Subject: Re: All's well
From: Nicholas Bohm <nbohm@ernest.net>
Date: 03/02/2009, 11:55
To: satoshi@vistomail.com

Satoshi Nakamoto wrote:

> No further trouble; but whereas the UI at first showed your transfer as:
>
> 35 blocks 01/02/2009 16:25   Received with: !Me
> 1CHE5JRfc5mr8ZtVUP7nnsS5HC4bWcXoc6 +100.00
>
> it now (the morning after) shows:
>
> 98 blocks 01/02/2009 16:25   Received with: Satoshi Nakamoto
> 1CHE5JRfc5mr8ZtVUP7nnsS5HC4bWcXoc6 +100.00

> Everyone promptly presses "Change..." and labels their
> own address with my name.

I hadn't touched "Change" in case of bungling something. When I did, it showed your name against what I took to be my address - some sort of default?

By playing I see that I can have multiple addresses with different names; and if the idea is to use them to distinguish the origin of payments, I could of course name each with the name of the person I intend to give it to for payment purposes.

This seems a bit uncertain, though - presumably if I give person A my address for payments, nothing stops them giving it to Person B; and then I'll think payments from Person B are from Person A. Or have I missed something?

> I need to figure out some way to convey that it's showing the
> address you received it with, in just one or two words
>
> Maybe:
> "Receiving address: "
> "Incoming address: "
>
> Or the way e-mail programs do it:
> "To: "
> "Recipient: "
>
> Which one do you think would work best, or is it just too much
> to overcome the predisposition to expect it to say who it's from
> no matter what it's labelled?
>
> This would probably work best:
> "From: unknown, To: Your Address 1cc...."
> or
> "From: anonymous, To: Your Address 1cc...."

Please treat my comments with caution, as my grasp of Bitcoin is pretty superficial, to put it mildly; but I hope naive comments may still be useful.

My preference is "From: unknown, to: your address 1cc...."

I prefer "unknown" because I assume the system truly does not know the source; "anonymous" suggests that it was the choice of the sender to conceal their name.

I would see some merit in keeping the record of well understood operations like receipts and payments on a separate page from the record of generation and maturity, which are operations quite different from those of ordinary bank accounts. (There could be separate tabs in the one pane, for example. Receipts and payments could have separate columns for the amount, like many conventional bank statements.)

Is it useful to keep forever lines such as:

0/unconfirmed   02/02/2009 04:21   Generated (not accepted)   0.00 ?

And I was initially baffled by legends like:

97 blocks   02/02/2009 19:23   Generated (50.00 matures in 23 blocks)

because I thought that if it required 23 blocks to mature and I already had 97, it ought surely to be mature already. (I worked it out in due course; but I would have understood at once if it had said "matures in 23 more blocks".)

No doubt in due course a User Guide and FAQ will tackle a lot of things like this.

Regards,

Nicholas
--
Salkyns, Great Canfield, Takeley,
Bishop's Stortford CM22 6SX, UK

Phone 01279 870285   (+44 1279 870285)
Mobile 07715 419728   (+44 7715 419728)

PGP public key ID: 0x899DD7FF. Fingerprint:
5248 1320 B42E 84FC 1E8B A9E6 0912 AE66 899D D7FF