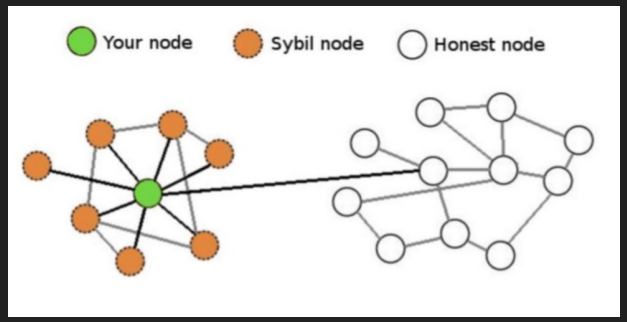
Limitations of Blockchains

- Sybil attack (the 51% attack)
- Computational and energetic matters
- Cryptocurrency management and ledger lockup/theft
- Confidentiality of transactions in many blockchains
- Transactions cannot be refused or rolled back

Sybil Attack Resistance

- The probability of a transaction being reversed decreases exponentially with the number of confirmations it has received
- An attacker controlling more than half of the network (miners) can cancel transactions (and double spend)



TECH › VIRTUAL CURRENCY

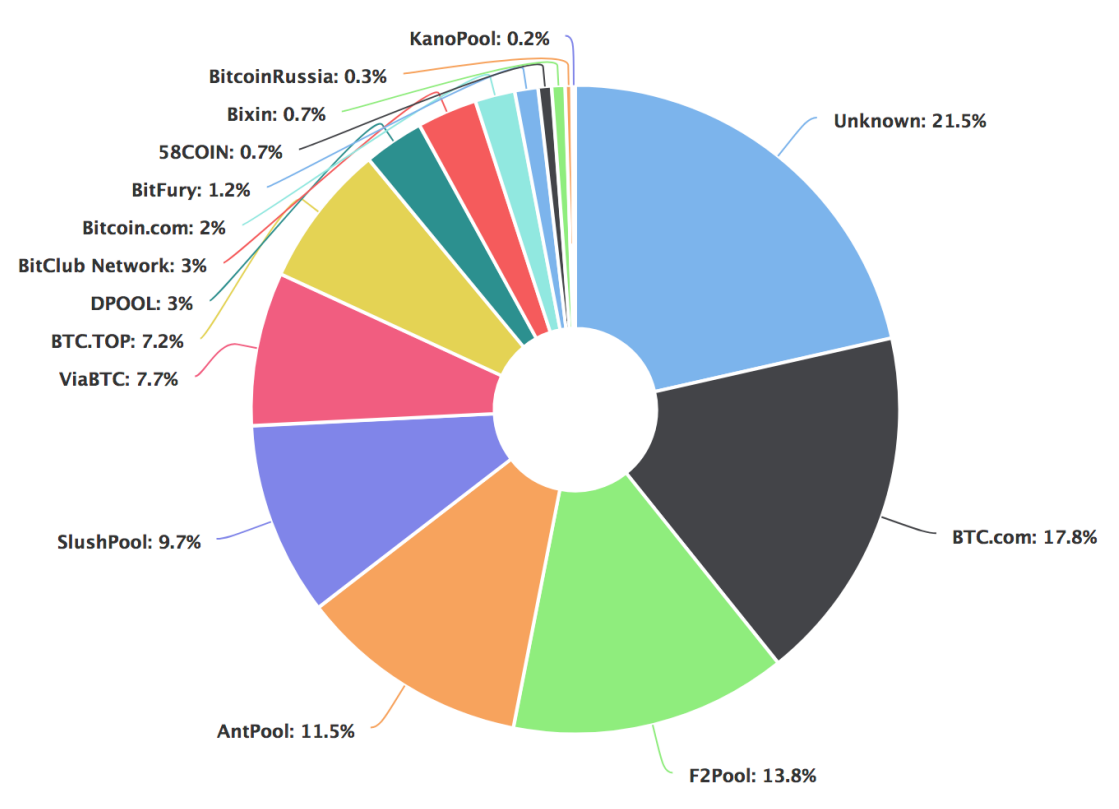
51% Attack

REVIEWED BY JAKE FRANKENFIELD | Updated Jul 5, 2018

DEFINITION of 51% Attack

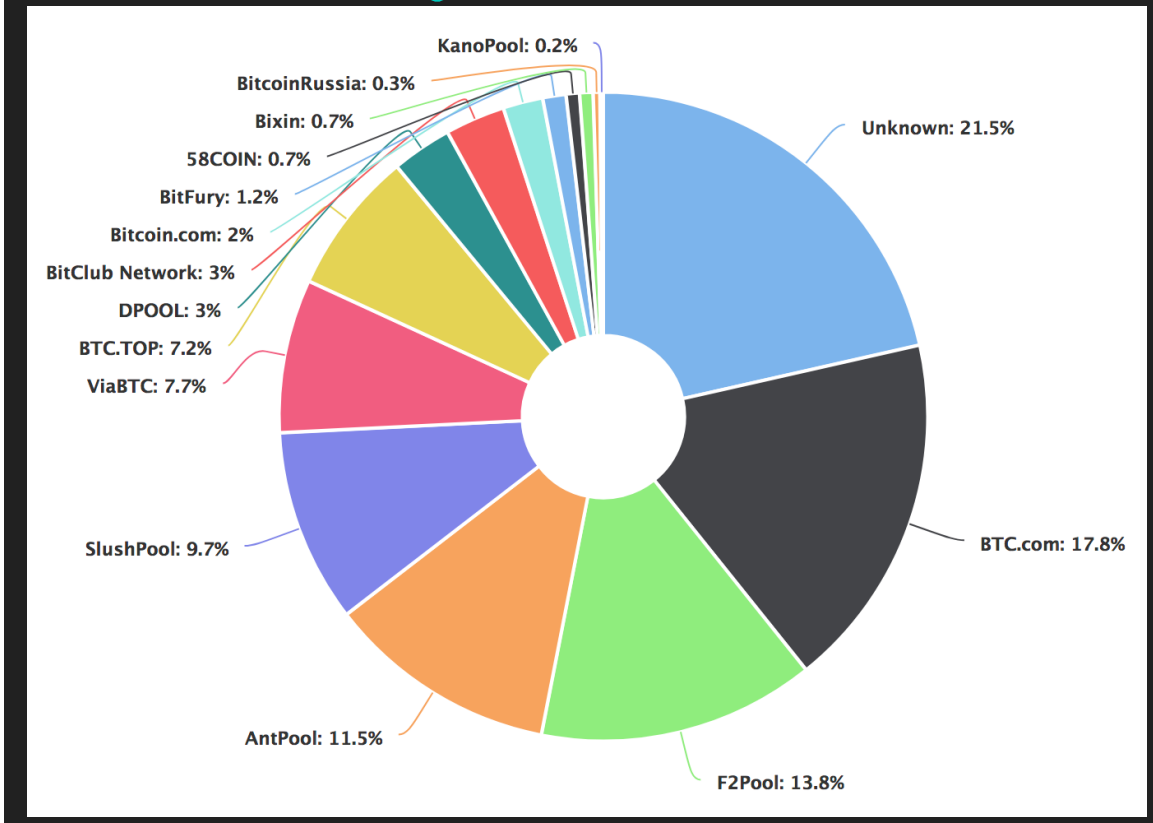
51% attack refers to an attack on a blockchain – usually bitcoin's, for which such an attack is still hypothetical – by a group of miners controlling more than 50% of the network's mining hashrate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.

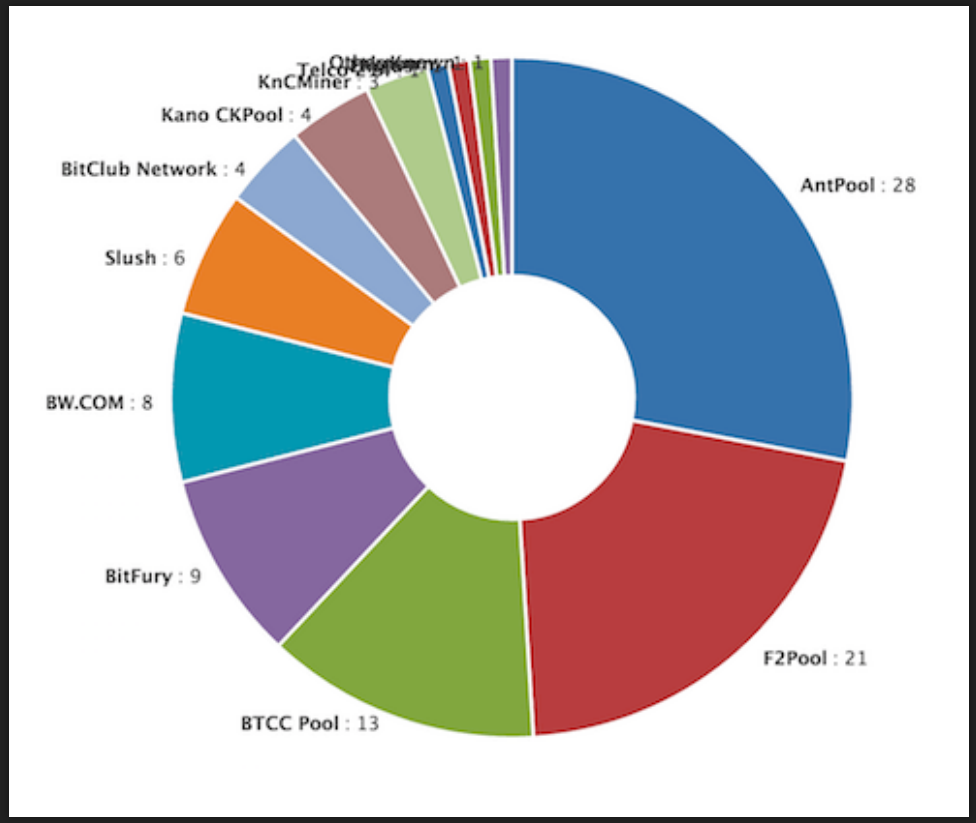
Mining Pools and hashrate distribution - 2019



- Miners associate in "teams" termed mining pools
  - Bitcoin mining pools are a way for miners to pool their resources together and share their hashing power (protocol coordinates activities of pool miners)
  - reward split equally according to the amount of shares they contributed to solving a block
  - hash rate distribution is best when split among more Bitcoin mining pools (avoid potentially harmful concentration of hashing power)
- The diagram depicts the biggest Bitcoin mining pools (source: Blockchain's hashrate distribution chart -)

Mining Pools and hashrate distribution – 2022





Bitcoin nodes worldwide - 2019

- https://bitnodes.earn.com

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Feb 06 2019 23:54:24 GMT+0100 (CET).

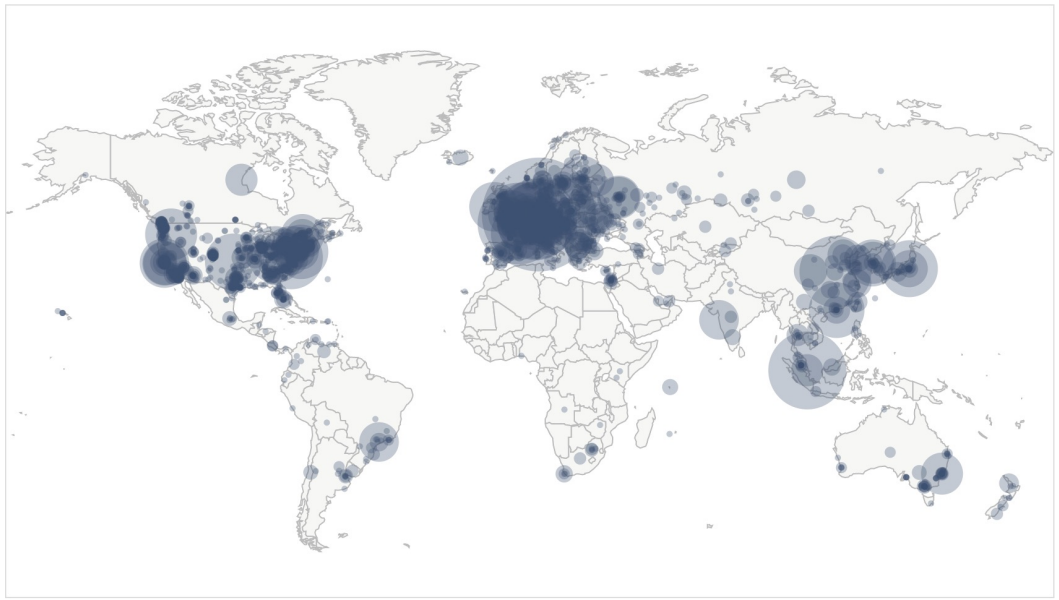
10377 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2561 (24.68%)
2	Germany	1966 (18.95%)
3	France	695 (6.70%)
4	Netherlands	516 (4.97%)
5	China	409 (3.94%)
6	Canada	386 (3.72%)
7	United Kingdom	367 (3.54%)
8	Singapore	317 (3.05%)
9	Russian Federation	272 (2.62%)
10	Japan	247 (2.38%)

More (102) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Bitcoin nodes worldwide - 2022

GLOBAL BITCOIN NODES DISTRIBUTION
Reachable nodes as of Thu Feb 17 00:55:10 2022 CET.

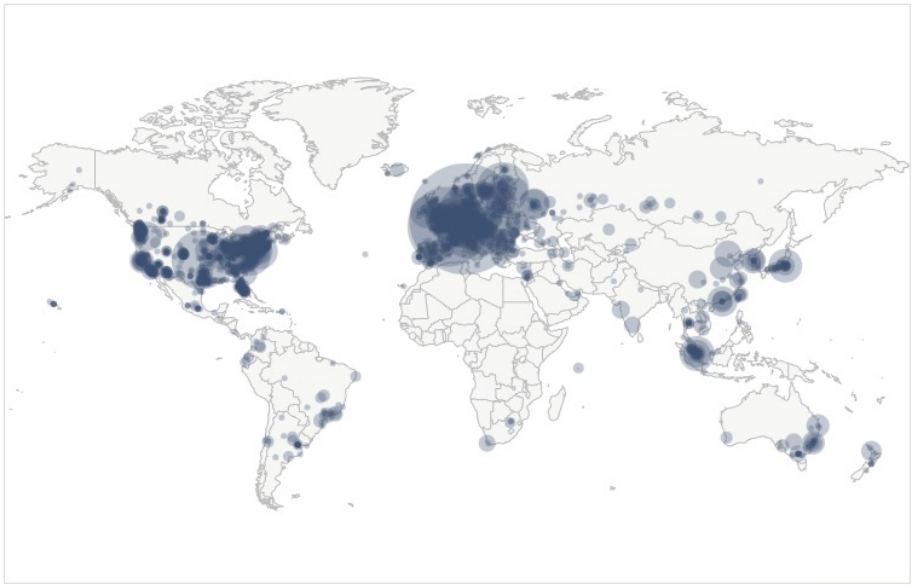
15294 NODES

24h | 90d | 1y

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	8148 (53.28%)
2	United States	1865 (12.19%)
3	Germany	1758 (11.49%)
4	France	525 (3.43%)
5	Netherlands	391 (2.56%)
6	Canada	308 (2.01%)
7	United Kingdom	231 (1.51%)
8	Finland	201 (1.31%)
9	Russian Federation	164 (1.07%)
10	Singapore	129 (0.84%)

More (85) »

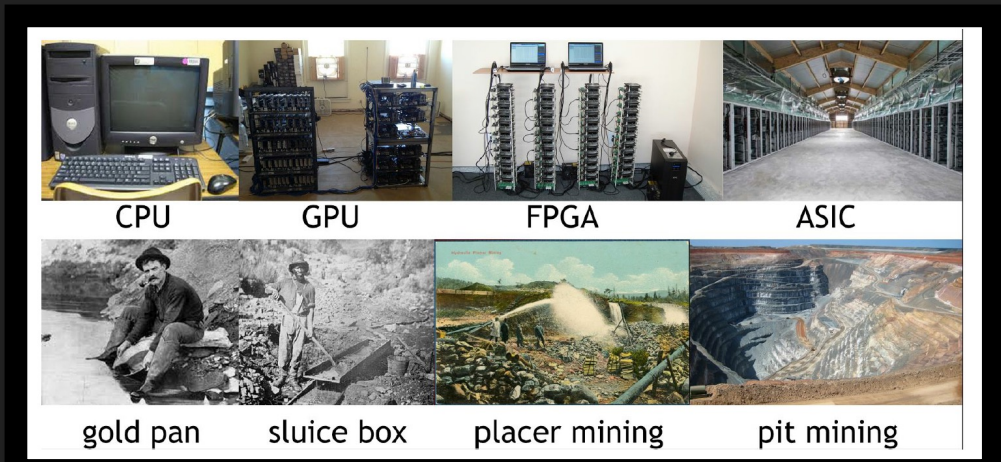


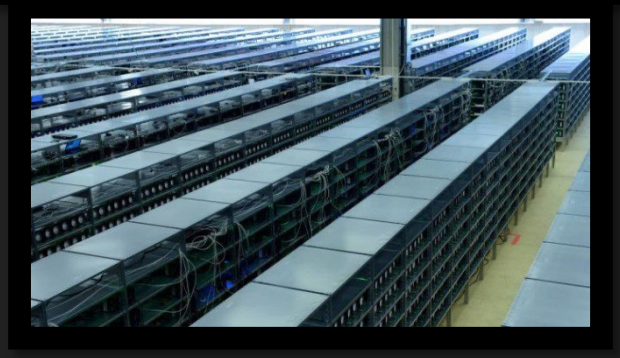
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Mining and energy consumption

- For earning bitcoins, one has to compute hashes and therefore consume energy
  - SHA-256 Hash function
  - Applied twice to a bitcoin block
- Mining hardware:
  - Almost impossible for normal computers
  - CPU/GPU mining (2010 OpenCL)
  - Arithmetic Logic Units (ALUs)
  - Field Programmable Gate Arrays (FPGAs)
  - Application –Specific Integrated Circuits (ASICs)
- Based on an Antminer S9 (ASIC) electric consumption, computing a block hash is worth about 3000 euros
- Total hashing work estimates : 250-1000 MW
  - from a major city to a small country consumption!
  - Professional mining: farms





Coin management and transfer

- You have a private key means: you have the money , i.e., the right to transfer coins attached to the key (mined or transferred to you)
- Storage: Wallets
  - PCs / mobile phones – stored in an encrypted file
    - Threat: malware attacks to intercept decryption key or to access coins when file is decrypted
  - Smart card / Tamper-proof module (TPM)
  - WYSIWYS (What You See Is What You Sign) terminals

More Challenges of Blockchains (1/3)

- Node data volume and required processing time – competing solutions:
  - SegWit (Segregated Witness): signatures are moved outside of the blockchain by establishing a bidirectional channel between the two parties. The size of each transaction is reduced by 60%. More transactions can be added to each block. This soft fork was activated into BC on August 2017, 24th, starting from block 481824
  - Lightning networks: bidirectional transactions that are not broadcasted to the blockchain, routed through an untrusted infrastructure – Blockchain is involved only as an arbiter to rule in case of non-cooperation between the two parties.
  - Bitcoin Unlimited : an evolution of Bitcoin Core – the size of blocks is decided by the client (larger thant the megabyte limit hardcoded into Bitcoin Core by Nakamoto in 2010) – the miners decide the maximum size they agree to process (there may be spam issues with overly large sizes)
  - Side chains: transactions are performed in additional blockchains equipped with sidecoins. Coin is locked to enable transactions based on sidecoin (two-way pegs between main blockchain and sidechains).

More Challenges of Blockchains (2/3)

- Eclipse attacks and variants (Double Spending without controlling 51% nodes)
  - Verification performed by nodes depends on the reception of new blocks
  - Blocks are dispatched through the underlying P2P network
  - Eclipse attacks may be used to isolate nodes and trick them to see only transactions that the attacker sends them
- Hacking: implementation vulnerabilities or design faults may be exploited
  - smart contract code abuse
  - Code bugs / implementation issues
  - Also on the client side: cryptocurrency mining malware (e.g. CookieMiner), cryptojacking malware

Bitcoin vulns (CVEs)

Common Vulnerabilities and Exposures

Clipper la diapositive

CVE	Announced	Affects	Severity	Attack is...	Flaw	Net
CVE-2010-5137	2010-07-28	wxBitcoin and bitcoind	DoS[1]	Easy	OP_LSHIFT crash	100%
CVE-2010-5141	2010-07-28	wxBitcoin and bitcoind	Theft[2]	Easy	OP_RETURN could be used to spend any output.	100%
CVE-2010-5138	2010-07-29	wxBitcoin and bitcoind	DoS[1]	Easy	Unlimited SigOp DoS	100%
CVE-2010-5139	2010-08-15	wxBitcoin and bitcoind	Inflation[3]	Easy	Combined output overflow	100%
CVE-2010-5140	2010-09-29	wxBitcoin and bitcoind	DoS[1]	Easy	Never confirming transactions	100%
CVE-2011-4447	2011-11-11	wxBitcoin and bitcoind	Exposure[4]	Hard	Wallet non-encryption	100%
CVE-2012-1909	2012-03-07	Bitcoin protocol and all clients	Netsplit[5]	Very hard	Transaction overwriting	99%
CVE-2012-1910	2012-03-17	bitcoind & Bitcoin-Qt for Windows	Unknown[6]	Hard	MingW non-multithreading	100%
BIP 0016	2012-04-01	All Bitcoin clients	Fake Conf[7]	Miners[8]	Mandatory P2SH protocol update	99%
CVE-2012-2459	2012-05-14	bitcoind and Bitcoin-Qt	Netsplit[5]	Easy	Block hash collision (via merkle root)	99%
CVE-2012-3789	2012-06-20	bitcoind and Bitcoin-Qt	DoS[1]	Easy	(Lack of) orphan txn resource limits	99%
CVE-2012-4682		bitcoind and Bitcoin-Qt	DoS[1]			98%
CVE-2012-4683	2012-08-23	bitcoind and Bitcoin-Qt	DoS[1]	Easy	Targeted DoS by CPU exhaustion using alerts	98%
CVE-2012-4684	2012-08-24	bitcoind and Bitcoin-Qt	DoS[1]	Easy	Network-wide DoS using malleable signatures in alerts	98%
CVE-2013-2272	2013-01-11	bitcoind and Bitcoin-Qt	Exposure[4]	Easy	Remote discovery of node's wallet addresses	97%
CVE-2013-2273	2013-01-30	bitcoind and Bitcoin-Qt	Exposure[4]	Easy	Predictable change output	97%
CVE-2013-2292	2013-01-30	bitcoind and Bitcoin-Qt	DoS[1]	Hard	A transaction that takes at least 3 minutes to verify	0%
CVE-2013-2293	2013-02-14	bitcoind and Bitcoin-Qt	DoS[1]	Easy	Continuous hard disk seek	97%
CVE-2013-3219	2013-03-11	bitcoind and Bitcoin-Qt 0.8.0	Fake Conf[7]	Miners[8]	Unenforced block protocol rule	100%
CVE-2013-3220	2013-03-11	bitcoind and Bitcoin-Qt	Netsplit[5]	Hard	Inconsistent BDB lock limit interactions	97%
BIP 0034	2013-03-25	All Bitcoin clients	Fake Conf[7]	Miners[8]	Mandatory block protocol update	99%
BIP 0050	2013-05-15	All Bitcoin clients	Netsplit[5]	Implicit[9]	Hard fork to remove txid limit protocol rule	97%
CVE-2013-4627	2013-06-??	bitcoind and Bitcoin-Qt	DoS[1]	Easy	Memory exhaustion with excess tx message data	57%
CVE-2013-4165	2013-07-20	bitcoind and Bitcoin-Qt	Theft[10]	Local	Timing leak in RPC authentication	57%
CVE-2013-5700	2013-09-04	bitcoind and Bitcoin-Qt 0.8.x	DoS[1]	Easy	Remote p2p crash via bloom filters	61%
CVE-2014-0160	2014-04-07	Anything using OpenSSL for TLS	Unknown[6]	Easy	Remote memory leak via payment protocol	Unknown
CVE-2015-3641	2014-07-07	Bitcoind and QT prior to 0.10.2	DoS[1]	Easy	(Yet) Unspecified DoS	

1. ↑ 1.00 1.01 1.02 1.03 1.04 1.05 1.06 1.07 1.08 1.09 1.10 1.11 Attacker can disable some functionality, for example by crashing clients

TheDAO attack

- An ICO that did not go so well…
  - Largest crowdfunding in history
  - Raised over 150 million dollars from more than 11,000 contributors
  - Lost 3.6 million ethers (60 million dollars at the time) to a hacker that abused the smart contract code and drained the money to a "child DAO »
- Attempts to recover the stolen funds resulted in a hard fork of the Ethereum community
  - ETH vs. ETC (classical, the older one)
  - In the ETH blockchain, the code for TheDAO has been patched (hence the smart contract was stopped)

More Challenges of Blockchains (3/3)

- Phishing: e.g., already initialized wallets
- Crypocurrencies and unregulated smart contracts:
  - public blockchains face a huge legal and regulatory threat
  - especially given their adoption for unlawful usages
- Confidentiality / Privacy / Processing geolocation in a public blockchain!
  - Cryptography may not withstand attacks indefinitely (especially in IoT systems)
  - Big Data may often be de-anonymized using additional knowledge
  - Linkability of transactions means that de-anonymization may propagate further
  - Vulns may also leak seemingly protected information

Conclusions

- Blockchains represent an great opportunity for the deployment of digital services
  - Distributed and self-managed infrastructure
  - Platform for deploying applications
- Blockchains support:
  - Decentralized trust establishment without trusted third parties
    - Cryptographic protection
    - Distributed validation
  - High availability through data replication and decentralized consensus
  - Immutable data storage
  - Cryptocurrencies
- Blockchains will also likely form the backbone infrastructure for
  - Deploying security mechanisms for IT
  - Handling data in future applications (IoT, autonomous vehicles …)
- Easy to create a blockchain, yet what about balkanization?