Hub.pl

WIADOMOŚCI BITCOIN

Tajemnice kodu Bitcoin | Górnicy, Timechain, Atomy, IRC i wirtualny poker

Przez Maciej Kosior Ostatnia aktualizacja Mar 16, 2019

Istnieje wstępnie wydany kod Bitcoina, w którym Satoshi zawarł kilka interesujących zapisów. Okazuje się, że przed oficjalną premierą Satoshi rozpowszechniał prywatną wersję kodu kilku wybrańcom. Co zawierają zapisy?

Przedpremierowy kod Bitcoin

Zwolennicy kryptowaluty dyskutują o wczesnej wersji oryginalnego kodu źródłowego Bitcoin, który pojawił się w tym tygodniu w sieci. Stary list na forum i lista mailingowa Satoshiego sugerują, że przed uruchomieniem Bitcoina 3 stycznia 2009 r. istniała prywatna wersja kodu, którą Mistrz rozesłał do kilku osób.

> **Francis Pouliot**
> @francispouliot_
>
> Accidentally discovered a mind-blowing artefact of Bitcoin history. I had heard rumors of its existence.
>
> I give you: the pre-release source code of Bitcoin!
> bitcointalk.org/index.php?topi…
>
> Confirmation by Satoshi many had access to code when he mined Genesis: metzdowd.com/pipermail/cryp…
>
> 796 04:55 - 14 mar 2019
>
> Ludzie o tym mówią: 306

Dyskusja rozpoczęła się 13 marca, kiedy znany rzecznik BTC Francis Pouliot podzielił się starą wersją kodu źródłowego Satoshiego i listem twórcy, w którym opisał on, że wysłał „główne pliki" do Jamesa A. Donalda: „Wysłałem Ci główne pliki (dostępne obecnie na życzenie, pełne wydanie

wkrótce)", napisał Nakamoto 17 listopada 2008 roku.

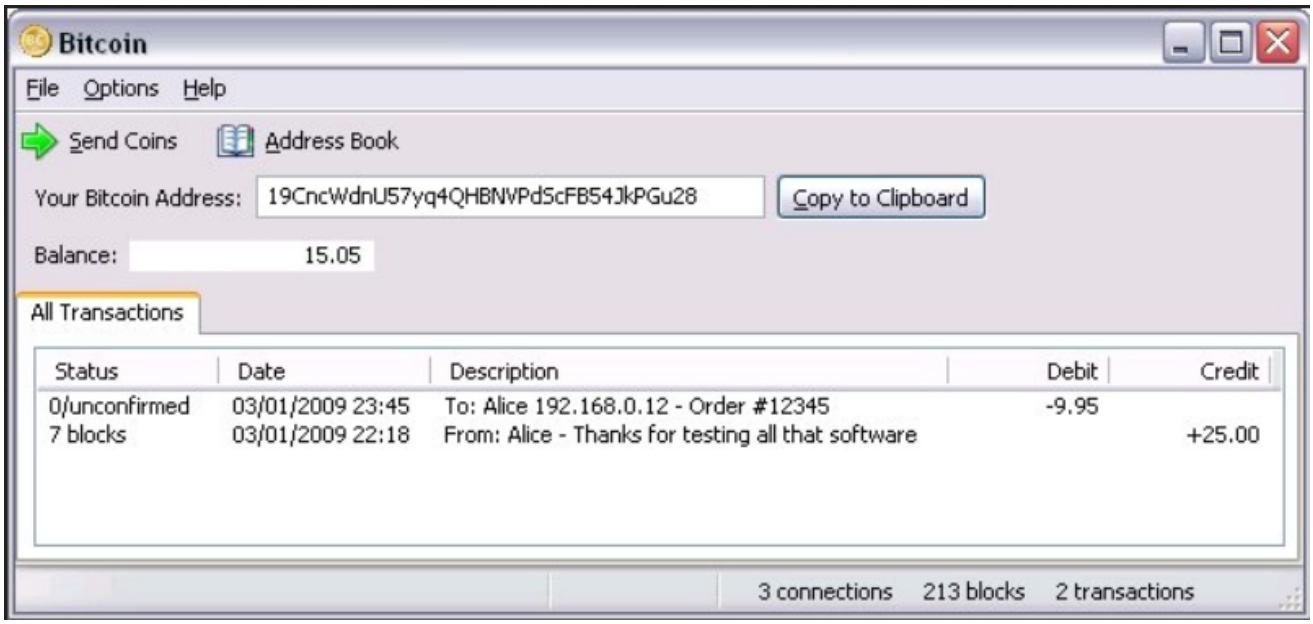
I believe I've worked through all those little details over the last year and a half while coding it, and there were a lot of them. The functional details are not covered in the paper, but the sourcecode is coming soon. I sent you the main files.
(available by request at the moment, full release soon)

Satoshi Nakamoto

Źródło: tutaj

Timechain

W kodzie źródłowym, który został wysłany do członka Bitcointalk.org „Cryddit", znajdują się interesujące znaleziska. Na przykład kod wspomina termin „bitcoin miner", który wydaje się być pierwszym przypadkiem, kiedy Nakamoto opisuje uczestników sieci jako górników. Co ciekawe, termin „górnicy" nie występował w manifeście Bitcoina. Występował za to termin „węzły". Dodatkowo, termin blockchain naprawdę nazywał się „timechain", zgodnie z zapisami kodu przesłanymi Credditowi przez Satoshiego.



Screenshot z 3 stycznia 2009 (ta sama data co blok genesis) z 213 blokiem i trzema innymi połączeniami wg użytkownika Bitcointalk.org Deepceleron 23 grudnia 2013 roku.

> „Łańcuch czasu jest strukturą drzewa, począwszy od bloku genesis. Z każdym blokiem potencjalnie może być wielu kandydatów do następnego bloku. pprev i pnext łączą ścieżkę przez główny / najdłuższy łańcuch. Indeks bloku może mieć wiele pprev wskazujących na to, ale pnext będzie wskazywał tylko najdłuższą gałąź lub będzie zerowy, jeśli blok nie jest częścią najdłuższego łańcucha.”

W tekście czytamy dalej:

> „Węzły gromadzą nowe transakcje w bloku, mieszają je w drzewo i skanują wartości niepowiązane, aby wartość skrótu bloku spełniała wymagania proof-of-work. Kiedy rozwiązują dowód pracy, rozgłaszają blok wszystkim i blok jest dodawany do timechain. Pierwsza transakcja w bloku to specjalna transakcja, która tworzy nową monetę należącą do twórcy bloku.”

Monety, centy i atomy

Innym intrygującym znaleziskiem we wczesnym kodzie jest fakt, że Satoshi nazwał mniejsze jednostki Bitcoinów „monetą” (1 000 000) i „centami” (10 000), a nie „satoshi”. Istnieje również wiersz tekstu, który mówi o „atomach” i „recenzjach użytkowników”, które odnoszą się do jakiegoś systemu oceny.

BitcoiN historians, STOP WHAT YOU ARE DOING AND GET ON THIS


Cryddit
Legendary

Activity: 910
Merit: 1037

Re: Bitcoin source from November 2008.
December 23, 2013, 07:30:00 PM

Code:

```
class CTransaction;
class CBlock;
class CBlockIndex;
class CWalletTx;
class CKeyItem;

static const unsigned int MAX_SIZE = 0x02000000;
static const int64 COIN = 1000000;
static const int64 CENT = 10000;
static const int64 TRANSACTIONFEE = 1 * CENT; /// c
///static const unsigned int MINPROOFOFWORK = 40; /
static const unsigned int MINPROOFOFWORK = 20;  ///



extern map<uint256, CBlockIndex*> mapBlockIndex;
```

[/pre]

202 05:01 - 14 mar 2019

Ludzie o tym mówią: 36

```
if (hashTimeChainBest == hash)
    RelayInventory(CInv(MSG_BLOCK, hash));

// Add atoms to user reviews for coins created
vector<unsigned char> vchPubKey;
if (ExtractPubKey(vtx[0].vout[0].scriptPubKey, false, vchPubK
{
    uint64 nRand = 0;
    RAND_bytes((unsigned char*)&nRand, sizeof(nRand));
    unsigned short nAtom = nRand % (USHRT_MAX - 100) + 100;
    vector<unsigned short> vAtoms(1, nAtom);
    AddAtomsAndPropagate(Hash(vchPubKey.begin(), vchPubKey.er
}
```

Według developera Bitcoin Mike'a Hearn'a, Satoshi zamierzał zintegrować rynek peer-to-peer (P2P) wewnątrz protokołu. Nigdy jednak nie dokończył kodu i pomysł został odłożony na półkę. **Źródło ma również odrzucony blok genezy w kodzie, który ma zupełnie inny hash.** Zakładając, że hash był pierwszym blokiem testowym genesis, został on stworzony 10 września 2008 roku.

IRC i wirtualna gra w pokera

Poza pre-wydaniem kodu przed uruchomieniem 3 stycznia 2009 roku, oryginalny kod 0.1.0 Bitcoin zawiera również kilka fascynujących szczegółów. Na przykład oryginalne oprogramowanie Bitcoin zawierało klienta IRC, który miał na celu stworzenie łatwiejszego sposobu ładowania wiadomości. Co więcej, oryginalne repozytorium kodu 0.1.0 Bitcoina, zawierało również ramy w celu stworzenia wirtualnej gry w pokera. Została ona dodana 16 kwietnia 2008 roku. Po oficjalnym uruchomieniu sieci, pomysły takie jak rynek P2P i wirtualna gra w pokera nigdy nie doszły do skutku. Klient IRC zatrzymał się na kilka wydań, ale po wersji 0.8.2 Bitcoina, obsługa ładowania IRC została całkowicie usunięta.

```
1572
1573 CPokerLobbyDialogBase::CPokerLobbyDialogBase(wxWindow* parent, wxWindowID id, const wxString& title, const wxPoint& pos, const
1574 {
1575     this->SetSizeHints(wxDefaultSize, wxDefaultSize);
1576     this->SetBackgroundColour(wxSystemSettings::GetColour(wxSYS_COLOUR_BTNFACE));
1577
1578     wxBoxSizer* bSizer156;
1579     bSizer156 = new wxBoxSizer(wxHORIZONTAL);
1580
1581     m_treeCtrl = new wxTreeCtrl(this, wxID_ANY, wxDefaultPosition, wxDefaultSize, wxTR_HAS_BUTTONS|wxTR_HIDE_ROOT|wxTR_LINES_AT
```

Tajemnice Satoshiego

Nikt nie wie, dlaczego Satoshi użył pewnych definicji terminologii Bitcoin i dlaczego postanowił zrezygnować z rynku P2P i wirtualnego pokera. Najstarszą dostępną historią dowodu działania wersji Bitcoin 0.1.0 jest czytelny dla człowieka dziennik debugowania. Satoshi pracował nad kodem Bitcoin aż do wersji 0.3.19, ale później odszedł w 2010 roku, przekazując ster Gavinowi Andresenowi.

Co sądzisz o przedpremierowym kodzie źródłowym i niektórych terminach Satoshi używanych w tekście? Zapraszam do komentowania!

Powiązane terminy:

- Termin: Peer to Peer
- Termin: Górnicy
- Termin: Transakcja
- Termin: Satoshi
- Termin: Blok
- Termin: Hash

Maciej Kosior