In-person meatspace protocol to prove unconditional possession of a private key

2019 Oct 01 See all posts

Recommended pre-reading: https://ethresear.ch/t/minimal-anti-collusion-infrastructure/5413

Alice slowly walks down the old, dusty stairs of the building into the basement. She thinks wistfully of the old days, when quadratic-voting in the World Collective Market was a much simpler process of linking her public key to a twitter account and opening up metamask to start firing off votes. Of course back then voting in the WCM was used for little; there were a few internet forums that used it for voting on posts, and a few million dollars donated to its quadratic funding oracle. But then it grew, and then the game-theoretic attacks came.

First came the exchange platforms, which started offering "dividends" to anyone who registered a public key belonging to an exchange and thus provably allowed the exchange to vote on their behalf, breaking the crucial "independent choice" assumption of the quadratic voting and funding mechanisms. And soon after that came the fake accounts - Twitter accounts, Reddit accounts filtered by karma score, national government IDs, all proved vulnerable to either government cheating or hackers, or both. Elaborate infrastructure was instituted at registration time to ensure both that account holders were real people, and that account holders themselves held the keys, not a central custody service purchasing keys by the thousands to buy votes.

And so today, voting is still easy, but initiation, while still not harder than going to a government office, is no longer exactly trivial. But of course, with billions of dollars in donations from now-deceased billionaires and cryptocurrency premines forming part of the WCM's quadratic funding pool, and elements of municipal governance using its quadratic voting protocols, participating is very much worth it.

After reaching the end of the stairs, Alice opens the door and enters the room. Inside the room, she sees a table. On the near side of the table, she sees a single, empty chair. On the far side of the table, she sees four people already sitting down on chairs of their own, the high-reputation Guardians randomly selected by the WCM for Alice's registration ceremony. "Hello, Alice," the person sitting on the leftmost chair, whose name she intuits is Bob, says in a calm voice. "Glad that you can make it," the person sitting beside Bob, whose name she intuits is Charlie, adds.

Alice walks over to the chair that is clearly meant for her and sits down. "Let us begin," the person sitting beside Charlie, whose name by logical progression is David, proclaims. "Alice, do you have your key shares?"

Alice takes out four pocket-sized notebooks, clearly bought from a dollar store, and places them on the table. The person sitting at the right, logically named Evan, takes out his phone, and immediately the others take out theirs. They open up their ethereum wallets. "So," Evan begins, "the current Ethereum beacon chain slot number is 28,205,913, and the block hash starts `0xbe48`. Do all agree?". "Yes," Alice, Bob, Charlie and David exclaim in unison. Evan continues: "so let us wait for the next block."

The five intently stare at their phones. First for ten seconds, then twenty, then thirty. "Three skipped proposers," Bob mutters, "how unusual". But then after another ten seconds, a new block appears. "Slot number 28,205,917, block hash starts `0x62f9`, so first digit 6. All agreed?"

"Yes."

"Six mod four is two, and as is prescribed in the Old Ways, we start counting indices from zero, so this means Alice will keep the third book, counting as usual from our left."

Bob takes the first, second and fourth notebooks that Alice provided, leaving the third untouched. Alice takes the remaining notebook and puts it back in her backpack. Bob opens each notebook to a page in the middle with the corner folded, and sees a sequence of letters and numbers written with a pencil in the middle of each page - a standard way of writing the key shares for over a decade, since camera and image processing technology got powerful enough to recognize words and numbers written on single slips of paper even inside an envelope. Bob, Charlie, David and Evan crowd around

the books together, and each open up an app on their phone and press a few buttons.

Bob starts reading, as all four start typing into their phones at the same time:

"Alice's first key share is, `6-b-d-7-h-k-k-l-o-e-q-q-p-3-y-s-6-x-e-f`. Applying the 100,000x iterated SHA256 hash we get `e-a-6-6...`, confirm?"

"Confirmed," the others replied. "Checking against Alice's precommitted elliptic curve point A0... match."

"Alice's second key share is, `f-r-n-m-j-t-x-r-s-3-b-u-n-n-n-i-z-3-d-g`. Iterated hash `8-0-3-c...`, confirm?"

"Confirmed. Checking against Alice's precommitted elliptic curve point A1... match."

"Alice's fourth key share is, `i-o-f-s-a-q-f-n-w-f-6-c-e-a-m-s-6-z-z-n`. Iterated hash `6-a-5-6...`, confirm?"

"Confirmed. Checking against Alice's precommitted elliptic curve point A3... match."

"Adding the four precommitted curve points, x coordinate begins `3-1-8-3`. Alice, confirm that that is the key you wish to register?"

"Confirm."

Bob, Charlie, David and Evan glance down at their smartphone apps one more time, and each tap a few buttons. Alice catches a glance at Charlie's phone; she sees four yellow checkmarks, and an "approval transaction pending" dialog. After a few seconds, the four yellow checkmarks are replaced with a single green checkmark, with a transaction hash ID, too small for Alice to make out the digits from a few meters away, below. Alice's phone soon buzzes, with a notification dialog saying "Registration confirmed".

"Congratulations, Alice," Bob says. "Unconditional possession of your key has been verified. You are now free to send a transaction to the World Collective Market's MPC oracle to update your key."

"Only a 75% probability this would have actually caught me if I didn't actually have all four parts of the key," Alice thought to herself. But it seemed to be enough for an in-person protocol in practice; and if it ever wasn't then they could easily switch to slightly more complex protocols that used low-degree polynomials to achieve exponentially high levels of soundness. Alice taps a few buttons on her smartphone, and a "transaction pending" dialog shows up on the screen. Five seconds later, the dialog disappears and is replaced by a green checkmark. She jumps up with joy and, before Bob, Charlie, David and Evan can say goodbye, runs out of the room, frantically tapping buttons to vote on all the projects and issues in the WCM that she had wanted to support for months.