Privacy

Digital Assets - Week 7 (Pre-record)

Rhys Bidder
rhys.m.bidder@kcl.ac.uk

KBS, QCGBF

Autumn 2024

Disclaimer 1: Any opinions expressed, errors or omissions should be regarded as those of the author and not necessarily those of KCL, KBS, QCGBF, QCB, CBI, BoE, or ChainLink Labs.

Disclaimer 2: These notes on cryptography are heavily simplified and leave out many important details. For any real-world security applications these notes should not be relied upon. Instead you should consult appropriate security resources and reliable security professionals.

Disclaimer 3: Cryptoasset transactions are illegal in some jurisdictions. Do not violate these or any other laws. I am not promoting the use of crypto in countries where it is illegal in any form and these slides are not a promotion of crypto or an invitation to participate in crypto-related activities in such countries. They are purely for educational purposes.

Disclaimer 4: I currently am an advisor to Chainlink Labs.

Privacy in blockchain

- The pseudonymity of using a public address a sense of privacy on the blockchain
- However, the transparency of transactions on public permissionless chains means that there are various ways in which someone can be identified - or have certain characteristics identified
- Permissioned blockchains, with a limited and known group of participants offer even more of a challenge (recall the wholesale CBDC pilots that emphasized 'privacy enhancing techniques)
- Tensions arise between the legitimate demand for privacy of most users, with government/regulatory concern with money laundering, terrorist financing and so forth
- Arguably this is an additional tradeoff - a privacy-safety dilemma - to add to the more technical 'trilemma' we discussed previously

Readings

Excellent readings on this topic (included in the reading list and/or uploaded):

- Ch. 5 in *Build your own blockchain*
- Chs. 3&4 in *Crypto Launderers*

Various blogs from forensic blockchain analysis companies are worth reading

- Chainalysis and Ellipitic
- The author of *Crypto Launderers* is at Elliptic

Linking addresses to identities

Certain patterns can be detected that help inform the analysis

- Which nodes received the broadcasted transaction first?
- At what times are the transactions initiated?
- Do they align with monthly salary payments or rent?
- Do the tx sizes/frequency suggest type of transaction?

Linking addresses to identities

There are externalities to a particular participant being identified

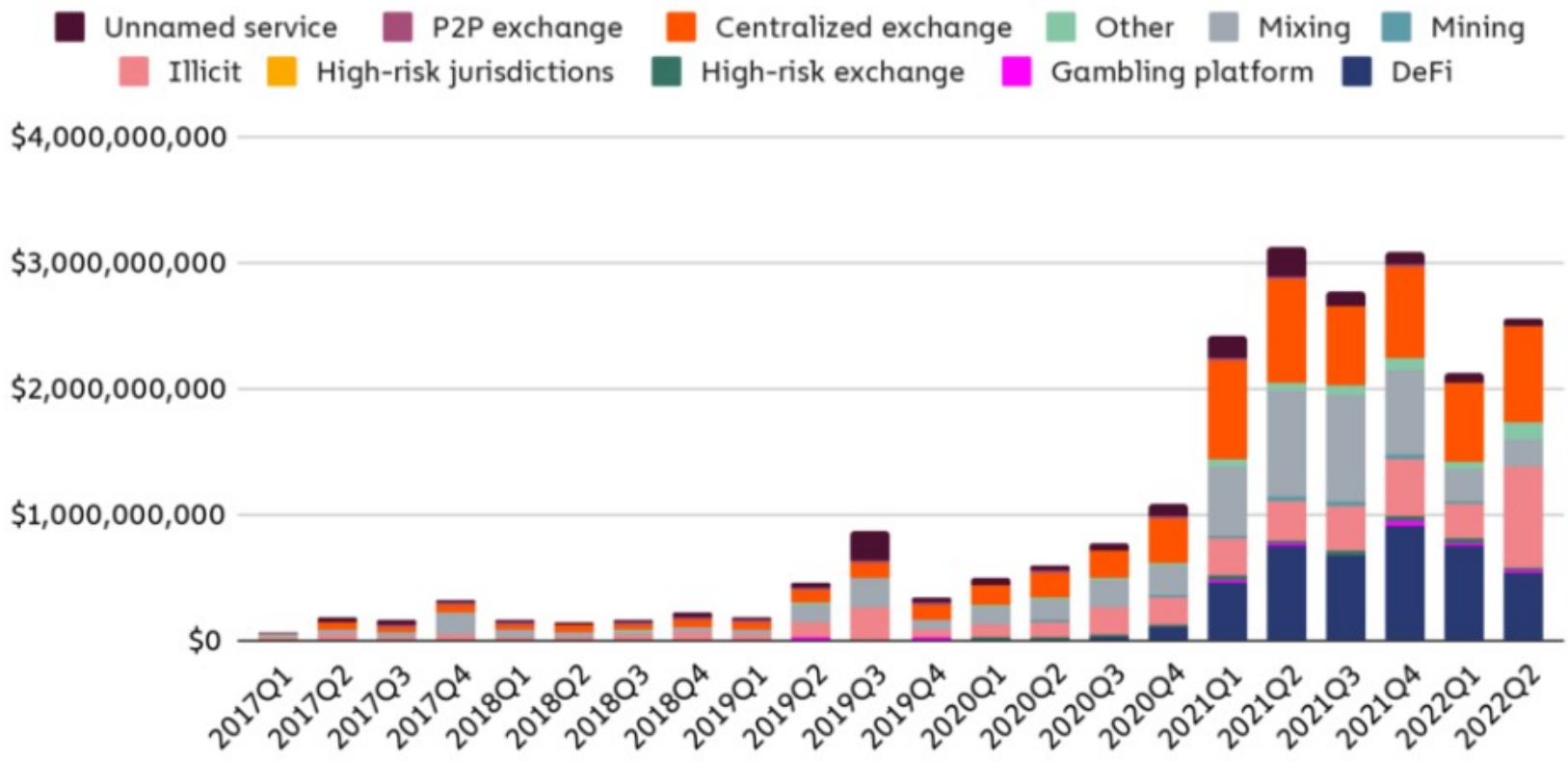
- Some parties are publicly identified (intentionally or not)
- Transactions involving these wallets - directly or indirectly - can then help reveal other participants' characteristics
- Recall the UTXO chain in Bitcoin, but this applies more generally through graphing transactions on Ethereum etc.
- Even if use different Bitcoin addresses to receive different payments, combining them in a transaction connects them forever

Big data/machine learning can extract patterns - especially if provided with additional information from off-chain sources

- One can buy 'wallet labels' that purport to identify or at least classify addresses (good for research and AML/compliance)

Mixers

- Mixers combine payment input from multiple transactions through intermediate steps before making various payment outputs that are difficult - perhaps impossible - to trace back to the corresponding input
- The pooling of the payments, and the randomization of the output payments' timing and amount obfuscate who is receiving what, from whom (could be someone laundering their own money)
- Three important types of mixer are:
  - Centralized custodial mixers
  - CoinJoins
  - Smart contract mixers
- There are legitimate uses for mixers (and other attempts to avoid traceability) but illicit parties often use mixers and they account for a significant fraction of their use



Quarterly values received by mixers, by source. *Source:*Chainalysis, 2022

Quarterly values sent to mixers from illicit addresses, by category.
*Source:*Chainalysis, 2022

Centralized custodial mixers

- A single operator takes custody of funds temporarily
- For a fee, mixes and redirects the payments
- Relies on trust in the mixer operator and its systems
- Simple target for regulators and attackers

CoinJoins

- Decentralized and non-custodial
- A group of participants agree to engage in a CoinJoin
  - Can be tricky to coordinate
  - Masking more effective the larger the number/value in the pool
  - Limits the scale of any money laundering
- Multiple inputs are combined in a single transaction
- Particular outputs cannot be connected to particular inputs
- Transaction only valid if all signatures are provided for the various inputs
- Also makes the transactions ‘smaller’ - fewer fees (not a privacy issue)

CoinJoin example I

- Laundering example:
  - Four users input 2, 4, 6 and 8 for a total of 20
  - CoinJoin transaction creates 20 separate outputs each worth 1
  - Outputs allocated to each user in the same amounts they originally contributed
  - Equal output value $\Rightarrow$ should be impossible identify which of the new addresses are controlled by which of the original users

CoinJoin example II

- Disguising payments example:
  - A purchases an item from B, C purchases an item from D, and E purchases an item from F
  - With CoinJoin, only one single transaction is recorded: crypto was paid from A, C, and E addresses to B, D, and F
  - Doesn't show who received which transaction, but all users received correct amount

Smart contract mixers

- A prominent/infamous example is Tornado Cash
- Non-custodial and decentralized, but does not require explicit coordination among sets of users (like CoinJoin)
- User deposits assets in an on-chain smart contract pool
- On doing so they receive a unique key
- Can then withdraw those same assets using a ZKP to show they know the key (or have a relayer provide the proof)
- Can withdraw to a different address, without any link between the transactions (assuming reasonable liquidity/activity in the pools)

Tornado Cash - OFAC sanctions

- Tornado Cash smart contracts are software and its original designers have destroyed the private keys controlling them
- Ostensibly in response to money laundering and usage by NK entities (Lazarus Group), OFAC sanctioned Tornado Cash contracts in 2022
- This makes it illegal for US citizens to use it (and soon after the sanctions, Github removed code for the SCs)

Tornado Cash - OFAC sanctions

- And yet, as long as Ethereum runs, so will Tornado Cash - though one question is whether miners located in the US are breaking the law in including transactions in a block that use Tornado Cash
- Raised concerns in crypto industry (and among libertarians) that *software* is an unprecedented target of sanctions - rather than addresses using the SCs (see Coinbase note on Keats)
- More recently, a Dutch court convicted a Tornado Cash founder of laundering

Privacy coins

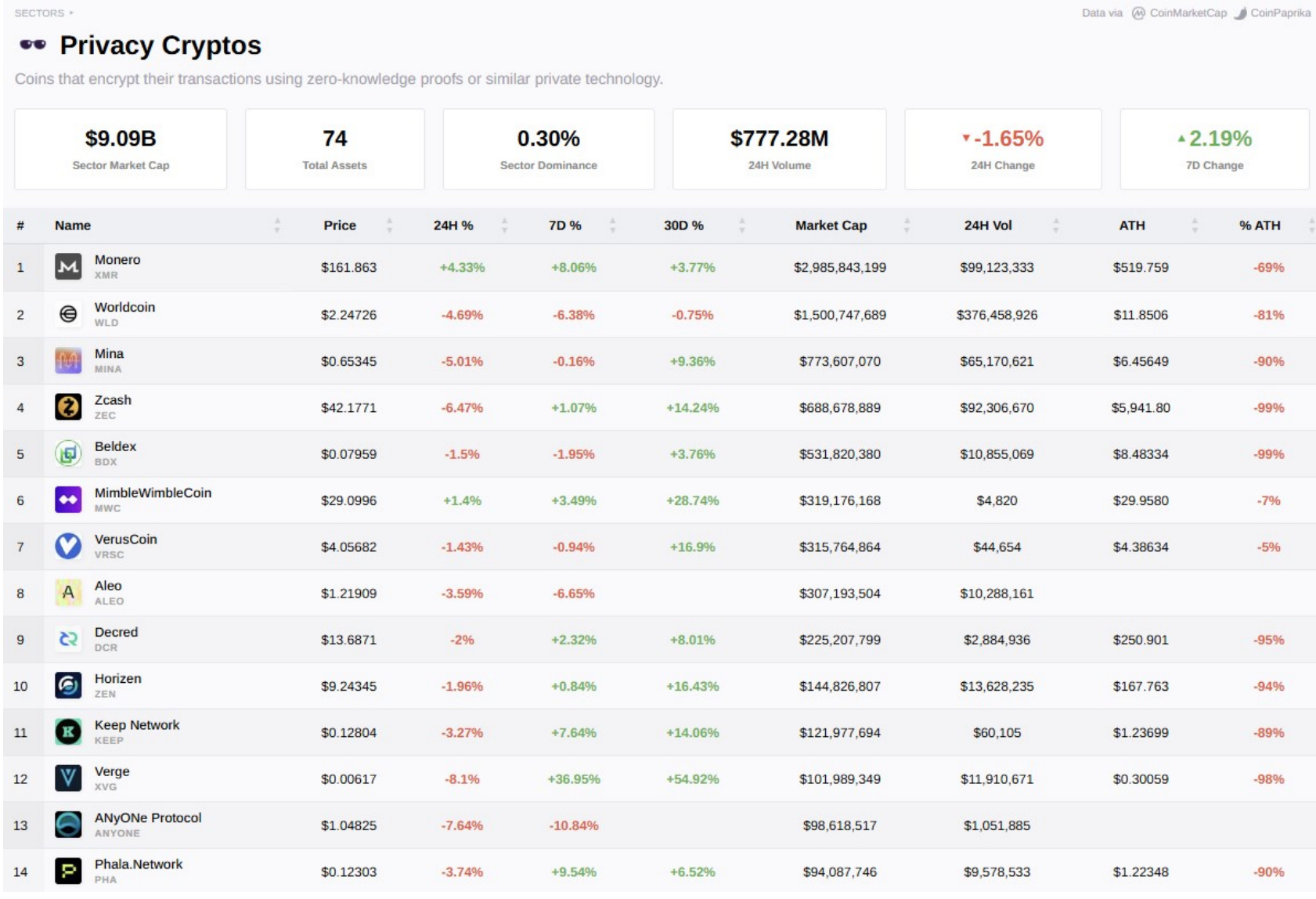
- The methods to enhance privacy discussed above are built on top of blockchains
- Privacy coins are based on amended blockchain protocols - so are embedded in the core structure of the blockchain's transaction format

ZeroCash / ZCash

- A prominent privacy coin, the ZeroCash protocol (with specific implementation, ZCash), emerged from a Bitcoin hard fork
- Transactions on the ZeroCash blockchain have their details, including the amounts, shielded
- Instead, only zero knowledge proofs (specifically, zk-SNARKS) are recorded and validated on chain (details here)
- Zcash is listed on Coinbase, but some privacy coins have been delisted and can be illiquid and difficult to develop SCs for

Monero

- Monero blockchain allows masking of transaction details through the use of ring signatures and stealth addresses
  - *Ring signatures:* Can sign on behalf of a group, without revealing who within the group signed (see here and here)
  - *Stealth addresses:* A sender of a transaction creates a random single-use address on behalf of the recipient (see here)



SECTORS ▸

Data via CoinMarketCap CoinPaprika

Privacy Cryptos

Coins that encrypt their transactions using zero-knowledge proofs or similar private technology.

$9.09B	74	0.30%	$777.28M	▾ -1.65%	▴ 2.19%
Sector Market Cap	Total Assets	Sector Dominance	24H Volume	24H Change	7D Change

#	Name	Price	24H %	7D %	30D %	Market Cap	24H Vol	ATH	% ATH
1	Monero XMR	$161.863	+4.33%	+8.06%	+3.77%	$2,985,843,199	$99,123,333	$519.759	-69%
2	Worldcoin WLD	$2.24726	-4.69%	-6.38%	-0.75%	$1,500,747,689	$376,458,926	$11.8506	-81%
3	Mina MINA	$0.65345	-5.01%	-0.16%	+9.36%	$773,607,070	$65,170,621	$6.45649	-90%
4	Zcash ZEC	$42.1771	-6.47%	+1.07%	+14.24%	$688,678,889	$92,306,670	$5,941.80	-99%
5	Beldex BDX	$0.07959	-1.5%	-1.95%	+3.76%	$531,820,380	$10,855,069	$8.48334	-99%
6	MimbleWimbleCoin MWC	$29.0996	+1.4%	+3.49%	+28.74%	$319,176,168	$4,820	$29.9580	-7%
7	VerusCoin VRSC	$4.05682	-1.43%	-0.94%	+16.9%	$315,764,864	$44,654	$4.38634	-5%
8	Aleo ALEO	$1.21909	-3.59%	-6.65%		$307,193,504	$10,288,161		
9	Decred DCR	$13.6871	-2%	+2.32%	+8.01%	$225,207,799	$2,884,936	$250.901	-95%
10	Horizen ZEN	$9.24345	-1.96%	+0.84%	+16.43%	$144,826,807	$13,628,235	$167.763	-94%
11	Keep Network KEEP	$0.12804	-3.27%	+7.64%	+14.06%	$121,977,694	$60,105	$1.23699	-89%
12	Verge XVG	$0.00617	-8.1%	+36.95%	+54.92%	$101,989,349	$11,910,671	$0.30059	-98%
13	ANyONe Protocol ANYONE	$1.04825	-7.64%	-10.84%		$98,618,517	$1,051,885		
14	Phala.Network PHA	$0.12303	-3.74%	+9.54%	+6.52%	$94,087,746	$9,578,533	$1.22348	-90%

Coins that encrypt their transactions using zero-knowledge proofs or similar private technology. *Source:*Coinslate, Nov 20, 2024

Warning: Some privacy solutions are illegal to use in some countries. Be aware. I am not encouraging their use anywhere and I discourage their use where they are illegal.

Validiums

- We previously discussed zero knowledge rollups
- A particular form of such rollups is known as a 'validium'
- Purely the verification of a correct transaction is stored on chain, in the form of a zero knowledge proof
- All computation and associated data are stored off-chain
- This is another way to have greater control over data - particular for sensitive data that should not in any form be on a public blockchain
- As a side effect (as previously discussed) this will also help with scalability of blockchains, ideally without compromising security and decentralization

KYC/AML tensions

- In later lectures we will discuss regulation, but clearly there is a tension between many of these privacy methods and KYC/AML
- This tension is perhaps slowly being relaxed through
  - ZK proofs
  - Partial encryption (not all details of a transaction need to be known by a regulator - e.g. see wholesale CBDC pilots Inthanon, Khokha and Helvetia)
  - Fully homomorphic encryption (FHE) where encrypted data can still be operated on /used in calculations without decryption
- But what about quantum computing?