What is Double Public Key Authentication (DPKA)?

If you recall how FIDO works, it's extremely suitable to use for privacy based use cases. DPKA is essentially using the login mechanism in FIDO but without the submission of any private identity/information/credentials.

In MFA we have 3 characteristics which are "Something we know", "Something we have" and "Something we are".

"Something we know" commonly refers to password/passphrase.

"Something we have" commonly refers to we own devices such as phone, laptop and desktop.

"Something we are" commonly refers to the biometrics traits that exist in all human bodies which commonly consist of fingerprint, voice and face.

If you use password to login only, attackers or criminals may break your passwords and they can login into your account. By using the PIN or number along with passwords, it makes attackers or criminals harder to have access to your account. The idea of MFA is to make it harder for an attacker or criminal to get access to your account.

In all previous MFAs, they work for security use cases but not for privacy use cases. Let's have a look at how DPKA works.

DPKA requires 2 different devices in order to function properly. The devices can be made up from laptop, desktop or mobile phone. It doesn't really matter what devices you use. You only need to guarantee you don't reuse the same device.

By using the same login mechanism as FIDO, you choose device A and B. Device A is laptop whereas device B is phone.

You first sign up with the exact same login mechanism shown in FIDO with device A. If the operation does not require MFA, you can just use the device to login without any trouble.

If there's a need to use MFA, first you were required to do the same sign up process on device B (your phone) just like device A.

Once you have sign up with 2 different devices, you will first login with device A then login with device B by using the same login mechanism that was used in FIDO.

This is in general how DPKA works. It relies on you holding the device rather than submitting private information such as device ID (Given by manufacturers or Google or Microsoft or other applicable companies), MAC Address (https://www.youtube.com/watch?v=ouxFr9Wk9hA), IP Address, Email Address, phone numbers and other applicable data.

Pros (Advantage)

1. Users data especially any form of private identity was not collected. Hence, user receives little to no targeted attacks such as social engineering or other applicable attacks.
2. This process involves no user secret such as password or passphrase on server side. It also means that there's no password/passphrase to leak. Leaking the public key is not in criminal's interest as they can't get private key through public key.
3. This process if done correctly, user does not need to rely on problematic passwords to login anymore as this mechanism guarantees the same security for all users.

Cons (Disadvantage)

1. This mechanism was relatively new and introducing it will deliver user experience issues towards the user.
2. It is impossible to know whether the user uses the same device for double public key authentication
3. It is an increased risk on user side as losing either of the devices will cause serious troubles to user
4. Depending on the situation, there's a chance that hackers can change the public keys with their own public keys which may or may cause some troubles to users despite there's no literal meaningful value on them doing so. (It can be solved with smart contract in Block Chain. However, Block Chain smart contract will also have its own drawbacks).
5. Assuming that public key does not get swapped by malicious hackers/attackers, it's impossible to know whether the owner behind the public keys have been changed or stayed the same.
6. Assuming that public key does not get swapped by malicious hackers/attackers, it's impossible to know whether the added device really belongs to the owner.