Threats and security of cryptocurrencies

A story told short

Łukasz Klasiński

IT department of
University of Wrocław

Blockchain and it's applications

Agenda

1. Threats of cryptocurrency market
2. Future threats
3. Cryptocurrency in crime
4. Frauds & Scams
5. Anonymity & privacy
6. Security layers of crypto

Threats of cryptocurrency market

- Value of currency

Threats of cryptocurrency market

- Value of currency
  - no organizations controlling market and no inflation

Threats of cryptocurrency market

- Value of currency
  - no organizations controlling market and no inflation
  - determined by value of transactions made by participants

Threats of cryptocurrency market

- Value of currency
  - no organizations controlling market and no inflation
  - determined by value of transactions made by participants
  - loss of confidence may result in collapse of trading activities and value

Threats of cryptocurrency market

- Value of currency
  - no organizations controlling market and no inflation
  - determined by value of transactions made by participants
  - loss of confidence may result in collapse of trading activities and value
  - liquidity concerns

Threats of cryptocurrency market

- Value of currency
  - no organizations controlling market and no inflation
  - determined by value of transactions made by participants
  - loss of confidence may result in collapse of trading activities and value
  - liquidity concerns

Strategy

Mining companies try to avoid exceeding the 51% confidence limit in order to make value of cryptos more stable

Threats of cryptocurrency market

- Value of currency
  - no organizations controlling market and no inflation
  - determined by value of transactions made by participants
  - loss of confidence may result in collapse of trading activities and value
  - liquidity concerns

Strategy

Mining companies try to avoid exceeding the 51% confidence limit in order to make value of cryptos more stable

Example

GHash.IO bitcoin mining pool exceeded 51% pool threshold in July 2014.

Threats of cryptocurrency market

- Operational risks

Threats of cryptocurrency market

- Operational risks
  - not possible to reverse transactions

Threats of cryptocurrency market

- Operational risks
  - not possible to reverse transactions
  - access to monies not possible after loosing keys

Threats of cryptocurrency market

- Operational risks
  - not possible to reverse transactions
  - access to monies not possible after loosing keys
  - can't block/stop crypto wallet after loosing keys

Threats of cryptocurrency market

- Operational risks
  - not possible to reverse transactions
  - access to monies not possible after loosing keys
  - can't block/stop crypto wallet after loosing keys

Strategy

Keeping backup of your keys, encrypting them, splitting monies into multiple wallets

Threats of cryptocurrency market

- Regulatory risks

Threats of cryptocurrency market

- Regulatory risks
  - some countries may prevent use of cryptocurrencies

Threats of cryptocurrency market

- Regulatory risks
  - some countries may prevent use of cryptocurrencies
    - no control over taxes paid per transactions

Threats of cryptocurrency market

- Regulatory risks
  - some countries may prevent use of cryptocurrencies
    - no control over taxes paid per transactions
    - government doesn't like decentralized things

Threats of cryptocurrency market

- Regulatory risks
  - some countries may prevent use of cryptocurrencies
    - no control over taxes paid per transactions
    - government doesn't like decentralized things
    - government depend on 'real' monies (that are outranked by crypto)

Threats of cryptocurrency market

- Regulatory risks
  - some countries may prevent use of cryptocurrencies
    - no control over taxes paid per transactions
    - government doesn't like decentralized things
    - government depend on 'real' monies (that are outranked by crypto)
    - transactions may break anti-money laundering regulations

Threats of cryptocurrency market

- Regulatory risks
  - some countries may prevent use of cryptocurrencies
    - no control over taxes paid per transactions
    - government doesn't like decentralized things
    - government depend on 'real' monies (that are outranked by crypto)
    - transactions may break anti-money laundering regulations

Currently banned in

Algeria, Egypt, Morocco, Canada(banking), Bolivia, Columbia, Ecuador, Saudi Arabia, Iran, Bangladesh, India(banking), Nepal, Pakistan, China, Taiwan, Cambodia, Indonesia, Thailand(banking), Vietnam.

Threats of cryptocurrency market

- Cyber risks

Threats of cryptocurrency market

- Cyber risks
  - tempting target for hackers and criminals

Threats of cryptocurrency market

- Cyber risks
  - tempting target for hackers and criminals
  - viruses that drain crypto wallets and steals crypto

Threats of cryptocurrency market

- Cyber risks
  - tempting target for hackers and criminals
  - viruses that drain crypto wallets and steals crypto
  - investors must rely on their own security or third parties

Threats of cryptocurrency market

- Cyber risks
  - tempting target for hackers and criminals
  - viruses that drain crypto wallets and steals crypto
  - investors must rely on their own security or third parties
  - cryptocurrency is highly reliant upon unregulated companies, including some that may lack appropriate internal controls and may be more susceptible to fraud and theft than regulated financial institutions

Threats of cryptocurrency market

- Cyber risks
  - tempting target for hackers and criminals
  - viruses that drain crypto wallets and steals crypto
  - investors must rely on their own security or third parties
  - cryptocurrency is highly reliant upon unregulated companies, including some that may lack appropriate internal controls and may be more susceptible to fraud and theft than regulated financial institutions
  - the software needs to be regularly updated and suspect at times

Threats of cryptocurrency market

- Market risks

Threats of cryptocurrency market

- Market risks
  - currency trades only on demand

Threats of cryptocurrency market

- Market risks
  - currency trades only on demand
  - finite amount of the currency

Threats of cryptocurrency market

- Market risks
  - currency trades only on demand
  - finite amount of the currency
  - limited ownership may make it susceptible to market manipulation

Threats of cryptocurrency market

- Market risks
  - currency trades only on demand
  - finite amount of the currency
  - limited ownership may make it susceptible to market manipulation
  - more volatile than other physical currencies

Threats of cryptocurrency market

- Risks for business

Threats of cryptocurrency market

- Risks for business
  - costs involved in mitigation

Threats of cryptocurrency market

- Risks for business
  - costs involved in mitigation
  - anti-money laundering and privacy laws problems with global range

Threats of cryptocurrency market

- Risks for business
  - costs involved in mitigation
  - anti-money laundering and privacy laws problems with global range
  - individuals can seek to circumvent tax regulations

Threats of cryptocurrency market

- Risks for business
  - costs involved in mitigation
  - anti-money laundering and privacy laws problems with global range
  - individuals can seek to circumvent tax regulations
  - liquidity concerns (again)

Threats of cryptocurrency market

- Risks for business
  - costs involved in mitigation
  - anti-money laundering and privacy laws problems with global range
  - individuals can seek to circumvent tax regulations
  - liquidity concerns (again)
  - transaction fees

Threats of cryptocurrency market

- Risks for business
  - costs involved in mitigation
  - anti-money laundering and privacy laws problems with global range
  - individuals can seek to circumvent tax regulations
  - liquidity concerns (again)
  - transaction fees

Example

After about year and a half Steam ended support for bitcoin payments because of 'hight fees and volatility' of a bitcoin.

Future threats

- Energy consumption(bitcoin)

Future threats

- Energy consumption(bitcoin)
  - currently using 45TWh which is just greater then Portugal(52th in the world)

Future threats

- Energy consumption(bitcoin)
  - currently using 45TWh which is just greater then Portugal(52th in the world)
  - record use is estimated about 73TWh (just greater then Austria ranked 39th)

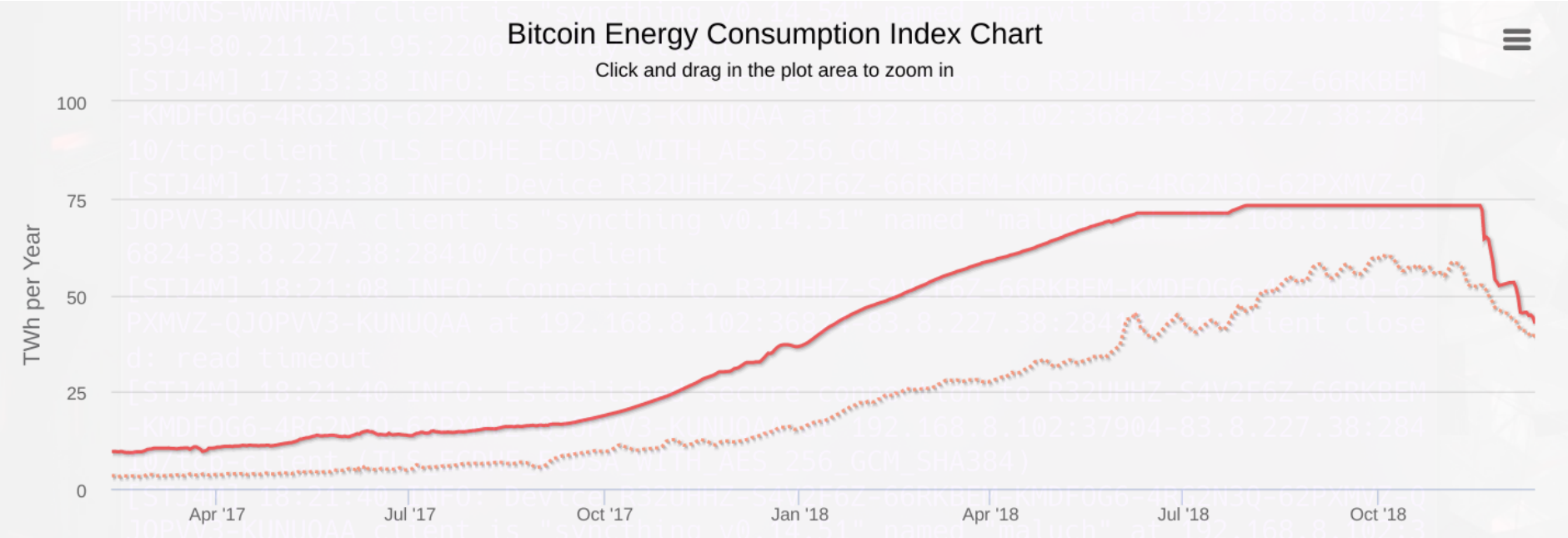
Future threats

- Energy consumption(bitcoin)
  - currently using 45TWh which is just greater then Portugal(52th in the world)
  - record use is estimated about 73TWh (just greater then Austria ranked 39th)
  - currently estimated cost of electricity of mining one bitcoin higher then value of bitcoin (4000$ vs 3100$)

Future threats

- Energy consumption(bitcoin)
  - currently using 45TWh which is just greater then Portugal(52th in the world)
  - record use is estimated about 73TWh (just greater then Austria ranked 39th)
  - currently estimated cost of electricity of mining one bitcoin higher then value of bitcoin (4000$ vs 3100$)
  - with electricity production costs rising and banning crypto mining in electricity-cheap countries (like China), mining may be unprofitable

Future threats



Future threats

- Scalability(bitcoin)

Future threats

- Scalability(bitcoin)
  - capacity is limited by block creation time of 10min

Future threats

- Scalability(bitcoin)
  - capacity is limited by block creation time of 10min
  - results in estimated 3-7 transactions per second

Future threats

- Scalability(bitcoin)
  - capacity is limited by block creation time of 10min
  - results in estimated 3-7 transactions per second
  - creates bottleneck when there is more then 3 transactions per second

Future threats

- Scalability(bitcoin)
  - capacity is limited by block creation time of 10min
  - results in estimated 3-7 transactions per second
  - creates bottleneck when there is more then 3 transactions per second
  - results in transaction fees skyrocketing and delayed processing of transactions

Future threats

- Scalability(bitcoin)
  - capacity is limited by block creation time of 10min
  - results in estimated 3-7 transactions per second
  - creates bottleneck when there is more then 3 transactions per second
  - results in transaction fees skyrocketing and delayed processing of transactions
  - block size limit problem

Future threats

- Node distribution

Future threats

- Node distribution
  - full and half nodes miners

Future threats

- Node distribution
  - full and half nodes miners
  - half nodes more preferable

Future threats

- Node distribution
  - full and half nodes miners
  - half nodes more preferable
  - unequal distribution of full nodes

Future threats

- Node distribution
  - full and half nodes miners
  - half nodes more preferable
  - unequal distribution of full nodes
  - problem with data propagation

Future threats

- Node distribution
  - full and half nodes miners
  - half nodes more preferable
  - unequal distribution of full nodes
  - problem with data propagation
  - overloaded full nodes

Future threats

- Quantum computing

Future threats

- Quantum computing
  - private key vulnerable to quantum algorithms

Future threats

- Quantum computing
  - private key vulnerable to quantum algorithms
  - new methods of authentications would be needed

Future threats

- Quantum computing
  - private key vulnerable to quantum algorithms
  - new methods of authentications would be needed
  - 'quantum safe cryptography' is the only hope

Future threats

- Quantum computing
  - private key vulnerable to quantum algorithms
  - new methods of authentications would be needed
  - 'quantum safe cryptography' is the only hope
  - some crypto claims to be 'quantum-safe' (NEO)

Future threats

- Bubble

Future threats

- Bubble
  - numerous experts in economics identify cryptocurrencies as 'economic bubbles'

Future threats

- Bubble
  - numerous experts in economics identify cryptocurrencies as 'economic bubbles'
  - e.g Paul Krugman, Robert J. Shiller, Joseph Stiglitz etc.

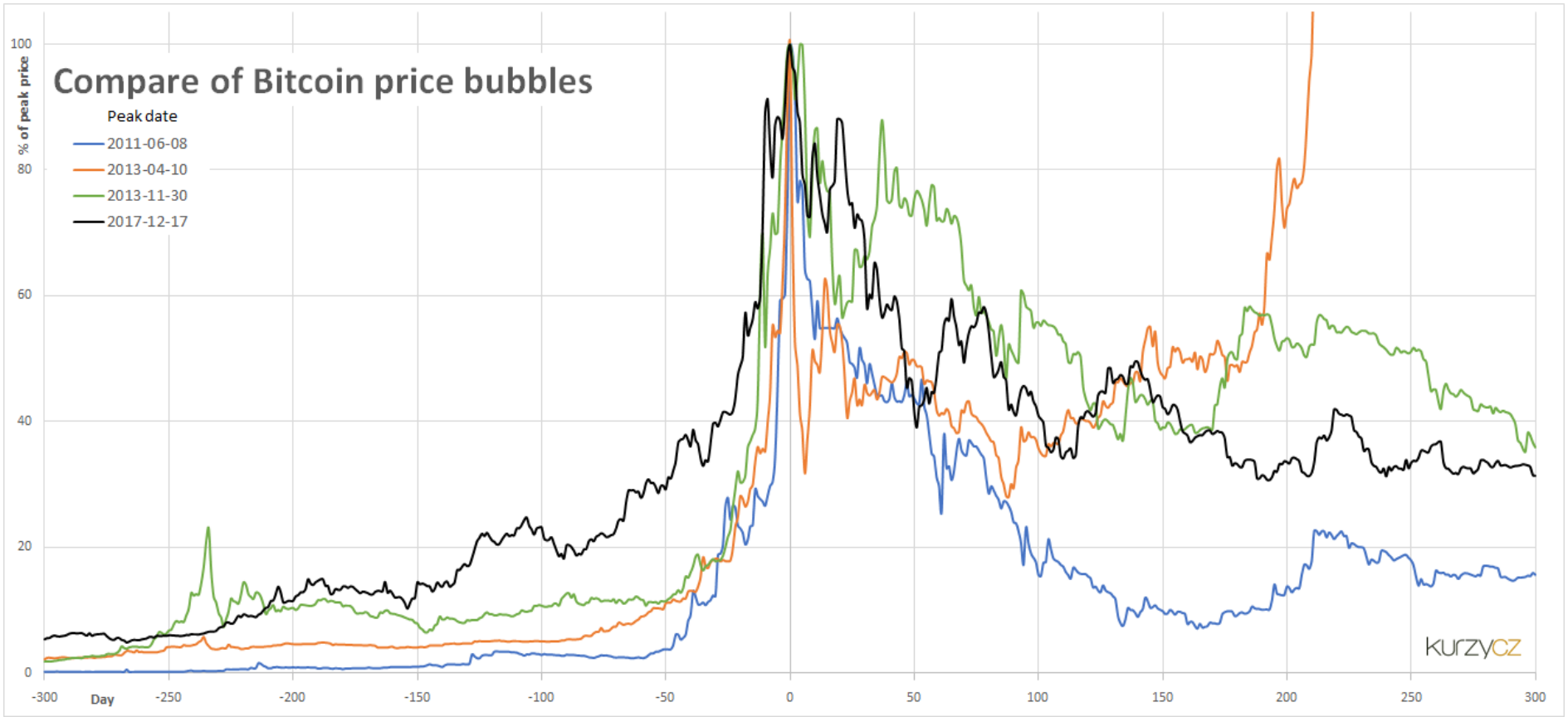
Future threats

- Bubble
  - numerous experts in economics identify cryptocurrencies as 'economic bubbles'
  - e.g Paul Krugman, Robert J. Shiller, Joseph Stiglitz etc.
  - 'newbies' to crypto markets may loose absurd amount of money because of 'bubbles'

Future threats

- Bubble
  - numerous experts in economics identify cryptocurrencies as 'economic bubbles'
  - e.g Paul Krugman, Robert J. Shiller, Joseph Stiglitz etc.
  - 'newbies' to crypto markets may loose absurd amount of money because of 'bubbles'
  - includes drops even by 80%(September 2018, MVIS, top 10 crypto)

Future threats



Future threats

Cryptocurrency in crime

- Medium of exchange

Black Markets

Bitcoin Ethereum Litecoin
Dogecoin Minero Zcash

Hacker Forums

Bitcoin Ethereum Litecoin
Dogecoin Minero Zcash

Black Markets
(Bitcoin Removed)

Ethereum Litecoin Dogecoin
Minero Zcash

Hacker Forums
(Bitcoin Removed)

Ethereum Litecoin Dogecoin
Minero Zcash

Cryptocurrency in crime

- Ransomware

Cryptocurrency in crime

- Ransomware
  - virus that encrypt data

Cryptocurrency in crime

- Ransomware
  - virus that encrypt data
  - ransomware payments prefers bitcoin

Cryptocurrency in crime

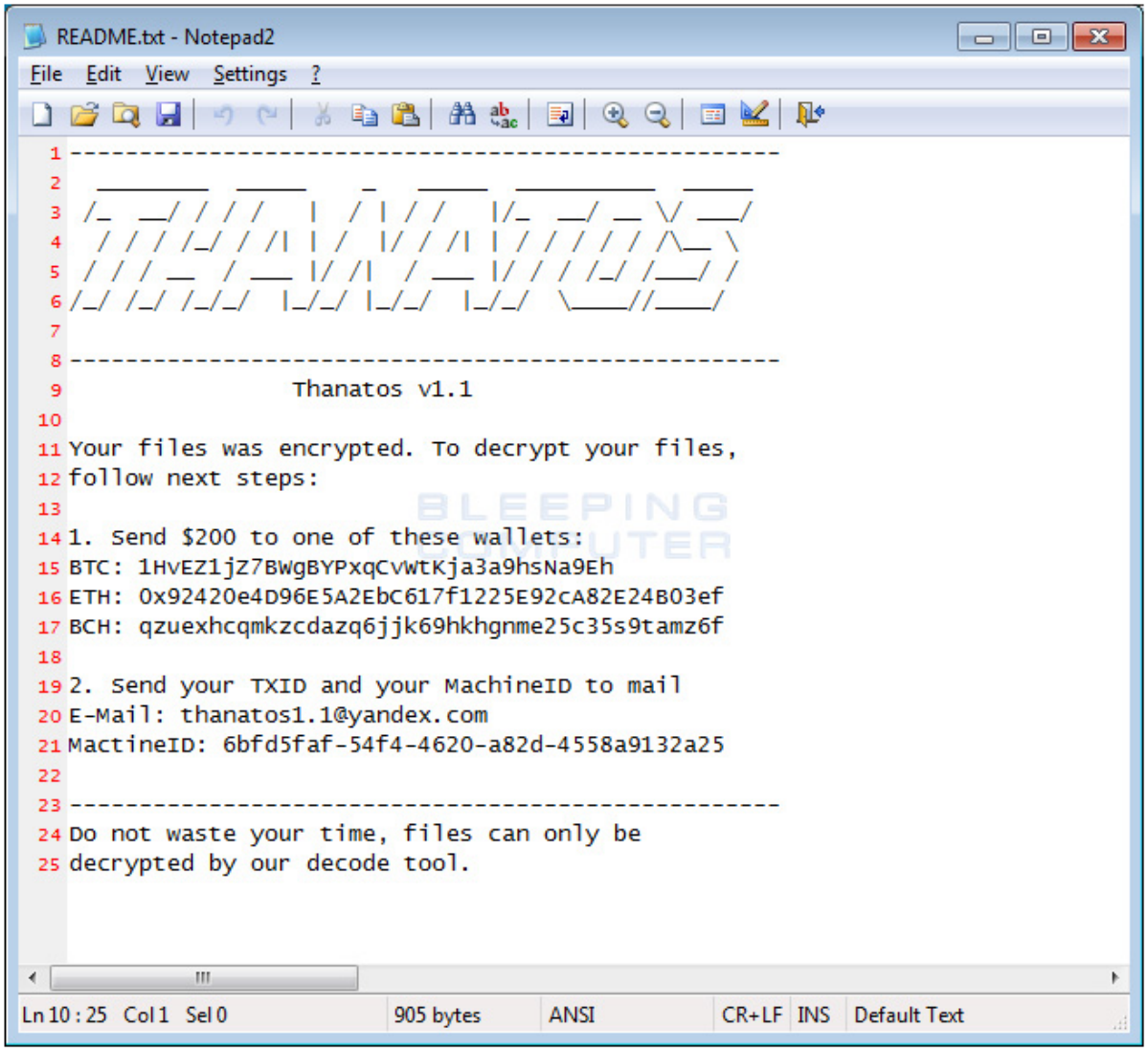
- Ransomware
  - virus that encrypt data
  - ransomware payments prefers bitcoin
  - even if you pay it doesn't mean you'll get your data

Cryptocurrency in crime

- Ransomware
  - virus that encrypt data
  - ransomware payments prefers bitcoin
  - even if you pay it doesn't mean you'll get your data
  - can be devastating for bigger companies

Cryptocurrency in crime

- e.g Thanatos(2018)



Thanatos Ransom Note

Cryptocurrency in crime

- Cryptojacking

Cryptocurrency in crime

- Cryptojacking
  - prefers monero

Cryptocurrency in crime

- Cryptojacking
  - prefers monero
  - can be mined on CPUs

Cryptocurrency in crime

- Cryptojacking
  - prefers monero
  - can be mined on CPUs
  - better privacy then bitcoin

Cryptocurrency in crime

- Cryptojacking
  - prefers monero
  - can be mined on CPUs
  - better privacy then bitcoin
  - originally people running miners on company hardware

Cryptocurrency in crime

- Cryptojacking
  - prefers monero
  - can be mined on CPUs
  - better privacy then bitcoin
  - originally people running miners on company hardware
  - evolved to worms dropping miners

Cryptocurrency in crime

- Cryptojacking
  - prefers monero
  - can be mined on CPUs
  - better privacy then bitcoin
  - originally people running miners on company hardware
  - evolved to worms dropping miners
  - possible in browser(using JavaScript)

Cryptocurrency in crime

- Cryptojacking
  - prefers monero
  - can be mined on CPUs
  - better privacy then bitcoin
  - originally people running miners on company hardware
  - evolved to worms dropping miners
  - possible in browser(using JavaScript)
  - hacking routers to insert code into https

Cryptocurrency in crime

- Cryptojacking
  - prefers monero
  - can be mined on CPUs
  - better privacy then bitcoin
  - originally people running miners on company hardware
  - evolved to worms dropping miners
  - possible in browser(using JavaScript)
  - hacking routers to insert code into https
  - possible on android systems

Cryptocurrency in crime

- Cryptojacking
  - prefers monero
  - can be mined on CPUs
  - better privacy then bitcoin
  - originally people running miners on company hardware
  - evolved to worms dropping miners
  - possible in browser(using JavaScript)
  - hacking routers to insert code into https
  - possible on android systems
  - 4000% increase in 2018

Cryptocurrency in crime

- Cryptojacking
  - prefers monero
  - can be mined on CPUs
  - better privacy then bitcoin
  - originally people running miners on company hardware
  - evolved to worms dropping miners
  - possible in browser(using JavaScript)
  - hacking routers to insert code into https
  - possible on android systems
  - 4000% increase in 2018

Example

Few weeks ago security firm Radiflow announced discovery of crypto mining malware in the monitoring network of water utility in Europe.

Cryptocurrency in crime

- e.g Worms

Worm	Date	Platform	Mines	Spreads
Otorun	Oct. 2012	Windows	BTC	.lnk
Darlloz	Nov. 2013	Linux	MNC, DOGE	PHP
Miner-C	Aug. 2016	Windows	XMR	FTP creds
Adylkuzz	May 2017	Windows	XMR	SMB
RubyMiner	Jan. 2018	Lin., Win.	XMR	PHP, IIS, Ruby
PyCryptoMiner	Jan. 2018	Linux	XMR	SSH creds, JBoss
WannaMine	Jan. 2018	Windows	XMR	SMB
ADB.Miner	Jan. 2018	Android	XMR	Android Debug Bridge

Cryptocurrency in crime

- Thieft

Cryptocurrency in crime

- Thieft
  - Wallets using vishing, smishing etc.

Cryptocurrency in crime

- Thieft
  - Wallets using vishing, smishing etc.
  - Exchanges

Cryptocurrency in crime

- Thieft
  - Wallets using vishing, smishing etc.
  - Exchanges
    - Mt. Gox, 2014 $450M in BTC
    - Bitfinex, 2016 $72M in BTC
    - Coincheck, 2018 $530M in NEM

Cryptocurrency in crime

- Thieft
  - Wallets using vishing, smishing etc.
  - Exchanges
    - Mt. Gox, 2014 $450M in BTC
    - Bitfinex, 2016 $72M in BTC
    - Coincheck, 2018 $530M in NEM
  - Tor proxy address rewrites $22K

Cryptocurrency in crime

- Thieft
  - Wallets using vishing, smishing etc.
  - Exchanges
    - Mt. Gox, 2014 $450M in BTC
    - Bitfinex, 2016 $72M in BTC
    - Coincheck, 2018 $530M in NEM
  - Tor proxy address rewrites $22K
  - Flaws in smart contracts

Cryptocurrency in crime

- Thieft
  - Wallets using vishing, smishing etc.
  - Exchanges
    - Mt. Gox, 2014 $450M in BTC
    - Bitfinex, 2016 $72M in BTC
    - Coincheck, 2018 $530M in NEM
  - Tor proxy address rewrites $22K
  - Flaws in smart contracts
  - Threat mails

Frauds & Scams

- Initial Coins Offerings(ICO)

Frauds & Scams

- Initial Coins Offerings(ICO)
  - Prodeum - fruit and veggies track system on Etherium blockchain ($2.4K)

Frauds & Scams

- Initial Coins Offerings(ICO)
  - Prodeum - fruit and veggies track system on Etherium blockchain ($2.4K)
  - PlexCoin - new cryptocurrency promising hight gains for inverstors ($15M)

Frauds & Scams

- Initial Coins Offerings(ICO)
  - Prodeum - fruit and veggies track system on Etherium blockchain ($2.4K)
  - PlexCoin - new cryptocurrency promising hight gains for inverstors ($15M)
  - AriseBank - 'New revolutional way of banking' ($4M)

Frauds & Scams

- Initial Coins Offerings(ICO)
  - Prodeum - fruit and veggies track system on Etherium blockchain ($2.4K)
  - PlexCoin - new cryptocurrency promising hight gains for inverstors ($15M)
  - AriseBank - 'New revolutional way of banking' ($4M)
  - PonziCoin - cryptocurrency made and presented as scam, still earns $250K

Frauds & Scams

- Initial Coins Offerings(ICO)
  - Prodeum - fruit and veggies track system on Etherium blockchain ($2.4K)
  - PlexCoin - new cryptocurrency promising hight gains for inverstors ($15M)
  - AriseBank - 'New revolutional way of banking' ($4M)
  - PonziCoin - cryptocurrency made and presented as scam, still earns $250K

> *Q: Is this a scam?*
>
> *A: Yes, it's as much a scam as 99% of the ICOs out there, but it's more transparent about it* 🙂

Frauds & Scams

- Ponzi schemes

Frauds & Scams

- Ponzi schemes
  - My Big Coin - same story($1.1M)

Frauds & Scams

- Ponzi schemes
  - My Big Coin - same story($1.1M)
  - CabbageTech - virtual currency trading advice($1.1M)

Frauds & Scams

- Ponzi schemes
  - My Big Coin - same story($1.1M)
  - CabbageTech - virtual currency trading advice($1.1M)
  - Bitconnect - alt-coin with wallet interest

Frauds & Scams

- Ponzi schemes
  - My Big Coin - same story($1.1M)
  - CabbageTech - virtual currency trading advice($1.1M)
  - Bitconnect - alt-coin with wallet interest

Frauds & Scams

- Pump-n-dump with bots

Frauds & Scams

- Pump-n-dump with bots
  - bot usage in crypto

Frauds & Scams

- Pump-n-dump with bots
  - bot usage in crypto
  - auto selling/buying when price fell below a certain point

Frauds & Scams

- Pump-n-dump with bots
  - bot usage in crypto
  - auto selling/buying when price fell below a certain point
  - can cause dramatic drop in price for a few sec

Frauds & Scams

- Pump-n-dump with bots
  - bot usage in crypto
  - auto selling/buying when price fell below a certain point
  - can cause dramatic drop in price for a few sec
  - in 2013 Markus and Willy bots caused bitcoin spike from $150 to $1000 over 60 days by trading with bitcoins they didn't own

Frauds & Scams

- Pump-n-dump with bots
  - bot usage in crypto
  - auto selling/buying when price fell below a certain point
  - can cause dramatic drop in price for a few sec
  - in 2013 Markus and Willy bots caused bitcoin spike from $150 to $1000 over 60 days by trading with bitcoins they didn't own

Example

In 2017 price of Etherium dropped to 10 cents for few sec, causing bots to cascade sell. The cause was a multimillion sell order on the exchange.

Mining strategies

- Temporary block withholding

Mining strategies

- Temporary block withholding
  - miner (or pool) try to withhold mined valid block byt submit partial share

Mining strategies

- Temporary block withholding
  - miner (or pool) try to withhold mined valid block byt submit partial share
  - holding valid blocks won't increase difficulty of mining puzzle

Mining strategies

- Temporary block withholding
  - miner (or pool) try to withhold mined valid block byt submit partial share
  - holding valid blocks won't increase difficulty of mining puzzle
  - can earn profits only for large miner or big pools

Mining strategies

- Temporary block withholding
  - miner (or pool) try to withhold mined valid block byt submit partial share
  - holding valid blocks won't increase difficulty of mining puzzle
  - can earn profits only for large miner or big pools
  - can be detected but also easly obfuscated

Mining strategies

- Temporary block withholding
  - miner (or pool) try to withhold mined valid block byt submit partial share
  - holding valid blocks won't increase difficulty of mining puzzle
  - can earn profits only for large miner or big pools
  - can be detected but also easly obfuscated

Strategy

Mine valid block, as long as block chain has one less block then you, mine new blocks. When main block catches up to you(off by one block) publish your blocks, making your chain the longest and becoming new main root.

Mining strategies

- Majority miner

Mining strategies

- Majority miner
  - with majority of computation power can collect all mining rewards

Mining strategies

- Majority miner
  - with majority of computation power can collect all mining rewards
  - just ignore all other blocks and build your own chain

Mining strategies

- Majority miner
  - with majority of computation power can collect all mining rewards
  - just ignore all other blocks and build your own chain
  - it would be statistically always the longest one

Mining strategies

- Majority miner
  - with majority of computation power can collect all mining rewards
  - just ignore all other blocks and build your own chain
  - it would be statistically always the longest one
  - can ignore/censor chosen transactions

Mining strategies

- Majority miner
  - with majority of computation power can collect all mining rewards
  - just ignore all other blocks and build your own chain
  - it would be statistically always the longest one
  - can ignore/censor chosen transactions
  - can become by colluding of smaller miners and emulating majority miner strategy

Mining strategies

- Maintaining exchange rates

Mining strategies

- Maintaining exchange rates
  - some non-compilant strategies that affect stability in a visible way might undermine public confidence

Mining strategies

- Maintaining exchange rates
  - some non-compilant strategies that affect stability in a visible way might undermine public confidence
  - causing weaken demand for bitcoins in the short run

Mining strategies

- Maintaining exchange rates
  - some non-compilant strategies that affect stability in a visible way might undermine public confidence
  - causing weaken demand for bitcoins in the short run
  - strategies that can quickly earn many bitcoins are likely to crash exchange rate once discovered

Mining strategies

- Maintaining exchange rates
  - some non-compilant strategies that affect stability in a visible way might undermine public confidence
  - causing weaken demand for bitcoins in the short run
  - strategies that can quickly earn many bitcoins are likely to crash exchange rate once discovered
  - and it's difficult to cash out before crash given the liquidity limits

Mining strategies

- Maintaining exchange rates
  - some non-compilant strategies that affect stability in a visible way might undermine public confidence
  - causing weaken demand for bitcoins in the short run
  - strategies that can quickly earn many bitcoins are likely to crash exchange rate once discovered
  - and it's difficult to cash out before crash given the liquidity limits
  - so the strategy is to do not use unfair strategies and try to prevent others from using them

Mining strategies

- Maintaining exchange rates
  - some non-compilant strategies that affect stability in a visible way might undermine public confidence
  - causing weaken demand for bitcoins in the short run
  - strategies that can quickly earn many bitcoins are likely to crash exchange rate once discovered
  - and it's difficult to cash out before crash given the liquidity limits
  - so the strategy is to do not use unfair strategies and try to prevent others from using them
  - since most big miners have capital tied up to mining hardware which will loose value if exchange rate declines

Mining strategies

- Goldfinger attack

Mining strategies

- Goldfinger attack
  - really just a majority miner strategy but with bad intentions

Mining strategies

- Goldfinger attack
  - really just a majority miner strategy but with bad intentions
  - attacker wish to damage given cryptocurrency stability can just buy 51%(or redirect his own) of computing power

Mining strategies

- Goldfinger attack
  - really just a majority miner strategy but with bad intentions
  - attacker wish to damage given cryptocurrency stability can just buy 51%(or redirect his own) of computing power
  - then he can easly cause side effects of major miner strategy

Mining strategies

- Goldfinger attack
  - really just a majority miner strategy but with bad intentions
  - attacker wish to damage given cryptocurrency stability can just buy 51%(or redirect his own) of computing power
  - then he can easly cause side effects of major miner strategy
  - practically impossible on bigger players(like bitcoin, etherium), but possible on smaller ones

Mining strategies

- Goldfinger attack
  - really just a majority miner strategy but with bad intentions
  - attacker wish to damage given cryptocurrency stability can just buy 51%(or redirect his own) of computing power
  - then he can easly cause side effects of major miner strategy
  - practically impossible on bigger players(like bitcoin, etherium), but possible on smaller ones
  - have beed observed through altcoin infanticide on CoiledCoin in 2012 (rip)

Mining strategies

- Feather-forking

Mining strategies

- Feather-forking
  - strategy that can blacklist given addresses

Mining strategies

- Feather-forking
  - strategy that can blacklist given addresses
  - publicly promise that if target address is in certain block, miner ignores it and attempt to create fork

Mining strategies

- Feather-forking
  - strategy that can blacklist given addresses
  - publicly promise that if target address is in certain block, miner ignores it and attempt to create fork
  - the attacker fork will continue until it outraces main branch or falls by k blocks, at which point attacker will concede

Mining strategies

- Feather-forking
  - strategy that can blacklist given addresses
  - publicly promise that if target address is in certain block, miner ignores it and attempt to create fork
  - the attacker fork will continue until it outraces main branch or falls by k blocks, at which point attacker will concede
  - on expectation an attacker with $\alpha \leq 50\%$ of the mining power will loose monies but will succeed in blocking blacklisted transaction with positive probability

Mining strategies

- Feather-forking
  - strategy that can blacklist given addresses
  - publicly promise that if target address is in certain block, miner ignores it and attempt to create fork
  - the attacker fork will continue until it outraces main branch or falls by k blocks, at which point attacker will concede
  - on expectation an attacker with $\alpha \leq 50\%$ of the mining power will loose monies but will succeed in blocking blacklisted transaction with positive probability
  - attacker convince others to join by rasing fee necessary to commit a "blacklisted" transaction to $\alpha * U$, where U is the average reward from a block

Anonymity & privacy

- Deanonymization

Anonymity & privacy

- Deanonymization
  - in most crypto addresses are public when making transaction

Anonymity & privacy

- Deanonymization
  - in most crypto addresses are public when making transaction
  - so a seller can check amount of monies on buyers addresses

Anonymity & privacy

- Deanonymization
  - in most crypto addresses are public when making transaction
  - so a seller can check amount of monies on buyers addresses
  - same with companies and mining pools

Anonymity & privacy

- Deanonymization
  - in most crypto addresses are public when making transaction
  - so a seller can check amount of monies on buyers addresses
  - same with companies and mining pools
  - it is also possible to trace flow of monies and conclude addresses that belong to the same individuals

Anonymity & privacy

- Deanonymization
  - in most crypto addresses are public when making transaction
  - so a seller can check amount of monies on buyers addresses
  - same with companies and mining pools
  - it is also possible to trace flow of monies and conclude addresses that belong to the same individuals
  - one way to prevent it (seller) is to link every transaction to new address

Anonymity & privacy

- Deanonymization
  - in most crypto addresses are public when making transaction
  - so a seller can check amount of monies on buyers addresses
  - same with companies and mining pools
  - it is also possible to trace flow of monies and conclude addresses that belong to the same individuals
  - one way to prevent it (seller) is to link every transaction to new address
  - by contrast customer may need to assemble payment amount from multiple addresses he owns

Anonymity & privacy

- Deanonymization
  - in most crypto addresses are public when making transaction
  - so a seller can check amount of monies on buyers addresses
  - same with companies and mining pools
  - it is also possible to trace flow of monies and conclude addresses that belong to the same individuals
  - one way to prevent it (seller) is to link every transaction to new address
  - by contrast customer may need to assemble payment amount from multiple addresses he owns
  - identification of regular user address may be possible for authorities since most data pass through providers

Anonymity & privacy

- Deanonymization
  - in most crypto addresses are public when making transaction
  - so a seller can check amount of monies on buyers addresses
  - same with companies and mining pools
  - it is also possible to trace flow of monies and conclude addresses that belong to the same individuals
  - one way to prevent it (seller) is to link every transaction to new address
  - by contrast customer may need to assemble payment amount from multiple addresses he owns
  - identification of regular user address may be possible for authorities since most data pass through providers

Example

Chainalysis is a company specializing in connecting crypto addresses to real identities and other analysis over blockchains. They work with governments to find identities of criminals.

Anonymity & privacy

- Improving anonymity

Anonymity & privacy

- Improving anonymity
  - **Coin-Join**

Anonymity & privacy

- Improving anonymity
  - **Coin-Join**
  - User wanting to perform transaction seek for others

Anonymity & privacy

- Improving anonymity
  - **Coin-Join**
  - User wanting to perform transaction seek for others
  - They combine their transaction into one 'big' with inputs corresponding to their addresses and outputs to recipients

Anonymity & privacy

- Improving anonymity
  - **Coin-Join**
  - User wanting to perform transaction seek for others
  - They combine their transaction into one 'big' with inputs corresponding to their addresses and outputs to recipients
  - Thanks to that there is no way to map inputs to outputs

Anonymity & privacy

- Improving anonymity
  - **Coin-Join**
  - User wanting to perform transaction seek for others
  - They combine their transaction into one 'big' with inputs corresponding to their addresses and outputs to recipients
  - Thanks to that there is no way to map inputs to outputs
  - User can benefit without others using multiple accounts

Anonymity & privacy

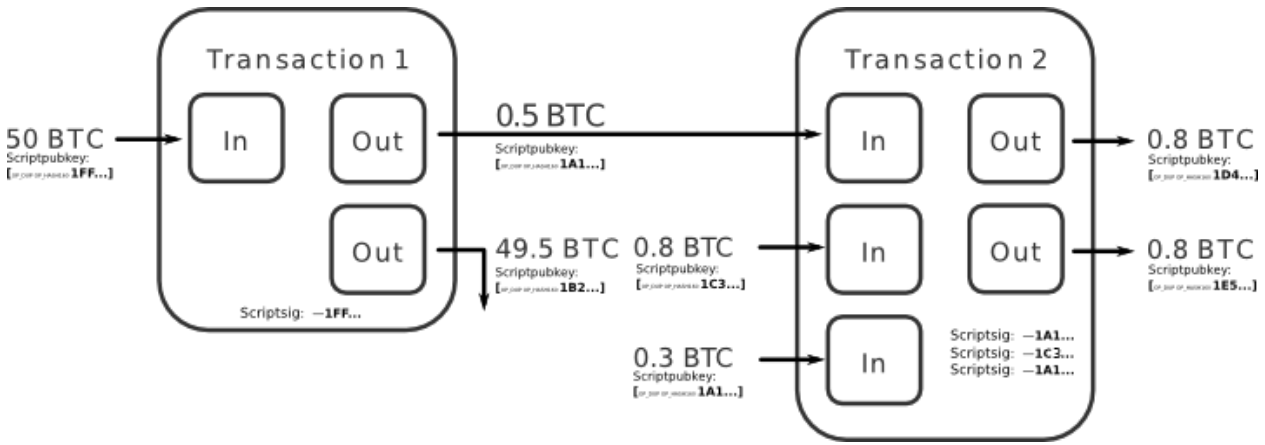
- Improving anonymity
  - **Coin-Join**
  - User wanting to perform transaction seek for others
  - They combine their transaction into one 'big' with inputs corresponding to their addresses and outputs to recipients
  - Thanks to that there is no way to map inputs to outputs
  - User can benefit without others using multiple accounts
  - and u cant be sure if those aren't other users

Anonymity & privacy

- Improving anonymity
  - **Coin-Join**
  - User wanting to perform transaction seek for others
  - They combine their transaction into one 'big' with inputs corresponding to their addresses and outputs to recipients
  - Thanks to that there is no way to map inputs to outputs
  - User can benefit without others using multiple accounts
  - and u cant be sure if those aren't other users
  - in practice need dedicated servers to create merged transactions

Anonymity & privacy

- Improving anonymity
  - **Coin-Join**
  - User wanting to perform transaction seek for others
  - They combine their transaction into one 'big' with inputs corresponding to their addresses and outputs to recipients
  - Thanks to that there is no way to map inputs to outputs
  - User can benefit without others using multiple accounts
  - and u cant be sure if those aren't other users
  - in practice need dedicated servers to create merged transactions
  - newest protocol don't allow participants to know what addresses are at inputs



Anonymity & privacy

- Improving anonymity

Anonymity & privacy

- Improving anonymity
  - **Mixcoin**

Anonymity & privacy

- Improving anonymity
  - **Mixcoin**
  - multiple users send monies to one pot

Anonymity & privacy

- Improving anonymity
  - **Mixcoin**
  - multiple users send monies to one pot
  - then they receive back the same amount from coins submitted by other users of the mix onto new address

Anonymity & privacy

- Improving anonymity
  - **Mixcoin**
  - multiple users send monies to one pot
  - then they receive back the same amount from coins submitted by other users of the mix onto new address
  - this provides anonymity toward external entities

Anonymity & privacy

- Improving anonymity
  - **Mixcoin**
  - multiple users send monies to one pot
  - then they receive back the same amount from coins submitted by other users of the mix onto new address
  - this provides anonymity toward external entities
  - there are many existing services that do it for small fee

Anonymity & privacy

- Improving anonymity

Anonymity & privacy

- Improving anonymity
  - **Zerocoin**

Anonymity & privacy

- Improving anonymity
  - **Zerocoin**
  - extension to bitcoin protocol that improves bitcoin anonymity

Anonymity & privacy

- Improving anonymity
  - **Zerocoin**
  - extension to bitcoin protocol that improves bitcoin anonymity
  - allows conversion of non-anonymous bitcoins to secure, anonymous zerocoins

Anonymity & privacy

- Improving anonymity
  - **Zerocoin**
  - extension to bitcoin protocol that improves bitcoin anonymity
  - allows conversion of non-anonymous bitcoins to secure, anonymous zerocoins
  - presentation topic material?

Security layers of crypto

- How to choose cryptocurrency?

Security layers of crypto

- How to choose cryptocurrency?
  - divide it into layers

Security layers of crypto

- How to choose cryptocurrency?
  - divide it into layers
  - decide what is most important to you

Security layers of crypto

- How to choose cryptocurrency?
  - divide it into layers
  - decide what is most important to you
  - choose!

Security layers of crypto

- The First layer: Coins and Tokens

Security layers of crypto

- The First layer: Coins and Tokens
  - When choosing cryptocurrency you are taking all the risks of the protocol

Security layers of crypto

- The First layer: Coins and Tokens
  - When choosing cryptocurrency you are taking all the risks of the protocol
  - if someone finds flaws in protocol they can compromise entire network

Security layers of crypto

- The First layer: Coins and Tokens
  - When choosing cryptocurrency you are taking all the risks of the protocol
  - if someone finds flaws in protocol they can compromise entire network
  - find out if it can be centralized. E.g. in case of bitcoin it is centralized around few biggest mining pools. This means that if they cooperate, they can compromise entire network

Security layers of crypto

- The First layer: Coins and Tokens
  - When choosing cryptocurrency you are taking all the risks of the protocol
  - if someone finds flaws in protocol they can compromise entire network
  - find out if it can be centralized. E.g. in case of bitcoin it is centralized around few biggest mining pools. This means that if they cooperate, they can compromise entire network
  - look at the genesis - who holds what

Security layers of crypto

- The First layer: Coins and Tokens
  - When choosing cryptocurrency you are taking all the risks of the protocol
  - if someone finds flaws in protocol they can compromise entire network
  - find out if it can be centralized. E.g. in case of bitcoin it is centralized around few biggest mining pools. This means that if they cooperate, they can compromise entire network
  - look at the genesis - who holds what
  - be aware of etherium based ICOs and possible roll backs from founders

Security layers of crypto

- The Second layer: Exchanges

Security layers of crypto

- The Second layer: Exchanges
  - exchange services are written in custom code with infrastructure security that has nothing to do with blockchain

Security layers of crypto

- The Second layer: Exchanges
  - exchange services are written in custom code with infrastructure security that has nothing to do with blockchain
  - so the most important is trust and credibility

Security layers of crypto

- The Second layer: Exchanges
  - exchange services are written in custom code with infrastructure security that has nothing to do with blockchain
  - so the most important is trust and credibility
  - a lot of exchanges started business recently and didn't invest into proper security measures

Security layers of crypto

- The Second layer: Exchanges
  - exchange services are written in custom code with infrastructure security that has nothing to do with blockchain
  - so the most important is trust and credibility
  - a lot of exchanges started business recently and didn't invest into proper security measures
  - ...but if someone steals monies from an exchange it's almost impossible to do anything about it

Security layers of crypto

- The Second layer: Exchanges
  - exchange services are written in custom code with infrastructure security that has nothing to do with blockchain
  - so the most important is trust and credibility
  - a lot of exchanges started business recently and didn't invest into proper security measures
  - ...but if someone steals monies from an exchange it's almost impossible to do anything about it
  - it's best to check the security part of exchange websites

Security layers of crypto

- The Third layer: Wallet

Security layers of crypto

- The Third layer: Wallet
  - Hot wallet

Security layers of crypto

- The Third layer: Wallet
  - Hot wallet
  - Cold wallet

Fin

Thanks for your attention!