

GM! ordering it
Odds is
burn or not.
Num.

We outline the blockchain address protocol for Bitcoin Pay to Public Key Hash (P2PKH) [2], with respect to which we prove our construction secure and unseizable in Section 5. It is parametrized by a signature scheme S and a hash function H (for completeness, we give a construction which includes the concrete hash functions and checksums