Why Cryptofinance Needs Natural Randomness

As Bitcoin and other cryptocurrencies ramp up towards mass-market deployments, blockchain technology faces an under-appreciated technical challenge. In order to securely hold and transfer blockchain documents, all participants will need to create truly unguessable encryption keys. For this purpose, we've all come to rely on the random-number source that's built into the Linux operating system. Unfortunately, the Linux generator's hardware randomness source, the spinning hard drive, is becoming obsolete. I know this all too well, because I published the first disk-based key generator, more than twenty years ago.

A further difficulty is cloud computing, because by design, virtual machines have no physically-variable hardware from which noisy measurements can be extracted. Increasingly, the blockchain industry will very often run either on virtual machines, or on computers that have only solid-state disks. Hence, the financial industry's blockchain deployments will not be able to generate secure encryption keys as readily as the e-commerce industry commonly did five or ten years ago.

At the same time, the financial industry's embrace of blockchain will greatly expand the need for highly secure random keys. Even though stealing Bitcoins, for example, often offers only limited direct profit, electronic attackers will want to steal cryptocurrency for other reasons:

- Since detected theft is destructive, the thief will naturally tend towards ransom or blackmail;
- High-value institutional positions in cryptocurrency will be targets of attack, just so as to undermine an institution's market standing;
- If the theft isn't detected immediately, the thief may be able to spend or convert coins, so as to gain some direct profit;
- Even if the theft is detected, it's still possible to launder stolen coins, via dilution <link1>.

With financial institutions entering the blockchain industry, attackers will be highly motivated to steal and decrypt the institutions' cryptocurrency wallets. Indeed, enough wealth will be in play to attract the concerted efforts of even some state actors.

So, encrypting such high-value blockchains will require extreme care, not only in choosing and operating an encryption mechanism, but especially in creating and managing truly-unpredictable encryption keys. Unfortunately, today's usual key-generation advice will become inadequate for high-value applications. Today, blockchain tutorials commonly tell readers how to seed a secure pseudorandom number generator (PRNG), but it would be irresponsible to use pseudorandom keys to protect billion-dollar holdings.

Even before these blockchain developments, Natural Randomness was the gold standard for high-value key generation. In contrast to a PRNG, whose outputs are very hard to predict or deduce, a natural randomness source offers outputs that are inherently unpredictable, because the source relies on a physical process whose unpredictability is mathematically well-established, typically quantum physics or nonlinear dynamics. So, for creating highly-sensitive PKI key pairs, the best practice has long been to use a truly-random number generator.

As an example of the dangers of entrusting theft worthy data to a pseudorandom one-time pad, consider the famous TJX compromise in 2007: The company transferred sensitive customer data with the Wired Equivalent Privacy protocol (WEP), which used the RC4 stream cipher to encrypt TJX's wireless traffic. RC4, like other stream ciphers, is essentially a seeded pseudorandom-number generator. Both ends of the channel share the RC4 key in advance, and then each side uses RC4's pseudorandom output as a one-time pad. In this case, attackers exploited a cryptographic defect in the WEP protocol's use of the RC4 cipher. By eavesdropping TJX's encrypted packets with a WiFi antenna made from a Pringles potato-chip can <link2>, the attackers were able to reconstruct TJX's shared RC4 keystream, so as to steal sensitive customer data.

Large-scale blockchain finance will introduce a big challenge for the computer security industry, by more commonly creating encrypted targets of very high value - much more commonly than we have done before. For all these reasons, large financial deployments will need to naturally-random numbers, to use as encryption keys.

link1: https://www.cryptocoinsnews.com/launder-stolen-bitcoins/
link2: http://www.pressherald.com/2013/04/06/cybercrime-hitting-home-has-maine-targets-reeling_2013-04-07/