Privacy Coins Past, Present, and Future

GHOST PII

Capnion, Inc. March 2022

Who is the speaker?

30 second resume:

- an ancient metro Saint Louis townie
- grew up in University City
- University City High School 2003
- B.A. Washington University 2007 (econ and math)
- Ph.D. University of Michigan 2013 (math)
- a few years of data science
- founded data privacy tech company Capnion, Inc.

Slides URL:

`https://github.com/capnion/random/blob/master/acm_capnion_privacy_coin.pdf`

Agenda

Basics

- What is a privacy coin?
- Why Bitcoin and others are not privacy coins

Flash under the hood

- Zero-knowledge proof
- Transaction bundling

The landscape right now

- Why you want it, Why you don’t...
- What’s out there?

Focus on Ethereum features and non-features

What is a privacy coin?

The original blockchain architecture is merely *pseudonymous*. Privacy coins employ advanced cryptographic techniques, notably *zero-knowledge proof*, to make the distributed ledger truly anonymous.

Well-known privacy coins

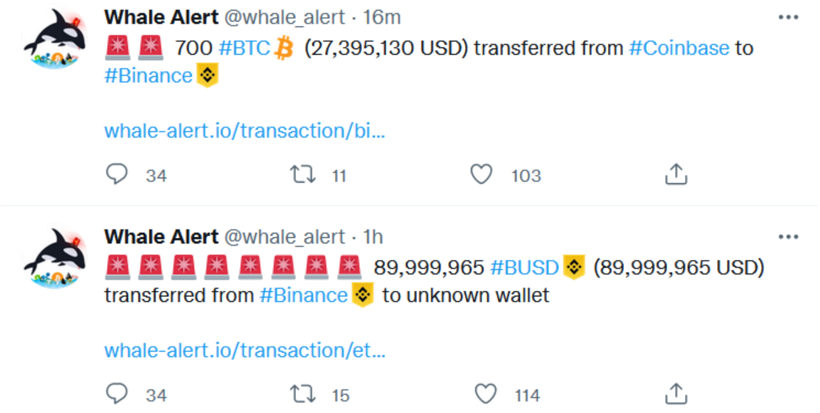
- Zcash, Monero
- Litecoin just recently via Mimblewimble

Well-known not- privacy coins

- Bitcoin
- Ethereum has some cool privacy functions but is not a privacy coin. As we will discuss later, this might be the right spot.

Blockchain Transparency 1

https://twitter.com/whale_alert



Whale Alert @whale_alert · 16m

🚨 🚨 700 #BTC (27,395,130 USD) transferred from #Coinbase to #Binance

whale-alert.io/transaction/bi...

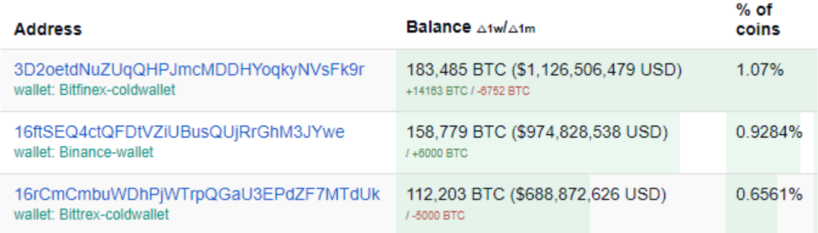
Whale Alert @whale_alert · 1h

🚨 🚨 🚨 🚨 🚨 🚨 🚨 🚨 89,999,965 #BUSD (89,999,965 USD) transferred from #Binance to unknown wallet

whale-alert.io/transaction/et...

Blockchain Transparency 2

`https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html`



Address	Balance △1w/△1m	% of coins
3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r wallet: Bitfinex-coldwallet	183,485 BTC ($1,126,506,479 USD) +14163 BTC / -6752 BTC	1.07%
16ftSEQ4ctQFDtVZiUBusQUjRrGhM3JYwe wallet: Binance-wallet	158,779 BTC ($974,828,538 USD) / +6000 BTC	0.9284%
16rCmCmbuWDhPjWTrpQGaU3EPdZF7MTdUk wallet: Bittrex-coldwallet	112,203 BTC ($688,872,626 USD) / -5000 BTC	0.6561%

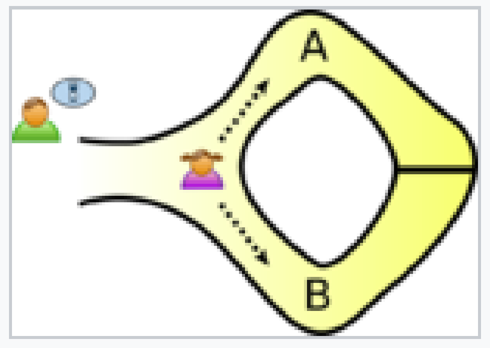
What is a zero knowledge proof?

A **zero-knowledge proof** is a method by which a *prover*, traditionally called Peggy, proves to a *verifier*, traditionally called Victor, that

- Peggy possess a particular piece of information, and...
- Peggy does not reveal that information to Victor.

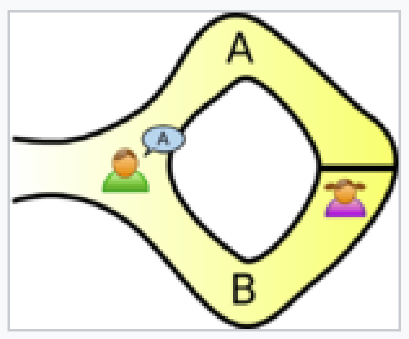
Example Many digital signature algorithms fit our definition well: Peggy proves to Victor that she holds the private key corresponding to a particular public key but Victor does not receive any information about the private key itself.

Classic Cave Example 1



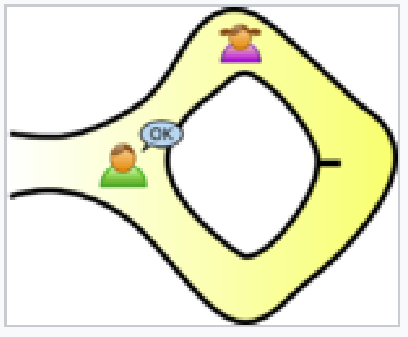
Peggy wishes to prove to Victor that she can open the magic door in the back of a donut-shaped cave, yet she wants to keep her method for opening the door a secret from Victor.

Classic Cave Example 2



After Peggy has entered the cave by one path or the other, Victor shouts into the cave whether Peggy should return by Path A or Path B.

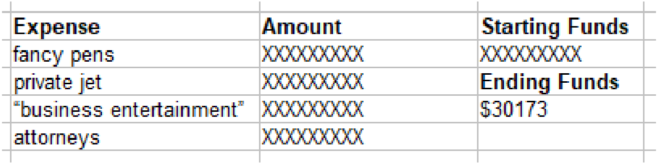
Classic Cave Example 3



If Peggy can consistently return by the path Victor requests, she has demonstrated that she has a method for passing through the magic door, yet Victor has not seen Peggy open the door.

Blind Double Spending Check

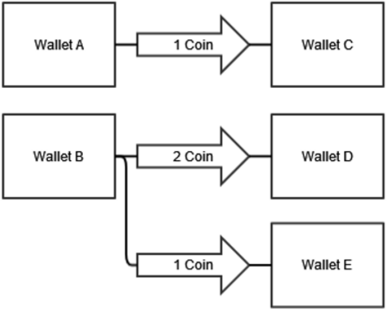
Why does the original blockchain give everyone the whole ledger? So they can verify there is no double spending...



Expense	Amount	Starting Funds
fancy pens	XXXXXXXXX	XXXXXXXXX
private jet	XXXXXXXXX	**Ending Funds**
"business entertainment"	XXXXXXXXX	$30173
attorneys	XXXXXXXXX	

Privacy coins put specially encrypted information on the blockchain and performs this check via mathematical tricks - an example of a zero-knowledge proof.

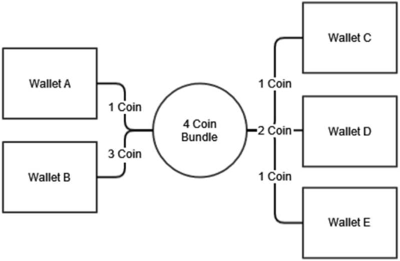
No Bundling: Original Blockchain



While the owners of various wallets may be unknown, in the original (and current) Bitcoin architecture the source, destination, and amount of all transactions is public.

Increased Privacy With Bundling

In this example, cryptographic techniques have been used to bundle transactions and create uncertainty about who is paying how much to whom. In practice, many more transactions would be bundled providing considerable more privacy than in this diagram.



Monero had some dumb, interesting early fumbles...

Why you (don't) want it...

Pros: Privacy

Cons: Inevitably slower, and also privacy again

- Increased regulatory attention (⇒ hard to buy)
- Unsavory bedfellows - criminals love privacy
- Developer errors may also be private

Examples from Zcash

- "Moon math" from a centralized company
- "The Powers of Tau Ceremony" - cool but shady

From a market standpoint, there is probably a "private enough" optimum level of privacy in a cryptocurrency.

What's Out There

Zcash uses a very advanced (not necessarily good) type of zero-knowledge proof called a *zk-SNARK* and provides nearly complete anonymity.

Mimblewimble (used in MimblewimbleCoin) is a popular protocol incorporating a similar zero-knowledge proof called a *Bulletproof*.

Litecoin recently became a privacy coin by adopting the Mimblewimble protocol.

Monero originally used a bundling approach only but has since adopted Bulletproofs as well.

Privacy features in the Ethereum ecosystem

All the magic tricks discussed are available or coming soon in the Ethereum ecosystem as add-ons. Notables include...

- Tornado - a transaction mixer (live now).
- Aztec Protocol - a decentralized exchange employing zero-knowledge anonymity (live now).
- Zether - a smart contract for anonymous transactions (prototype live with some holes).
- Secret Network - privacy techniques for data in smart contracts (not live, might be a minute).

Questions and Conversation

Any questions?

`acmueller@capnion.com`

`https://twitter.com/capnion`

`https://www.linkedin.com/in/alexander-c-mueller-phd-0272a6108/`