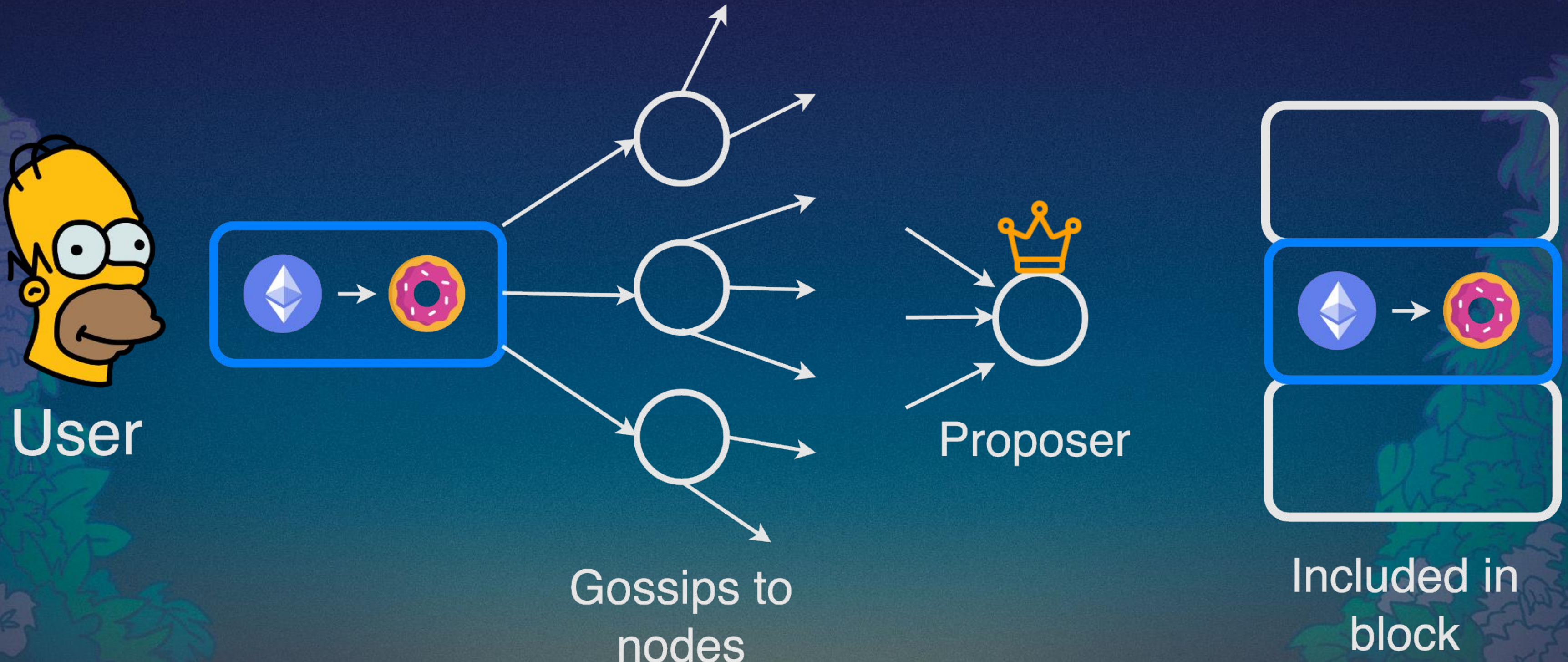
DC7 SEA

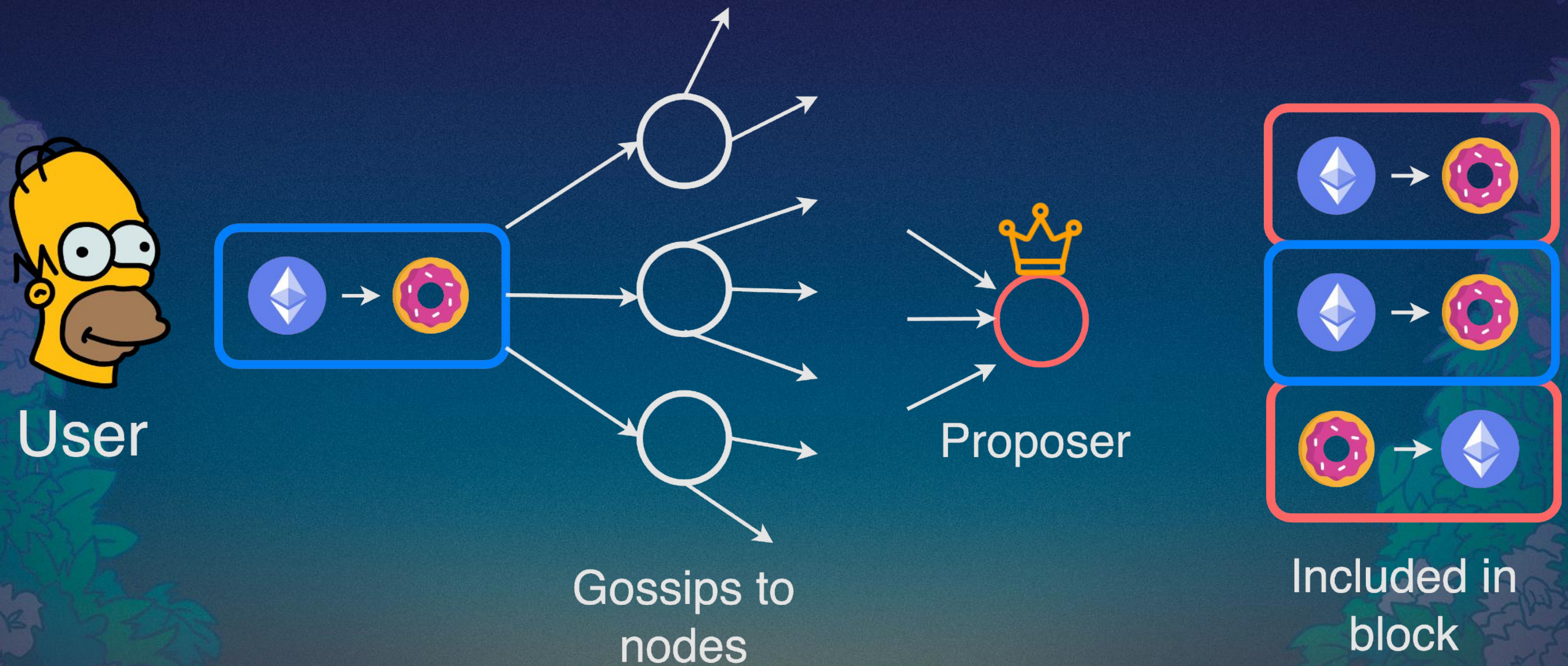
Encrypted Mempools: a path to Ethereum L1

Marc Harvey-Hill

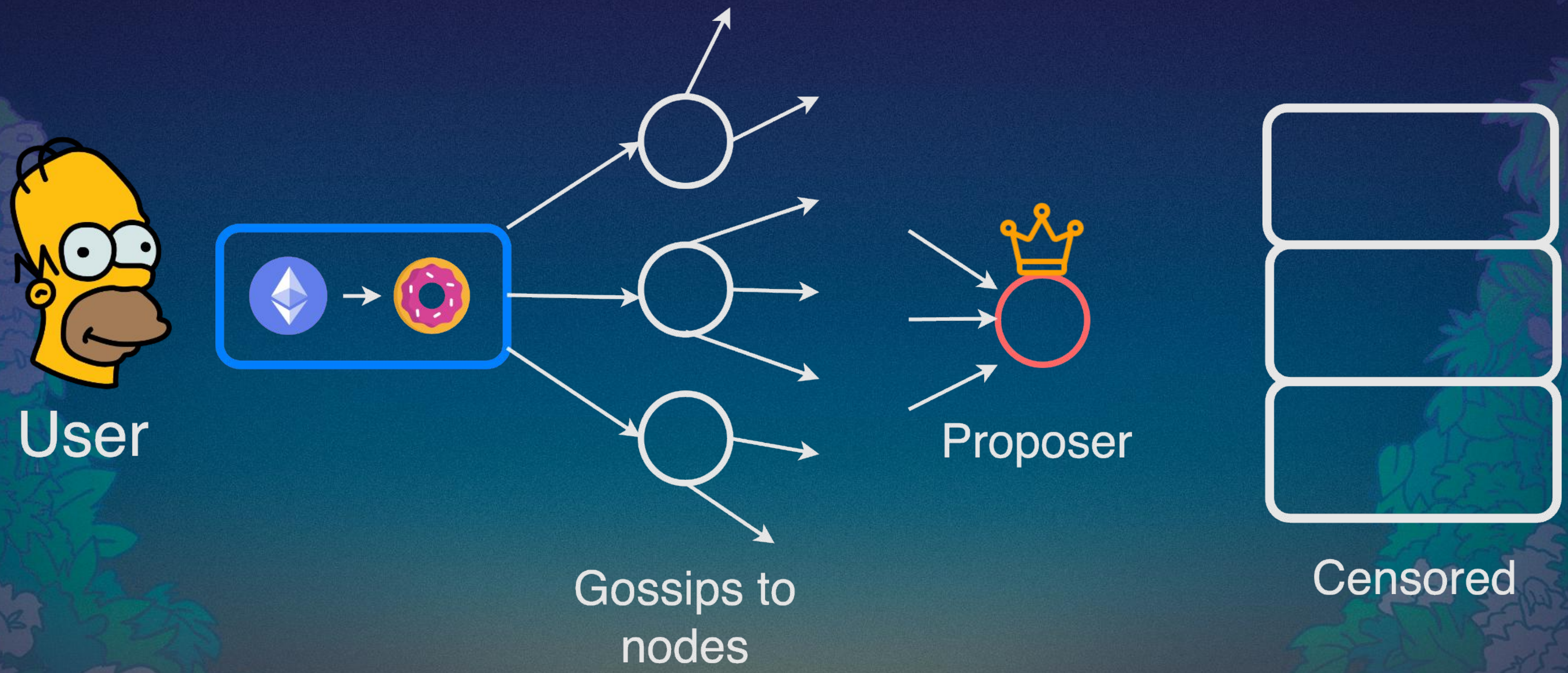
Including a transaction onchain



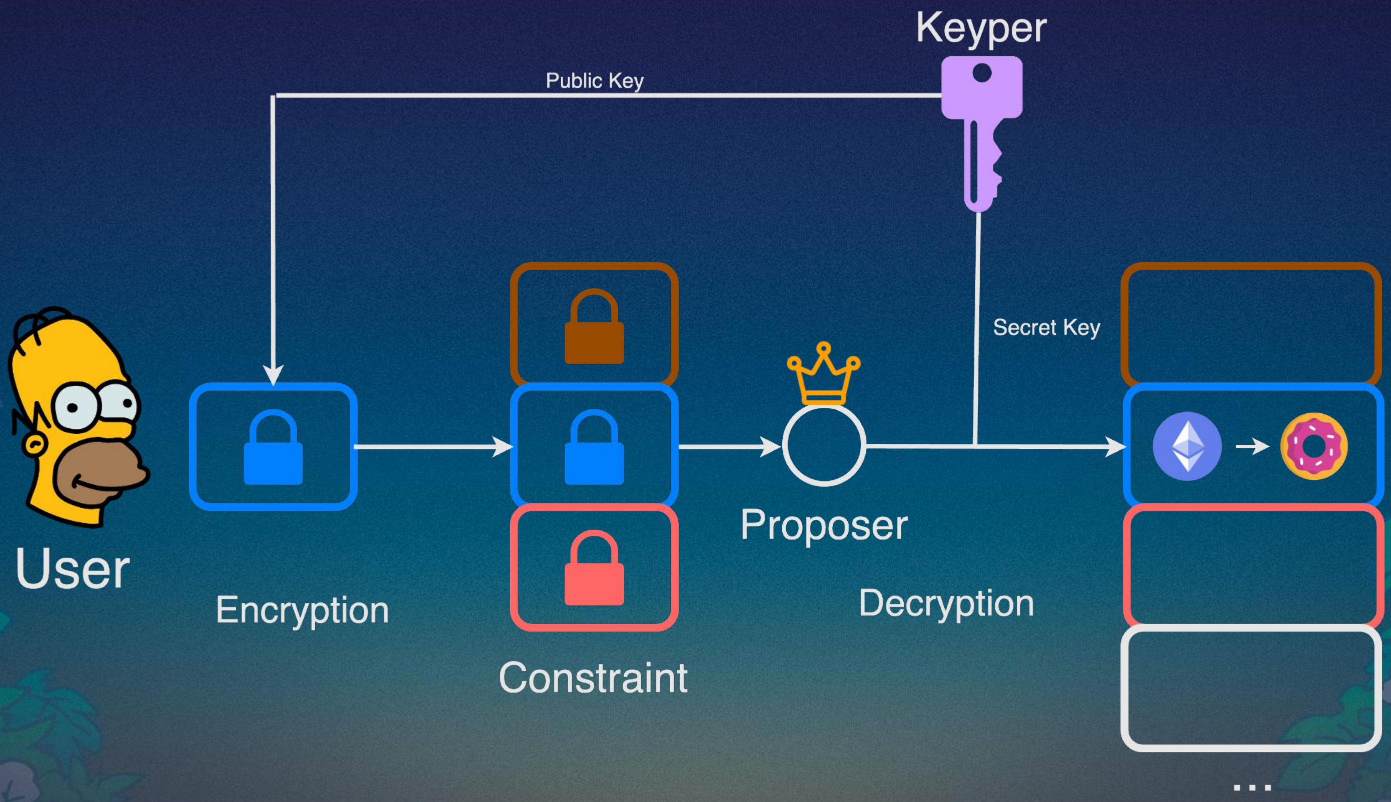
Problem 1: Frontrunning / Sandwiching



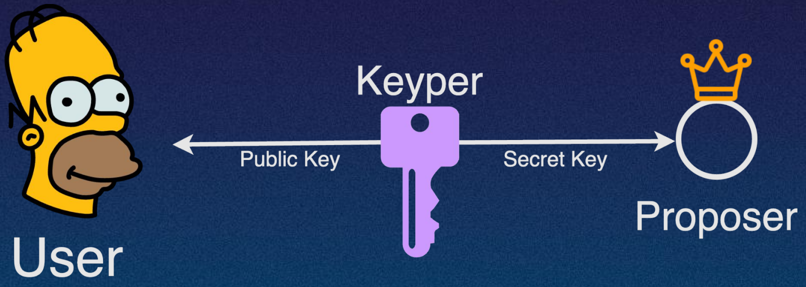
Problem 2: Censorship



Solution: Encrypted mempool



Keyper designs



Trusted → Trustless

Trusted party	Secure enclave	Threshold	Delay
eg. Flashbots protect	Trusted hardware eg. SUAVE	Majority trust assumption eg. Shutter	Cryptographic & hardware assumptions

Posting encrypted transactions

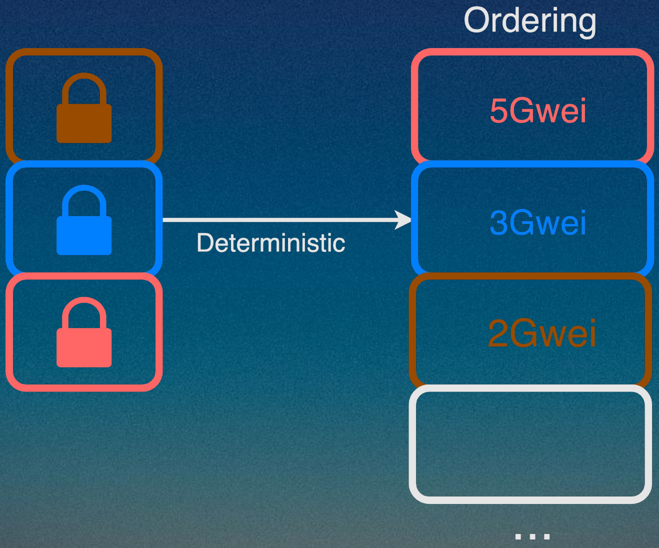
Public constraint to encrypted txs that will be included. Must be:

- Available: all can verify proposer’s block honours constraint
- Permissionless: users can add txs to constraint without being censored

Constraint

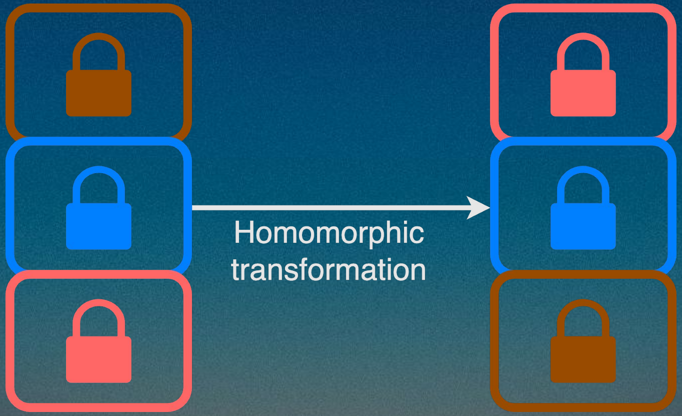
Ordering

- Deterministic mapping from constraint to ordering
- e.g. First come first served, Order by priority fee



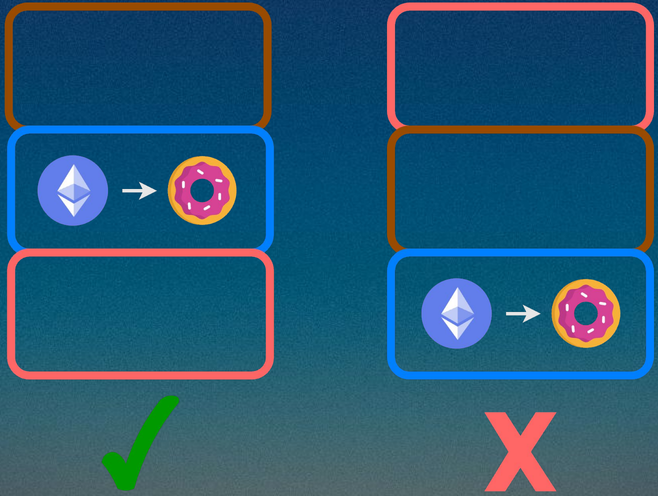
Ordering in the future

- More complex ordering / block building performed on encrypted data with homomorphic encryption
- Matches functionality of secure enclave mempools like SUAVE
- Can impose constraints like allowing backrunning but no frontrunning



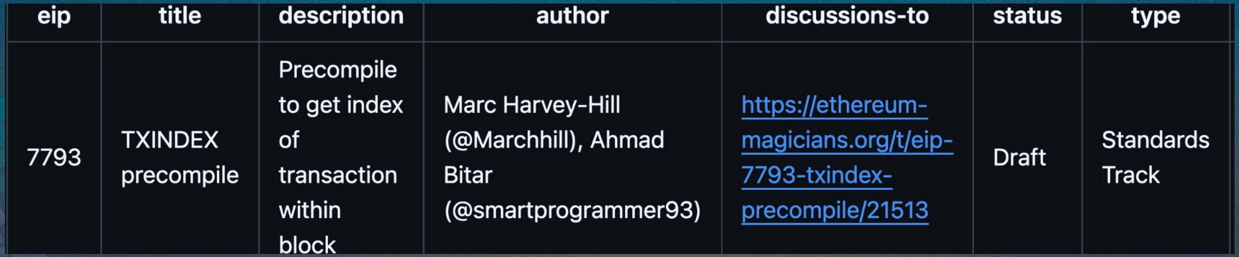
Enforcing proposer inclusion

- Proposer must include **all** valid txs they are constrained to in correct order, or all txs invalidated. Proposer could also be slashed
- Must choose between censoring all or none



Enforcing proposer inclusion

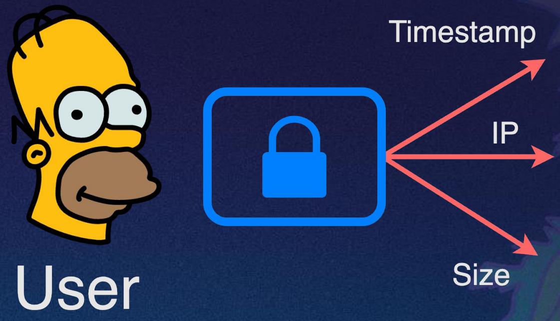
Enshrined	Out-of-protocol
Block validity tied to correct inclusion	Enforced by smart contract / account
Significant protocol change	Minimal change (EIP-7793 TXINDEX precompile)
Long term solution	Short term solution
Simpler	Complexity: different mempools competing for top of block



eip	title	description	author	discussions-to	status	type
7793	TXINDEX precompile	Precompile to get index of transaction within block	Marc Harvey-Hill (@Marchhill), Ahmad Bitar (@smartprogrammer93)	https://ethereum-magicians.org/t/eip-7793-txindex-precompile/21513	Draft	Standards Track

Hiding metadata

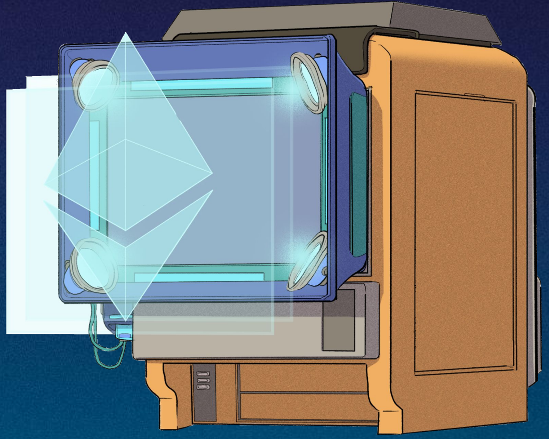
Metadata can leak information:



Metadata	Hiding method
IP address	Tor
Size	Padding to power of 2 bytes Homomorphic packing
Timestamp	Regular dummy transactions
Tx info (signature, gas, etc.)	Encrypted + zk validity proof

Q&A

Thanks for listening!



Thanks to Justin Drake and Aikaterini-Panagiota Stouka for feedback.

Image credits:

- Homer Simpson icon by Icons8
- Ethereum assets by Ethereum Foundation CC4.0