Subject: Re: All's well
From: Satoshi Nakamoto <satoshin@gmx.com>
Date: 03/02/2009, 16:42
To: Nicholas Bohm <nbohm@ernest.net>

> 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?

You're the second person to tell me they don't remember labelling their address with my name. Surely you must have entered "!Me" at some point and then later replaced it with my name. The software doesn't have my name coded into it anywhere and has no way to get it other than from the user.

I think I know what happened: if you copied the address, thinking it was my address, and entered it into your address book, it would have changed the label for your address. The entry would have failed to show up in the address book. I need to make it check the address when you enter a new address in the address book and if it's yours, give an error explaining it's one of yours.

The address labelling feature is inherently confusing. I've only stuck with it because it would be a necessity in advanced scenarios, but as an advanced feature it isn't really needed until much later. I'm thinking I'll hide it, at least for now. Let it be simple for as long as possible.

I'm still wavering between:
"Received with address 18cc..."
and
"From: unknown, To: 18cc..."

But if "Received with: (something) 18cc..." left 2 out of 2 people thinking the address was the sender's address, then "Received with address 18cc..." might not be different enough to overpower the natural expectation to see the sender's address there. What do you think? From/To still better?

> 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?

True for e-mail, maybe less so when paying a bill. For instance, "send 9.95 to 18cc... to activate your account" or "please make payment for this invoice to 18cc...".

> 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.

No, that's exactly what I need, it's very helpful. I don't know how someone who doesn't already know all about Bitcoin will interpret things. You only get once chance to see how something looks for the first time, and I already spent all of mine.

BTW, did you figure out that you could doubleclick on a transaction to open a details window?

> but I would have understood at once if it had said "matures in
> 23 more blocks".)

Good idea, definitely an improvement.

Satoshi