Bitcoin and Blockchain Technology

Bitcoin Transactions, Forensic, and Fungibility

v2021.03.12

Comments, corrections, and questions: [https://drive.google.com/open?id=1FpudunEqrBY8WLTSLzwThOoFxMKGTCho](https://drive.google.com/open?id=1FpudunEqrBY8WLTSLzwThOoFxMKGTCho)
Table of Contents

1. Bitcoin Transactions
2. Addresses and WIFs
3. Bitcoin Script Language
4. Standard Transactions
5. Blockchain Forensic
6. Fungibility and the Future of Transactions
Bitcoin: A Protocol and a Currency

- **Bitcoin**: protocol, software, and community
- **bitcoins**: units of the currency

*bitcoins are sent using the Bitcoin protocol*

*bitcoins are the native digital asset intrinsic to the Bitcoin protocol*
Bitcoin: The Protocol

- Distributed public ledger of transactions
- Shared with peer-to-peer technology
- Massively duplicated across computer network nodes
- Allowing ownership transfer of a native digital scriptural asset
- Its native “digital token” can be exchanged, but not duplicated
- Keeps records of every transaction forever
Bitcoins: The Currency

- Only exist as public ledger documented transactions
- Are associated to public address(es) like

```
1FEz167JCVgBvhJBahpzmrsTNewhiwgWVG
```

- the bitcoin distributed public ledger certifies for everybody how many bitcoins are associated to any address

https://blockstream.info/address/1FEz167JCVgBvhJBahpzmrsTNewhiwgWVG

It is mine; you are REALLY encouraged to tip
Pseudonymity, Anonymity

Bitcoin is pseudonymous, not anonymous:

- The bitcoin address does not provide direct information about the actual bitcoin owner
- All transactions are transparent to everybody’s inspection
- Perfect persistent public account history: the public ledger is forever

https://blockstream.info
http://blockexplorer.com/
Asymmetric Cryptography: Public/Private Key Pair

Two mathematically linked keys perform opposite digital signature functions:

- The private (secret) key is used to generate digital signatures
- The public key is used by anyone to verify those signatures

- The public key derives from the private key, but the private key cannot be derived from the public one

- The bitcoin address is derived from the public key, but the public key cannot be derived from the address
Asymmetric Cryptography: Public/Private Key Pair

- private key $\rightarrow$ public key $\rightarrow$ bitcoin address(es)
- the private key allows spending the bitcoin associated to the corresponding address(es)

![Bitcoin Address QR Code]

https://www.bitaddress.org
A Bitcoin Transaction: From Alice’s **Address** to Bob’s **Address**

- Transaction message: bitcoin amount to transfer + Bob’s address (+ Alice’s **public** key)
- Alice’s **private** key digitally signs the transaction message
- The transaction message is broadcasted to the network
- With Alice’s **public** key any network node can verify that:
  - The amount is at Alice’s **address** disposal
  - The digital signature is valid, i.e. the transaction message has not been tampered or modified
  - The transaction message has been signed by the **private** key associated to Alice’s **address**
- The public ledger is updated with the new transaction
- Everybody knows Bob’s **address** has received that amount
Transactions Cannot Be Altered, They Could Be Censored

- Transactions cannot be altered

- Bitcoins cannot be redirected

- Transactions could only be censored, preventing their registration on the public ledger, as if they never happened; anyway, this is hard to achieve
Bitcoin Safe Custody

- Bitcoins are effectively owned by whoever can spend them
- i.e. whoever can access the private key needed to spend them
- Securing private keys is crucial for safe storage
- Software (and hardware) wallets can be used to manage keys and addresses:
  - Desktop client: Bitcoin Core, Electrum
  - Mobile client: Samurai Wallet (Android), Green (iOS / Android), BreadWallet (iOS), Bitcoin Wallet (Android), Copay (iOS / Android)
  - Hardware wallet: Trezor, Ledger
  - Cold storage: never exposed to Internet, stored away
Table of Contents

1. Bitcoin Transactions
2. **Addresses and WIFs**
3. Bitcoin Script Language
4. Standard Transactions
5. Blockchain Forensic
6. Fungibility and the Future of Transactions
Encoding Numbers With Different Digit Sets

- **Binary** (two) digits: 01

- **Decimal** (ten) digits: 0123456789

- **Hexadecimal** (sixteen) digits: 0123456789ABCDEF

- **Base58** (fifty-eight) digits: all alphanumeric characters (numbers, uppercase, and lowercase) omitting 0 (zero), O (capital o), I (capital i) and l (lower case L)
  123456789ABCDEFHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz
Parsimonious Big Number Representation

The larger is the available digit set
↓↓
The lesser digits are required to represent big numbers

e.g. $16^5 - 2$:

- Binary: 11111111111111111110
- Decimal: 1048574
- Hexadecimal: FFFFE
- Base58: 6Nhs
**Base58 Check Encoding**

1. **Payload**
2. **Prefix** || **Payload** || **Suffix** = **ExtPayload**

   * **double SHA256 Checksum Calculation**
     a. **ExtPayload**
     b. **SHA256(ExtPayload)**
     c. **SHA256(SHA256(ExtPayload))**
     d. **Checksum** = first 4 bytes of previous step

3. **ExtPayload** || **Checksum**
4. **Base58 Check encoding** = **Base58(ExtPayload || Checksum)**

*The Base58 Check decoding stage will first use the checksum to detect possible errors in ExtPayload before actual decoding*
Public/private Keys: Base58 Representation

Base58 is used for the compact representation of Bitcoin public/private keys:

- **Address**: *(some form of)* public key in Base58 representation
- **Wallet Import Format**: private key in Base58 representation

Base58 encoding help to transport information across channels that are designed to deal with textual data instead of binary data.
# Table of Contents

1. Bitcoin Transactions
2. Addresses and WIFs
3. **Bitcoin Script Language**
4. Standard Transactions
5. Blockchain Forensic
6. Fungibility and the Future of Transactions
Stack Data Structure

- Based on the *Last In First Out (LIFO)* principle

- Operators *push* data on the top of the stack or *pop* out data from the top of the stack

- Conditional operators evaluate a condition, pushing a *TRUE/FALSE* result on the top of the stack
“The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime. Because of that, I wanted to design it to support every possible transaction type I could think of. The problem was, each thing required special support code and data fields whether it was used or not, and only covered one special case at a time. It would have been an explosion of special cases. The solution was script, which generalizes the problem so transacting parties can describe their transaction as a predicate that the node network evaluates. The nodes only need to understand the transaction to the extent of evaluating whether the sender's conditions are met.”

(Satoshi Nakamoto)

https://bitcointalk.org/index.php?topic=195.msg1611#msg1611
Bitcoin Script Language

A very simple Forth-like language that uses reverse-polish notation
1. no loops or complex flow control capabilities
2. ensure termination, i.e. finite time execution (implied by 1)
3. memory access is stack-based: there are no variables, calculations are performed on the stack

Bitcoin Script is purposefully stateless and not Turing-complete

Limited flexibility is a deliberate security feature, preventing vulnerability from the transaction validation mechanism
Bitcoin Script Language: Goals

Fundamentally different programming model than ordinary programming: it favors a verification model, not a computation model
- provability (prove proof in finite time)
- solvability of the halting problem (impossible for Turing complete)

It is possible to verify arbitrary code execution, without the need for Turing-completeness

- Computational efficiency (all nodes will verify the script: provide proofs, do not require excessive computation)
- Soundness (keep it simple: sophistication must not introduce attack vectors)
- Privacy
- Compactness (small impact on blockchain, less data also increases efficiency and privacy)
(Un)Locking The Script

- Locking Puzzle: ‘+3=5’

- Unlocking Puzzle: ‘2’

- Unlocking + Locking Puzzle: ‘2+3=5’

- Locking ScriptPubKey:
  3 OP_ADD 5 OP_EQUAL

- Unlocking ScriptSig:
  2

- ScriptSig + ScriptPubKey:
  2 3 OP_ADD 5 OP_EQUAL
Verify $2+3=5$ Using Script

### Stack

- $2$
- $3$
- OP_ADD
- $5$
- OP_EQUAL
Verify $2+3=5$ Using Script

2 3 OP_ADD 5 OP_EQUAL

→ 2
- 3
- OP_ADD
- 5
- OP_EQUAL

Stack

- 2
Verify $2+3=5$ Using Script

```
2 3 OP_ADD 5 OP_EQUAL
```

- 2
- $\rightarrow$ 3
- OP_ADD
- 5
- OP_EQUAL

Stack:
```
3
2
```
Verify 2+3=5 Using Script

2 3 OP_ADD 5 OP_EQUAL

- 2
- 3
→ OP_ADD
- 5
- OP_EQUAL

Stack

- 5
Verify $2+3=5$ Using Script

```
2 3 OP_ADD 5 OP_EQUAL
```

- 2
- 3
- OP_ADD
→ 5
- OP_EQUAL

```
Stack

5
5
```
Verify $2+3=5$ Using Script

$2$  $3$  $OP\_ADD$  $5$  $OP\_EQUAL$

- 2
- 3
- OP_ADD
- 5
→ OP_EQUAL

Stack

- TRUE
Interactive Script Playgrounds


- convert Script to JavaScript http://www.crmash.com/script-playground/

- https://ide.bitauth.com/
Operators

256 opcodes total (15 disabled, 75 reserved)

- Arithmetic
- If/then
- Logic/data handling
- Crypto
  - Hashes
  - Signature verification
  - Multi-signature verification
Operators

- **OP_DUP** duplicates the top stack value
- **OP_HASH160** performs double hashing of the top stack value, first using SHA256 and then RIPEMD160
- **OP_HASH256** performs double hashing of the top stack value using SHA256
- **OP_EQUAL** returns TRUE if the two top stack values are exactly equal, FALSE otherwise
- **OP_VERIFY** marks transaction as invalid if top stack value is not TRUE. The top stack value is removed
- **OP_EQUALVERIFY** is equivalent to OP_EQUAL followed by OP_VERIFY
- **OP_CHECKSIG** checks that the input signature is a valid signature using the input public key for the hash of the current transaction
- **OP_RETURN** marks transaction as invalid. A standard way of attaching extra data to transactions is to add a zero-value TxO with a scriptPubKey consisting of OP_RETURN followed by exactly one pushdata operator

© 2021 Digital Gold Institute

https://en.bitcoin.it/wiki/Script
Alternative to Script: e.g. Simplicity

- SegWit introduced the possibility of having alternative scripting languages, affecting only the involved transactions

- E.g.: Simplicity
Table of Contents

1. Bitcoin Transactions
2. Addresses and WIFs
3. Bitcoin Script Language
4. **Standard Transactions**
5. Blockchain Forensic
6. Fungibility and the Future of Transactions
Transaction Script

- **TxOs** include a *scriptPubKey* locking mathematical puzzle (usually including, in some way, the bitcoin **address** or the **public key**)

- The puzzle must be solved in order to spend the **UTxO**

- The spending **TxIn** provides *scriptSig* unlocking solution (usually including, in some way, the **private key** signature)
Script Evaluation

- The Unlock+Lock script \((\text{scriptSig} + \text{scriptPubKey})\) is evaluated.

- If the script fails or its result is \(\text{FALSE}\), then the \(\text{TxIn}\) is invalid.

- A \(\text{UTxO}\) is unaffected by failed attempts to spend it.

- A \(\text{TxIn}\) that satisfies the \(\text{UTxO}\) conditions does spend it: the \(\text{TxO}\) remains in the blockchain, but it is removed from the \(\text{UTxO}\) pool.
Scripts are not really concatenated anymore: executed separately for security reason, stack being transferred between the two
Standard Transactions

Many different scripts are possible, but for security reason a transaction is usually relayed only if $\text{IsStandard()}$, i.e.

- does not violate good network behavior rules
- its scripts match a small set of believed-to-be-safe templates

Valid non-standard transactions, if included in blocks, are accepted.
Table of Contents

1. Bitcoin Transactions
2. Addresses and WIFs
3. Bitcoin Script Language
4. Standard Transactions
5. Blockchain Forensic
6. Fungibility and the Future of Transactions
Blockchain Analysis Companies: Chainalysis

We provide blockchain data and analysis to government agencies, exchanges, and financial institutions across 40 countries. Our compliance and investigation tools, education, and support help our customers understand what’s happening on blockchains.

Cryptocurrency Businesses
Use the same compliance solution trusted by the world’s largest cryptocurrency businesses, banks, and law enforcement agencies.

Financial Institutions
Understand your exposure to crypto, monitor ongoing customer activity, and comply with regulatory guidance.

Government Agencies
Understand the real-world entities behind every cryptocurrency transaction and combat serious crimes.

© 2021 Digital Gold Institute
Blockchain Analysis Companies: Chainalysis

Building trust in blockchains

We create transparency for a global economy built on blockchains, enabling banks, businesses, and governments to have a common understanding of how people use cryptocurrency.

WHAT WE DO

We provide blockchain data and analysis to government agencies, exchanges, and financial institutions across 40 countries. Our compliance and investigation tools, education, and support help our customers understand what's happening on blockchains.
Chainalysis KYT (Know Your Transaction) combines industry-leading blockchain intelligence, an easy-to-use interface, and a real-time API to reduce manual workflows while helping cryptocurrency businesses comply with local and global regulations.
CRYPTOCURRENCY FORENSICS

Chainalysis Reactor

Explore. Investigate. Take Action. Reactor is the investigation software that connects cryptocurrency transactions to real-world entities, enabling you to combat criminal activity on the blockchain.
<table>
<thead>
<tr>
<th>Month</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>May</td>
<td>Intelligence Brief: Farhad Exchange</td>
</tr>
<tr>
<td>May</td>
<td>Intelligence Brief: The FutureNet Ponzi Scheme</td>
</tr>
<tr>
<td>May</td>
<td>Intelligence Brief: Bullet-proof Hosting Provider Transacting with North Korean Actor?</td>
</tr>
<tr>
<td>Mar</td>
<td>Markets Report: What Causes Market Events?</td>
</tr>
<tr>
<td>Mar</td>
<td>Markets Report: Mining Pool Market Power</td>
</tr>
<tr>
<td>Feb</td>
<td>Cryptocurrency Typologies: Our Guide to Who's Who on the Blockchain</td>
</tr>
<tr>
<td>Jan</td>
<td>Cryptocricne Report: Money Laundering, Darknet Markets, Scams, and More</td>
</tr>
</tbody>
</table>
Total cryptocurrency sent and received by illicit entities vs. Illicit share of all cryptocurrency transaction volume, 2017-2019

- Share of cryptocurrency volume that is illicit
- Total received by illicit entities
- Total sent from illicit entities
Share of total cryptocurrency transaction volume by illicit subcategory

- Terrorism financing
- Stolen funds
- Scams
- Sanctions
- Ransomware
- Darknet markets
- Child abuse material

© 2021 Digital Gold Institute
CypherTrace

Cryptocurrency Intelligence Solutions for More than 87% of Global Virtual Assets

*Trace Transactions, Comply with AML Regulations, and Monitor Risk*

See how CipherTrace—with unparalleled support for more than 800 tokens—detects money laundering, powers law enforcement investigations, and enables regulatory supervision.
Protecting Business Against Financial Crime In Crypto

Financial institutions and cryptocurrency companies rely on Elliptic's blockchain analytics to manage risk and meet regulatory compliance worldwide.

REQUEST A DEMO
Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics

Mark Weber*
MIT-IBM Watson AI Lab
mrweber@mit.edu

Giacomo Domeniconi*
IBM Research
Giacomo.Domeniconi1@ibm.com

Jie Chen
MIT-IBM Watson AI Lab
chenjie@us.ibm.com

Daniel Karl I. Weidele
IBM Research AI
daniel.karl@ibm.com

Claudio Bellei
Elliptic
claudio@elliptic.co

Tom Robinson
Elliptic
tom@elliptic.co

Charles E. Leiserson
MIT CSAIL
cel@mit.edu

Figure 4: Chronograph User Interface: User can navigate through time-sliced transaction data and observe transaction patterns and patterns of change. Illicit transactions are dyed red. Further statistics are displayed on the left.
https://uif.bancaditalia.it/adempimenti-operatori/contrasto/index.html

**Liste**

**ONU**
Sezione del sito dell’ONU relativa alle sanzioni finanziarie disposte dal Consiglio di Sicurezza (Comitato per le Sanzioni 1267) nei confronti dei soggetti ed entità collegati alle organizzazioni terroristiche ISIL e Al-Qaida.
La lista consolidata dei nominativi è disponibile a questo [link](https://uif.bancaditalia.it/adempimenti-operatori/contrasto/index.html).

**Unione Europea**
Sezione del sito della Commissione Europea relativa alle sanzioni finanziarie previste dall’Unione Europea.
La lista consolidata di tutte le persone, gruppi ed entità oggetto di congelamento nel territorio europeo è consultabile - previa registrazione di credenziali per l’accesso al sito (indirizzo e-mail e password) - al seguente [link](https://uif.bancaditalia.it/adempimenti-operatori/contrasto/index.html). L’elenco comprende i soggetti designati dalle Nazioni Unite e dai Paesi appartenenti all’Unione Europea nell’ambito delle misure di contrasto al finanziamento del terrorismo e all’attività dei Paesi che minacciano la pace e la sicurezza internazionale.

**OFAC**
Sezione del sito del Dipartimento del Tesoro degli Stati Uniti relativa alle sanzioni finanziarie previste dall’OFAC (Office of Foreign Assets Control)
La lista consolidata delle persone ed entità oggetto di sanzioni finanziarie da parte delle autorità americane è consultabile al seguente [link](https://uif.bancaditalia.it/adempimenti-operatori/contrasto/index.html).
Refinitiv World-Check

KYC SCREENING AND DUE DILIGENCE

Refinitiv World-Check Risk Intelligence

Help protect your business from financial crime and reduce risk by fulfilling your KYC due diligence screening obligations with accurate and structured information. World-Check Risk Intelligence is used and trusted by the world’s biggest companies.
Tu sei qui: Home › Ufficio Stampa › Ultime notizie › Anno 2019 › Luglio › Bitcoin ed evasione fiscale - Intermediario abusivo nasconde 750mila euro al fisco

Bitcoin ed evasione fiscale - Intermediario abusivo nasconde 750mila euro al fisco

Udine, 11 luglio 2019

Comando Provinciale Udine

Mentre illustrava, urbi et orbi, le enormi opportunità di guadagno offerte dagli investimenti in bitcoin, celava, al Fisco, la sua lucrosa attività spacciandosi per semplice “colezionista” di criptovalute.

Il suo attivismo non è, però, sfuggito ai Finanzieri del Comando Provinciale di Udine che:

Opendime

THE BITCOIN CREDIT STICK

FIRST BITCOIN BEARER INSTRUMENT
Opendime

THE BITCOIN CREDIT STICK
OFF-CHAIN & 100% PRIVATE

The 1st Bitcoin Bearer Instrument or just call it a "Bitcoin Stick"

Opendime is a small USB stick that allows you to spend Bitcoin like a dollar bill. Pass it along multiple times. Connect to any USB to check balance. Unseal anytime to spend online. Trust no one.
Monero: Listed on the following Exchanges

https://monero.org/services/exchange/
Europol on Wasabi Wallet

What happened?
In the last period, Europol’s EC3 started to notice an increasing number of investigations involving Wasabi Wallet. Wasabi is a light wallet that implemented a very effective method of mixing bitcoin using a so-called “coinjoin”. This means that it merges coins originating from different users into one transaction and redistributes these into many standardised amounts on the output side, which makes it difficult to correctly link inputs with their respective outputs.

Wasabi claims to be an open source, non-custodial, privacy-focused Bitcoin wallet for desktop use, which implements trustless coin shuffling with mathematically provable anonymity.
European Cybercrime Centre: Wasabi Bits

- Wasabi is a very effective decentralized method of mixing bitcoin using a «coinjoin» with many privacy-focused options
- Possibly the most convenient and secure way to mix bitcoins
- Increasing number of cases featuring Wasabi Wallet, also involving criminal activities

- ECC law enforcement-relevant considerations:
  - Easy to visually identify Wasabi wallet transaction;
  - Tracing tools identify most of the addresses but do not demix the transactions;
  - Possible to follow the money but high probability of staying undetected
Custodians

CheckSig
TRANSPARENT BITCOIN CUSTODY

Institutional-focused custody firms for digital assets

The Block
Workshops

A&C Law has promoted a series of three webinars:

- Bitcoin's legal qualification
- Bitcoin as asset eligible for portfolio allocation
- Technological and regulatory requirements for investments in Bitcoin
Profilazione del Rischio

<table>
<thead>
<tr>
<th>VALUTAZIONE DEL RISCHIO DI RICICLAGGIO E DI FINANZIAMENTO AL TERRORISMO - PERSONE FISICHE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLIENTE (NOME COGNOME)</td>
</tr>
<tr>
<td>DATA COMPILAZIONE PROFILO DI RISCHIO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CLASSIFICAZIONE DELLA PRATICA AI FINI ANTIRICICLAGGIO:</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMPOSSIBILITA' DI PROCEDERE CON L'OPERAZIONE</td>
</tr>
<tr>
<td>RISCHIO BASSO</td>
</tr>
<tr>
<td>RISCHIO MEDIO BASSO</td>
</tr>
<tr>
<td>RISCHIO MEDIO ALTO</td>
</tr>
<tr>
<td>RISCHIO ALTO</td>
</tr>
<tr>
<td>CLIENTE GIA' IDENTIFICATO CON PROFILO DI RISCHIO PIU' ALTO:</td>
</tr>
<tr>
<td>[Inserire il profilo che era gia' stato assegnato]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QUADRO 1 - CLIENTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Dove si risiede il Cliente?</td>
</tr>
<tr>
<td>2. Quale professione svolge il Cliente?</td>
</tr>
<tr>
<td>3. Qual è il settore economico nell'ambito del quale il Cliente svolge la propria attività?</td>
</tr>
<tr>
<td>4. Qual è il luogo di localizzazione dell'attività svolta o comunque degli affari del Cliente (Solo se diverso da residenza sia per paese che per regione)?</td>
</tr>
<tr>
<td>5. Il Cliente ha rapporti di corrispondenza transfrontalieri con Banche o Istituti finanziari di un Paese extra UE</td>
</tr>
</tbody>
</table>

© 2021 Digital Gold Institute
Mining and Money Laundering

Money laundering can be effectively performed using mining:

- Buying bitcoin from miner at premium
- Operating mining facilities at economic loss
Table of Contents

1. Bitcoin Transactions
2. Addresses and WIFs
3. Bitcoin Script Language
4. Standard Transactions
5. Blockchain Forensic
6. Fungibility and the Future of Transactions
Bitcoin isn’t technically anonymous

Insufficient financial privacy can have serious security and privacy implications for both commercial and personal transactions:

- thieves can focus their efforts on high-value targets
- competitors can learn business details
- negotiating positions can be undermined
Fungibility

- Cash provenance is not to be assessed: this makes cash fungible and cash transactions very efficient
- Electronic money requires travel rule, usually taken care of by financial institutions
- In the case of crypto-assets, who is going to take care of travel rule?
- To check a blacklist (or, even worse, a whitelist) before receiving/sending criptoasset is impractical
- New addresses can be generated on the fly
a lack of fungibility could profoundly impact the very foundations of the system. Clean coins may fetch a premium, while older ones would be less valuable given their history.

Gold is fungible: for bitcoin to be the digital equivalent of gold it must be fungible.
Exclusive: Fake-branded bars slip dirty gold into world markets

Peter Hobson

LONDON (Reuters) - A forgery crisis is quietly roiling the world’s gold industry.
CoinJoin

- A privacy-preserving technique where multiple senders and receivers are combined within a single transaction.

- The goal is to make it difficult for a blockchain observer to link specific senders and receivers, thereby enabling the entities within the CoinJoin to claim plausible deniability.

- CoinJoin is identifiable and as such it can be blacklisted.
Confidential Transactions

- Confidential Transactions (CT) are a step beyond the privacy offered by Bitcoin’s blockchain: pseudonymous (but public) identities
- CT encrypt the amount value, visible only to the transaction parties (and those they choose to reveal the blinding key to)
- Encryption ensures that no bitcoins can been created or destroyed within a transaction
Monero

- Use CT in combination with constructs called *ring signatures* to achieve anonymity and fungibility
- Obfuscate sending and receiving addresses, as well as transacted amounts
- Transactions are confidential and untraceable
- Monero is fungible: by virtue of obfuscation, Monero cannot become tainted through participation in previous transactions
MimbleWimble

- A blockchain protocol for increased privacy, better network scalability, and fungibility
- Published on July 2016 by pseudonymous Tom Elvis Jedusor (French name of Voldemort from Harry Potter)
- It uses blinding factors of balancing inputs and outputs in a commitment scheme as private keys
- Sender and receiver must interact to construct a joint signature to authorize a transfer of funds
- Blocks in MimbleWimble have all their constituent transactions aggregated into one giant transaction, erasing the original transaction boundaries
- Initial block download further benefits from cut-through, in which all spent outputs cancel against corresponding inputs, erasing most of the blockchain history
Schnorr and Taproot

- A foundational upgrade for the Bitcoin protocol designed to increase Bitcoin's fungibility, improve the functionality of scripts, and improve privacy by making all transactions appear the same to external blockchain observers
- Schnorr is a better elliptic curve signature scheme
  - has a formal security proof
  - provably non-malleable
  - linear: enable signature aggregation making multiple signature indistinguishable from a single signature
- Taproot allows complex tree of scripts: at spending time only the single one being satisfied is revealed
Cross-input Aggregation

- It will introduce an additional obfuscation mechanism at the Bitcoin protocol level

- Enable the construction of Schnorr-based CoinJoin transactions with $N$ signers that look like regular, single-signer transactions to outsiders

- Enable CoinJoin to be more easily implemented in popular wallets without strenuous engineering, which may increase the network’s overall anonymity set, or the number of users using this technique
Nothing in this document constitutes an offer to buy or sell, or a solicitation of an offer to buy or sell, any financial instruments. It is not intended to represent the conclusive terms and conditions of any security or transaction, nor to notify you of any possible risks, direct or indirect, in undertaking such a transaction. No entity in Digital Gold Institute shall be responsible for any loss whatsoever sustained by any person who relies on this document.

Nessun contenuto presente in questo documento costituisce un'offerta all'acquisto o alla vendita o sollecitazione all'investimento in relazione a strumenti finanziari e non è inteso a rappresentare i termini e le condizioni definitivi di ogni strumento finanziario ovvero di ogni offerta avente ad oggetto strumenti finanziari, né i rischi diretti od indiretti connessi alla stessa offerta. Nessuna entità di Digital Gold Institute è responsabile delle perdite sostenute da una persona che si affida a questo documento.