SUNELECTRUM: A SOLAR POWERED DIGITAL CURRENCY SYSTEM

Leo Edwardsson
Founder, SunElectrum

October 1, 2017

Abstract

Digital currencies have proliferated widely since the invention of Bitcoin. Most digital currencies rely on a Proof of Work mechanism, requiring peer nodes in a blockchain distributed ledger network to solve cryptographic puzzles, in order to prevent double spending of currency tokens. Proof of Work avoids the need for any trusted central authority outside the peer-to-peer network to validate transactions, but at the cost of deliberately wasting energy on complex computations.

The SunElectrum digital currency system solves the double spending problem in a similarly distributed way, but instead of consuming energy to create Proof of Work hash values, it uses Proof of Watts. SunElectrum modules, equipped with Physical Unclonable Function (PUF) devices, measure electric power output from solar panels. Every node on the SunElectrum blockchain network proves by PUF to all other SunElectrum nodes that it's a true, honest peer, generating useful solar power. This distributed web of trust cannot be subverted by imposters because no imposter can counterfeit a PUF signature. The PUF-equipped peers communicate with each other and use proof signatures based on verified distributed production, not consumption, of electricity to build the blockchain ledger.

1. Introduction

Digital currencies based on peer-to-peer blockchain systems have become a fast growing field at the intersection of information technology, industry, and commerce. Starting with the creation of Bitcoin, the number of these digital currency systems has steadily increased, with a series of technical changes designed to solve problems such as scalability and transaction processing speed.

In order to create and award new digital currency tokens, and prevent double-spending of tokens, most digital currency systems require peer computers on the blockchain network to solve difficult cryptographic problems, and broadcast their solutions in the form of mathematical hashes to the rest of the peer-to-peer network.

This system is called Proof of Work. The peer computers that perform this work are called miners.

Proof of Work is intrinsically wasteful of resources. By design, it forces miners on the blockchain network to use extreme quantities of computing power, and thus excessive quantities of electricity, to find hashes that have no utility beyond the peer-to-peer digital currency network itself.

SunElectrum solves the double-spending problem more efficiently, by attaching PUF-equipped microprocessor chips to photovoltaic solar panels, and using these devices to generate Proof of Identity Signatures (henceforth abbreviated "proof signatures"). The proof signatures are used instead of the hashes used by Proof of Work blockchains.

PUF devices are uncounterfeitable. They can't be impersonated by software programs emulating the PUF device, because such emulation is not technically feasible. Other members of the SunElectrum peer-to-peer blockchain network can be certain that messages from a PUF-chipped node on the network are trustworthy.

The other functions of the PUF devices are timing, communication with the blockchain network, tamper resistance, and power output metering. These functions enable the proof signatures generated by the PUF devices to be integrated into new blocks in the blockchain, and enable the PUF-chipped solar station to create and claim new digital currency units as a reward for helping to operate the SunElectrum network.

2. The SunElectrum PUF Device-Based Blockchain

The SunElectrum network awards newly created digital currency tokens, called sundivis, to peer nodes based on the amount of solar electric power they produce. The uncounterfeitability of the PUF device proves that it was truly photovoltaic panels that generated the measured electricity. This is Proof of Watts. SunElectrum nodes aren't rewarded for consuming power excessively to operate a blockchain network, they're rewarded for capturing solar energy and operating the blockchain network efficiently. SunElectrum nodes aren't miners, they're harvesters.

Double spending of sundivis is prevented by a distributed timestamp server, similar to the system used by Bitcoin. Sundivi transaction timestamps are written into blocks created by SunElectrum nodes. Instead of hash values generated by solving puzzles, the PUF-chipped solar power stations add proof signatures to new blocks they create on the blockchain.

Other members of the blockchain network confirm that these proof signatures are valid by recognizing the uncounterfeitable PUF devices that add them to the new blocks. Confirming the validity of the proof signatures also confirms the validity of sundivi transactions in each new block. The proof signatures take the place of the hashes used by Proof of Work-based blockchain networks, connecting the blocks in series on the chain.

The SunElectrum PUF device is attached directly to the photovoltaic solar panel at the point where it connects to transmission wiring. Attaching the SunElectrum module at this point prevents electricity from external sources being substituted for power from a photovoltaic panel, and thus fraudulently claimed as solar power output. Tampering with the SunElectrum module either destroys it, or triggers tamper detection functions in the device causing it to stop communicating in its normal way with the blockchain network.

3. Mitigation of Conflicting, Simultaneously Created New Blocks

Miners in Proof of Work-based blockchain networks race to solve a puzzle, and therefore take a highly variable amount of time to generate a mathematical hash before adding that hash to a new block. This timing variability naturally mitigates the problem of forks in the blockchain caused by two or more miners accidentally adding new blocks simultaneously. Because PUF device-based SunElectrum peers don't race to a puzzle solution this way, they can all theoretically add a new block to the blockchain at any time. There is a significant chance in the SunElectrum system that two or more nodes will add conflicting new blocks to the blockchain at the same time, creating forks in the chain. To mitigate this, SunElectrum nodes that successfully add a block to the blockchain start a wait timer to reduce the chance of such conflicts. They stop trying to add a new block to the blockchain until the timer expires.

Even with wait timers in operation, it is still possible for conflicting new blocks to appear on the blockchain simultaneously. As a first step to break the tie in such cases, a subset of nearby SunElectrum nodes act as a Judging Panel, deciding which new block to approve and therefore which branch of the blockchain is the main chain. In the unlikely event that two different SunElectrum Judging Panels issue conflicting decisions about which block comes next, the network convenes a Level 2 Judging Panel, composed of the most reliable nodes on the entire network, to arrive at a final decision.

This hierarchy of tie-breaker judging panels is analogous to the consensus mechanisms used in other blockchain systems.

4. Delegation of Proof Authority to Proxy Nodes at Sunless Times

The PUF-chipped solar station nodes can only operate the SunElectrum network directly at times when the sun is shining. To fulfill their network operation duty while they're unable to generate electricity, all SunElectrum solar stations must appoint two proxy nodes for redundancy. SunElectrum proxy nodes are general purpose computers running SunElectrum proxy node software. The proxy nodes receive a private key from the solar station, and the solar station broadcasts the corresponding public key to the rest of the SunElectrum network.

When the solar station is down because the sun isn't shining, one of its proxy nodes takes over for it until the solar station starts producing electricity again. The active proxy node creates new blocks to facilitate SunElectrum transactions, and participates in confirmation of new blocks created by other nodes. The network validates proof signatures written into blocks by the active proxy node by using the public-private key pair in a challenge-response protocol.

Proxy nodes create new blocks and help to validate blocks created by other nodes, but they cannot claim new sundivis because they don't generate power. The new blocks they create can include tokenbase transactions (new sundivi claims) from solar station nodes, but proxy nodes don't add tokenbase transactions of their own.

When the sun comes out and the solar station node comes back online, it broadcasts a message to the SunElectrum network and takes over from its proxy node again.

5. Simplified Diagram of the SunElectrum PUF Device-Based Blockchain Network

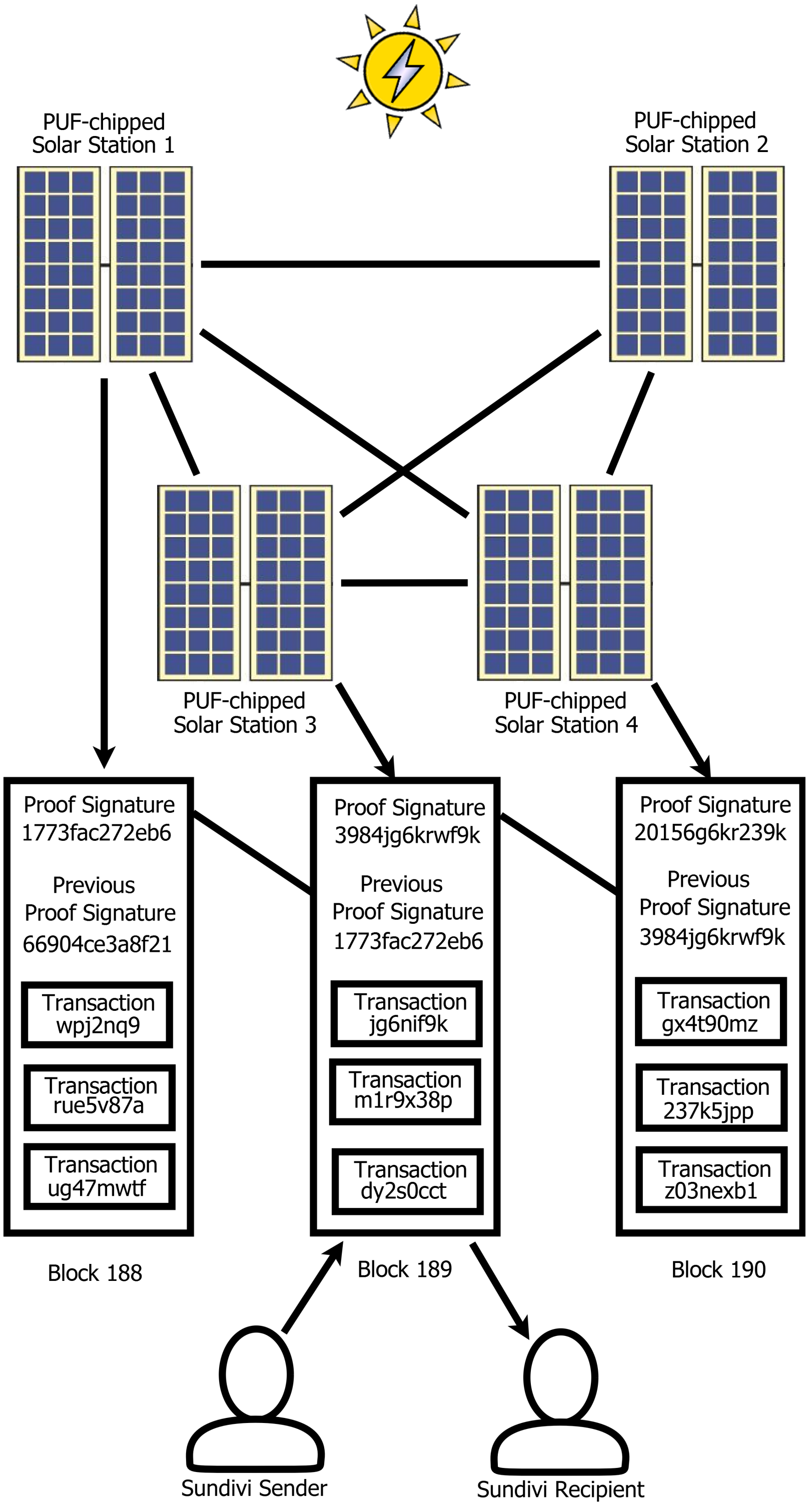
PUF-chipped Solar Station 1
PUF-chipped Solar Station 2
PUF-chipped Solar Station 3
PUF-chipped Solar Station 4
Proof Signature 1773fac272eb6
Previous Proof Signature 66904ce3a8f21
Transaction wpj2nq9
Transaction rue5v87a
Transaction ug47mwtf
Block 188
Proof Signature 3984jg6krwf9k
Previous Proof Signature 1773fac272eb6
Transaction jg6nif9k
Transaction m1r9x38p
Transaction dy2s0cct
Block 189
Proof Signature 20156g6kr239k
Previous Proof Signature 3984jg6krwf9k
Transaction gx4t90mz
Transaction 237k5jpp
Transaction z03nexb1
Block 190
Sundivi Sender
Sundivi Recipient

Figure 1.

6. SunElectrum Blockchain Operations Depicted in Figure 1

Four PUF-chipped photovoltaic solar power stations are shown communicating with each other in a peer-to-peer network. Solar Station 1 has created Block 188 on the blockchain, including proof signature 1773fac272eb6 which is verified by the other PUF-chipped solar stations in the blockchain network. The proof signature will link Block 188 to subsequent blocks, maintaining the continuity and integrity of the blockchain. Solar Station 1 also includes transactions in the block. One of the transactions is Solar Station 1's own claim to create new sundivis, based on Solar Station 1's electrical power output since its previous such claim. These new sundivi claims are called tokenbase transactions. They work just like the equivalent coinbase transactions on the Bitcoin blockchain. Solar Station 1 has also included tokenbase transactions from other PUF-chipped solar stations in Block 188.

Solar Station 3 has subsequently created Block 189 in a similar fashion. Solar Station 3 includes its own proof signature 3894jg6krwf9k, the previous proof signature 1773fac272eb6 to link Block 189 to previous blocks in the chain, its own tokenbase transaction, tokenbase transactions from other PUF-chipped solar stations, and sundivi transfer transaction dy2s0cct. Transaction dy2s0cct records a transfer of sundivis from the sundivi sender to the sundivi recipient.

Solar Station 4 has repeated the block creation process to create Block 190. This process continues indefinitely, maintaining and extending the PUF device-based blockchain.

Because this is a simplified diagram, the blocks are depicted with only three transactions records each, but in practice the blocks will contain many more transactions. The simplified diagram includes only solar station nodes, not proxy nodes. In the operational SunElectrum network, proxy nodes will often take the place of solar station nodes, the only major difference being the absence of self-generated tokenbase transactions (i.e. sundivi claims) from new blocks created by proxy nodes.