5 Analysis

We now move on to the analysis of our scheme. As the scheme is deterministic, its correctness is straightforward to show.

Theorem 1 (Correctness). *The proof-of-burn protocol Π of Section 3 is correct.*

Proof. Based on Algorithm 3, $\mathsf{BurnVerify}(1^\kappa, t, \mathsf{GenBurnAddr}(1^\kappa, t)) = \text{true}$ if and only if $\mathsf{GenBurnAddr}(1^\kappa, t) = \mathsf{GenBurnAddr}(1^\kappa, t)$, which always holds as GenBurnAddr is deterministic. □

We now state a simple lemma pertaining to the distribution of Random Oracle outputs.

Lemma 1 (Perturbation). *Let $p(\kappa)$ be a polynomial and $F : \{0,1\}^\kappa \longrightarrow \{0,1\}^\kappa$ be a permutation. Consider the process which samples $p(\kappa)$ strings $s_1, s_2, \dots, s_{p(\kappa)}$ uniformly at random from the set $\{0,1\}^\kappa$. The probability that there exists $i \neq j$ such that $s_i = F(s_j)$ is negligible in κ.*

We will now apply the above lemma to show that our scheme is unspenable.

Theorem 2 (Unspendability). *If H is a* Random Oracle, *then the protocol Π of Section 3 is* unspendable.

Proof. Let $\mathcal{A}$ be an arbitrary probabilistic polynomial time SPEND-ATTACK adversary. $\mathcal{A}$ makes at most a polynomial number of queries $p(\kappa)$ to the Random Oracle. Let MATCH denote the event that there exist $i \neq j$ with $s_i = F(s_j)$ where $F(s) = s \oplus 1$.

If the adversary is successful then it has presented t, pk, pkh such that $H(pk) = pkh$ and $H(t) \oplus 1 = pkh$. Observe that $\text{SPEND-ATTACK}_{\mathcal{A},\Pi}(\kappa) = \text{true} \Rightarrow \text{MATCH}$. Therefore $\Pr[\text{SPEND-ATTACK}_{\mathcal{A},\Pi}(\kappa)] \leq Pr[\text{MATCH}]$. Apply Lemma 1 on F to obtain $\Pr[\text{SPEND-ATTACK}_{\mathcal{A},\Pi}(\kappa)] \leq \mathsf{negl}(\kappa)$. □

We note that the security of the signature scheme is not needed to prove unspendability. Were the signature scheme of the underlying cryptocurrency ever found to be *forgeable*, the coins burned through our scheme would remain unspendable. We additionally remark that the choice of the permutation $F(x) = x \oplus 1$ is arbitrary. Any one-to-one function beyond the identity function would work equally well.

Preventing proof-of-burn. It is possible for a cryptocurrency to prevent proof-of-burn by requiring every address to be accompanied by a

Algorithm 5 The collision adversary $\mathcal{A}^*$ against H using a proof-of-burn BIND-ATTACK adversary $\mathcal{A}$.

```
function A*_A(1^κ)
    (t, t', _) ← A(1^κ)
    return (t, t')
end function
```

proof of possession [27]. To the best of our knowledge, no cryptocurrency features this.

Next, our binding theorem only requires that the hash function used is collision resistant and is in the standard model.

Theorem 3 (Binding). *If H is a* collision resistant *hash function then the protocol of Section 3 is* binding.

Proof. Let $\mathcal{A}$ be an arbitrary adversary against Π. We will construct the Collision Resistance adversary $\mathcal{A}^*$ against H.

The collision resistance adversary, illustrated in Algorithm 5, calls $\mathcal{A}$ and obtains two outputs, t and t'. If $\mathcal{A}$ is successful then $t \neq t'$ and $H(t) \oplus 1 = H(t') \oplus 1$. Therefore $H(t) = H(t')$.

We thus conclude that $\mathcal{A}^*$ is successful in the COLLISION game if and only if $\mathcal{A}$ is successful in the BIND-ATTACK game.

$$\Pr[\text{BIND-ATTACK}_{\mathcal{A},\Pi}(\kappa) = \text{true}] = \Pr[\text{COLLISION}_{\mathcal{A}^*,H}(\kappa) = \text{true}]$$

From the collision resistance of H it follows that $\Pr[\text{COLLISION}_{\mathcal{A}^*,H} = \text{true}] < \mathsf{negl}(\kappa)$. Therefore, $\Pr[\text{BIND-ATTACK}_{\mathcal{A},\Pi} = \text{true}] < \mathsf{negl}(\kappa)$, so the protocol Π is binding. □

We now posit that no adversary can predict the public key of a secure signature scheme, except with negligible probability. We call a distribution *unpredictable* if no probabilistic polynomial-time adversary can predict its sampling. We give the formal definition, with some of its statistical properties, in Appendix B.2.

Lemma 2 (Public key unpredictability). *Let $S = (Gen, Sig, Ver)$ be a secure signature scheme. Then the distribution ensemble $X_\kappa = \{(sk, pk) \leftarrow Gen(1^\kappa); pk\}$ is unpredictable.*

The following lemma shows that the output of the random oracle is indistinguishable from random if the input is unpredictable (for the

Uhh, 1^κ, and t, Still, that only proves you made the address, I want to know you funded it.

Charles gets angry and makes a rant video

Ken tells Charles that look: I burnt my addr only I know the key!

Game Theory:
Bob tells Charles Hopkinson: "TOO MUCH ADA, BURN, BABY, BURN!"
Charles Hopkinson tells BoB: "please, for the n-1th time, go burn your own addr at disco.inferno.io"
BoB says OKAY, creates a burn address and has innocent people send money to it.