Proof of Burn Challenge Notes

(Note: before judging me too harshly, I've never done any Blockchain dev before the second cohort... and I'm fairly new to Cardano, but I LOVE the community, ethos, it's just a great thing to be a part of, anyway...)

Currently working on the PoB Challenge, for which I actually have some questions... Concerning backwards compatibility: can we use P2PKH style addresses in Cardano? Since the paper uses their Random Oracle Model to demonstrate indistinguishability between burn addresses and P2PKH addresses... At least, that is what I took from it. I've been stumbling across all kinds of old Cardano docs (Cardano SL) and I'm curious, if we generated our own address using:

1:
$ADDR_{init} = base58(ADDR_{hf} \mid\mid CRC32(ADDR_{hf}))\ ;\ \exists\, ADDR_{hf} = hf(k_{pub}) \mid k_{pub} \in K_{derivation\ scheme}$

Then, as 'hf' is a hashing function that provides a public key hash, we can modify the initial public key address, to create our burn address:

2: $ADDR_{burn} = ADDR_{init} \mid ADDR_{hf} = \left[\, hf(k_{pub}) \oplus 1 \,\right]$

This means our 'silly person who wishes to burn ADA' can create a UTxO from the init address, which only he/she has the private key to (only he/she can spend that UTxO, as wallet mnemonics are unique, meaning only his/her seed could create that public key address and only he could have the secret key, unless he/she shared it), then he (or she, sorry!) could create a transaction on the blockchain by sending signing over the entire value of the UTxO to the burn address.

Right...

If my thinking is correct, this should still produce an indistinguishable key if one was to use the Random Oracle Model outlined in the PoB paper. Furthermore, it would make the final address non-spendable, since there would be no matching private key to sign the UTxO. Thus, ADA = burnt!

You may be wondering: why in the hell would you go to all this hassle when IOHK have implemented the same mechanism through the use of a single tag? Again, my thinking is: if one is, as Charles put it, stupid enough to request the burning of ADA, they should burn their own ADA. So, in addition to being able to verify the address is a burn address, personally, I would also like to see one more property added to the list of requirements for Proof-of-Burn, this would be: Individual Verifiability:

1. Mnemonic seeds are unique.
2. Thus only one person can have any given set of public-private key pairs.
3. Thus only one person can have a specific public key hash address.
4. Thus modifying their public key and encoding it given §2 means they cannot possibly spend any UTxO from the newly encoded public key hash (an address, if you will).
5. This makes it a 'burn address'.
6. Further, you can verify it is a burn address given the wallets public key and repeating the encoding.
7. Further, you can verify the author of the transaction generated the address, as he/she is the only one who could sign that UTxO, thereby signing ownership of the ADA from the init address to the burn address.

My Motivation Behind This Writing

I would want to know that the individual who said: "BURN, BABY BURN" is in fact visiting the "Disco" in an infernal style (I apologise, terrible joke). Assuming the proposed scheme works[1] this would provide a fairly solid proof for the proposed bootstrapping mechanism, should you wish to have one.

Footnotes

[1]. I've seen OLD documentation to say that Cardano addresses have been built like this in the past, however, I have no idea if this address formatting is still compatible with the current version of Cardano, and if ouroboros would verify this transaction?