Financial privacy implications of cryptocurrencies

https://github.com/a1icey/BitcoinPrivacyDocumentation

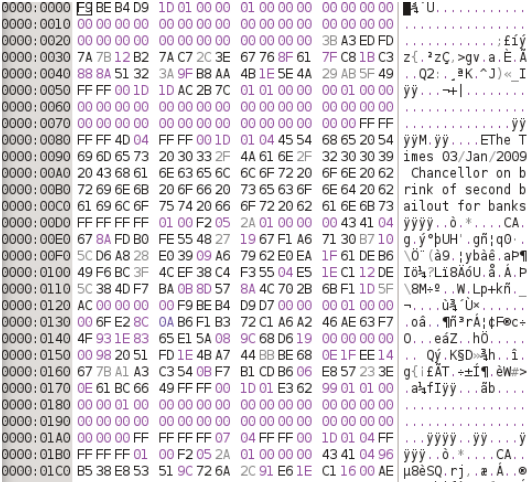
Alice Townes, Richard Downe

February 9, 2014

Bitcoin overview

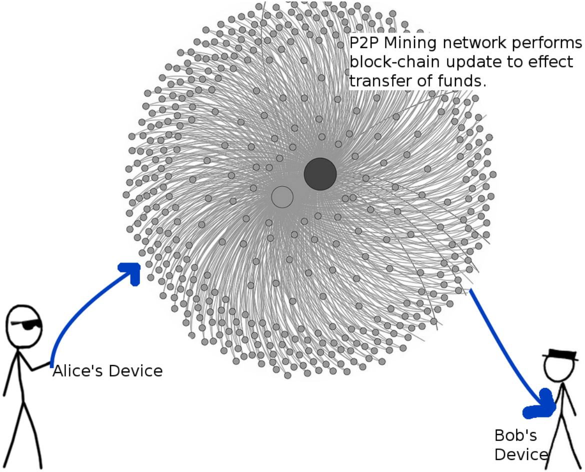
- Entire supply is encoded in a lengthy cryptographic hash.
- Money changes hands when the owner of a quantity reassigns it by appending the register and cryptographically “signing” it.
- Ownership defined in terms of “address”, a hash computed from a user’s public key.
- Loss of the key used for signing constitutes a permanent loss of value from the supply.
- All transactions are visible to the public.
- Identities of users cannot directly be inferred from blockchain, without associating external data.

View of the blockchain



```
0000:0000 F9 BE B4 D9  1D 01 00 00  01 00 00 00  00 00 00 00 █¾´U............
0000:0010 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
0000:0020 00 00 00 00  00 00 00 00  00 00 00 00  3B A3 ED FD ............;£íý
0000:0030 7A 7B 12 B2  7A C7 2C 3E  67 76 8F 61  7F C8 1B C3 z{.²zÇ,>gv.a.È.Ã
0000:0040 88 8A 51 32  3A 9F B8 AA  4B 1E 5E 4A  29 AB 5F 49 ..Q2:.¸ªK.^J)«_I
0000:0050 FF FF 00 1D  1D AC 2B 7C  01 01 00 00  00 01 00 00 ÿÿ...¬+|........
0000:0060 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
0000:0070 00 00 00 00  00 00 00 00  00 00 00 00  00 00 FF FF ..............ÿÿ
0000:0080 FF FF 4D 04  FF FF 00 1D  01 04 45 54  68 65 20 54 ÿÿM.ÿÿ....EThe T
0000:0090 69 6D 65 73  20 30 33 2F  4A 61 6E 2F  32 30 30 39 imes 03/Jan/2009
0000:00A0 20 43 68 61  6E 63 65 6C  6C 6F 72 20  6F 6E 20 62  Chancellor on b
0000:00B0 72 69 6E 6B  20 6F 66 20  73 65 63 6F  6E 64 20 62 rink of second b
0000:00C0 61 69 6C 6F  75 74 20 66  6F 72 20 62  61 6E 6B 73 ailout for banks
0000:00D0 FF FF FF FF  01 00 F2 05  2A 01 00 00  00 43 41 04 ÿÿÿÿ..ò.*....CA.
0000:00E0 67 8A FD B0  FE 55 48 27  19 67 F1 A6  71 30 B7 10 g.ý°þUH'.gñ¦q0·.
0000:00F0 5C D6 A8 28  E0 39 09 A6  79 62 E0 EA  1F 61 DE B6 \Ö¨(à9.¦ybàê.aÞ¶
0000:0100 49 F6 BC 3F  4C EF 38 C4  F3 55 04 E5  1E C1 12 DE Iö¼?Lï8ÄóU.å.Á.Þ
0000:0110 5C 38 4D F7  BA 0B 8D 57  8A 4C 70 2B  6B F1 1D 5F \8M÷º..W.Lp+kñ._
0000:0120 AC 00 00 00  00 F9 BE B4  D9 D7 00 00  00 01 00 00 ¬....ù¾´Ù×......
0000:0130 00 6F E2 8C  0A B6 F1 B3  72 C1 A6 A2  46 AE 63 F7 .oâ..¶ñ³rÁ¦¢F®c÷
0000:0140 4F 93 1E 83  65 E1 5A 08  9C 68 D6 19  00 00 00 00 O...eáZ..hÖ.....
0000:0150 00 98 20 51  FD 1E 4B A7  44 BB BE 68  0E 1F EE 14 .. Qý.K§D»¾h..î.
0000:0160 67 7B A1 A3  C3 54 0B F7  B1 CD B6 06  E8 57 23 3E g{¡£ÃT.÷±Í¶.èW#>
0000:0170 0E 61 BC 66  49 FF FF 00  1D 01 E3 62  99 01 01 00 .a¼fIÿÿ...ãb....
0000:0180 00 00 01 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
0000:0190 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
0000:01A0 00 00 00 FF  FF FF FF 07  04 FF FF 00  1D 01 04 FF ...ÿÿÿÿ..ÿÿ....ÿ
0000:01B0 FF FF FF 01  00 F2 05 2A  01 00 00 00  43 41 04 96 ÿÿÿ..ò.*....CA..
0000:01C0 B5 38 E8 53  51 9C 72 6A  2C 91 E6 1E  C1 16 00 AE µ8èSQ.rj,.æ.Á..®
```

Anatomy of a bitcoin transaction

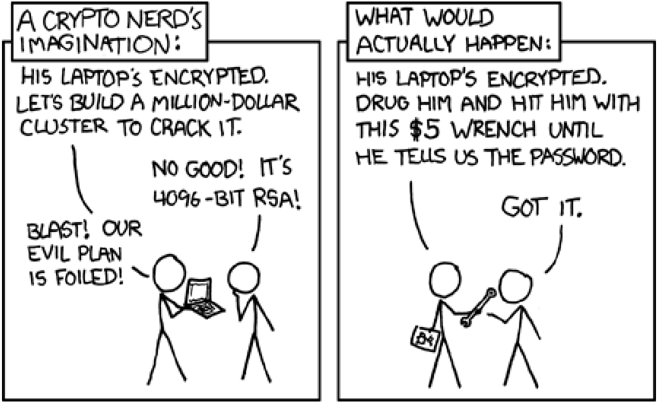


P2P Mining network performs block-chain update to effect transfer of funds.

Alice's Device

Bob's Device

Limitations of cryptography


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.