CRYPTIX
LABS

Privacy Taxonomy Part Two: Privacy Infrastructure

The development and maintenance of privacy-preserving technology is complex, requiring both skilled engineers and agile teams.

The potential for analysis of digital transactions and information patterns, however, is an increasingly lucrative business, with groups such as Chainsafe[1] gaining massive amounts of funding and industry attention. As such, privacy-preserving technology must also contend with the pressure of being in an arms race with these groups, alongside the technical and engineering skill required to build this technology. There are numerous approaches to the creation and integration of this technology with regards to blockchain technology, the most notable of which will be discussed herein.

The first - and perhaps most well known - of these technologies is CoinJoin[2]. This is a technique that has been discussed since the early days of Bitcoin[3] as an experimental feature to be added to early privacy-oriented wallets[4], and has since become a staple aspect of numerous software and hardware wallet solutions such as Samurai Wallet's Whirlpool software and nodl Dojo[5], the Wasabi Wallet[6] – which uses CoinJoin by default – and (now defunct) online platforms like JoinMarket. Before discussing how performing a CoinJoin obfuscates the relation between the particular sender and receiver of a transaction, we must first understand how standard Bitcoin transactions work. A transaction consists of one or more inputs which are spent and one or more outputs which the transaction amount is spent to, with the sending and receiving addresses involved in this transaction being publicly visible on the Bitcoin blockchain. All of these input addresses typically refer to one address; if even one of these pseudonymous addresses can be linked to a real-world identity, then the transaction cannot be said to be private. CoinJoin allows for the assumed links between inputs and outputs to be obfuscated, thus allowing for far greater transactional privacy on arguably the biggest blockchain. It does this by combining or pooling inputs and outputs from multiple addresses into a single transaction, therefore obfuscating the links between senders and receivers, even to these parties themselves. Furthermore, this technique is advantageous to all users of Bitcoin, "[s]ince a combination of inputs no longer necessarily means that all of the input-addresses belong to the same user, [therefore making] clustering [...] become a less powerful analytics tool in general."[7] One further advantage to technique is that it requires no modifications to the Bitcoin protocol itself, thus allowing for multiple implementations and accelerated development not requiring a fork.

Another technology that is worth discussing here is Blind Off-chain Lightweight Transactions (previously referred to as BOLT, now developed by Bolt Labs[8] as zkChannels).[9] Although the original BOLT protocol was Bitcoin-specific, the zkChannel project is now chain-agnostic, building on the architecture of the Bitcoin's Lightning Network.[10] Much like the Lightning Network, it merely utilizes the blockchain to create a deposit between two parties who wish to transact. These parties transact 'off-chain' directly - "adjusting the respective

ownership shares of the deposit"[11] - only interact with the blockchain in order to either close the 'payment channel' or resolve a dispute. The numerous privacy issues of the Lightning Network are mitigated by the utilization of blind ECDSA signatures as well as having the data for the payment channel kept "asymmetrically", meaning that "only one party (i.e., the customer) knows the channel balance and the identity of the second party (i.e., the merchant)".[12]

The next project is instead being built as an additional layer for the already privacy-preserving cryptocurrency Monero. Kovri[13] is a C++ implementation of the I2P network which aims to sidestep the issues surrounding I2P as it currently stands – that it is difficult to use and difficult to develop with as it is written in Java – which will be integrated via an "easy-to-use interface integrated with Monero's GUI in addition to being a stand-alone I2P router".[14] There are several significant privacy advantages to be gained from this, involving the mitigation of txid and IP address linking, metadata leakage, and node partitioning attacks. One interesting aspect of this technique is that by re-implementing a tested technology such as I2P and allowing for all Monero transactions to occur over this network, both Monero and I2P networks mutually benefit: it will strengthen the I2P network by increasing the number of participants whilst simultaneously increasing the privacy set for Monero RingCT. Although only in Alpha currently, this is definitely a project to follow.

Finally, StarkWare,[15] a "2017-founded privacy and scalability protocol"[16] offer scalability and privacy solutions built out of a technology stack they are developing, with impressive benchmarks having already been met, including a fully operational STARK system built with WASM in-browser on a mobile phone at the Web3 conference.[17] They currently have two projects under active development. The first of these is the DeversiFi[18] Decentralized Exchange (DEX), which builds upon the architecture laid out by the Lightning Network with a Layer 2 solution atop the Ethereum network. By 'Layer 2', this means that their technology does not require any modification to the underlying blockchain software itself, thus greatly speeding up development. StarkWare does this via the utilization of Zero Knowledge Non-interactive pRoofs of Knowlege (zkSNARKs), which allow for the completely secure and private transactions, albeit with some potential issues such as a trusted setup.[19] This supposedly allows for 9000+ private and secure transactions a minute. The second of these similarly builds upon Lightning with StarkPay, a micro-payment and payment channel project utilizing zk-STARKs, allowing for private and scalable transactions via combining both on-chain (i.e. 'standard') and off-chain (see above) transactions. The off-chain components do most of the heavy lifting within the StarkPay architecture, involving a "A Payment Processor, which interacts with Payers and Payees [, the] Payers' balances tree: these are updated by the Prover, and their availability is ensured (see further discussion below) [, and a] Prover, which generates STARK proofs attesting to the validity of batches of payments provided by the Payment Processor, and to the validity of the update to the Payers' balances." The on-chain components, similar to Bolt Labs' zkChannels, are merely for significant events and arbitration, involving an 'On/Off Ramp' smart contract which stores the balance commitment, and a verifier contract, which both verifies the proofs created off-chain and communicates with the verifier smart contract.

There are notable exceptions that exist parallel to the above mentioned projects such as NuCypher – who are offering "the privacy layer of the decentralized internet"[20] via proxy re-encryption and fully homomorphic encryption services – and Orchid,[21] the 'blockchain powered VPN'. All of these technologies offer significant advantages for many blockchains, enabling a secondary layer of privacy to further bolster the significant advances already made by privacy coins.

[1] https://www.chainalysis.com/
[2] A detailed account of which can be found here: https://smeiklej.com/files/bitcoin15.pdf and here: https://arxiv.org/pdf/1706.05432.pdf
[3] Most often cited as being first proposed by Gregory Maxwell in 2013.
[4] Dark Wallet
[5] See https://samouraiwallet.com/whirlpool and https://samouraiwallet.com/nodl
[6] https://www.wasabiwallet.io/
[7] https://bitcoinmagazine.com/articles/coinjoin-combining-bitcoin-transactions-to-obfuscate-trails-and-increase-privacy-1465235087
[8] https://boltlabs.tech/
[9] https://eprint.iacr.org/2016/701.pdf
[10] https://lightning.network/
[11] https://eprint.iacr.org/2016/701.pdf
[12] https://medium.com/boltlabs/zkchannels-for-bitcoin-f1bbf6e3570e
[13] https://gitlab.com/kovri-project/kovri/
[14] https://forum.getmonero.org/9/work-in-progress/86967/anonimal-s-kovri-full-time-development-funding-thread
[15] https://starkware.co/#hero
[16] https://cryptoslate.com/consensys-backed-starkware-is-powering-9000-transactions-second-on-this-ethereum-based-dex/
[17] https://medium.com/starkware/the-road-ahead-in-2019-8589fedfbc7a
[18] https://www.deversifi.com/
[19] For more on this see the previous document in this series 'Privacy Taxonomy Part One: Privacy Coins'
[20] NuCypher site
[21] Orchid site