RESEARCH REPORT

Privacy Coins

INTELLIGENT TRADING

The Privacy Coins Market

Source: Tradingview

Summary

Cryptocurrencies are creating a trustless, decentralized environment and replacing traditional middleman with technologies grounded in cryptography. The enabled decentralization, however, often comes at the cost of loss of confidentiality. The blockchains of popular coins such as bitcoin or Ethereum are public, transparent and permanent, and the pseudonymous blockchain addresses provide only a limited level of privacy. The users of these blockchains are facing the risk of deanonymization, and privacy issues are becoming a large concern for users of Distributed Ledger Technologies. Privacy coins are attempting to provide a solution for this concern by combining several technical solutions to allow for on-chain privacy and the obfuscation of the linkability of personal information to these public blockchain addresses.

Strengths & Opportunities

- Offering solutions to the concern of privacy of public blockchains
- Strong focus on technologies and development
- Many see Increasing demand for privacy coins in 2018*
- Potential adoption by large companies owing to enhanced privacy features

Weaknesses & Threats

- Current privacy-enhancing technologies increase the transaction size and decrease the scalability of blockchains
- Typically affiliate to darknet and/ or shadow economy/ black market
- The cryptocurrency market is dominated by bitcoin and Ethereum, so if they implement privacy into their blockchain, privacy coins may lose some of their advantages
- Regulatory authorities may threaten the privacy coins by disabling the infrastructure, e.g. exchanges

*2018 Predictions on Hackernoon, podcasts, Cryptoticker, Coinsquare 2018 prediction by Clayton Danie on Monero

Privacy Coins

Issue of Privacy
- **Anonymity in bitcoin**
  - Linkability
  - Blockchain privacy

Technology Solutions
- **Solutions for linkability**
- **Blockchain privacy solutions**
  - Stealth Address
  - Mixing
    - CoinJoin
    - Ring signature
    - Zero proof protocols
  - Pedestrian commitment
    - Confidential Transactions
    - Mimblewimble

Market Analysis
- **Players**
  - Top Three
    - Monero
    - Dash
    - ZCash
  - New Players

Strategic Analysis
- Strengths
- Weaknesses
- Opportunities
- Threats

Issue of Privacy

Anonymity in bitcoin

Cryptocurrencies are based on the principle of a trustless environment in which multiple participants can exchange information and create a tamper-proof history of transactions. This trust is facilitated not by a third party, but by cryptographic technologies. The middleman thus removed, enables the decentralization of the whole network. The tradeoff here, however, is confidentiality, as the entire blockchain is exposed and transparent and ALL transactions are publicly stored on the blockchain network.

To better illustrate the issue of privacy by example, we analyze the anonymity of bitcoin, the base coin for the majority of altcoins on the market. In this analysis, there are two key elements of privacy in consideration: firstly, the linkability of personal information to the blockchain addresses, and secondly the on-chain privacy.

Linkability

Linkability describes the ability to connect personal information (e.g. IP addresses) with different addresses or transactions of the same user, or the sender and recipient of a transaction. The public ledger of bitcoin (and most of the popular cryptocurrencies such as Ethereum) allows for linkability, making it pseudonymous.

The pseudonymous character of the bitcoin blockchain means that even though the users can be anonymous, it is still possible to link the different interactions of one user with the system. Once a profile is linked, it can be deanonymized by a variety of channels. For example, when using bitcoin services that request the real personal information, such as exchanges.

An example of a deanonymization method is the use of leaks of payment information from merchants that accept online bitcoin payments for their goods and services. In the research article When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies, the authors show how a third-party web tracker can link the blockchain transactions to the user's cookies. The second attack demonstrates how linking two purchases of the same user can enable the tracker to identify the user's entire cluster of addresses and transactions on the blockchain.

Blockchain privacy

On-chain privacy is concerned with the transparent nature of the ledger of transactions. Even when the real identity is not linked to a blockchain address, there is a lot of information on the blockchain. Every transaction involving bitcoin is recorded on the bitcoin ledger. The ledger shows the number of bitcoins transacted in every transaction and both the sending and receiving addresses of the parties involved. And if the information is linked, privacy is jeopardized to a greater extent than in traditional banking. Due to the permanent and transparent nature of the public blockchains, the transaction history is (by design) completely exposed to the public.

Using techniques such as clustering or structural patterns, observations in the transaction graph can compromise the privacy of the blockchain. As the market capitalization of cryptocurrencies grows, the techniques evolve. At the beginning of 2018, the Bitfury Group proposed a new clustering algorithm, combining the blockchain information and off-chain information from the internet for constructing the clustering model. This allows for a higher level of accuracy when tracing the bitcoin addresses.

There are companies, like e.g. Elliptic and Chainanalysis, dedicated to deanonymizing bitcoin's blockchain and tracking the transactions made on it. In the summer of 2017, the Daily Beast unearthed a contract between the IRS (Internal Revenue Service) and Chainanalysis for services to identify the owners of digital wallets. Governmental agencies are not the only parties pushing for blockchain transparency. In April this year, Amazon was granted a data gathering patent (filled in 2014) with a potential to cover tracking of the bitcoin transactions as well. In a response to this effort, several privacy solutions originated.

Technology solutions

Solution for linkability

The solution for the linkability issue brings nothing new in terms of technologies. Routing services such as VPN, I2P or TOR are well known in the online world as techniques for protecting the IP addresses of internet users.

When using a Virtual Private Network (VPN) the IP address visible to the network is that of the VPN service provider. This assures encryption of all incoming and outgoing network traffic but comes with the risk of using a third-party provider. I2P and TOR are both anonymizing proxy networks that allow for obfuscating the IP addresses and the traffic, and they both offer similar browsing experiences for the most part.

It is still possible to deanonymize the identities of users. The famous whistleblower Edward Snowden spoke against VPN assured privacy on his twitter. He warns that "Your VPN provider can see all of your activity. So can the NSA." There are also assumptions about the role of government authorities infiltrating and compromising aspects of TOR.

The Intercept reported on the NSA's ability to track senders and receivers of bitcoin. The Intercept, a news organization focusing on an adversarial journalism, based their report on classified documents provided by whistleblower Edward Snowden in 2013. The data was obtained through a VPN-like service called MONKEYROCKET, described in the documents as a "non-Western Internet anonymization service".

It is important to remember that the linkability is only one aspect regarding the issue of privacy. There are projects in the crypto market that provide a solution only to this layer of privacy, for example Verge (XVG). However, its primary features solve only the linkability issue, utilizing TOR and I2P. However, to be considered a true privacy coin, on-chain privacy should be considered as well.

Solution for blockchain privacy

Blockchain privacy is concerned with the issue of having a transparent chain of all transactions stored in a public blockchain. As this is one of the unresolved issues of the crypto world, there is a lot of research and development focused on making the blockchain more private. With time, several ways to enhance the on-chain privacy have been developed. Some of them are compatible with the bitcoin blockchain and can be added to it, some are implemented as an alternative to bitcoin through different altcoins.

Using multiple different payment addresses as a potential solution has already been mentioned in the bitcoin whitepaper. One-time payment addresses were the first step towards privacy. The next step was mixing, a technique used to obfuscate the path from the sender to recipient. Complete unlinkability among all addresses and transactions is extremely difficult to achieve thus the mixing works with an "anonymity set." The "anonymity set" is the crowd one that is trying to blend into.

Mixing was introduced by a third-party provider, and later was followed with decentralized mixing, utilized in technologies such as CoinJoin. The next step was automated mixing, implemented for example in CryptoNote protocol through Ring signature. The cryptographic mix is using the technology on a protocol-level, the mixing capability is embedded into the protocol itself, such as in the Zerocoin protocol.

Technology solutions

One time use payment address

Stealth Address

The method of Stealth Address utilizes the one-time use payment addresses as suggested in the bitcoin whitepaper, while making it easier to manage numerous addresses. The recipient does not have to communicate the changing addresses to the sender for each transaction, making only the stealth address public. The stealth address then serves as a parent public key to the recipient private address. The sender is asked to generate a unique address for each specific transaction to which that user sends the funds. The recipient is the only one who can calculate the one-time secret key to the payment address. In this way, even though there is a single address published (the stealth address), the payments are going to separate addresses which cannot be linked together.

This method can be used for sending bitcoin, however, it is not native to the bitcoin protocol. When the users want to send bitcoin through stealth transactions, they have to use specific wallet software, such as Dark Wallet. This makes it easier for the stealth transaction to be identified among the transparent transactions on the bitcoin blockchain. The utilization of Stealth Address makes more sense for privacy-oriented projects, where it can actually enhance the security of a recipient. That is why it is used (in combination with other techniques) in projects such as Monero or Zcash.

Mixing

Third party provider

When using the one-time use payment address, the path of the coins from one address to another is still trackable. Mixing enables the confusing of this path, representing the next step to privacy after the one-time use payment address.

Mixing was first introduced through third-party providers. Tumblers such as CoinMixer or Bitcoin Blender are services that receive bitcoins from multiple users, mix them together, break them into smaller amounts and send them to the recipients, complicating the tracing of the fund flow. This service is relatively simple, as any third-party exchange service with enough volume is able to implement this method.

There are two issues with third-party providers. The first is that they are a middleman that the users need to entrust with their funds. Using mixers thus limits the advantage of having a trustless cryptocurrency. The second drawback originates from the centralized character of the services. The centralization makes it easier for authorities to impose regulation on the service.

CoinJoin

An alternative to third-party providers is decentralized mixing. CoinJoin is an example of the decentralized solution that allows two and more users to jointly sign a transaction. It was introduced by Gregory Maxwell in 2013. The technique is utilizing the fact that a blockchain transaction can have multiple inputs and outputs. When more people join for one coinjoin transaction, the order of inputs and outputs for this one transaction can be randomized.

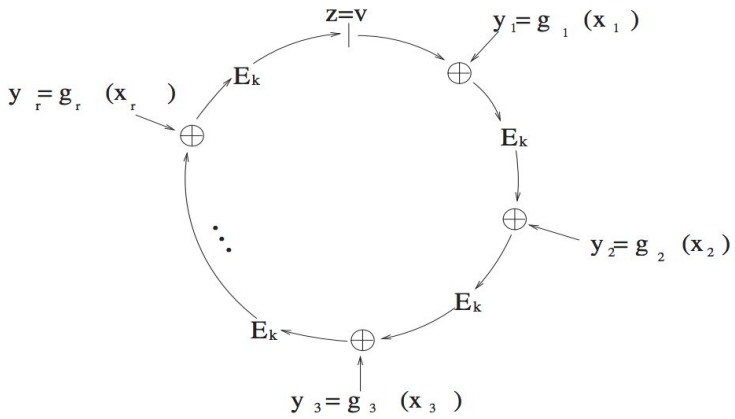
The level of privacy depends on the anonymity set, which is in CoinJoin in the size of three. This means that the transaction combines inputs from three users. The CoinJoin technology is implemented for example in the PrivateSend feature of Dash or in the DarkWallet.

Technology solutions

Ring Signatures

The blockchain transaction has to be signed by a digital signature. In order to verify this signature, the verifier needs to know the public key that created it. These links the public address to the transaction and enable the funds' trackability.

The Ring Signatures is a technology using a group of potential signers while not revealing the genuine author who sign the transaction. There is no mixer and the mixing is done automatically, which allows hiding the address of the sender, creating a transaction attributed to multiple public keys.



Source: River, R.L. et al (2001) How to Leak a Secret
https://doi.org/10.1007/3-540-45682-1_32

The picture demonstrates how the RIng Signature is created. The actual signer chooses an arbitrary set of possible signers. The signature is then computed using only the signer's secret key and the others' public keys. The output of one calculation becomes the input of the next. The verifier needs one of the keys to verify that the final output (z) is equal to the initial input (v).

The Ring Signatures technology has some limitations. Used by itself, it allows for double-spending and the level of anonymity depends on the set of signers. The first issue was solved in the CryptoNote protocol with the Traceable Ring Signatures. However, the issue of using the right set for the ring remains, as well as a dependency on the number of addresses used. Monero, where the Ring Signatures are implemented, is aiming to solve this by using triangular distribution, favoring newer coins as mixins over older ones.

Zero-knowledge proof

This method of protocol-level mixing utilizes a tool that has been used in cryptography since 1989: the Zero-knowledge proof. This technique is a cryptographic protocol allowing one party to prove that a statement is true without the need to reveal any other information. Jackson Palmer explained the principle in his podcast with the help of a simple example.

Take two people, “person A” and “person B.” Person A possesses the ability to count the exact number of jelly beans in a jar after a single look at it. Person A wants to prove this ability to person B, without revealing the actual number of jelly beans or the way he counted them. To prove this ability, person A closes his eyes and offers the person B the opportunity to either remove a jelly bean from the jar or leave it as it is. When person A opens his eyes, he will know if the person B added a jelly bean only if he actually possesses the ability to count them instantly. If person A guesses wrong, it is certain that he lied about his ability. If he guesses right, he may just have been lucky. But if person A and person B repeat this exercise multiple times, with each correct guess the probability of person A being able to count the jelly beans increases. This can prove person A’s ability without revealing the number of jelly beans and the method that person A is using to count them.

Technology solutions

In the example from the previous page, the person A and person B had to interact to obtain the zero-knowledge proof of person A's magical ability. With cryptography, this is no longer necessary, as it enables non-interactive proofs that are validated by a complex arithmetic circuit.

Zerocoin is one of the projects implementing the zero-knowledge proofs. As the mixing is embedded into the protocol, there is no need for the mixer. The path of the coins is obfuscated in two steps. In the first one, the coins are burnt in a so-called Zerocoin mint. The fact that the coins were indeed made unspendable is verified through the zero-knowledge proof, without revealing the specific coins. The proof entitles the original coin holder the right to an equivalent of what was burnt. In the second step, the holder redeems new coins, the Zerocoin spend.

The conversion breaks the transaction links between the original and new coins, providing a high level of privacy. Using the mint coins for mixing the transaction path allows for scaling of the anonymity set up to thousands. The drawback of this method is that it requires a one-time trusted setup generating the initial parameters. The big size of the proof also requires additional storage on the blockchain and additional computational resources to verify.

The **zk-SNARKs** protocol is aiming to solve those issues, decreasing the proof size and hiding the transaction amount. The trade-off is, however, a complicated trusted setup to generate the zk-SNARK proof. The cryptographic tool is also connected with a long generation time for the private transactions.

Bulletproof is a new implementation of the non-interactive zero-knowledge proof protocol. It is based on a 2016 improvement in the space efficiency of zero-knowledge proofs from Bootle et al. Unlike zk-SNARK, it does not require trusted setup and is compatible with the bitcoin blockchain. The efficiency gains offered by bulletproofs makes them more suitable for inclusion into active cryptocurrencies. The first version of bulletproof is currently being implemented in the bitcoin crypto library libsec256k1.

Pedersen Commitments

An alternative method to mixing is the Pedersen commitments scheme, using a method of "committing" to data by publishing a hash to it. The original data are not revealed to the public, unless the owner wants to. In order to reveal the information, the hash can be reproduced. The commitment preserves the addition and the sum of a set of commitments equals to the sum of the data they committed to. This enables for transferability of the commitments from one person to another, without revealing the hidden data.

Confidential Transactions

Pedersen Commitments were utilized for concealing the amount in so-called Confidential Transactions. The scheme was implemented in Monero in January 2017 and in September it was made mandatory for all transactions, combining Cryptonote with Confidential Transactions (RingCT).

Mimblewimble

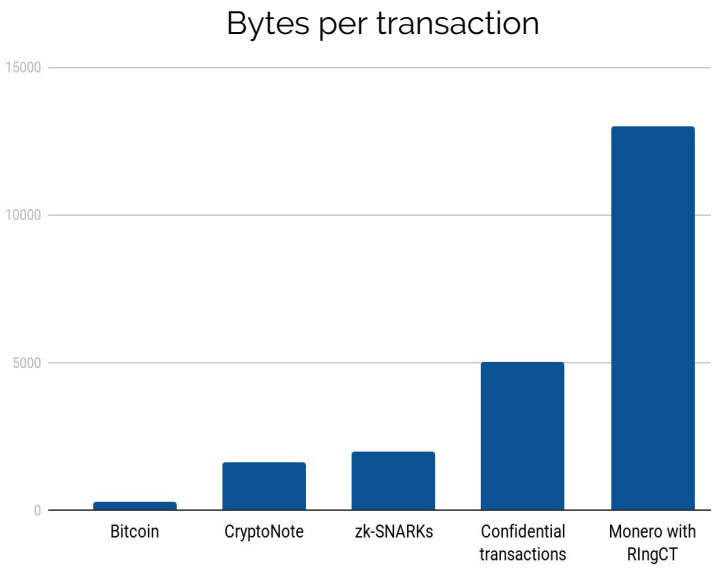
The Mimblewimble protocol utilizes a combination of CoinJoin and Confidential Transaction. The proposal was released in 2016, outlining the goal of adding privacy and scalability to bitcoin. The protocol allows for mixing together all transactions in every new block that is created. The multisignature public key enables signing all inputs and outputs of a transaction, which makes the transactions very light. The implementation of the protocol is currently WIP and there are still issues that need to be resolved (e.g. in order to execute the transactions, the participants need to be online).

Technology solutions

Comparison of solutions

The solutions introduced in the previous pages are focusing primarily on the privacy features of cryptocurrencies. The enhanced privacy is a relevant improvement, however, it comes with some associated drawbacks. Each method described requires additional cryptography and computations, which negatively affects the scalability of the solutions.

The large amount of data necessary for providing the on-chain privacy increases the size of transactions. The chart below shows the cost of confidentiality in bytes per transaction. The median bitcoin transactions size is here for comparison with these key privacy technology implementations. The table on the right shows the techniques used in each implementation.



Source: Yang, D. et. al. (2016), Survey of Confidentiality and Privacy Preserving Technologies for Blockchains

Implementation	Technique used
Confidential transactions	Pedersen commitments
CryptoNote	Ring Signatures Stealth Address
Monero with RingCT	Ring Signatures Stealth Address Pedersen commitments
Zcash	zk-SNARKs Stealth Address

Each solution has different limitations and not all solutions provide privacy for all aspects of the transaction. The table below summarizes the level of confidentiality of sender, recipient and the amount in each method.

Technology	Sender	Recipient	Amount
Stealth Address	🔴	🟢	🔴
CoinJoin	🟡	🟡	🔴
Pedersen Commitments	🔴	🔴	🟢
Ring Signatures	🟢	🔴	🔴
zk-SNARKs	🟢	🔴	🟢

🔴 Provides no confidentiality

🟡 Provides limited confidentiality

🟢 Provides strong confidentiality

Market Analysis

Market Players

The market of privacy coins has been dominated by three major players. Monero (XRM), ZCash (ZEC) and Dash (DASH) are featured at the top of nearly every list of privacy coins.* (Some of the contributors to this Research Report currently hold ZEC. Additionally, the Intelligent Trading Foundation has confirmed that it currently holds ZEC.) There are many other projects, but there is a distinction between privacy coins, focusing on both the linkability and on-chain privacy and coins with some privacy features. For example Verge (XVG) is solving only the IP addresses linkability using TOR, but not the privacy of the blockchain.

The top three listed coins are all focused on privacy and have privacy features that combine the technologies introduced in the previous section. Each project utilizes a different technology, which creates an ideal setting for comparison. As the technologies provide either limited privacy or only for a certain aspect of the transaction process when used alone, privacy coins are using combinations of those methods.

Top players

Monero (XRM)

Monero originated as a Bytecoin fork in 2014 under the name Bitmonero. The cryptocurrency is based on the CryptoNote protocol, utilizing the ring signatures method. In 2017 Monero implemented RingCT, an improved version of the ring signature. The RingCT is enabling an obfuscation of the amounts, origins, and destinations of transactions. In combination with the Stealth address, this provides full privacy.

Unlike bitcoin's blockchain, Monero's blockchain is not completely prunable.** This means that pruning cannot be used to reduce the chain size. In combination with the other cryptographic methods, this increases the transaction size and Monero RingCT transactions are as big as 12.6 kB, which severely limits the scalability and transaction speed. Monero plans to solve this with a dynamic block size update, removing the hard coded block size limit and theoretically enabling scaling up to over 1,000 transactions per second with modern hardware. This is still limited by the hardware requirements, as increased block sizes would mean a need for increased processing power. As a solution, the team is looking into Monero compatible bulletproofs, which are currently on testnet, with a planned release in September 2018. The bulletproofs-enabled space saving should bring an advancement in the scalability for Monero transactions.

Monero is the only coin from the top three with default privacy, shielding all the transactions, which makes it the potential winner in privacy coin segment. Prior to RingCT, the mixins (the group of public keys used for ring signature) were vulnerable to tracing analysis and can be deductible. The soundness of the privacy solution offered by Monero has improved significantly, but there are still some flaws to the method. The anonymity set is limited, the default ring size is currently 7, which means that there are four more addresses in the ring chosen by triangular distribution.

Overall, Monero remains to be one of the most popular privacy solutions, providing arguably the best privacy set by default. Previously, it was mostly associated with the darknet but the increase in interest in privacy coins may support its adoption.

* Hackernoon, Blockchain blog, Steemit,CDO Trends, Invest in Blockchain, CoinCodex, BitcoinExchangeGuide, Investopedia, CryptoTicker...
** Pruning is a method of deleting the data about fully spent transaction from the blockchain. Since these data are unnecessary, deleting them reduces the amount of data needed for transaction verification. The validating node works only with current unspent output and data to handle re-orgs (BitcoinWiki)

Market Analysis

Market Players (continued)

ZCash (ZEC)

The Zcash project originated in 2016 as a bitcoin fork. The goal of the project is to improve the flaws of the original currency, with a focus on privacy. The project forked from bitcoin is building on work done on Zerocoin, addressing some of its faults. One of the faults is the proof size, which Zcash decreases to 1 kB and speeds up the verification. The ZCash project is run by the Zerocoin Electric Coin Company and in March 2017 the Zcash Foundation was launched "to guide the evolution of Zcash".

For the privacy solution, Zcash implemented zk-SNARKs, which allows for shielding the transaction amount as well as the sender and recipient addresses. The acronym stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge" and is based on Zero-knowledge proofs. This enables participants to prove that the conditions for a valid transaction have been satisfied without revealing any crucial information about the addresses or values involved.

The Zero-knowledge proof solution enables a large anonymity set of all minted coins, providing a high degree of privacy. However, the size of up to 2 kB for average transaction makes it much less scalable. The issue of scalability is the main reason why the privacy is currently optional, not by default. Opt-in privacy is an issue, and at the time of writing, only 13.9 % of all transactions are shielded.

The questionable part of the solution is the initial trusted setup, which currently is the only way to produce zero-knowledge proofs that are non-interactive and short enough to be published on the blockchain. Zcash utilized a multi-party ceremony involving a 6-person set up. This is controversial, as you have to trust any of these 6 people that they destroyed the initial parameters and also trust that the ceremony was carried out correctly.

ZCash is developing a solution to the issues outlined above. The Sapling update, scheduled for November 2018 is promising improvements in the performance of the shielded transaction, reducing proving time and memory usage. What is more, the Sapling will rely on the Powers of Tau open-participation parameter setup. It is still a trusted setup but the open-participant characteristic enables multiple participants to join with a potential to scale to hundreds of participants. With the growing number, it becomes less and less possible to compromise all of them.

In January 2018 the whitepaper for zk-STARKs was released, promising a faster alternative to zk-SNARKs without the need for trusted setup. The size of the proof is currently too large to be implemented. In comparison to zk-SNARKs 288 bytes proof size, zk-STARKs proofs goes up to a few hundred kilobytes. However, the potential of the solution is still promising. The founders are not planning to launch their own coin as they are offering the solution to existing blockchains in what they call "Tech4Tokens (T4T)" model.

Market Analysis

Market Players (continued)

Dash (DASH)

Dash is in a good position in terms of market cap (at the time of writing, 14. on the CoinmMarketCap list, Monero 13. and ZCash 22.). However, mentioning Dash in the list of privacy coins is questionable. It is important to note that privacy is also optional in Dash and the high volume is driven mainly by the transactions without the privacy features.

Dash is offering two transaction options with additional features on top of the bitcoin's features set. The InstantSend and the PrivateSend. The PrivatSend transactions are significantly slower, originally with 1MB block allowing for 28 TPS. After a fork, the block size is increased to 2MB, which enables doubling of the number of transactions to 56 TPS. Nevertheless, the share of private transaction is still less than 1%.

The privacy technology utilized for PrivatSend is mixing through CoinJoin. The mixing process is expedited by a "masternode", a server which the users have to trust is not recording the users' information. The requirement of one thousand (1,000) DASH deposit to run a masternode should prevent malicious behavior of nodes. The CoinJoin solution is relatively simple and easy to implement on top of the blockchain, but the provided privacy is limited.

In comparison to ZCash, the anonymity set is restricted. CoinJoin is working with a set of three addresses of users for each round of mixing. The set requires mixing similar denominations (parts of transactions). If there are no users who want to mix the right denominations, the mix can be delayed. The users can decide how many rounds of mixing they want to choose for the private transaction with anonymity increasing with each round. The highest number of rounds is currently eight.

New players

Currently, there are over thirty privacy coins or coins with privacy features.

One of the new projects is Bitcoin Private (BTCP), originated as a co-fork of bitcoin and ZClassic. From the mainnet launch in March 3. the project has gained significant market share, ranking 45 in position on the CoinMarketCap list at the time of writing.

Bitcoin Private is combining the characteristics of both its ancestors' chains. It has a total supply of 21 million and uses the Proof-of-work consensus, the same as bitcoin. The ZClassic is a fork of ZCash, and as such, it implements ZCash privacy features. Bitcoin Private added the zk-SNARKs solutions and utilises the zero-knowledge proofs to enhance on-chain privacy, much like the parent ZCash coin.

With the ongoing development in the privacy field, there are new coins and new solutions emerging. An interesting project is called Grin, currently in the development phase, which is utilizing Mimblewimble technology.

In addition, as previously mentioned in this report, there have been mentioned other new technologies such as zk-STARKs or bulletproof that can potentially be implemented in existing blockchains.

Market

Market Players (continued)

Comparison

When comparing the top players, both the basic technical aspects and the privacy solution characteristic should be taken into account. The basic characteristics affect the scalability of the solution, for example, the dynamic block size of Monero allows for adapting to the need of the network. On the other hand, Monero is the one that does not have a prunable blockchain. From the perspective of the TPS metric (transaction per the second), ZCash is performing the worst of the three. However, in terms of privacy, the anonymity set of ZCash is obviously the best. However, the opt-in characteristic of ZCash and Dash is questionable and Dash is also the only of the three which is not hiding the number of coins sent.

	Zcash	Monero	Dash
Total supply	21 million	18.3 million + tail emission	18.9 million
Block size	2 MB	dynamic	2 MB
Block time	2.5 minutes	2 minutes	2.6 minutes
Prunable blockchain	Yes	No	Yes
TPS	6,7	In theory over 1,000, depends on the miners hardware	56 with 2MB block size
Privacy technology	zk-SNARKs zero proof protocol, Stealth address	Ring Signatures, Stealth Address, Pedersen Commitments	CoinJoin variant
Anonymity set per tx	All mint transactions	4 set by default	3 with each mix
Soundness depend on # of users	No	Yes	Yes
Privacy by default	No	Yes	No
Hides Sender	Yes	Yes	Yes
Hides Recipient	Yes	Yes	Yes
Hides Amount	Yes	Yes	No

Strategic Analysis

Strengths

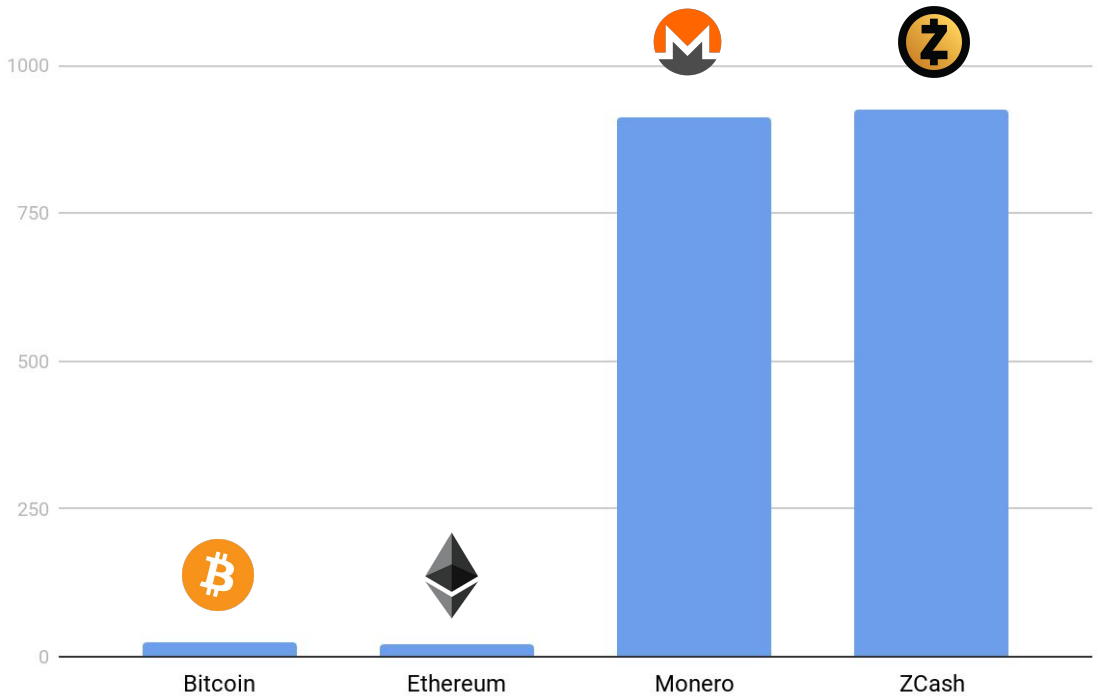
The main strength of the privacy coins is that they are resolving concerns of privacy, one of the main drawbacks of using bitcoin. Obfuscating the sender and receiver or even the transaction amount is an obvious advantage over the more broadly accepted coins such as bitcoin or ethereum.

The fact that the privacy coins are building on bitcoin's strengths and aiming to solve its privacy issues is considered a strength. As the privacy features are still under development, this predetermined the strong focus on the technology in the privacy coins projects.

The leading coins are promising many new updates and releases in their roadmaps. Monero is planning Kovri alpha release for 2018, a C++ implementation of the I2P network adding an extra layer of privacy and security and ZCash is coming with Overwinter and Sapling network upgrades later this year. Additionally, the ZCash team structure continues to display a focus on development, with a strong engineer base.

For comparison of the development activity we used the GitHub insights report for Monero, ZCash (Dash is omitted for its questionable position as a privacy coin), Ethereum and bitcoin. The forty-nine (49) weeks commits are divided by the market cap of each coin, to provide an unbiased comparison. The commits are individual changes to a file or set of files and serve as one of the measurements showing the activity on the Github developers community.

Github commits relative to market cap



Source: Github insights

Strategic Analysis

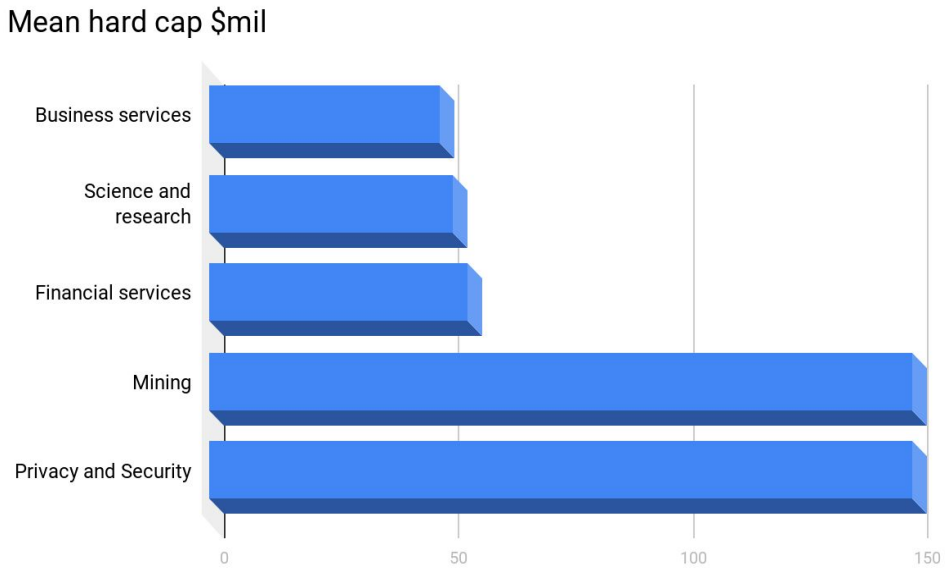
Weaknesses

As we have already seen in the comparison of the different privacy solutions on page eight, currently the enhanced privacy is offset by the decreased scalability. The advanced cryptography is increasing the size of the transactions, slowing down the transaction speed and boosting the size of the blockchain. Scalability is one of the reasons why the privacy is optional in ZCash and Dash. Improving the scalability is also one of the main goals of the new releases and updates of Monero and ZCash.

Another weakness of privacy coins is their association with the darknet. The focus on confidentiality while appealing to privacy-concerned user can limit the user base and push the privacy coins to the shadow economy and the black market.

Opportunity

With the growing crypto market capitalization, authorities are intensifying the effort to make the cryptocurrencies traceable and accountable to users. Companies such as Chainanalysis or Elliptic are working with law enforcement agencies, collecting blockchain data and statistics. This naturally fosters the demand for privacy solutions. ICO Market Research was tracking the ICOs in the 1Q18 and sorted the industries based on the average hard cap. Privacy and Security were in the lead of the top five, together with Mining, signaling the interest of the community in the privacy field.



Source: ICO Market Research report

Privacy is also one of the issues hindering the mass adoption of cryptocurrencies by the big companies concerned about potential data leakage. This opportunity for the privacy coins is already recognized by some of the big players. An example is J. P. Morgan, who partnered with ZCash to integrated zero-knowledge security layer to J.P.Morgan's enterprise blockchain platform, Quorum.

Another step toward fostering the mass adoption of privacy coins was announced May this year. Digital currency exchange Gemini listed ZCash, offering new trading pairs with bitcoin and ethereum. This made Gemini world's first licensed Zcash exchange and NYSDFS the first regulatory agency in the world to supervise Zcash.

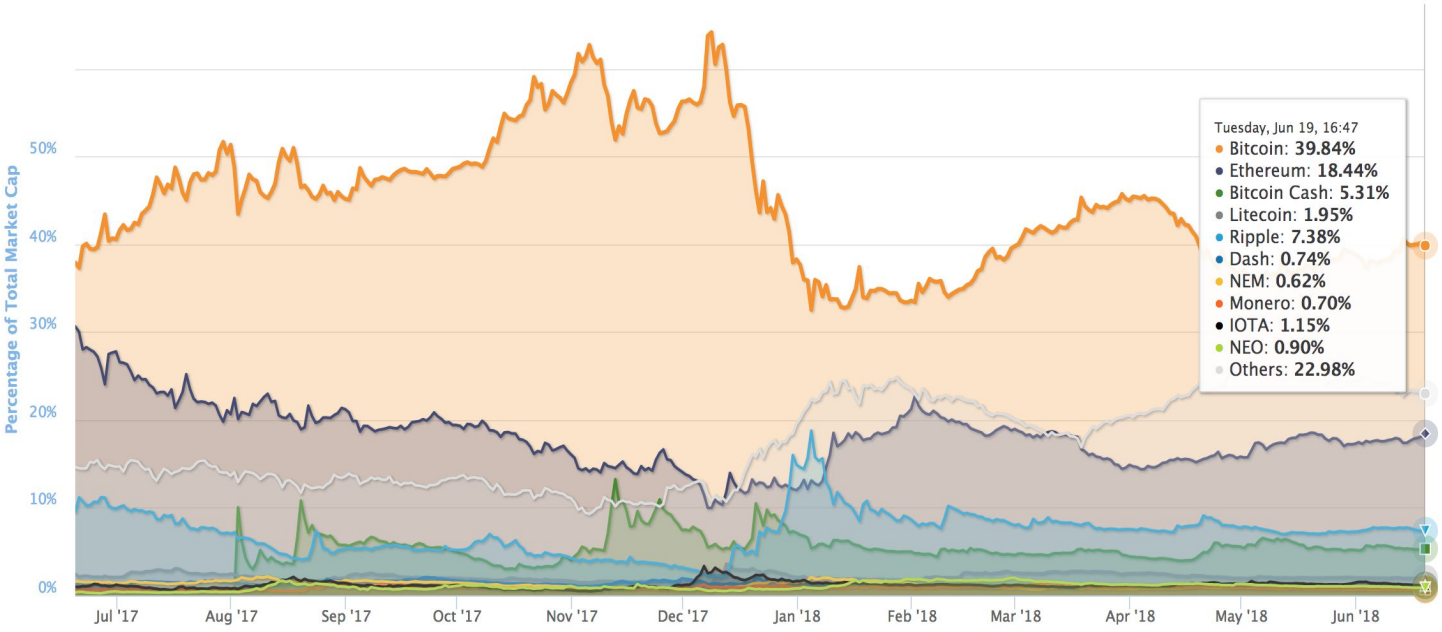
Strategic Analysis

Threats

The regulations are one of the main threats to the privacy coins. The attractiveness of cryptocurrencies to criminals has always been a strong concern and is a common argument for increased regulation. For example, the Reserve Bank of India banned private citizens and businesses from engaging in crypto-related transactions with regulated entities in April 2018.

The advanced confidentiality of privacy coins naturally draws the attention of authorities. Even in a crypto-progressive country such as Japan (first to officially recognize bitcoin), a discussion is being held about restricting the trade of privacy-focused altcoins. Regulating the decentralized coins is complicated, however, the infrastructure can be disabled. FSA (Financial Service Agency) has not issued an official plan yet, but it is pushing the registered exchanges to drop the privacy coins.

Another threat for the privacy coins is also the dominance of the base coins, Ethereum and bitcoin. The chart from CoinMarketCap shows that bitcoin still occupies a significant percentage of the market.



Source: CoinmarketCap Global Charts

This dominance is relevant also with respect to the privacy solutions. The new trend of implementing the privacy solutions on top of the existing blockchain can represent competition to the privacy coins. The "tech for token" zk-STARKs is one example, bulletproof promising not only privacy but also scalability is another. Ethereum added a building block in their public protocol that allows building zk-SNARKs transactions in the scope of the Byzantium hard fork.

If the widely adopted coins were to implement privacy solutions to their blockchain, the privacy coins could lose their advantage. However, the risk of adding untested solutions such as bulletproof to the bitcoin blockchain is too big. A more probable scenario is that the solutions are going to be implemented in the form of a sidechain to the main blockchain.

Suggestions for Investment

Driven primarily by the growing demand for confidentiality in cryptocurrencies, we believe the privacy sector of the cryptocurrency market has great potential and privacy coins deserve a spot in a balanced cryptocurrency portfolio.

There is a threat of more established coins such as bitcoin or ethereum introducing competitive privacy features, however, in the near future this is unlikely to jeopardize the position of privacy coins.

Although the three most well-known privacy coins analyzed in this report have a significant market share, there are many exciting new developments in this space and there are many other players in the market. Our next report will be focusing on a high-potential project outside of these top three.

Disclaimers

ITF, is engaged in providing trading services to the cryptocurrency trading market. Through its bot and other services it alerts its subscribers/followers ("Users") to certain market conditions based on those Users' preselected settings and trading preferences. Additionally, ITF does make available, from time to time, written or electronic communications that include research analysis, and/or a opinions concerning the DLT/cryptocurrency markets ("Reports"). The views expressed in such Reports are based solely on information available publicly/internal data/other sources believed to be true. The information is provided merely as a complementary service and do not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or as an official confirmation of any transactions or contract of any kind.

Research data and reports published/emailed/Telegrammed/etc. and or those made available/uploaded on social networking sites (e.g. Facebook, Twitter, LinkedIn, etc.) or disseminated in other print or electronic media by ITF, or entities with which it partners and any subsidiaries or partners thereof ("Affiliates"), or those opinions concerning cryptocurrencies expressed as and during the course of a public appearance, are for informational purposes only. Reports are provided for assistance and are not intended to, and must not, be used as the sole basis for an investment decision. The User assumes the entire risk of any use made of this information.

Reports may include projections, forecasts and other predictive statements which represent ITFs or its Affiliates' assumptions and expectations in the light of currently available information. These projections and forecasts are based on industry trends, circumstances and factors which involve risks, variables and uncertainties. The actual performance of a company, project, token or currency represented in a Report may vary from those projected. The projections and forecasts described in any Report should be evaluated keeping in mind the fact that they:

- are based on estimates and assumptions;
- are subject to significant uncertainties and contingencies;
- will vary from actual results and such variations may increase over a period of time;
- are not scientifically proven to guarantee certain intended results;
- are not published as a warranty and do not carry any evidentiary value; and
- are not to be relied on in contractual, legal or tax advice

Disclaimers Continued

Prospective investors/traders and others are cautioned that any forward-looking statements are not predictions and may be subject to change without notice. Reports based on technical analysis ("TA") are focused on studying charts and movements of a given currency or token's price movement and/or trading volume. As such, a Report based on TA may not match with a Report on fundamental analysis. Though Reports are reviewed for any untrue statements of material facts or any false or misleading information, ITF does not represent that ANY REPORT is accurate or complete and again emphasizes that NO REPORT should be relied on in connection with a purchase, investment, commitment, or contract by anyone whatsoever. ITF does not guarantee the accuracy, adequacy, completeness or availability of any information in any Report and therefore CANNOT be held responsible for any errors or omissions or for the results obtained from the use of such information. ITF, its Affiliates and the officers, directors, and employees of either, including analysts/authors shall not be in any way responsible for any direct, indirect, special or consequential damages that may befall any person from any information contained in any Report nor do they guarantee or assume liability for any omission of information from therein. Information contained in any Report cannot be the basis for any claim, demand or cause of action. These data, Reports, and information do not constitute scientific publications and do not carry any evidentiary value whatsoever.

ITF's Reports are proprietary and are not for public distribution. Reproduction or dissemination, directly or indirectly, of research data and/or ITF Reports, in any form, is prohibited except with the written permission of ITF. Persons into whose possession the Reports may come are required to observe these restrictions. Opinions expressed therein are current as of the date appearing on the report only. Data may be subject to update and correction without notice. While ITF endeavors to update (on a reasonable basis) the information discussed in the Reports, there may be regulatory, compliance, or other reasons that prevent ITF from doing so.
The Reports do not take into account the particular investment objectives, financial situations, risk profile or needs of any person, natural or otherwise. The User assumes the entire risk of any use made of this information. Each recipient of a Report should make such investigation as deemed necessary to arrive at an independent evaluation of an acquisition of the asset referred to in any Report (including the merits and risks involved).

Cryptocurrencies involve substantial risks and are not suitable for all investors/traders. Investors can lose their entire investment relatively easily in the cryptocurrency markets. Before acting on any advice or recommendation in this material, Users should consider whether it is suitable for their particular circumstances and, if necessary, seek professional advice. The price and value of investments referred to in research reports and the income from them may fluctuate.

Certain information set forth in this Report contains "forward-looking information", including "future oriented financial information" and "financial outlook", under potentially applicable securities laws (collectively referred to herein as "Forward-Looking Statements"). Except for statements of historical fact, information contained herein constitutes Forward-Looking Statements and includes, but is not limited to, the (i) projected financial performance of a company, project, token, or currency; (ii) completion of, and the use of proceeds from, the sale of tokens being offered to the public; (iii) the expected development of a company, project, token, or currency's business, projects and joint ventures; (iv) execution of the company's or the project, token, or currency's developers' vision and growth strategy; (v) sources and availability of funding for the company, project, token, or currency; (vi) completion of any projects that are currently underway, in development or otherwise under consideration; (vi) renewal of any material agreements; and (vii) future liquidity, working capital, and capital requirements. Forward-Looking Statements are provided to allow potential investors the opportunity to understand ITF's beliefs and opinions in respect to the future of a given company, project, token, or currency so that they may use such beliefs and opinions as one factor in evaluating an investment.

Disclaimers Continued

NO statement issued on ITF's website or in any Report is a guarantee of future performance and undue reliance should not be placed on them. Such Forward-Looking Statements necessarily involve known and unknown risks and uncertainties, which may cause actual performance and financial results in future periods to differ materially from any projections of future performance or result expressed or implied by such forward-looking statements.

Although Forward-Looking Statements contained in this presentation are based upon what ITF and/or its Affiliates believe are reasonable assumptions, there can be no assurance that Forward-Looking Statements will prove to be accurate, as actual results and future events could differ materially from those anticipated in such statements. Neither ITF nor any of its Affiliates undertake any obligation to update forward-looking statements if circumstances or management's estimates or opinions should change except as required by applicable laws. The User is cautioned not to place undue reliance on forward-looking statements.

The User should consult their own advisors to determine the merits and risks of ANY investment.