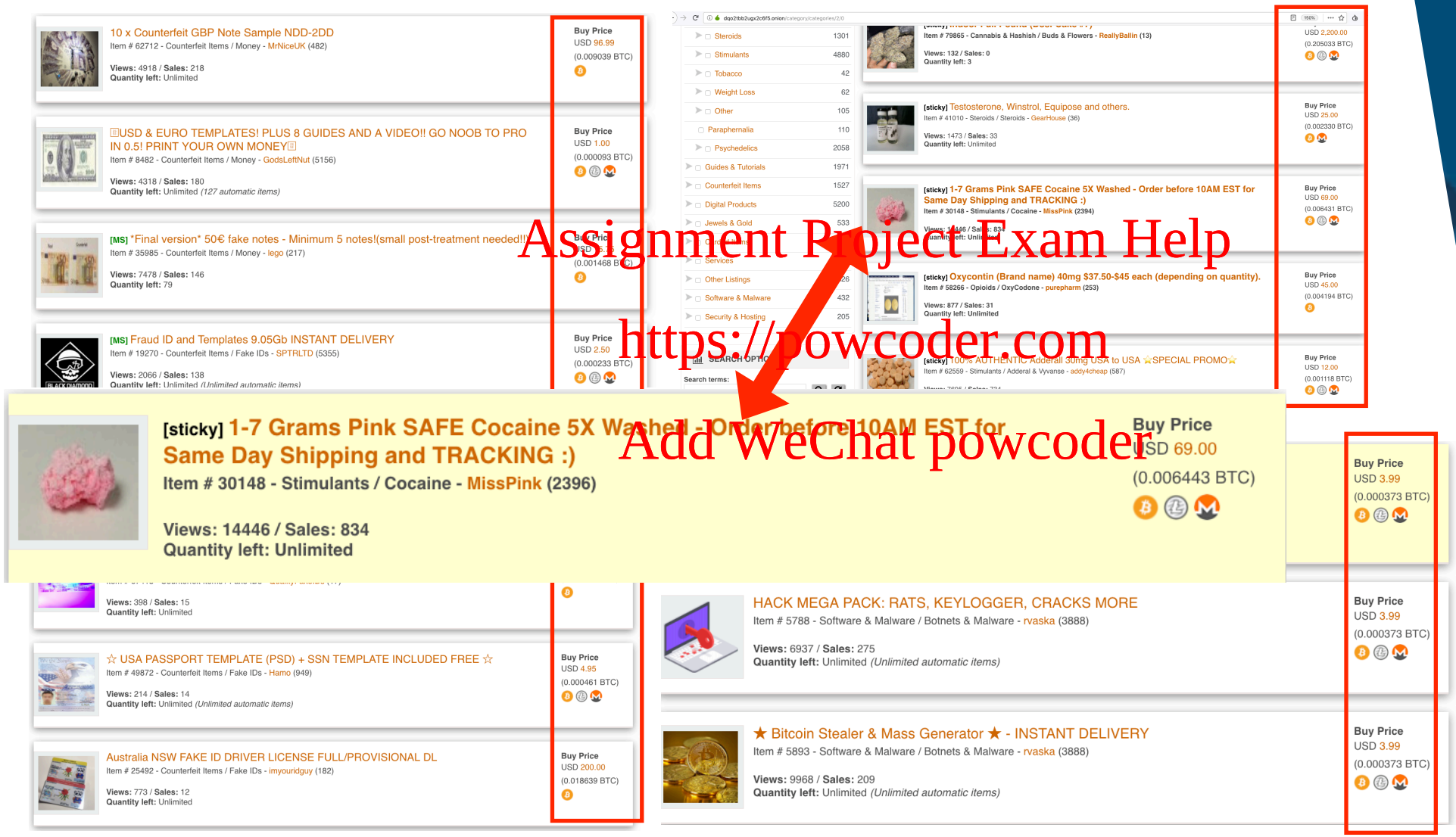
MONASH University

Darknet Market



Screenshots taken on 16th-July-2019 by Dr. Jiangshan Yu, for research purpose only.

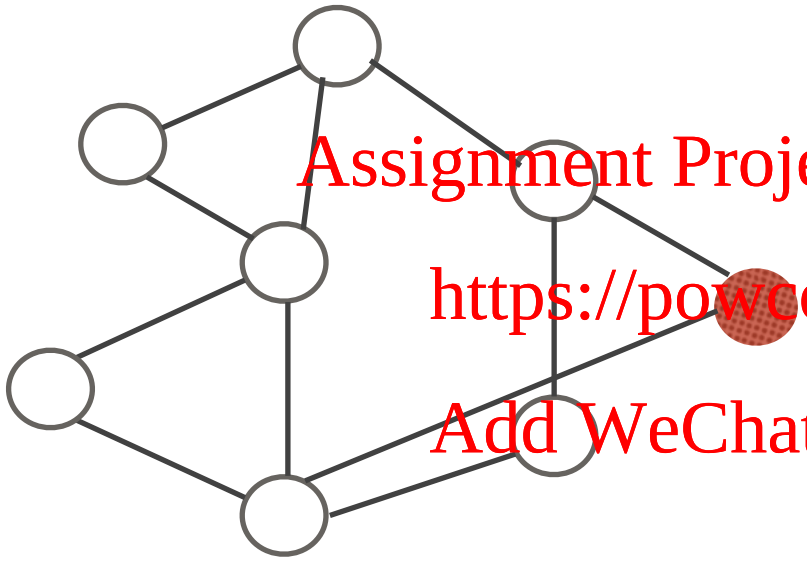
Darknet Market



Screenshots taken on 16th-July-2019 by Dr. Jiangshan Yu, for research purpose only.

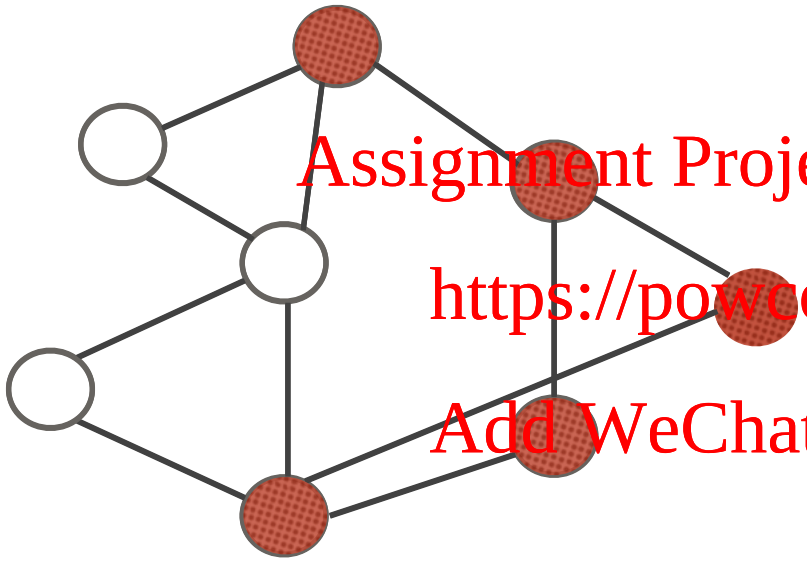
MONASH University

De-anonymization: an example



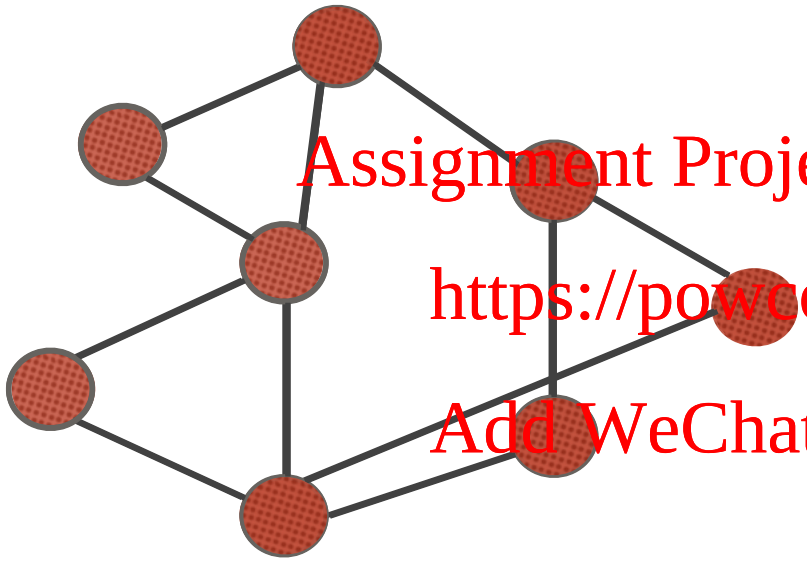
On the network, the first node (e.g. your mobile wallet) that sends out a new transaction, is likely to be the payer.

De-anonymization: an example



On the network, the first node (e.g. your mobile wallet) that sends out a new transaction, is likely to be the payer.

De-anonymization: an example

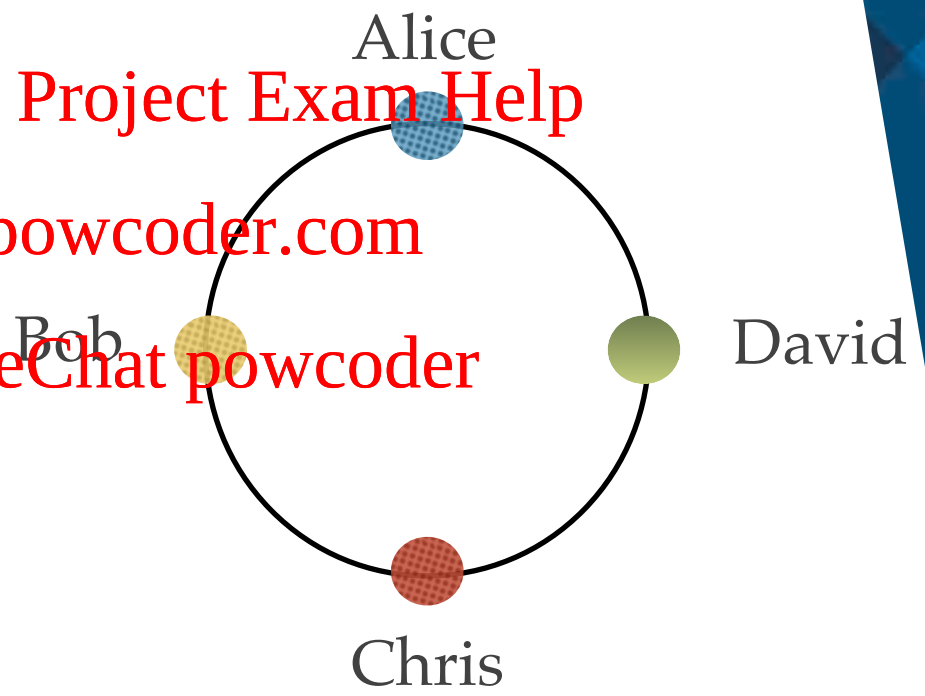


On the network, the first node (e.g. your mobile wallet) that sends out a new transaction, is likely to be the payer.

Ring signature (2001 by Rivest, Shamir, Tauman)

The signature scheme convinces a verifier that a document has been signed by one of n independent signers.

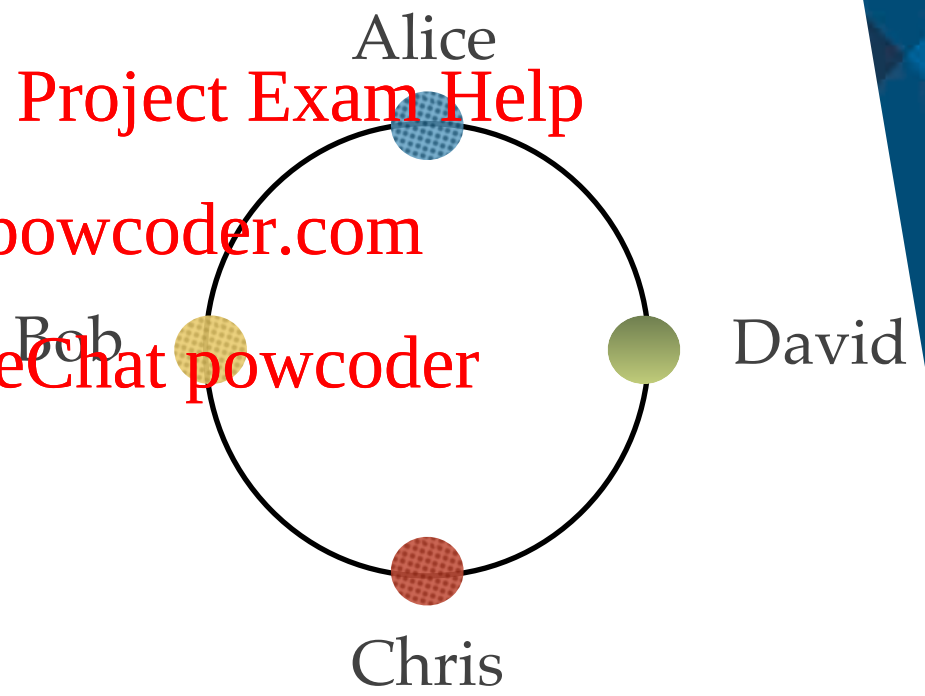
- When signing, other members do not need to cooperate
- The signer only needs to choose n-1 public-keys of other entities
- The actual signer is indistinguishable from other entities in the ring



Ring signature (2001 by Rivest, Shamir, Tauman)

The signature scheme convinces a verifier that a document has been signed by one of n independent signers.

- When signing, other members do not need to cooperate
- The signer only needs to choose n-1 public-keys of other entities
- The actual signer is indistinguishable from other entities in the ring



The signer gets some anonymity!

Ring signature (2001 by Rivest, Shamir, Tauman)

Example:

- Edward Snowden wants to anonymously reveal NSA's secrets.
- Any member i of NSA has a pair of keys (PK_i, SK_i) published on the NSA website.
- To reveal a secret, Snowden randomly chooses n-1 public keys from the NSA members, and creates a ring signature on the secret, so that:
  - A third party can verify that the signer of the revealed secret is one of the n members from NSA.
  - No one knows which member has revealed the secret.

Ring signature (2001 by Rivest, Shamir, Tauman)

Setting:

- A ring is an **arbitrary** set of participants including the actual signer.
- Each member i of the ring has a public encryption key PK_i.
- Only i knows the corresponding secret key SK_i.
- The signer and verifier need to known the public key of all ring members.

Ring signature (2001 by Rivest, Shamir, Tauman)

Keyed combining function

$$C_{k,v}(y_1, y_2, \ldots, y_n) = E_k(y_n \oplus E_k(y_{n-1} \oplus E_k(\ldots E_k(y_1 \oplus v)\ldots))) = v$$

Where the function takes (k, v, y_1, y_2, .., y_n) as input, and output value v.

E_k is symmetric key encryption with secret key k.

Ring signature (2001 by Rivest, Shamir, Tauman)

Keyed combining function

$$C_{k,v}(y_1, y_2, \ldots, y_n) = E_k(y_n \oplus E_k(y_{n-1} \oplus E_k(\ldots E_k(y_1 \oplus v)\ldots))) = v$$

Given (k, v) and any n-1 parameters of (y_1, y_2, …, y_n) as input, it is easy to calculate the remaining parameter (as both E_k and xor operation are invertible).

Ring signature (2001 by Rivest, Shamir, Tauman)

Signature generation on message m:

1. k=H(m).
2. Choose random v.
3. Choose random x_i for i for all other ring members and calculate corresponding $y_i = g_i(x_i)$, where g_i is a trapdoor function.
4. Solve the Keyed combining function for y_s is simple, where i=s is the signer

   $C_{k,v}(y_1, y_2, \ldots, y_n) = E_k(y_n \oplus E_k(y_{n-1} \oplus E_k(\ldots E_k(y_1 \oplus v)\ldots))) = v$
5. Calculating x_s from y_s is also simple $x_s = g_s^{-1}(y_s)$.
6. The ring signature is $(PK_1, PK_2, \ldots, PK_n; v; x_1, x_2, \ldots, x_n)$.

Ring signature (2001 by Rivest, Shamir, Tauman)

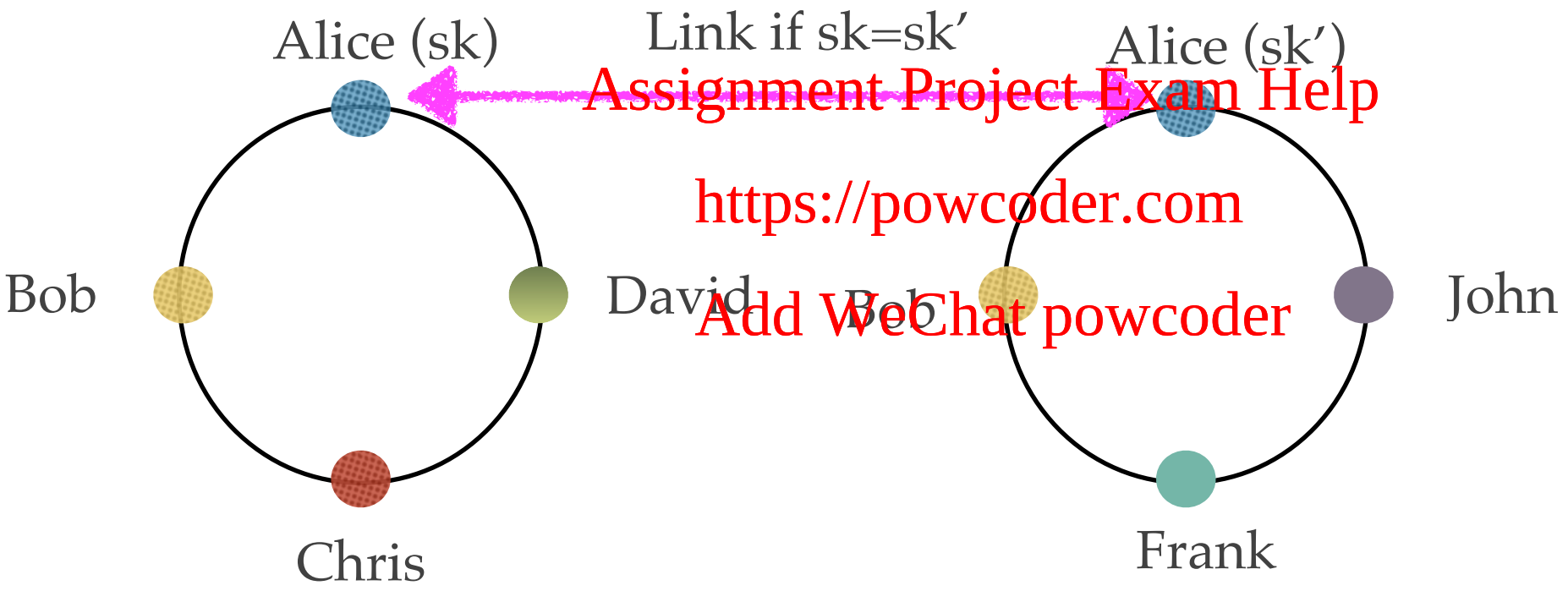
Signature verification on signed message m:

Signature is $(PK_1, PK_2, \ldots, PK_n; y; x_1, x_2, \ldots, x_n)$

1. For all x_i, calculate $y_i = g_i(x_i)$.
2. k=H(m).
3. Verify that

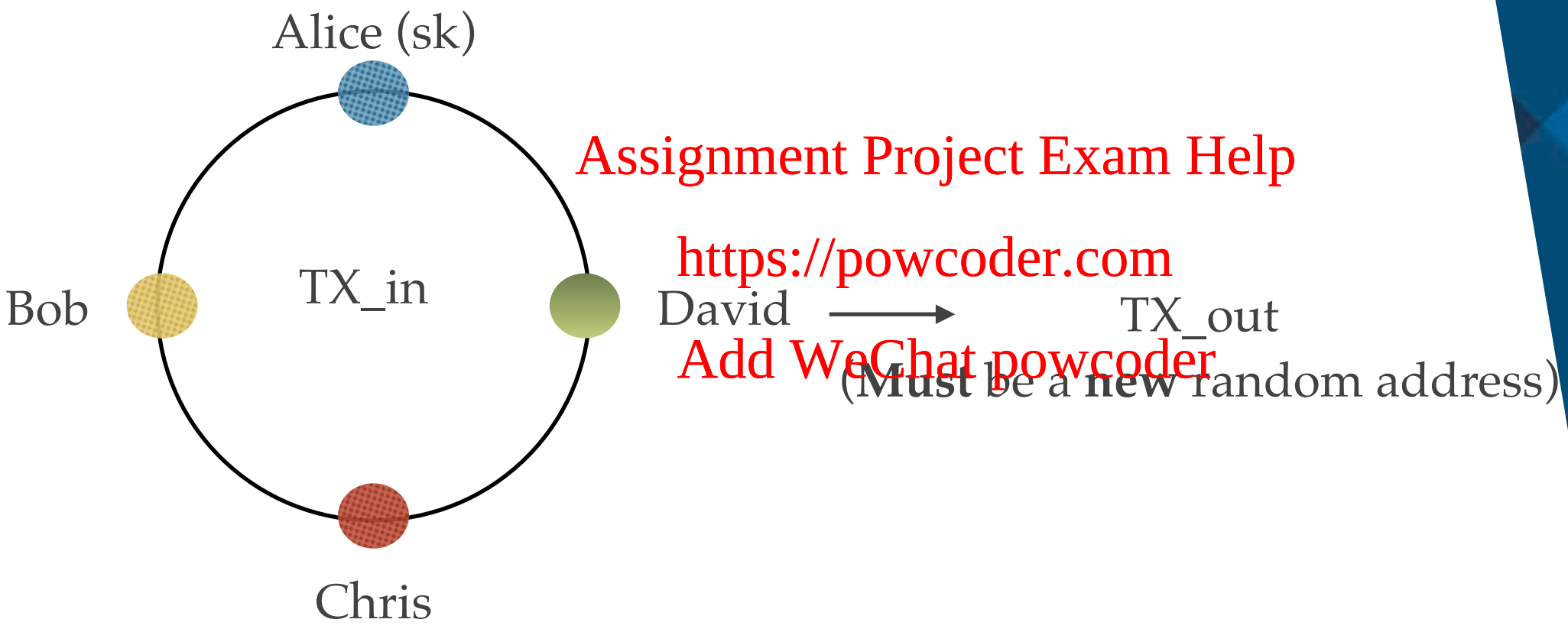
$$C_{k,v}(y_1, y_2, \ldots, y_n) = E_k(y_n \oplus E_k(y_{n-1} \oplus E_k(\ldots E_k(y_1 \oplus v)\ldots))) = v$$

Linkable ring signature

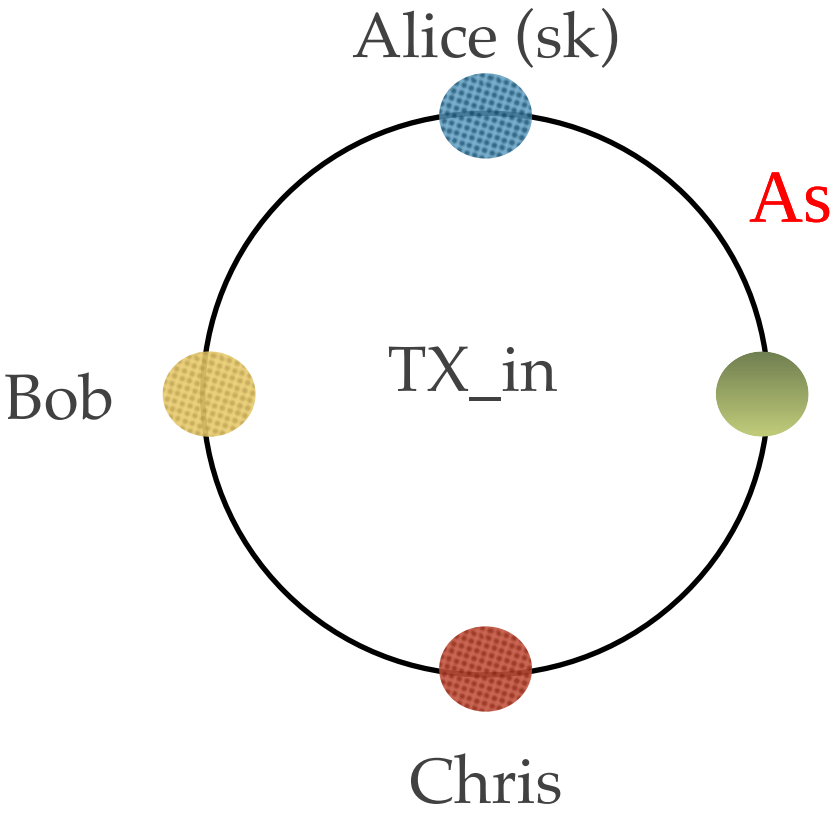


J.Liu et.al. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups, ACISP 2004.

CryptoNote



CryptoNote

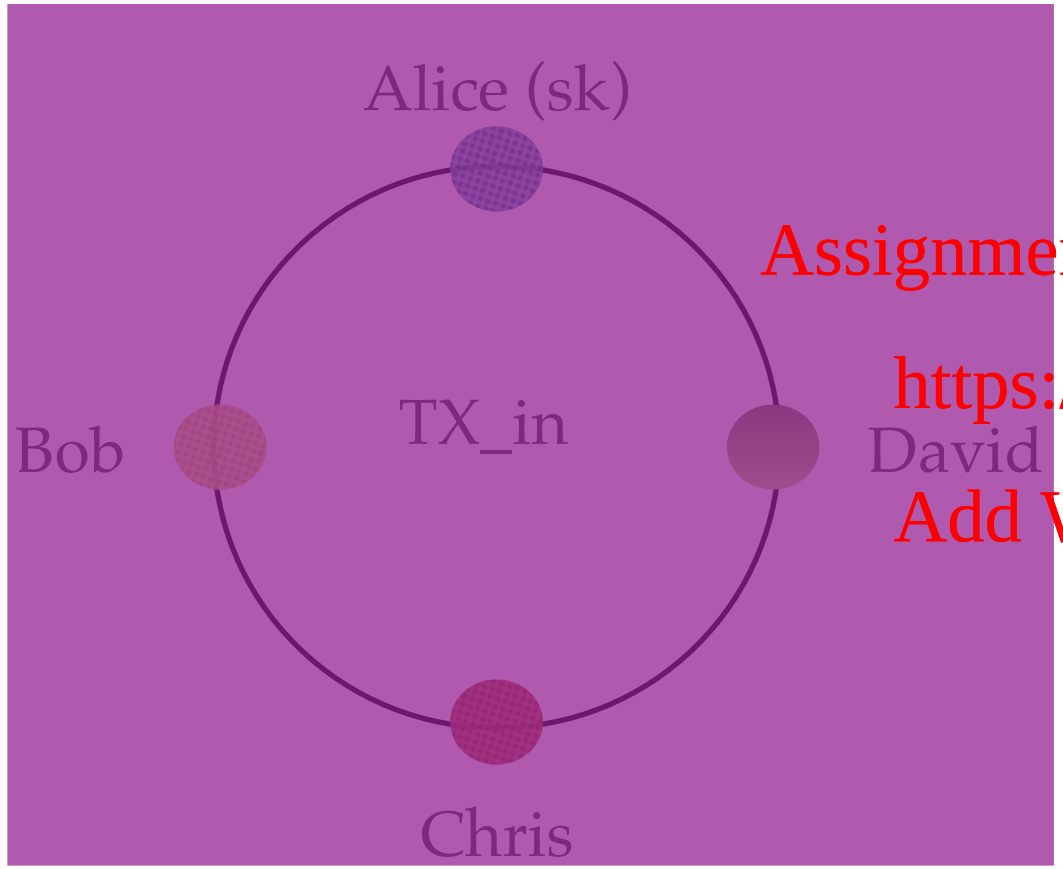


David ⟶ TX_out

(**Must** be a **new** random address)

Double spending will be identified!

CryptoNote



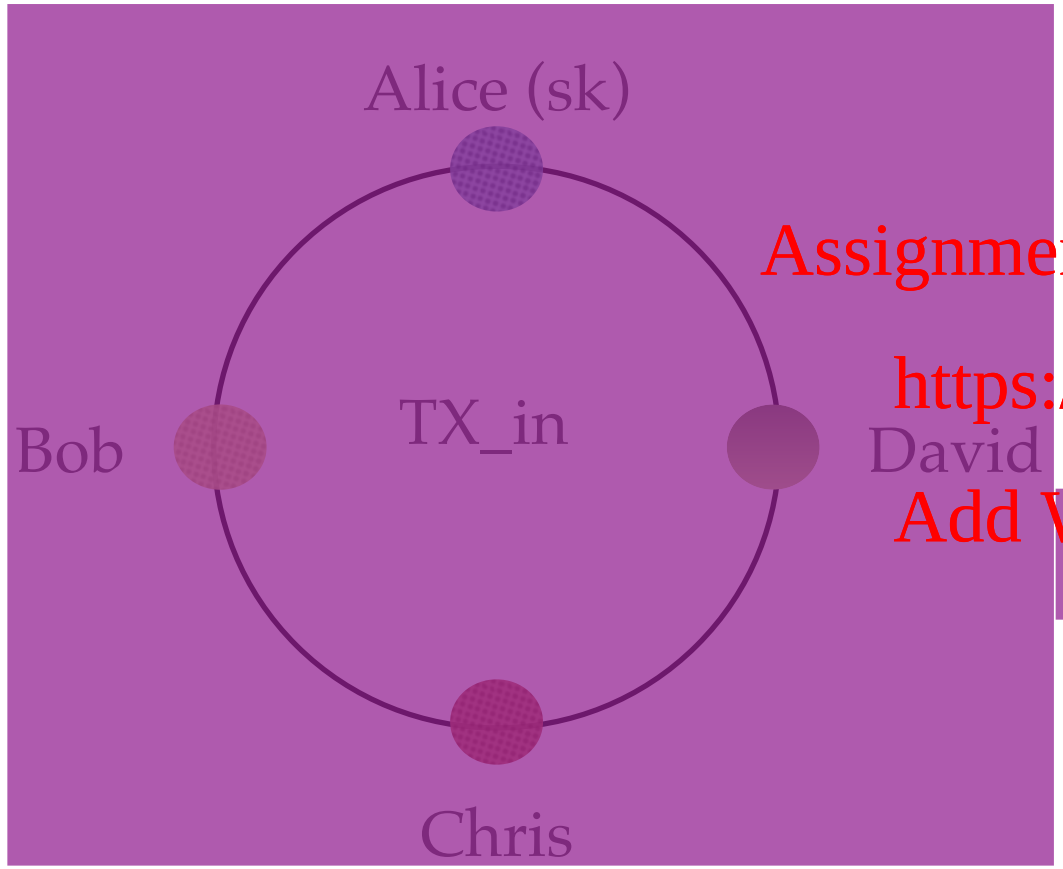
This provides **untraceability**

TX_in → TX_out

(**Must** be a **new** random address)

Double spending will be identified!

CryptoNote



This provides **untraceability**

TX_out

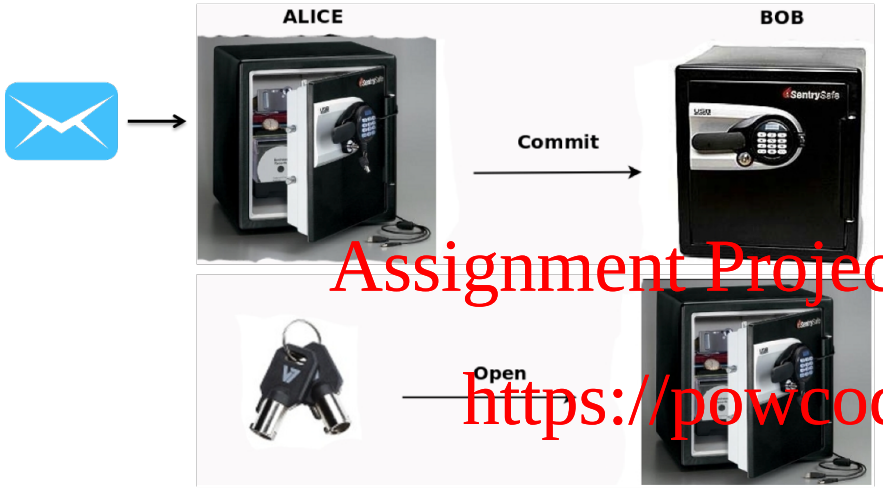
(**Must** be a **new** random address)

This is called stealth address, which **aims at** providing **unlinkability**

(as no public key address can be reused)

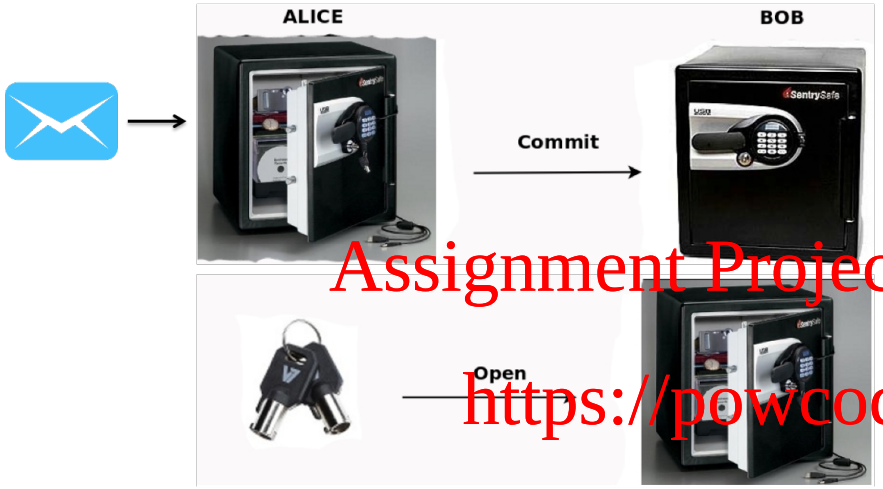
Double spending will be identified!

Commitment scheme



- A commitment scheme is a cryptographic primitive that allows the sender to commit to a value during the commit phase while keeping it hidden from the receiver(s), with the ability to reveal the committed value on a later point (the opening phase).
- A commitment scheme should be **binding**, meaning that after the commit phase the sender cannot change the committed value.
- A commitment scheme should be **hiding**, meaning that before the opening phase the receiver(s) cannot learn any information about the committed value.

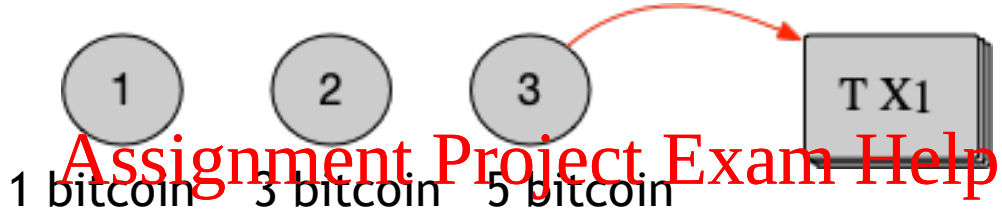
Commitments in Monero



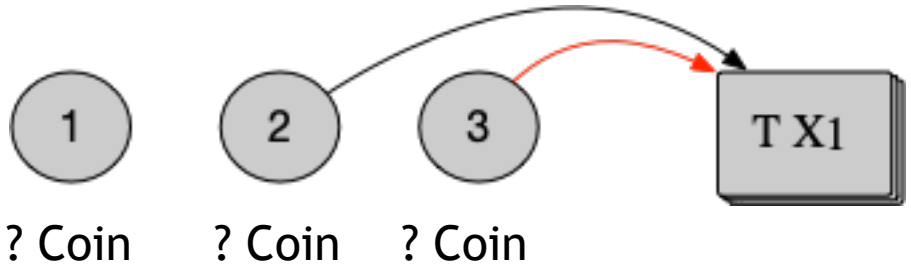
- The value of all Monero inputs and outputs are committed (hidden), with additional proofs that:
  1. The total amount of coins in the committed inputs is equal to the total amount of coins in the committed outputs plus the transaction fee.
  2. All committed values are positive. This is done using range proofs and guarantees that coins are not created out of thin air.

Comparison

Bitcoin



Monero



Recap: Monero

- Monero provides better privacy than Bitcoin
- One-time stealth address aims at providing unlinkability (e.g. preventing address clustering)
- Transaction values are hidden (by using a commitment scheme with the accompanying equality and range proofs).
- Linkable ring signature is used to provide untraceability (Money flow is hidden).

Monero mixin selection

Initially, Monero has not enforced the number of mixins of transaction.

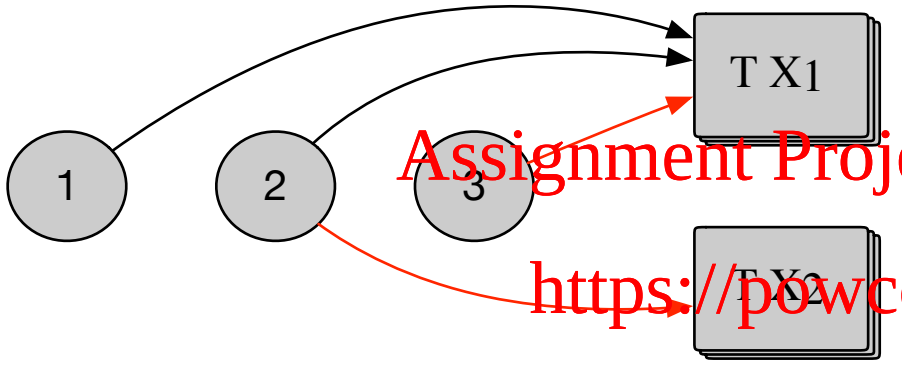
In Monero, 12158814 transaction inputs do not contain any mixins!

(64.04% of all inputs before April 15, 2017, block height 1288774)

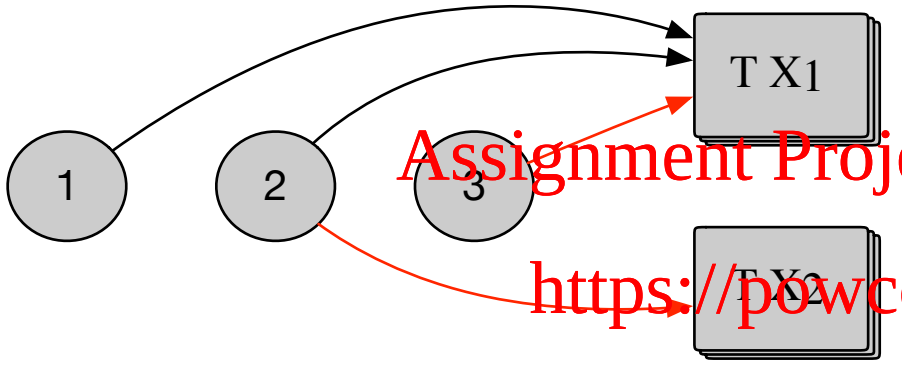
So what?

Amrit Kumar et. al. A Traceability Analysis of Monero's Blockchain, *ESORICS, 2017*.
Malte Moser et. al. *An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, 2018.*

Example:



Example:



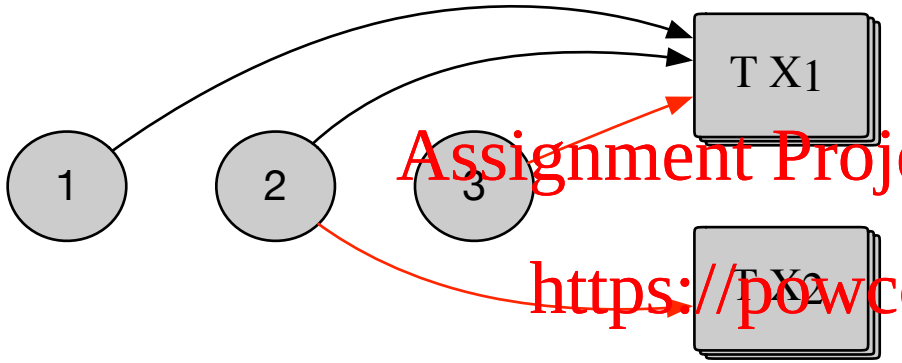
TX_2 is a 0-mixin transaction, and has no privacy guarantee!

Why 0-mixin?

Motivation:

In Monero, a transaction with smaller size pays **less transaction fee**.

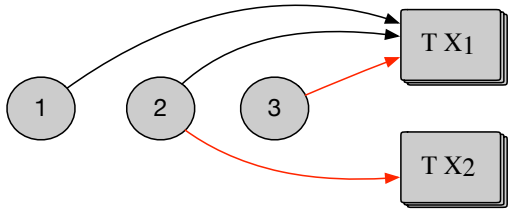
Zero Mixin attack



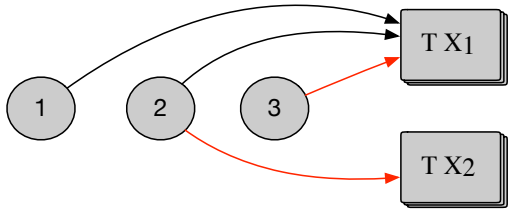
In order to save money, the owner of TX_2 chooses to give up its privacy, is this ok? Would it affect the privacy of others?

Zero Mixin attack

- The owner of TX_2 is traceable!

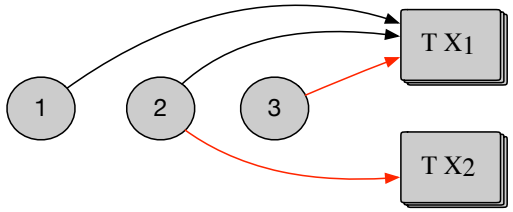


Zero Mixin attack



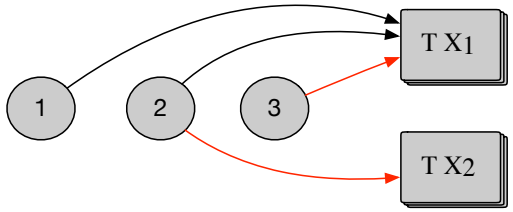
- The owner of TX_2 is traceable!
- The untraceability of the owner of TX_1 is reduced!

Zero Mixin attack



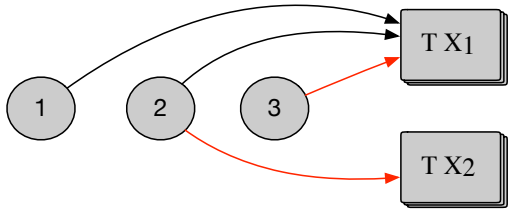
- The owner of TX_2 is traceable!
- The untraceability of the owner of TX_1 is reduced!
  - The probability of guessing the real input of TX_1 is expected to be 1/3.

Zero Mixin attack

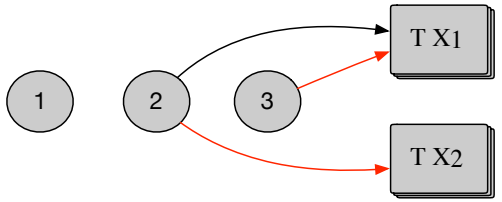


- The owner of TX_2 is traceable!
- The untraceability of the owner of TX_1 is reduced!
  - The probability of guessing the real input of TX_1 is expected to be 1/3.
  - Now, it is 1/2.

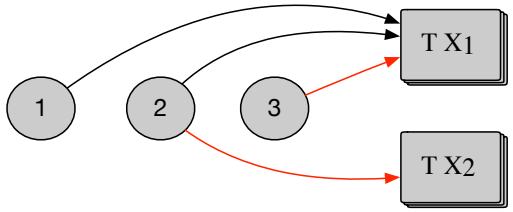
Zero Mixin attack



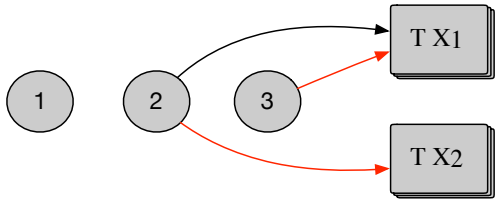
- The owner of TX_2 is traceable!
- The untraceability of the owner of TX_1 is reduced!
  - The probability of guessing the real input of TX_1 is expected to be 1/3.
  - Now, it is 1/2.



Zero Mixin attack



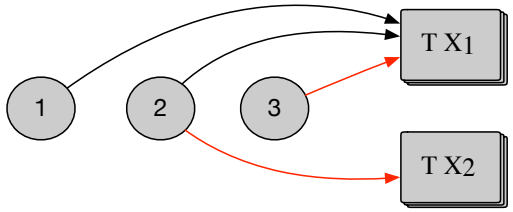
- The owner of TX_2 is traceable!
- The untraceability of the owner of TX_1 is reduced!
  - The probability of guessing the real input of TX_1 is expected to be 1/3.
  - Now, it is 1/2.



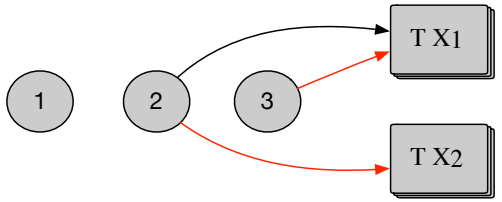
- The owner of both TX_1 and TX_2 is traceable!

(One coin can only be spent once, and coin 2 is spent in TX_2)

Zero Mixin attack

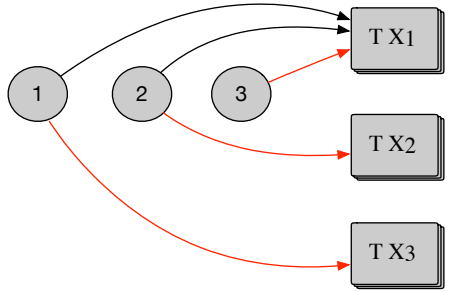


- The owner of TX_2 is traceable!
- The untraceability of the owner of TX_1 is reduced!
  - The probability of guessing the real input of TX_1 is expected to be 1/3.
  - Now, it is 1/2.



- The owner of both TX_1 and TX_2 is traceable!

(One coin can only be spent once, and coin 2 is spent in TX_2)



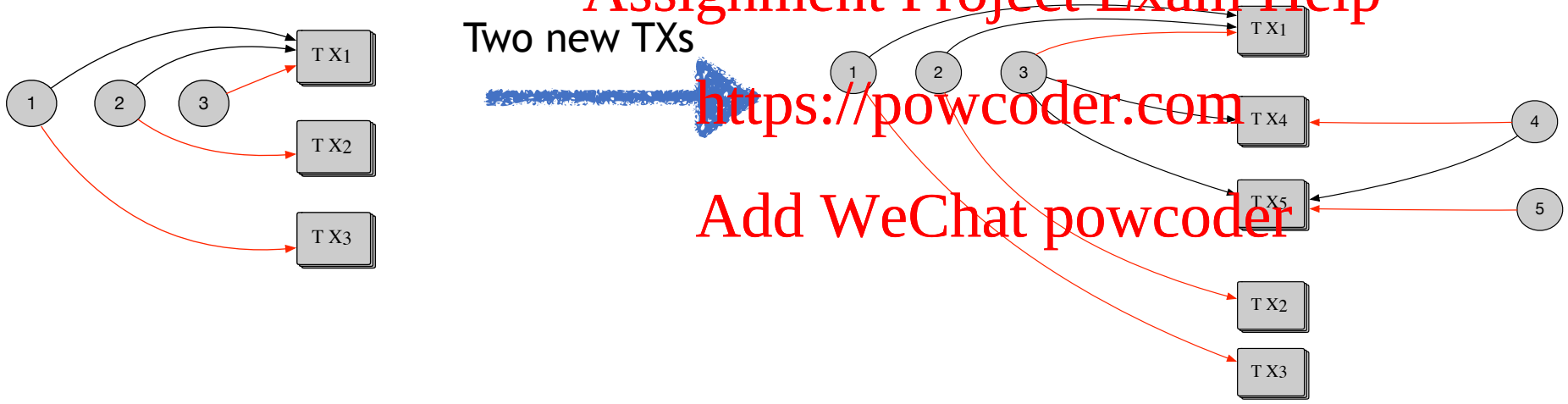
- The owner of both TX_1 and TX_2 is traceable!

(coin 2 is spent in TX_2 and coin 1 is spent in TX_3)

Zero Mixin attack

So, users should **NOT** choose a mixin that is used as a 0-mixin input!

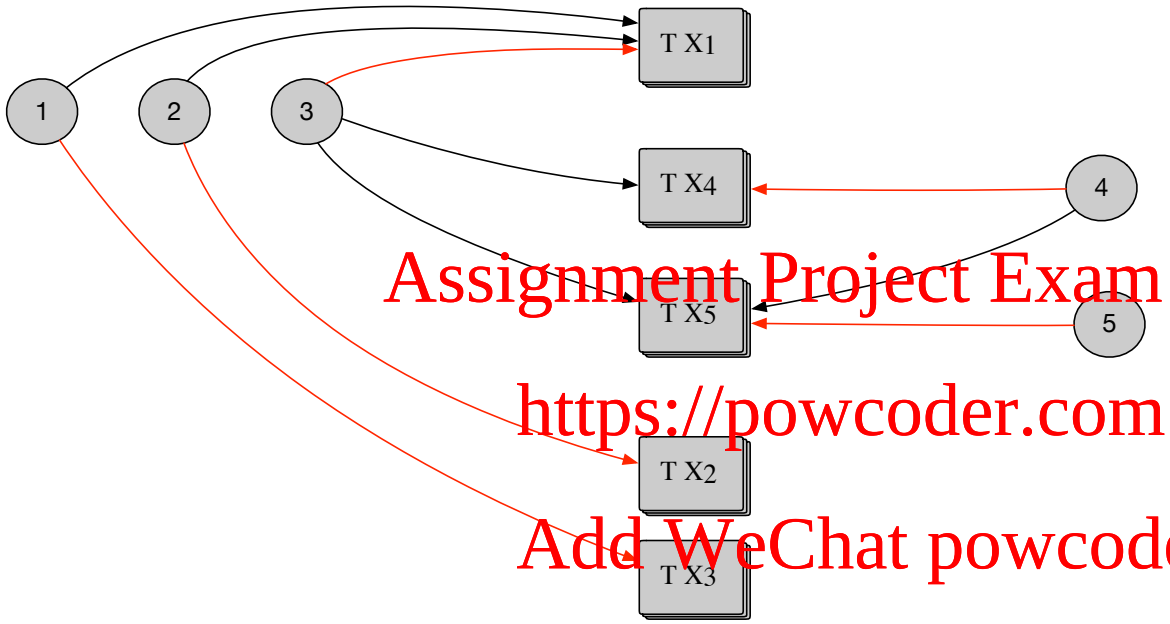
Quiz:



The owners of the two new transactions only choose coins that is not an input of 0-mix transactions

Question: The input of which transactions are identifiable?

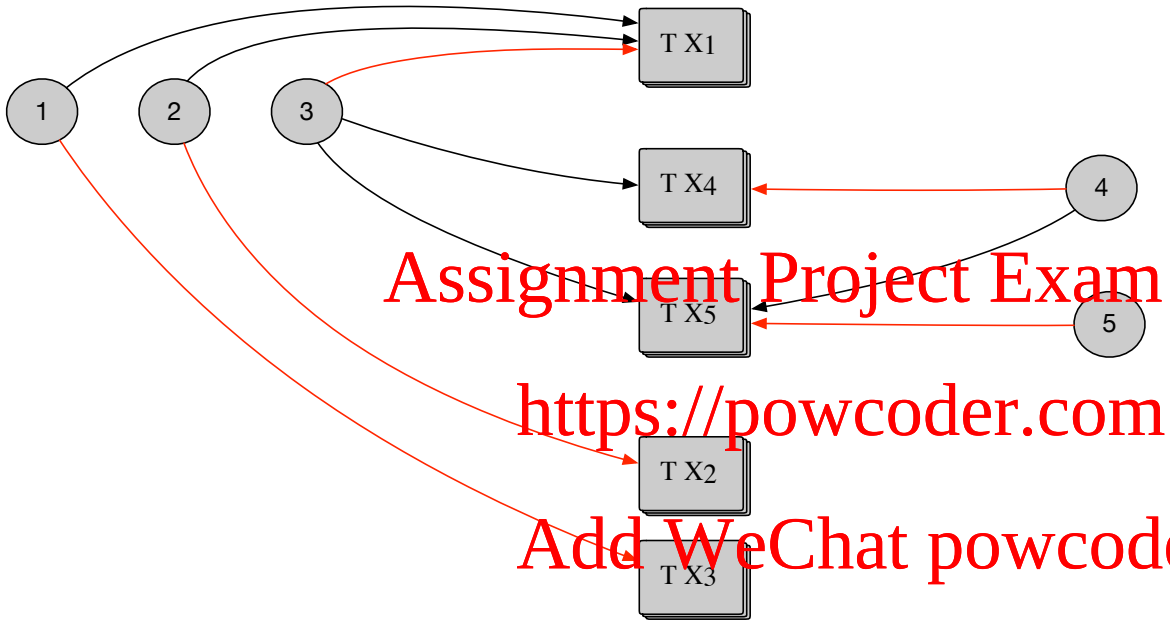
Even worse …



- The owners of TX_1, TX_2, TX_3 are traceable!

Amrit Kumar et. al. A Traceability Analysis of Monero's Blockchain, *ESORICS, 2017*.

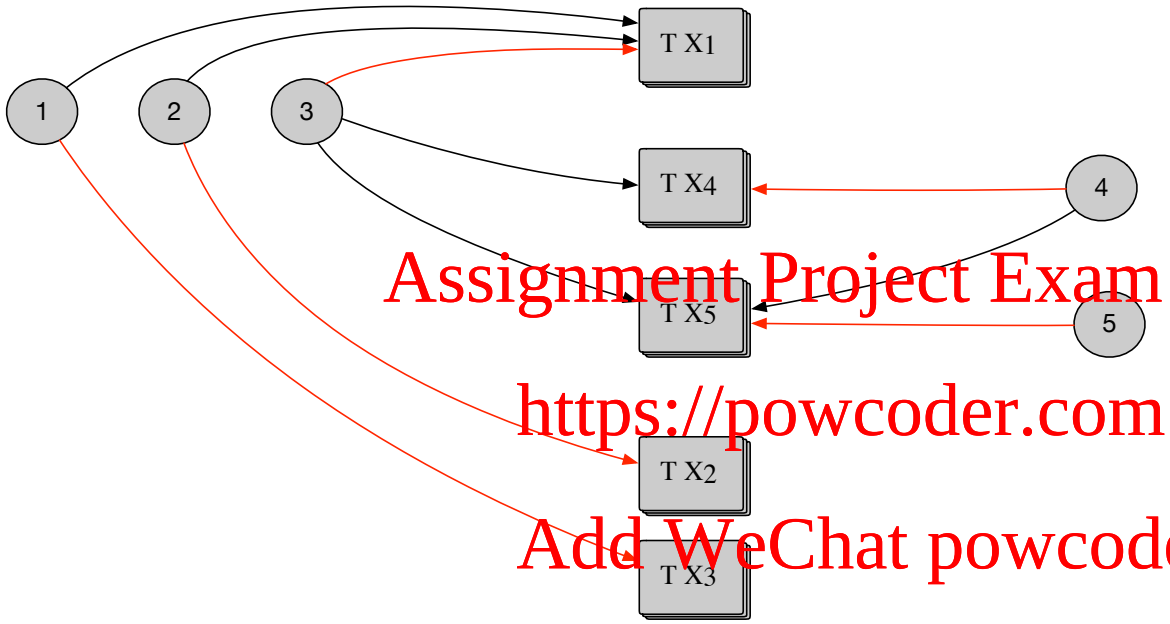
Even worse …



- The owners of TX_1, TX_2, TX_3 are traceable!
- So, coin 3 is also known to be spent in TX_1.

Amrit Kumar et. al. A Traceability Analysis of Monero's Blockchain, *ESORICS, 2017*.

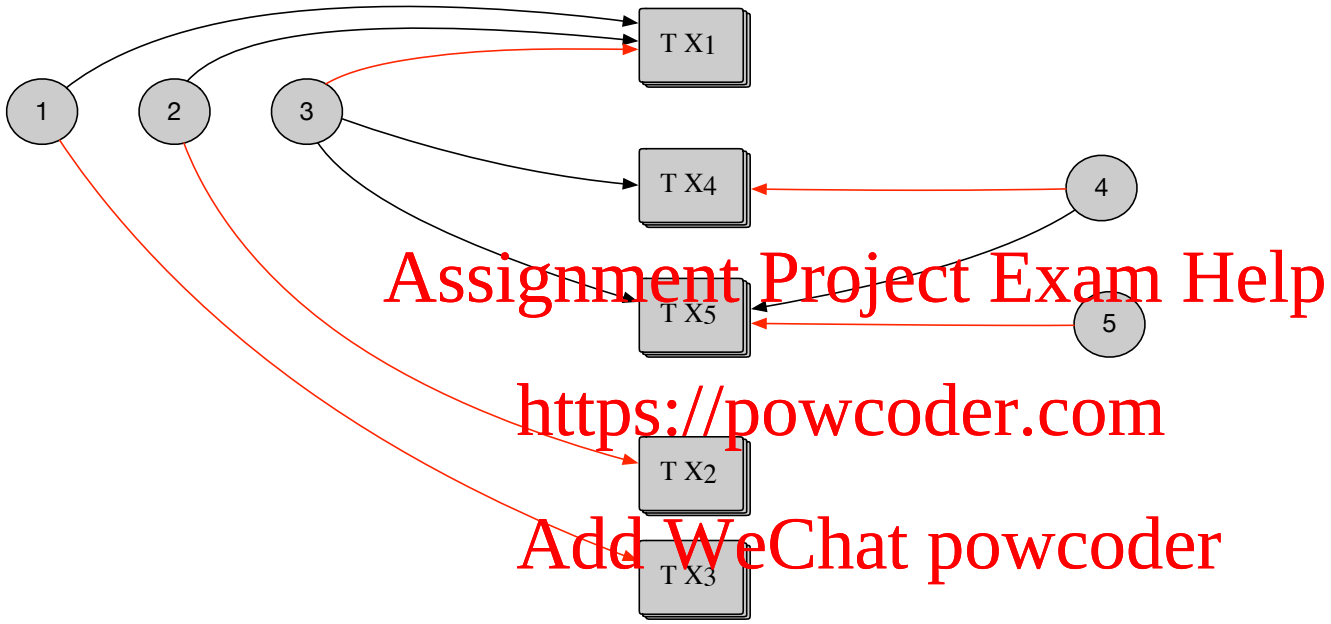
Even worse …



- The owners of TX_1, TX_2, TX_3 are traceable!
- So, coin 3 is also known to be spent in TX_1.
- Even though no input of TX_4 and TX_5 is used as 0-mixin input.

Amrit Kumar et. al. A Traceability Analysis of Monero's Blockchain, *ESORICS, 2017*.

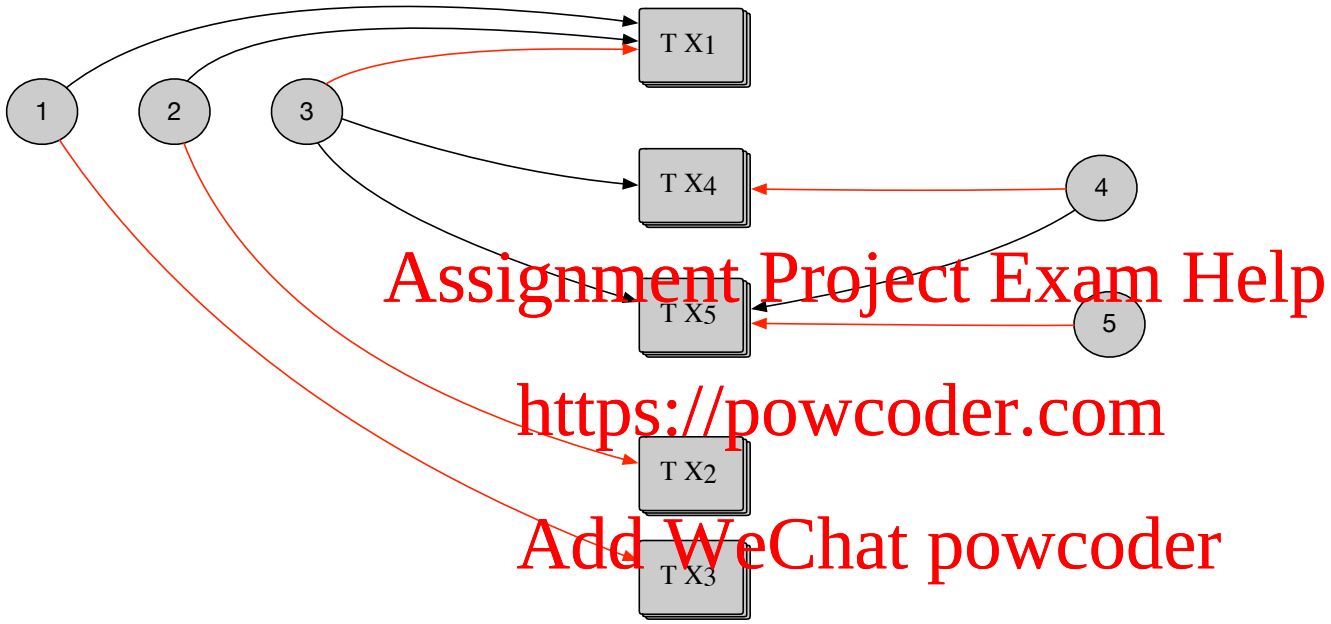
Even worse …



- The owners of TX_1, TX_2, TX_3 are traceable!
- So, coin 3 is also known to be spent in TX_1.
- Even though no input of TX_4 and TX_5 is used as 0-mixin input.
  - The owner of TX_4 is traceable!

Amrit Kumar et. al. A Traceability Analysis of Monero's Blockchain, *ESORICS, 2017*.

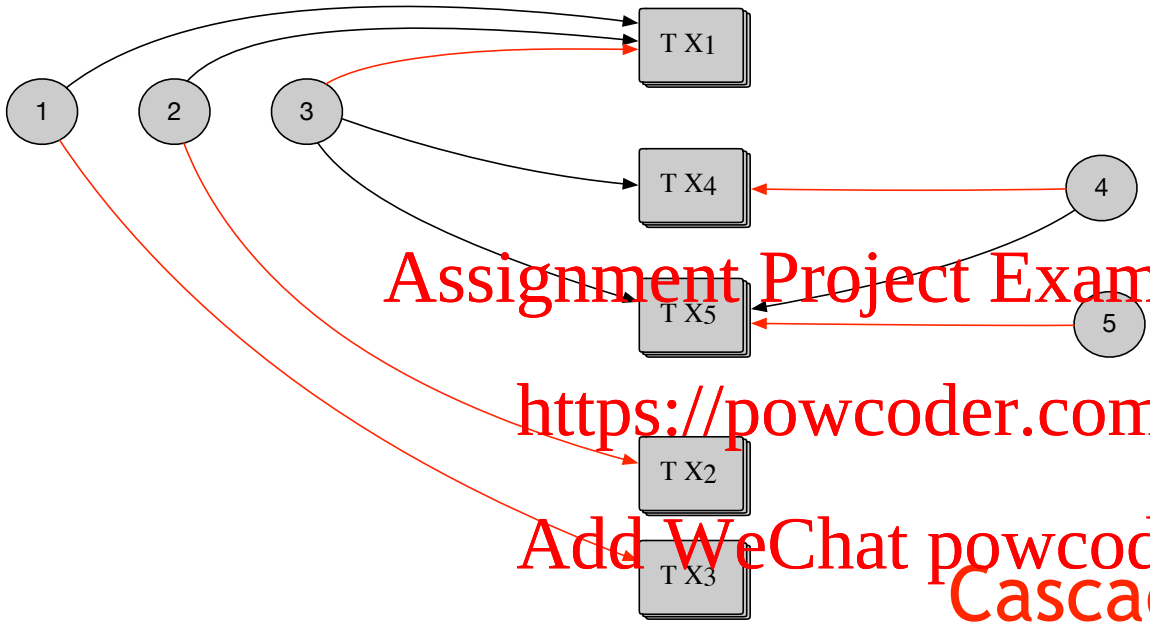
Even worse …



- The owners of TX_1, TX_2,TX_3 are traceable!
- So, coin 3 is also known to be spent in TX_1.
- Even though no input of TX_4 and TX_5 is used as 0-mixin input.
  - The owner of TX_4 is traceable!
  - The owner of TX_5 is traceable!

Amrit Kumar et. al. A Traceability Analysis of Monero's Blockchain, *ESORICS, 2017*.

Even worse …



Cascade effect!

- The owners of TX_1, TX_2,TX_3 are traceable!
- So, coin 3 is also known to be spent in TX_1.
- Even though no input of TX_4 and TX_5 is used as 0-mixin input.
  - The owner of TX_4 is traceable!
  - The owner of TX_5 is traceable!

Amrit Kumar et. al. A Traceability Analysis of Monero's Blockchain, *ESORICS, 2017*.

Zero Mixin attack

Before April 15, 2017, block height 1288774

- 12158814 transaction Monero inputs do not contain any mixins! (64.04% of all inputs)
- For the rest inputs (35.96%), 63% of them are deducable by the cascade effect!

Malte Moser et. al. *An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, 2018.*

Mixin selection

When the attack was observed, Monero developers enforced a network-wide rules on the minimum number of mixins, and miners reject transactions with number of mix-ins lower than that:

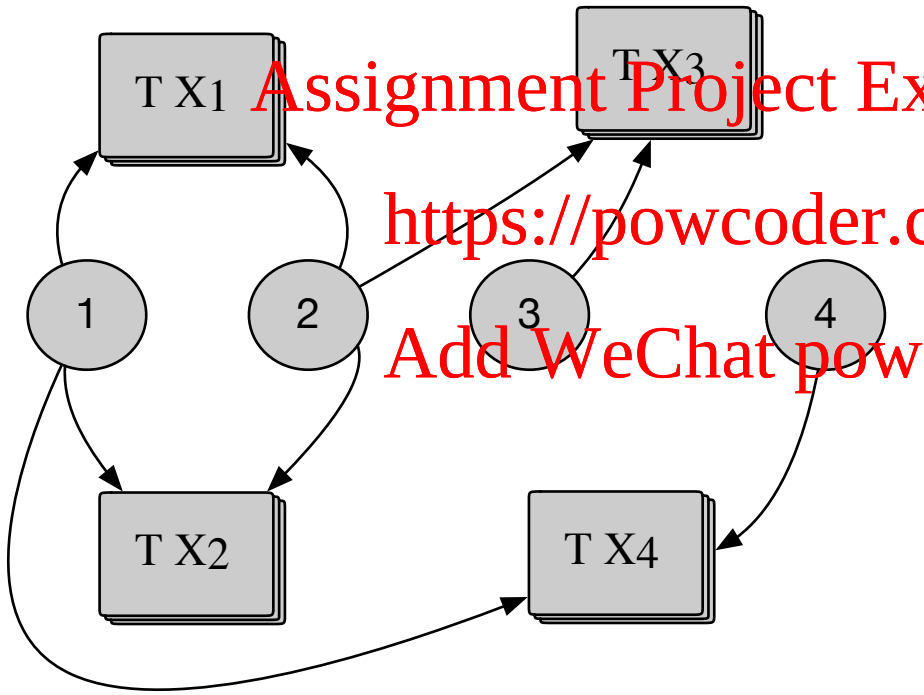
- **2016-03-23**, minimum mix-in of 2 (Ring size>=3)
- **2017-09-16**, minimum mix-in of 4 (Ring size>=5)
- **2018-03-29**, minimum mix-in of 6 (Ring size>=7)
- **2018-10-18**, **fixed Ring size=11**

Does this solve the problem?

https://github.com/monero-project/monero#monero-software-updates-and-consensus-protocol-changes-hard-fork-schedule

Passive inference attacks

Example 1: inputs of transactions are
TX_1= {1,2}, TX_2={1,2}, TX_3 ={2,3}, TX_4 ={1,4}

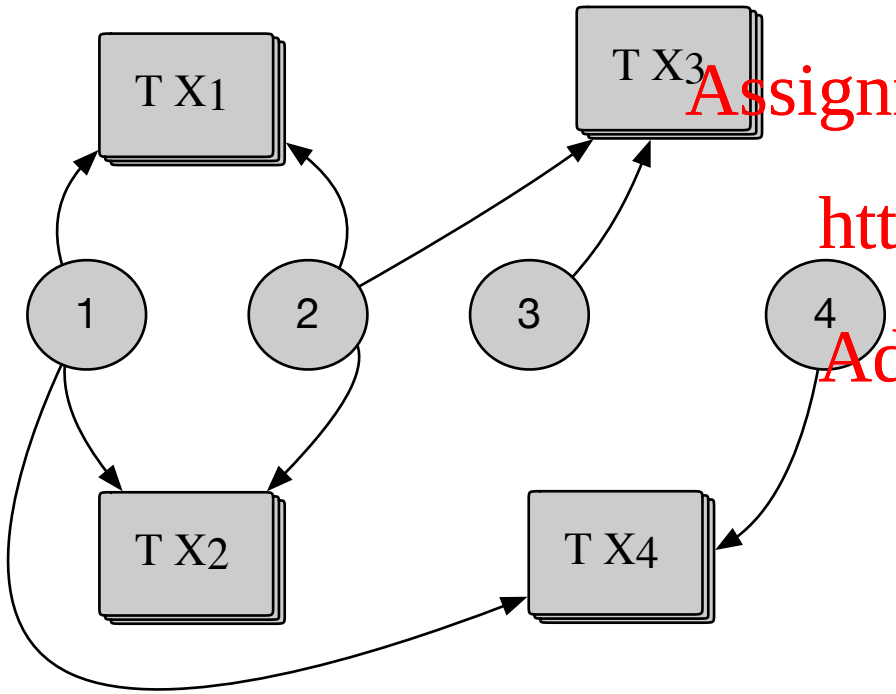


Can you identify the real input of any transaction? Why?

Jiangshan Yu et. al. *Re-thinking untraceability in the CryptoNote-style blockchain, IEEE Computer Security Foundations Symposium, 2019.*

Passive inference attacks

Example 1: inputs of transactions are
TX_1= {1,2}, TX_2={1,2}, TX_3 ={2,3}, TX_4 ={1,4}

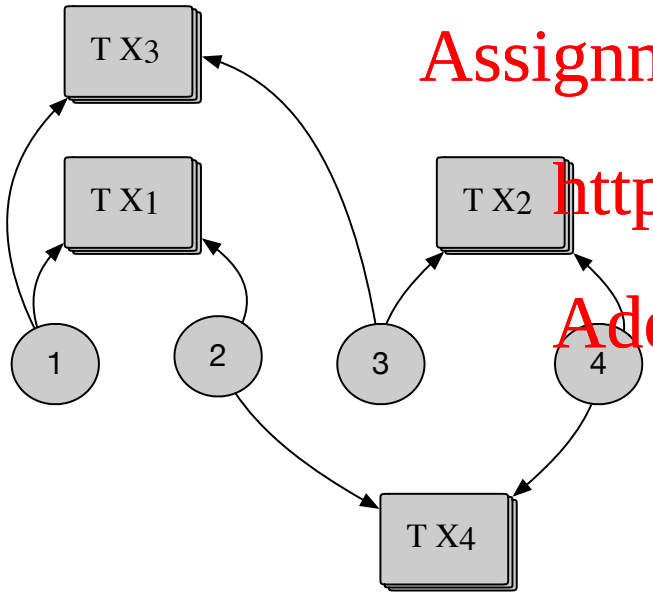


- Each coin can only be spent once, so coin 1 and 2 must have been spent in TX_1 and TX_2, but we don't know which coin is spent in which TX.
- Coin 3 is spent in TX_3
- Coin 4 is spent in TX_4

Jiangshan Yu et. al. *Re-thinking untraceability in the CryptoNote-style blockchain, IEEE Computer Security Foundations Symposium, 2019.*

Passive inference attacks

Example 2: inputs of transactions are
TX_1= {1,2}, TX_2={3,4}, TX_3 ={1,3}, TX_4 ={2,4}



Can you identify the real input of any transaction? Why?

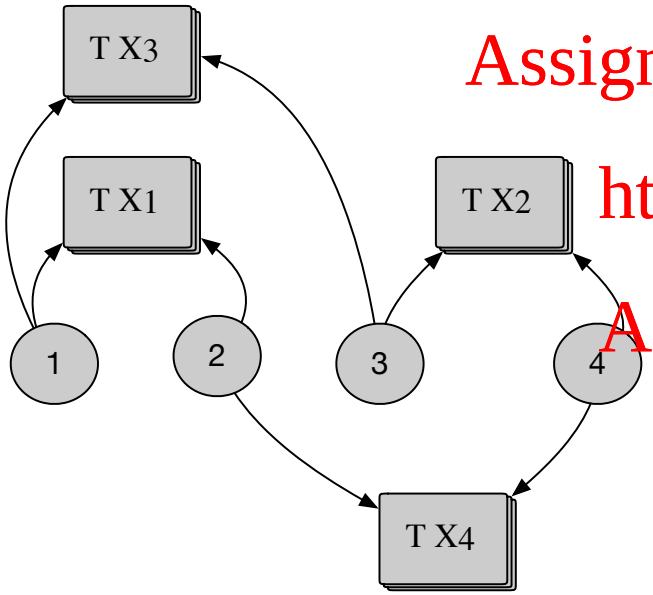
By observing, we cannot deanonymise any transaction.

But… What if the attacker is a Monero user?

Jiangshan Yu et. al. *Re-thinking untraceability in the CryptoNote-style blockchain, IEEE Computer Security Foundations Symposium, 2019.*

Active inference attacks

Example 2: inputs of transactions are
TX_1= {1,2}, TX_2={3,4}, TX_3 ={1,3}, TX_4 ={2,4}

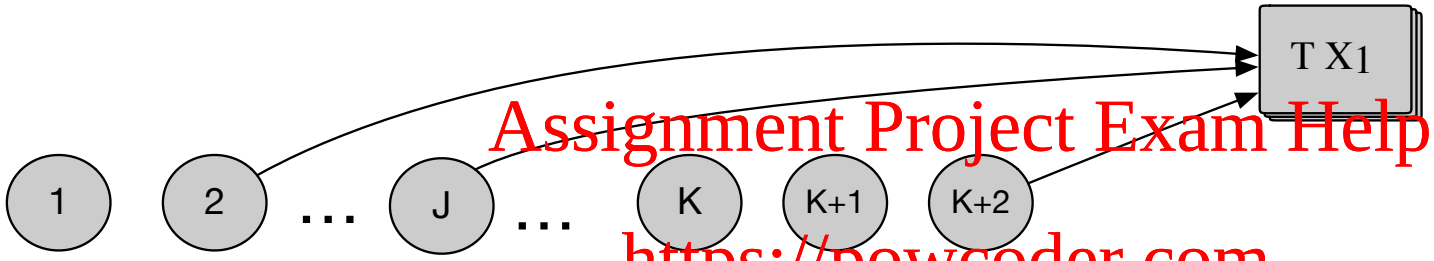


If the attacker is an owner of coin 1, and it is spent in TX1, then it knows

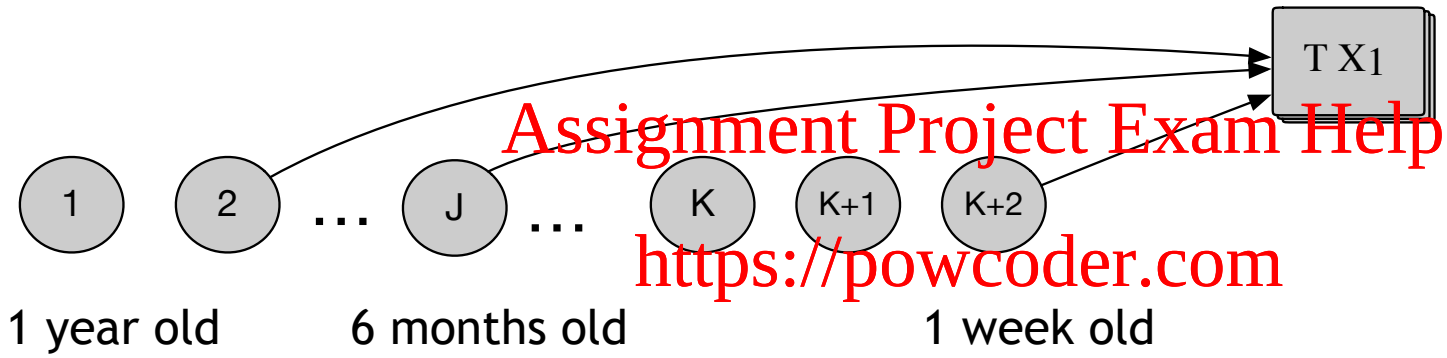
- Coin 3 is spent in TX_3
- Coin 4 is spent in TX_2
- Coin 2 is spent in TX_4

Jiangshan Yu et. al. *Re-thinking untraceability in the CryptoNote-style blockchain, IEEE Computer Security Foundations Symposium, 2019.*

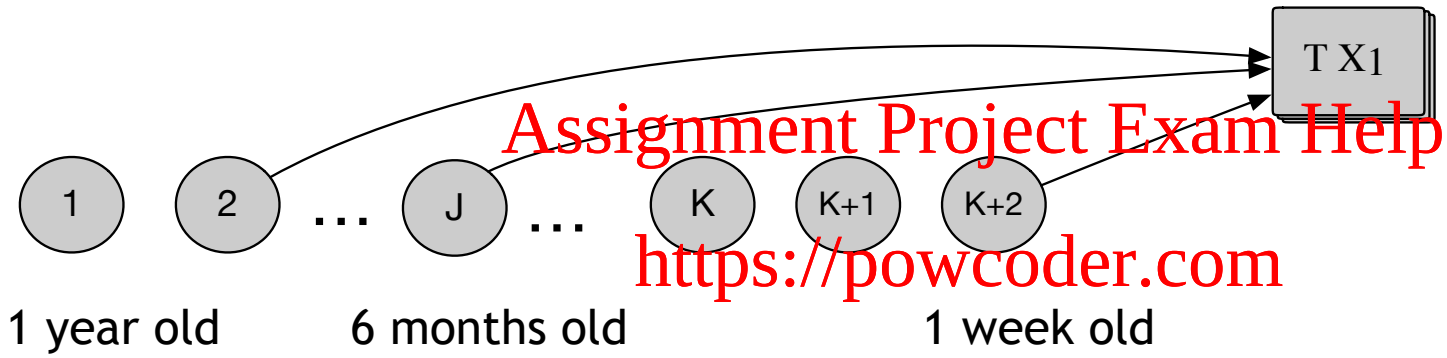
Temporal analysis



Temporal analysis



Temporal analysis



This has a very high probability to be the real input

Age distribution of inputs

(a) Age distribution among all inputs (mixins and real) from blocks 0.9M-1.2M

(b) Age distribution among all mixed-out mixins from blocks 0.9M-1.2M

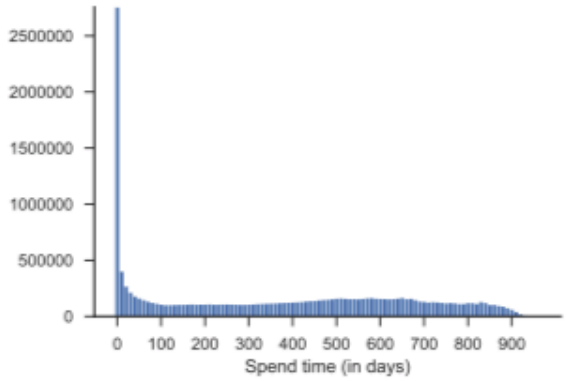
(c) Estimated age distribution of real inputs (recovered from deducible transactions, among blocks 0.9M-1.2M)

(a) Age distribution of all inputs
(b) Age distribution of inputs that are identified as mixins (from other attacks, e.g. 0-mixin)
(c) Estimated age distribution of real inputs

(a)-(b)=(c)

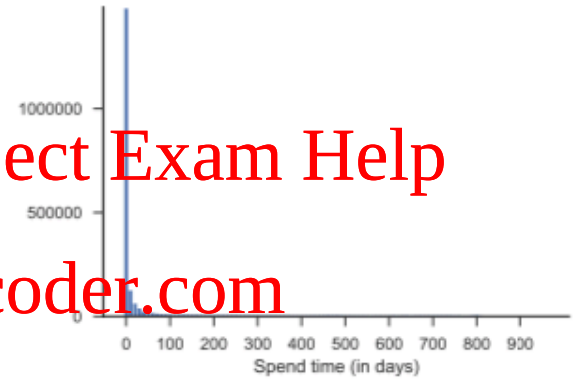
Malte Moser et. al. *An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, 2018.*

Age distribution of inputs



(a) Age distribution among all inputs (mixins and real) from blocks 0.9M-1.2M

(b) Age distribution among all mixins from blocks 0.9M-1.2M



(c) Estimated age distribution of real inputs (recovered from deducible transactions, among blocks 0.9M-1.2M)

The accuracy rate is about 80%, for all non-0-mixin coins!

Malte Moser et. al. *An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, 2018.*

Age distribution of inputs

(a) Age distribution among all inputs (mixins and real) from blocks 0.9M-1.2M

(b) Age distribution among all mixed-out mixins from blocks 0.9M-1.2M

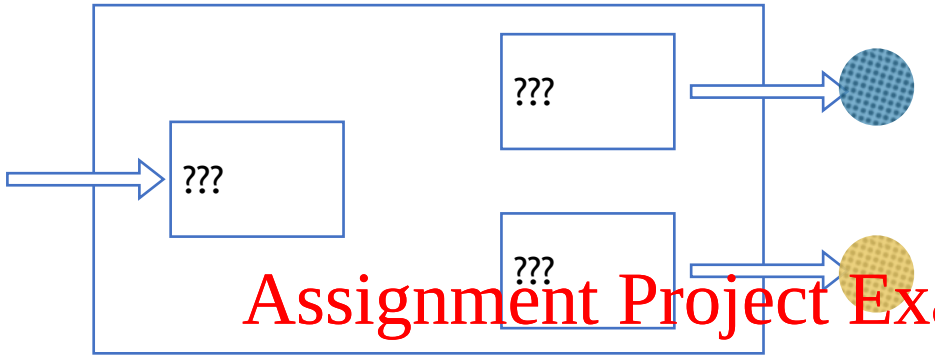
(c) Estimated age distribution of real inputs (recovered from deducible transactions, among blocks 0.9M-1.2M)

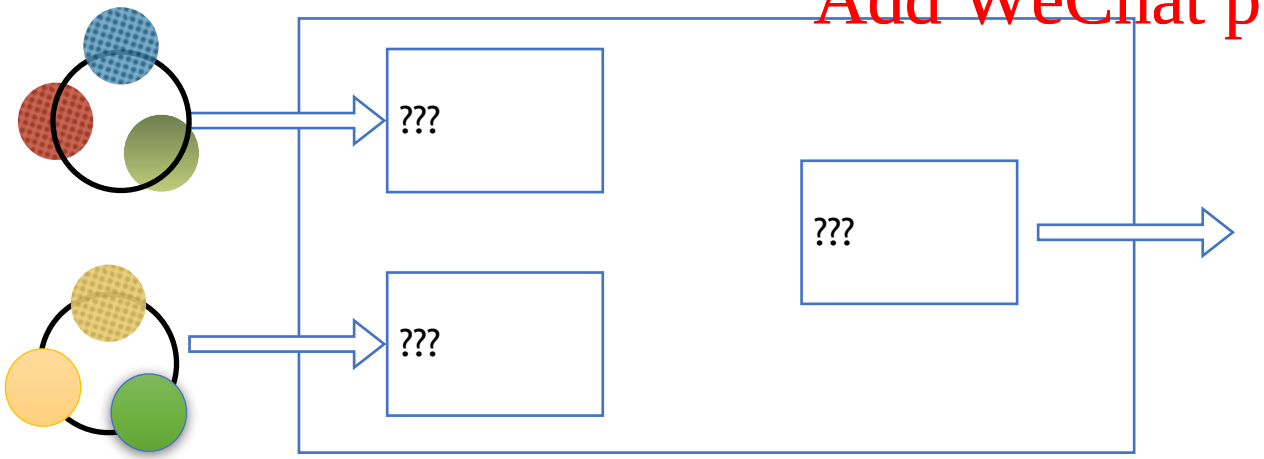
The accuracy rate is about 80%, for all non-0-mixin coins!

Solution: Choose more “recent” coins as mixins.

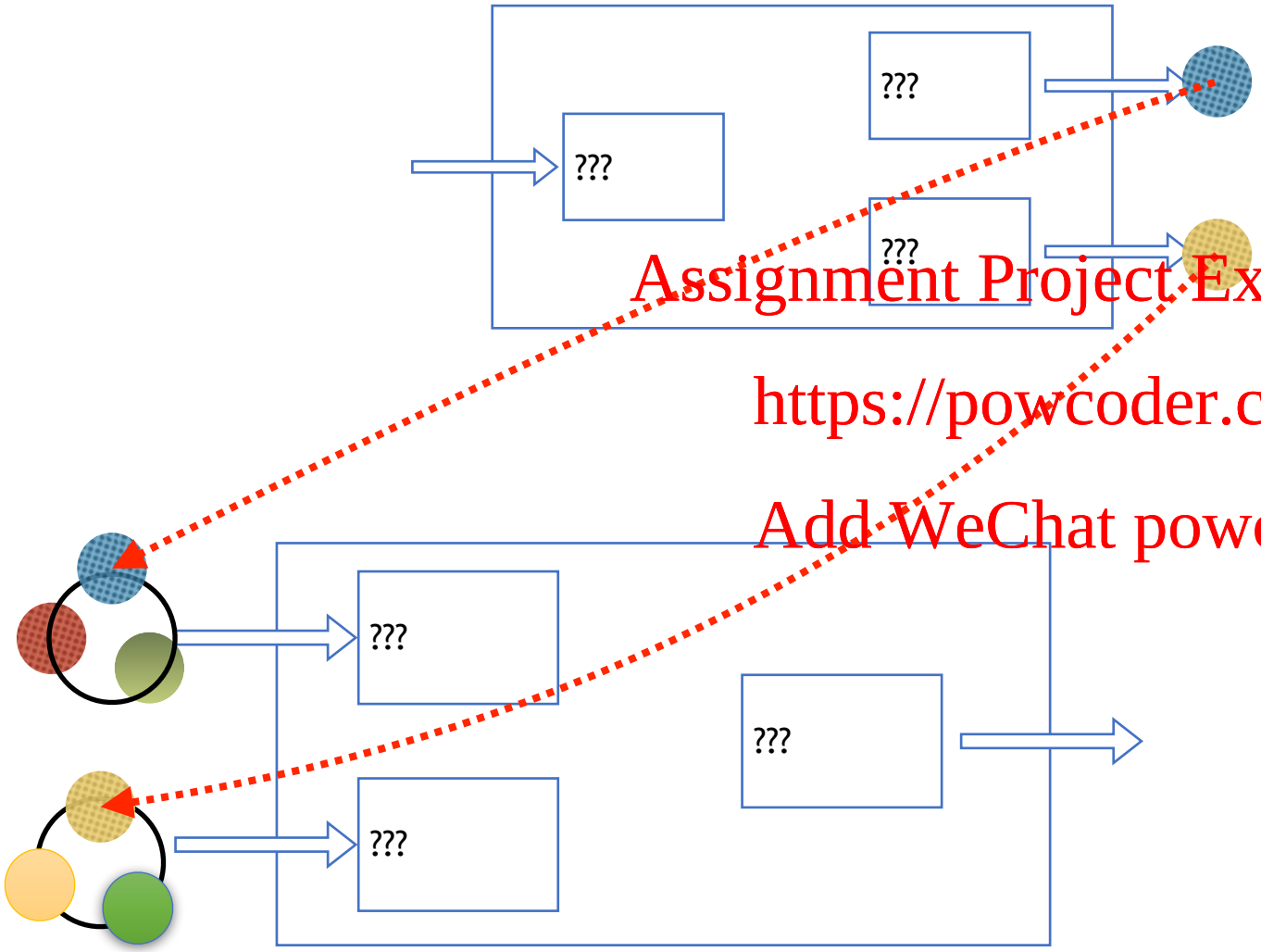
Malte Moser et. al. *An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, 2018.*

Merging of outputs

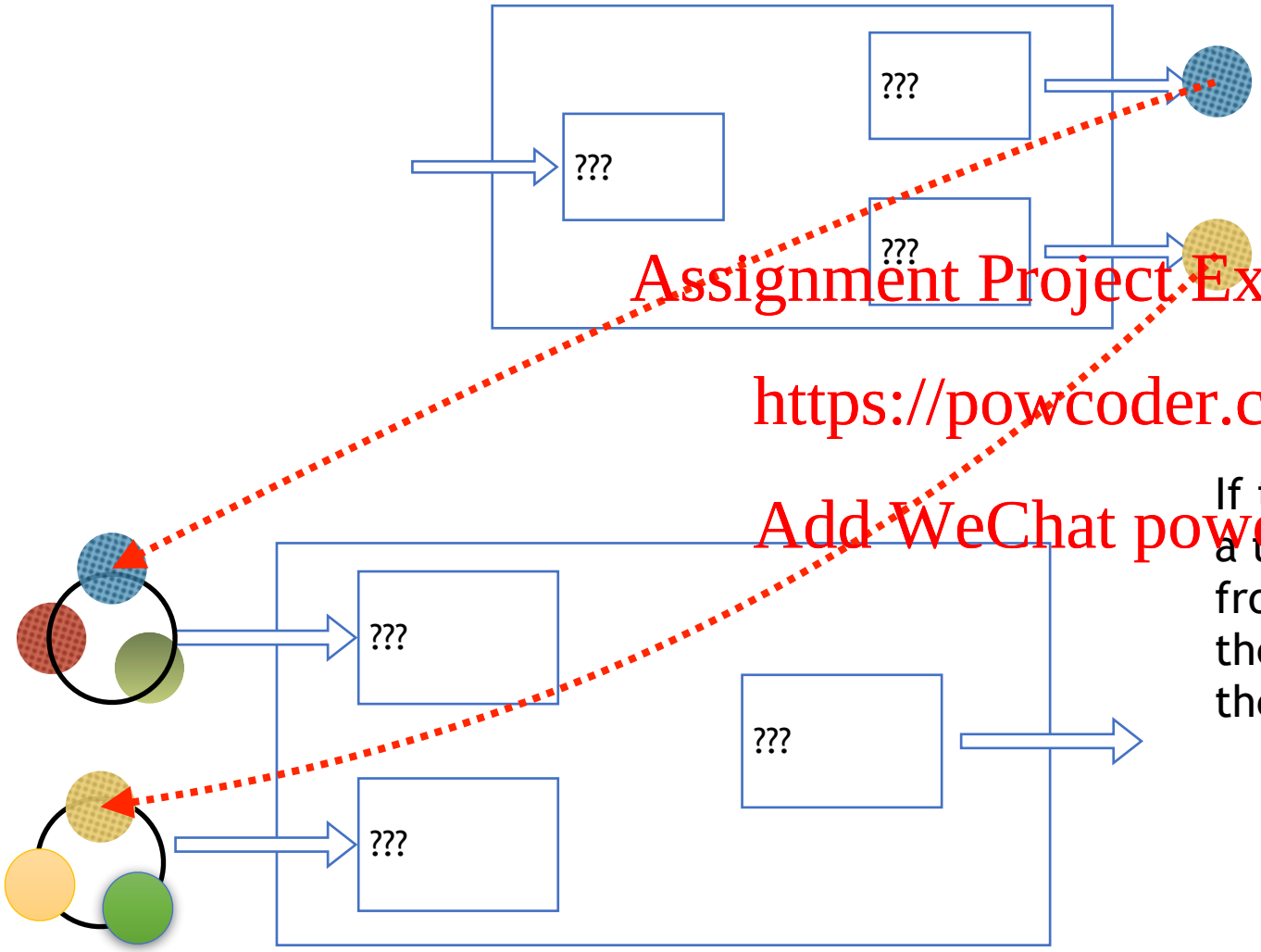




Merging of outputs

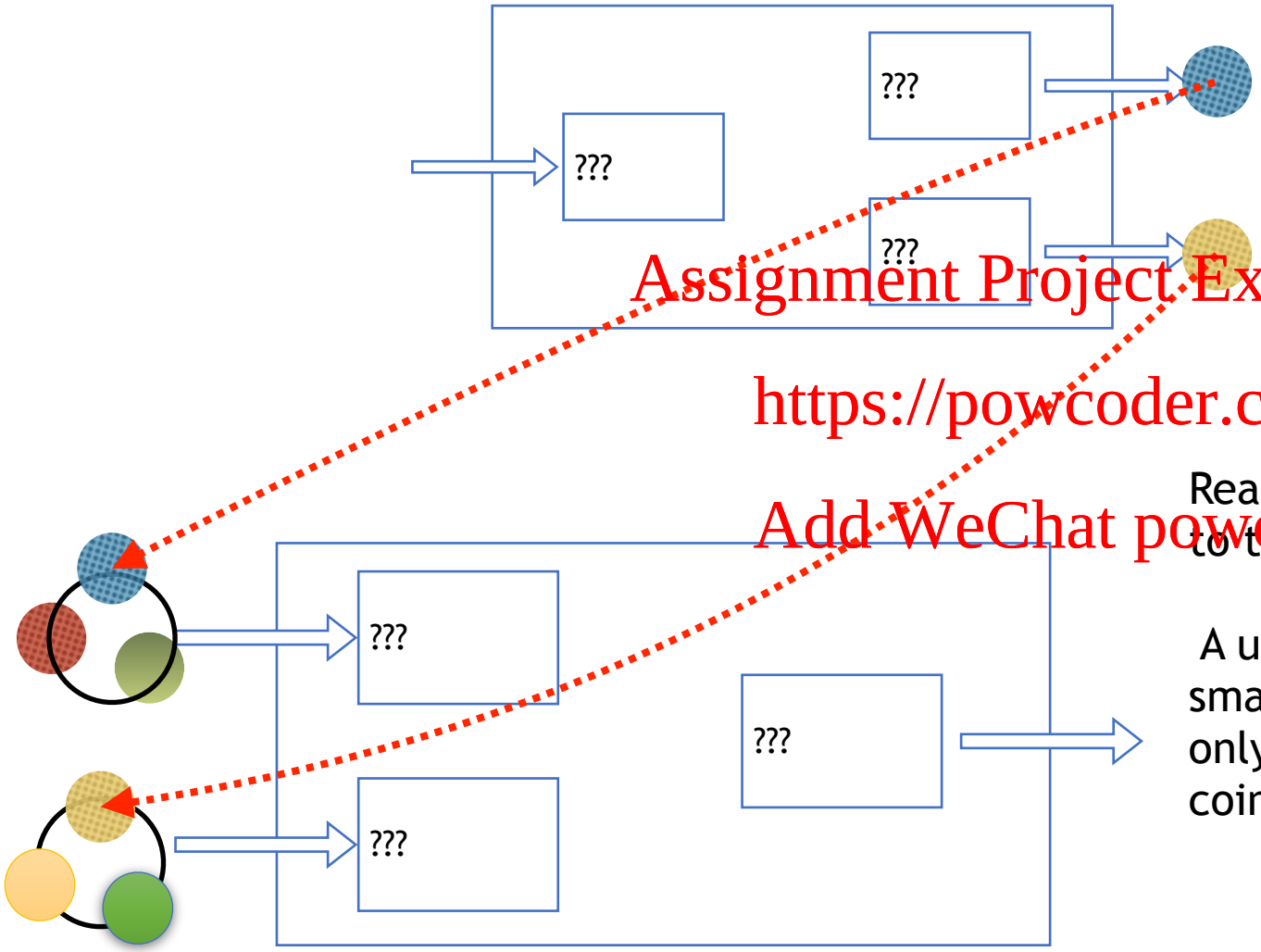


Merging of outputs



If two coins in two rings of a transaction are coming from the same transaction, then they are likely to be the real coin being spent.

Merging of outputs



Reasons to only send coins to the user itself:

A user might want to have small changes rather than only having a big amount of coin.

Zero-Knowledge Proofs

Goldwasser, Micali, and Rackoff (1985)

- Zero-Knowledge Proofs allow a prover to prove a statement to a verifier without revealing any secret information.
- It can be interactive or non-interactive.

Zcash

- Transactions can be transparent or shielded.
- By using a type of zero-knowledge proof called zk-SNARKs, Zcash allows shielded transactions to be verified without revealing the sender, the receiver or the transaction amount.
- *The vast majority of the transactions in Zcash are transparent.*

Next week: Byzantine Agreement