

Processor Affinity

- Two ways to modify affinity:
 - Specify the set of processors where a thread can be scheduled
 - Specify the optimal or “ideal” processor for a thread
 - On some NUMA systems, this can also set the preferred processor *node*



22-August-2008

© Copyright Ian D. Romanick 2008

Non-blocking Algorithms

- For singly-linked lists, Windows provides `SLIST_HEADER`
 - `InitializeSListHead`
 - `InterlockedPushEntrySList`
 - `InterlockedPopEntrySList`
 - `InterlockedFlushSList`
 - Only available on Windows XP / Windows Server 2003 and later



22-August-2008

© Copyright Ian D. Romanick 2008

Break



22-August-2008

© Copyright Ian D. Romanick 2008

Synchronize electrum updates that support PSBT and speed up Mnemonic decoding.

Users of Bitcoin wallet Electrum are facing a phishing attack, according to the Devi Security Lab. Hackers broadcast messages to the Electrum client through a malicious server, prompting the user to update to v4.0.0, and if the user follows the prompt to install this "backdoor-carrying client", the private key is stolen and all digital assets are stolen. At the time of writing, at least 1,450 BTCs worth about \$11.6 million had been stolen from phishing attacks that faked Electrum upgrade tips. DeViable Security Labs hereby suggests that versions of Electrum below 3.3.4 are vulnerable to such phishing attacks, and users using Electrum Wallet are requested to update to the latest version of Electrum 3.3.8 via the official website (electrum.org), which has not yet been officially released, and do not use the link in the prompt to avoid asset losses.

UBTC Electrum Light Wallet Multi-Sign Address Transfer Contract Token Tutorial.

The Bitcoin desktop wallet client Electrum has released a beta version 4.0, which adds support for several important updates such as the Lightning Network. This version is nearly a year away from the previous version of Electrum 3.3.8 (July last year)

Dynamic . . . Electrum wallet attacked nearly 250 bitcoins were stolen.

Electrum-LTC is a simple but powerful Litecoin wallet. Like its predecessor, the Electrum-Bitcoin wallet, the open source wallet is available on GitHub and anyone can view or upgrade the code.

Electrum-LTC is Electrum's community maintenance port, Litecoin's Bitcoin wallet. It is not the official product of Electrum Technologies GmbH, and it is not supported.

Electrum tweeted today about the incident, saying it was "a persistent phishing

attack on Electrum users" and imploring users to check the effectiveness of the resources they log on to.

Electrum Wallet is one of the most popular Bitcoin wallets and has been around for several years. However, Electrum wallet users often rely on electrum servers, which presents some security and privacy trade-offs. If you use an Electrum personal server, Electrum wallet users can connect locally to their own private servers, enjoying the convenience of Electrum without any trade-offs.

Wallet, Coldlar, Electrum, Huobi.

Several wallets - like Coinomi, Electrum and Wasabi - moved straight to this.

Cryptocurrencies Wallet Electrum has lost nearly 250 bitcoins (approximately \$914,000) as a result of the new phishing attack. Electrum has confirmed the authenticity of the attack. An attacker could induce a user to provide password information by creating a fake wallet.

In this demo, Electrum developer Chris Belcher shows how to set up and use electrum personal servers.

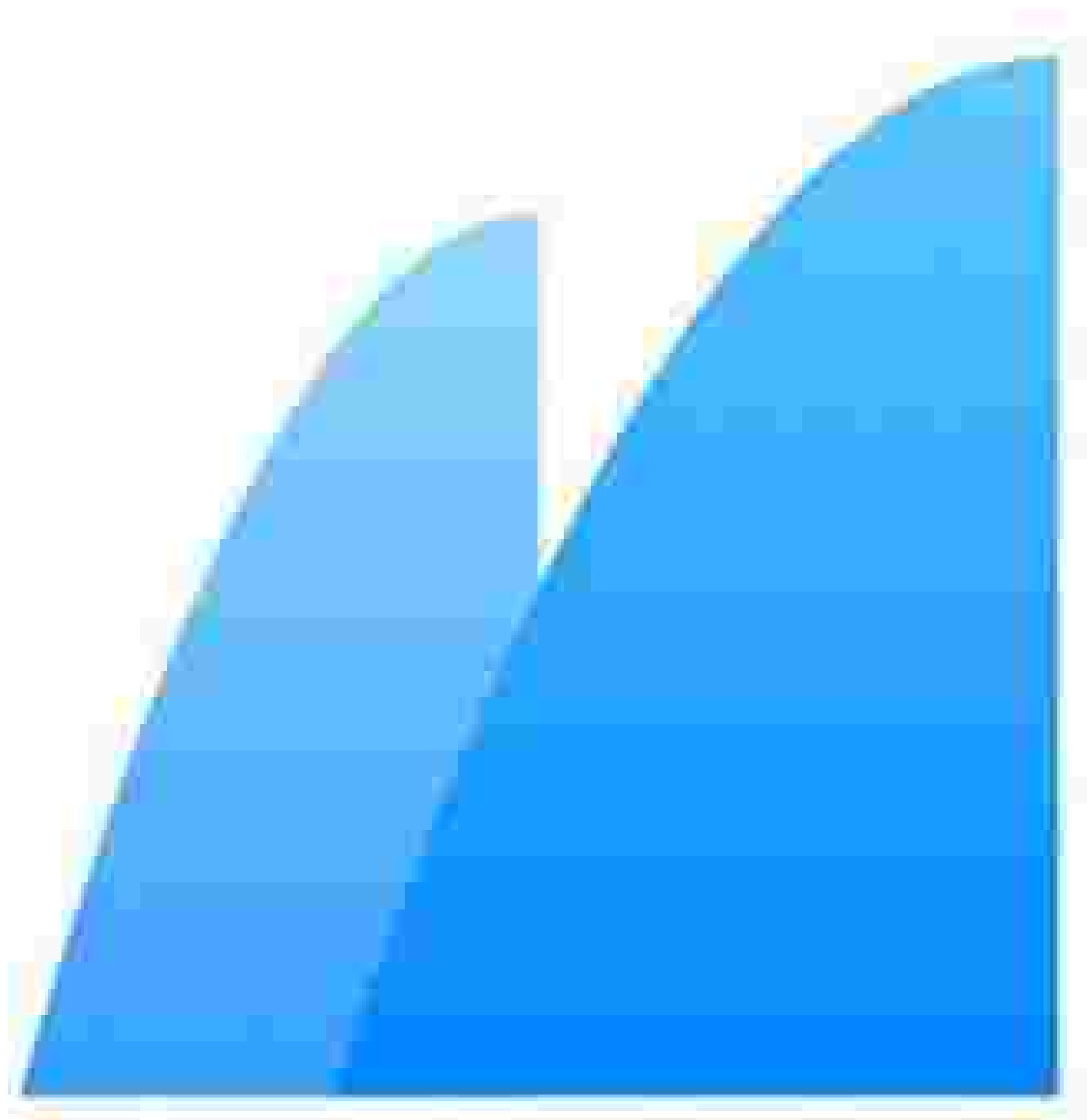
You can use Security Seeds to recover your wallet on any Electrum client, even on the Electrum Wallet online web program.

The Electrum team has also been developing other features. Electrum Wallet users can view the full release notes here.

Electrum-LTC is a simple but powerful Litecoin wallet. Like its predecessor, the Electrum-Bitcoin wallet, the open source wallet is available on GitHub and anyone can view or upgrade the code.

Dash releases Dash Electrum 3.3.8.4 version

The Electrum team has announced the attack in an official tweet, saying that "this is an ongoing phishing attack on Electrum users" and reminding them to check the authenticity of the client's source before logging in. The team published its official website, and the Electrum clients downloaded elsewhere may be problematic.



Thread-Local Storage

- We want some sort of *thread-local storage*
 - Create a handle with a global ID
 - In each thread, associate some storage with that handle
 - In the fair-lock implementation, it would be the node structure
 - Code that uses the TLS obtains the per-thread storage using the handle



22-August-2008

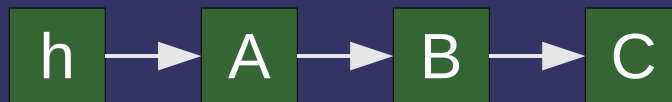
© Copyright Ian D. Romanick 2008

Non-blocking Algorithms

First thread:

fetch head \rightarrow &A

fetch A.next \rightarrow &B



Second thread:



pop A; pop B; push A;

cmpxchg (&head, &B
&A) \rightarrow success!



22-August-2008

© Copyright Ian D. Romanick 2008

Atomic Operations

➤ Example: TAS instruction on 68000

- Reads a byte from a memory location
- Writes the value back with the high bit set
- Tests the original high bit and sets the condition codes

Performed with
the bus “locked”

➤ Example: XCHG instruction on 8086

- Reads a byte from a memory location
- Writes a byte from a register to the memory location
- Stores the byte from memory in the register



22-August-2008

© Copyright Ian D. Romanick 2008

Non-blocking Algorithms

⇒ Most non-blocking algorithms look fairly similar:

```
void non_blocking_foo(volatile int *x)
{
    int old_value, new_value, ref_value;

    do {
        old_value = *x;
        new_value = do_something(old_value);
        ref_value =
            InterlockedCompareExchange(x, new_value,
                                       old_value);
    } while (ref_value != old_value);
}
```



22-August-2008

© Copyright Ian D. Romanick 2008