

## Notes and Further Reading

### Notes

1. A sophisticated reader may notice that in fact a Bitcoin address is the hash of the elliptic curve public key, and not the public key itself. However, it is in fact perfectly legitimate cryptographic terminology to refer to the pubkey hash as a public key itself. This is because Bitcoin's cryptography can be considered to be a custom digital signature algorithm, where the public key consists of the hash of the ECC pubkey, the signature consists of the ECC pubkey concatenated with the ECC signature, and the verification algorithm involves checking the ECC pubkey in the signature against the ECC pubkey hash provided as a public key and then verifying the ECC signature against the ECC pubkey.
2. Technically, the median of the 11 previous blocks.
3. Internally, 2 and "CHARLIE" are both numbers, with the latter being in big-endian base 256 representation. Numbers can be at least 0 and at most  $2^{256}-1$ .

### Further Reading

1. Intrinsic value: <https://tinyurl.com/BitcoinMag-IntrinsicValue>
2. Smart property: [https://en.bitcoin.it/wiki/Smart\\_Property](https://en.bitcoin.it/wiki/Smart_Property)
3. Smart contracts: <https://en.bitcoin.it/wiki/Contracts>
4. B-money: <http://www.weidai.com/bmoney.txt>
5. Reusable proofs of work: <http://www.finney.org/~hal/rpow/>
6. Secure property titles with owner authority: <http://szabo.best.vwh.net/securetitle.html>
7. Bitcoin whitepaper: <http://bitcoin.org/bitcoin.pdf>
8. Namecoin: <https://namecoin.org/>
9. Zooko's triangle: [http://en.wikipedia.org/wiki/Zooko's\\_triangle](http://en.wikipedia.org/wiki/Zooko's_triangle)
10. Colored coins whitepaper: <https://tinyurl.com/coloredcoin-whitepaper>
11. Mastercoin whitepaper: <https://github.com/mastercoin-MSC/spec>
12. Decentralized autonomous corporations, Bitcoin Magazine: <https://tinyurl.com/Bootstrapping-DACs>
13. Simplified payment verification: <https://en.bitcoin.it/wiki/Scalability#Simplifiedpaymentverification>
14. Merkle trees: [http://en.wikipedia.org/wiki/Merkle\\_tree](http://en.wikipedia.org/wiki/Merkle_tree)
15. Patricia trees: [http://en.wikipedia.org/wiki/Patricia\\_tree](http://en.wikipedia.org/wiki/Patricia_tree)
16. GHOST: [http://www.cs.huji.ac.il/~avivz/pubs/13/btc\\_scalability\\_full.pdf](http://www.cs.huji.ac.il/~avivz/pubs/13/btc_scalability_full.pdf)
17. StorJ and Autonomous Agents, Jeff Garzik: <https://tinyurl.com/storj-agents>
18. Mike Hearn on Smart Property at Turing Festival: <http://www.youtube.com/watch?v=Pu4PAMFPo5Y>

