and validating because when legal structures break down in society, these assets don't require those institutions to retain their value. Banks were born to secure and validate gold, and prior to Nixon's closing of the gold window in 1971, cash was considered to be a bearer asset because it represented a claim on gold owned by the central bank without the need to prove ownership outside of possession. Cash was a technological breakthrough as a bearer asset because, while it still required professional protection at a high enough value, authenticity was typically not difficult or expensive to validate. When cash could no longer be exchanged directly for gold, it lost its power as a bearer asset. It didn't lose its physical valuation properties per se, but it put a significant friction between the paper and the gold it represented, and people didn't want to be holding a significant amount of it out of fear of their government placing further frictions on it.

That leaves us with bitcoin, a very special bearer asset. It has all the benefits of frictionless proof of ownership and validation that reserve notes had over gold, and much much more. There is no risk of devaluation or frictions imposed by the central issuer because there is no central issuer. Bitcoin is created and issued by the protocol set in motion by Satoshi Nakamoto on January 3, 2009. The protocol, at the time of writing in September 2025, has issued approximately 913,000 "blocks", which represent bitcoin issued as reward (currently 3.125 bitcoin, but it was 50 bitcoin for its first 210,000 blocks) as well as transaction fees (a variable cost for a bitcoin user to get their transaction included and con-

firmed in the next block). It runs on a decentralized network of "nodes" which are validating computers all over the world that run the open source Bitcoin software and contain a record of every block ever issued and every transaction ever made on the network. No node or even group of nodes has the power to change the rules of the protocol, nor can they be exempted. Every node does its own validation, but it is part of the larger network. A node that wants to run different rules is free to do so, but they are unlikely to be able to spend their version of bitcoin as the other nodes will not recognize that node's coins as valid. Assuming everyone is following the rules of bitcoin, all that is required to prove ownership of their coins is to indicate to the network that you control the private keys, and this is a trivial exercise that can be performed via a digital signature.

The cryptographic model behind bitcoin is based on the fact that private keys do not exist physically and are virtually impossible to guess, yet are incredibly easy to validate. The non-physical nature of bitcoin is what makes it the most powerful bearer asset to have ever existed. Your bitcoin cannot be stolen through violence, and if you memorize a 12- or 24-word private key, you can store an unlimited amount of wealth in your mind. This might not seem like much to institutionalized Westerners who have trusted banks their entire lives without significant consequences, but anyone who lives outside of that bubble understands this power. Anyone who has ever experienced or thought of being a refugee, or has had their bank deny access to their funds during a bank run,