Uranium-X [URX]
WHITE PAPER v.1.0 January-2019

Collabowritten by the Uranium-X community[1]

Uranium-X (URX), a CPU-mineable, application-specific integrated circuit (ASIC) resistant, "super rare" coin that you can mine with your computer. There will be a total of 235,000 URX mineable over a period of 69 years. The coin launched on April 20, 2018 with a community of anonymous and pseudonymous supporters from backgrounds in science, arts, law, biology and other disciplines, collaborating to bring lasting "collector" value and unique features to the project. This community-drafted white paper describes the principles upon which the project is based, and the visions for the future.

1. Founder vision & community introduction

Uranium-X (URX), a CPU-mineable, "super rare" coin that you can mine with your computer. URX was launched on 4.20.2018 and as of January-2019 is currently traded on one exchange.[2] The founder was inspired by Unobtanium (UNO), what he considered to be the *"original* rare cryptocurrency."[3] The founder made several improvements on the UNO model and launched a coin that will be a fair, accessible—but rare—cryptocurrency. "Rare" because there are only 235,000 URX, unique because it's a decentralized project that the community is building together, and fair because there was no pre-mine or founder bonus.

The anonymous founder, (handle @uranium-x) invested his own money and resources to build a project that would become a community endeavor. As a result, this white paper advances that vision as it is written by community members that believe in the founder's vision. Today the URX community currently is a mix of technologists, artists, musicians, scientists, lawyers, gamers, blockchain enthusiasts, and first timers. Nowadays the founder is rarely involved, but checks in on the project from time to time. Hence URX has evolved into a decentralized open-source community based project open to all nations, just as the founder had designed.

2. Coin specifications

Our coin specification is based on the code from Bitcoin core, but with various settings aimed at meeting the unique goals of our project, while providing for future growth. Our specifications in a nutshell:

Current Algo:	Argon2ad
Ticker:	URX
Block Time:	~5 Minutes
Retarget:	Every block over a 50-60 minute average, Dark Gravity Wave
Max Supply:	235,000 URX
Emission Length:	69 Years
Current Block Reward:	.25 URX

[1] Community members that support this paper include (in random order): @wildraven, @Freaky_Angelus, @vcscooc, @uraniumx, @RicKillerZ, @SafeCoin, @papacabeza, @SteveO, @rplant, @.Mark, @Archimedes, @icemining.ca, @crypto.farm

[2] Since December, 2018 https://safe.trade is listing the URX/BTC pair

[3] *See* Bitcointalk Ann, [UNO], March, 23, 2014 available at https://bitcointalk.org/index.php?topic=527500.0. (UNO initially caught my attention and then quickly disappointed me because of its promise of 250,00 coins mined over 300 years. Later, this changed to 250,000 coins mined over 30 years. Of these, 190,000 coins (76%) were released in the first four years.)

Premine: 0%
Launch date: 4.20.18
Mining Hardware: ASIC resistant

Features: Cryptocurrency functions like Bitcoin, i.e. encrypted messaging, discreet funding transfers.
Twist: Familiar technology but with low coin supply, emphasis on "collectibility."
Future: Next is Quantum Resistance, then NUCLEAR resistance (power input independence)

2.1 Fun facts

The UraniumX founder and community has some fun numbers and stats with the coin:

2.1.1 235,000 Max Supply

A tribute to the atomic element Uranium-235, which naturally occurs in ~0.711% of Uranium Ore found in the ground.[4] U-235 easily fissiles with a neutron collision and is a key element needed to sustain (and start) a nuclear power reaction. You hear the term "enriched uranium" which requires centrifugal processing to increase the Uranium Ore U-235 weight percent to a range up to 10%. All American PWR reactors run on Enriched Uranium. Canada's CANDU nuclear stations as an example, are designed to run on Natural Uranium (0.711%) only. Weapons grade Uranium could be in the order of 10-90% U-235 enriched, whose whereabouts and facilities are government kept secrets for a good reason. URX interestingly enough, was designed and conceptualized *without* an initial nuclear application in mind.

2.1.2 Launch on 4.20

Time Magazine researched the origins of 4.20 and found some of the initial rabble-rousers that coined 4.20 at a high school in Marin County, California. "We got tired of the Friday-night football scene with all of the jocks. We were the guys sitting under the stands smoking a doobie, wondering what we were doing there."[5] We feel the same about crypto. For the URX Community, 4.20 is a date that represents a non-mainstream culture asserting itself---but also having fun.

2.1 Technical background on Bitcoin specifications

The Bitcoin code and project has been given to the world in open-source, and we're implementing a version of that. For more information about the original Bitcoin paper and the code that URX is based on, we recommend visiting www.bitcoin.org.

2.2 Choice of current mining algorithm

Argon2ad was originally a CPU-only hashing algorithm that maximizes resistance to ASIC cracking attacks by accessing the memory array in a password dependent order. The Argon2ad algorithm has evolved considerably since first publication in 2015.[6] As of January 2019, a GPU miner has been released, and hence the algo is no longer CPU-exclusive. The URX community is actively working on implementing a new algorithm

[4] *See* Natural Uranium on Wikipedia, *available at* https://en.wikipedia.org/wiki/Natural_uranium

[5] *See* Olivia B. Waxman, "Here's the Real Reason We Associate 420 With Weed," *Time* Apr 13, 2018, *available at* http://time.com/4292844/420-april-20-marijuana-pot-holiday-history/

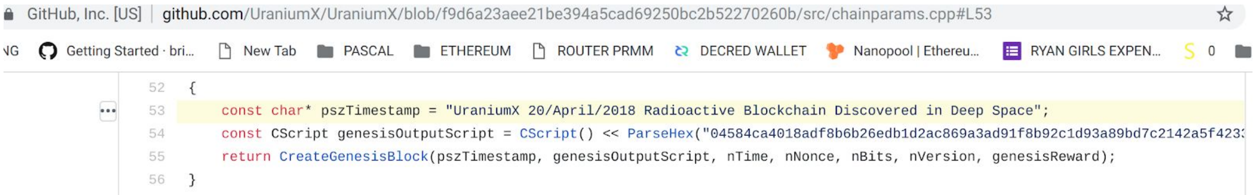
[6] *See* Alex Biyukov et. al., "Argon2: the Memory-hard function for password hashing and other applications," White Paper, V. 1.2.1 of Argon2 PHC release, Dec. 26, 2015, available at https://password-hashing.net/argon2-specs.pdf

that is GPU-resistant. However for now, both CPU and GPU may be used to mine URX. Whereas the original design intent (and URX active mandate) will always remain for mining to be as difficult and fair as possible, and only on CPU and finer architectures. This will help keep solo URX mining possible, as this is the coins original design that must be preserved over the next several decades.

Will the Argon2ad algo carry URX from now and into the future? Clearly not. In reality, we've developed our coin to have a 70 (actually now 69, see below) year emission; it would be just as silly for us to predict the mining algorithm we'll use in the future, as it would have been impossible for a company to declare a lifetime commitment to MS DOS in 1980; or to Microsoft Windows in the 1990s (or to Microsoft Windows ever); or Apple as the standard for personal computer; or to Google as the future of all browsers. Our mining algo is subject to technological change, by analogy, just as any operating system is.

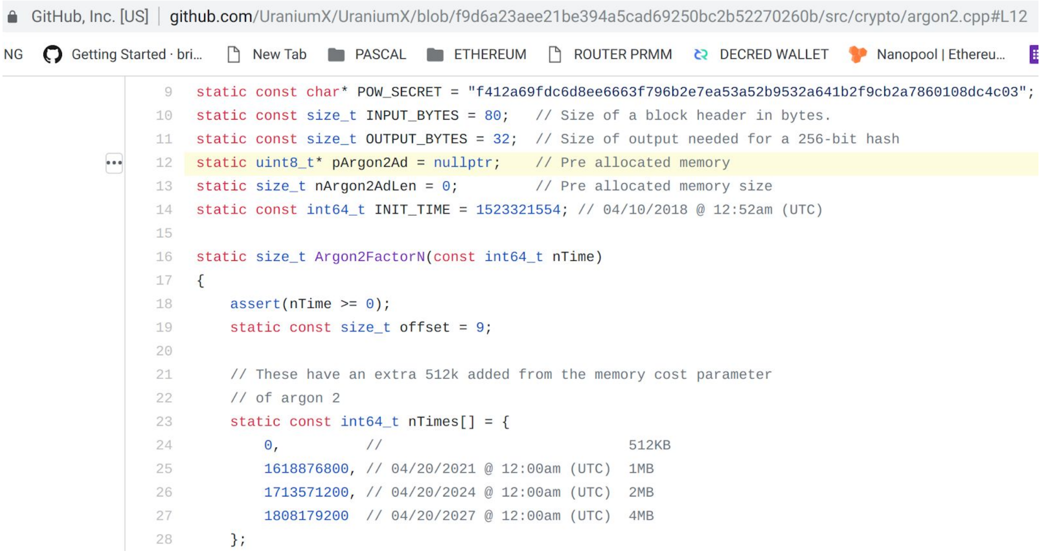
2.2.1. Watermarks

There is a watermark describing the Uranium-X Genesis block.[7]



```
{
    const char* pszTimestamp = "UraniumX 20/April/2018 Radioactive Blockchain Discovered in Deep Space";
    const CScript genesisOutputScript = CScript() << ParseHex("04584ca4018adf8b6b26edb1d2ac869a3ad91f8b92c1d93a89bd7c2142a5f423
    return CreateGenesisBlock(pszTimestamp, genesisOutputScript, nTime, nNonce, nBits, nVersion, genesisReward);
}
```

Additionally, the argon2ad memory schedule together with the dates and times anticipated for argon2ad changes algo to RAM usage.[8]



```
static const char* POW_SECRET = "f412a69fdc6d8ee6663f796b2e7ea53a52b9532a641b2f9cb2a7860108dc4c03";
static const size_t INPUT_BYTES = 80;   // Size of a block header in bytes.
static const size_t OUTPUT_BYTES = 32;  // Size of output needed for a 256-bit hash
static uint8_t* pArgon2Ad = nullptr;    // Pre allocated memory
static size_t nArgon2AdLen = 0;         // Pre allocated memory size
static const int64_t INIT_TIME = 1523321554; // 04/10/2018 @ 12:52am (UTC)

static size_t Argon2FactorN(const int64_t nTime)
{
    assert(nTime >= 0);
    static const size_t offset = 9;

    // These have an extra 512k added from the memory cost parameter
    // of argon 2
    static const int64_t nTimes[] = {
        0,          //                          512KB
        1618876800, // 04/20/2021 @ 12:00am (UTC)  1MB
        1713571200, // 04/20/2024 @ 12:00am (UTC)  2MB
        1808179200  // 04/20/2027 @ 12:00am (UTC)  4MB
    };
```

[7] *See* Github, UraniumX Repository, *available at:* https://tinyurl.com/y9lq5c9f
[8] *See* Github, UraniumX Repository, *available at:* https://tinyurl.com/y7prfrvt

2.3 Coin security & CVE bug

URX is a fork of BTC and susceptible to the same vulnerabilities. In late November-2018 URX was affected by the Bitcoin CVE bug that allows a user to make coins out of thin air and send them to other wallets including exchange wallets.[9] The hacker sold 2,118.25 URX coins and generated a loss with the exchange.

2.3.1 Effect on premine and chain

In the blockchain, coins bear responsibility for their own security, and when a breach of security causes a loss for an exchange, the coin (or the community) must cover that loss. The founder in consultation with community reduced the chain by 29.5 days, but produced coins to partially cover the loss. The founder and community donated money and time for the remainder. Hence the math was restructured and we are left with a 69-year emission rate.

2.3.2 Post mortem

The response to the attack by the community was quick and effective, showing that the care for the coin is real and the availability of expertise is large. The event brought two things to light that will make the project stronger: (i) we should have caught the monitoring notices for the CVE bug, and should have a plan to watch them more closely; and (ii) we have become more aware of additional attack vectors that may affect our coin in the long run, and are now looking at Quantum Resistance, before it's a problem.

2.3 [X] Labs

What's in the future for URX? [X] Labs is our informal label for these projects, some in testing, some underway, some very theoretical and far out.

2.3.1 Wallets (phase: implementing)

- ➔ *Paper Wallets:* In 1Q18 we've developed and launched a paper wallet together with some really interesting graphic designs.
- ➔ *Wall Certificates:* Users want to keep URX around for a long time, so we're making framable certificates with URX details. They're going to be really cool.
- ➔ *Mobile wallets:* We're making progress on collection for an Android wallet and will expand the effort to iPhone and web wallets ideally by 2019 year end and into 2020

2.3.2 Quantum Resistance (phase: studying)

We want URX to be useful forever, at least as long as the 69-year emission, and beyond. The CVE bug showed us that vulnerabilities in security exist today. Quantum computing is just around the corner, with some effects on mining, possibly, but would have a *devastating* effect on the cracking of the keys.[10] The debate isn't about if, but when. Quantum computing is even becoming more accessible by launches (soon) on platforms

[9] See Jimmy Song, "Bitcoin Core Bug CVE-2018–17144: An Analysis," *Medium*, Sep 27, 2018, available at https://hackernoon.com/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362

[10] *See* Jesse van Remmerden, "On quantum computing and blockchain security, "*Medium*, Dec 12 2018 available at https://medium.com/kryha/on-quantum-computing-and-blockchain-security-c4e484d2a728

like Amazon.[11] We don't mean to overstate the threat but community members have made clear (and some have very close perspectives to industry) that this is a real issue that needs to be addressed. We're on it, but we don't know what it'll look like. Our model enables us to select best-in-class open source solutions, for example:

- *Bitcoin Cash's* FSFA transaction mempool policy has similar ancestry as URX code and may be a solution. (see here).
- *QRL:* We're looking at the open-source code from the Quantum Resistant Ledger (QRL) project (see here)
- *NIST:* Finally, another option (e.g., followed by Snowblossom) is to implement a quantum-resistant key structure after the NIST process is complete (see here), although this could be several years away.

2.3.3 Decentralization

Another area we are closely watching is fairness for CPU miners. We're willing to fork and change as needed to respect this principle. We want decentralisation so that anybody who has a computer can start to mine without investing a lot of money.

2.3.3 Power side independance (phase: conceptual)

Powering the world is a global challenge. There are risks carried in evolution such as a nuclear attacks, loss of the electrical grid due to natural disasters, or other tragedies resulting in loss of societal power. Is this a real possibility? We think so; it would be a bummer, to say the least, to be in an apocalyptic situation and have all your money tied up in an electronic store that's offline. We want URX to work even if the power goes off and the grid goes down. Is this even possible? What does that look like, technically, how to keep our wallet communications alive? We have no idea. It's very far stage, come join a discussion with us.

2.3.4 Energy footprint (phase: conceptual)

Its vital to look at the electron energy e- pathways into the CPU architecture itself. By having high level requirements into the fairness and ever evolving URX structure to allow for self sustained mining, careful emphasis must be taken on the energy input side itself, as this plays a critical role in assigning the difficulty as well as the distributed output and carbon footprint. Modeling this electron ecosystem in a global capacity will be a mathematical system that needs to be developed in future [X] Lab funding efforts.

2.3.5 Nuclear resistance (phase: theoretical)

Nuclear is a broad term. For example, let's think about its radiation power, which can resemble familiar systems such as solar rays coming from the sun, or when you get X-rays at the dentist. These two examples are very different however. One is man-made technology (at the dentist) and the other is from the evolution of the universe (from the sun). How do we design our man made technology such as URX to become resistant to the energy influence (and temptation) of an evolutionary energy source? Efforts to design a "sun in a bottle" have been occurring since the 1960's. As an example, active research projects are developing the world's first energy 'sustaining' fusion chains, are already occurring at the International Thermonuclear Experimental Reactor

[11] George Nott, Amazon Web Services hints at quantum computing future, Computerworld, Dec 20 2018 available at https://www.computerworld.com.au/article/651052/amazon-web-services-hints-quantum-computing-future/

(ITER) project in the south of France.[12] However we don't expect building efficient commercial fusion reactors until the year 2050 or so. Does URX fall susceptible to the energy it consumes that we humans designed? Or can we steer it to fall back to the first, more natural part of the system that designed us?

3. URX domain assets: current and future areas of development

We are tracking community-lead projects in *Annex A*, as any community member can propose (and execute) a project for the coin's interest. We hope that more community members will join us for similar improvement projects and efforts in the future.

4.0 Conclusion

The last URX won't be mined until approximately year 2087. This gives us lots of time for development and adoption. Please come join us, and let's make URX last forever!

For further information:

Website:	https://uranium-x.com/
Website 2:	https://urx.zone
ANN:	https://bitcointalk.org/index.php?topic=3395511.0
Discord:	https://discord.gg/wNqwQC
Explorer:	https://explorer.uranium-x.com/
Pools:	https://icemining.ca; https://pool.rplant.xyz
Exchanges:	https://safe.trade

--The URX Community.

[12] *See* Wikipedia on ITER, International Thermonuclear Experimental Reactor *available at* https://en.wikipedia.org/wiki/ITER

Annex A

List of community-driven websites

https://uranium-x.com (owner: uranium-x)
status: ACTIVE - ONLINE

- Warning Rad levels high!
- Main landing site with tech spec
- showcases URX design and links to wallets and social communities

https://explorer.uranium-x.com (owner: uranium-x)
status: ACTIVE - ONLINE

- Block explorer
- Movement-Network-API Calls-Top100

https://icemining.ca (owner: icemining)
status: ACTIVE - ONLINE

- URX mining pool and active community member (note: self-home mining will always be a possibility even if with pools)

https://pool.rplant.xyz/ (owner: rplant)
status: ACTIVE - ONLINE

- Second major mining pool and active community member

https://urx.zone (owner: crypto.farm)
status: ACTIVE - ONLINE

- Secondary landing page for the project, used for publicity and advertising
- Focusing on driving traffic, and to find new members, peak human interest
- Future plans for block explorer v2 with live stats

uranium-x.net (owner: wildraven)
status: OFFLINE -OPEN FOR DEVELOPMENT OFFERS CURRENTLY

- potential site for additional development or lander page

urx.fund (owner: crypto.farm)
status: OFFLINE -OPEN FOR FUNDING OFFERS CURRENTLY

- potential site for receiving and issuing project grants and approving nuclear project spends and contracts

urx.exchange (owner: crypto.farm)
status: OFFLINE -OPEN FOR FUNDING OFFERS CURRENTLY

- potential site for direct URX buy and sell for large public audience. Exchange URX for real professional services in law and engineering.

- Also a site to exchange hash reports and useful data to advance the development

urx.earth (owner: crypto.farm)
status: OFFLINE-NO FUNDING - START THIS WEBSITE PROJECT by ~2035

- a place to visualize the energy consumption discussed in Sec 2.3.4 and compare it with the world norms
- start cold fusion research and feasibility

urx.farm (owner: crypto.farm)
status: OFFLINE -OPEN FOR FUNDING OFFERS CURRENTLY