Brief Tutorial on Bitcoins

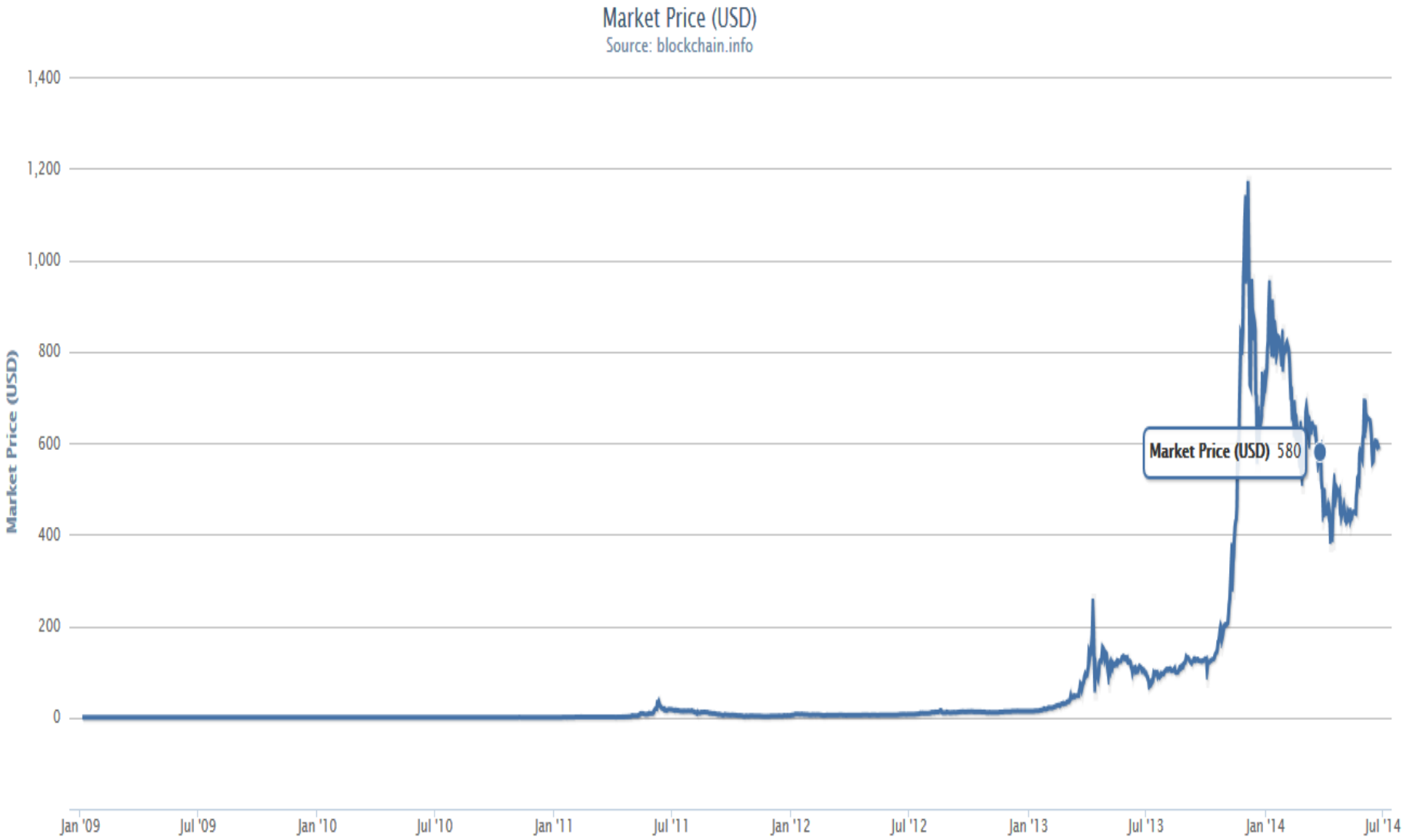
Abde Ali Kagalwalla

What is Bitcoin ?

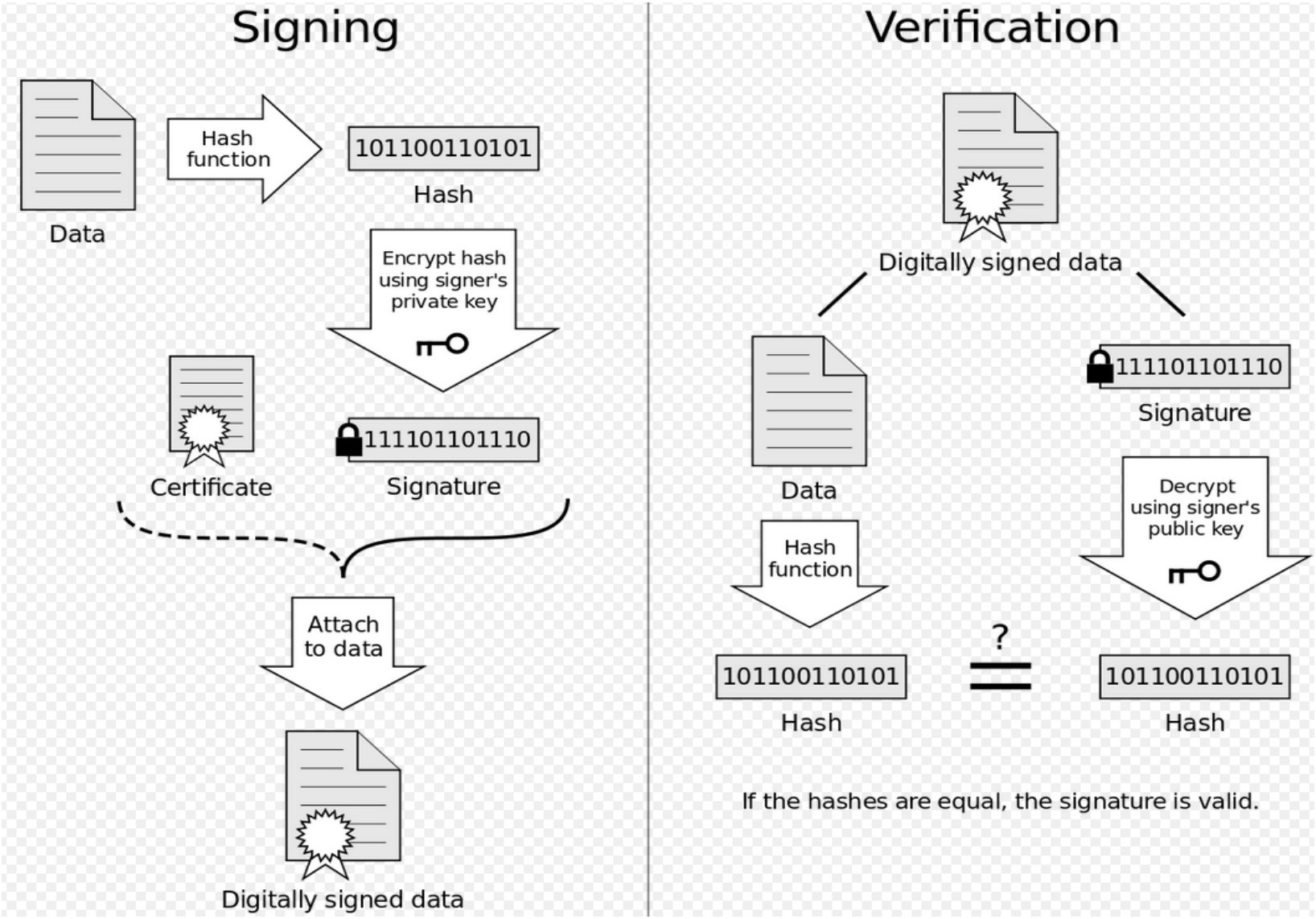
Casascuis

- Protocol to manage digital currency and process payments between users
- First proposed by “Satoshi Nakamoto”
- No central authority (Federal Reserve) or banks to manage transactions
- Decentralized, P2P system

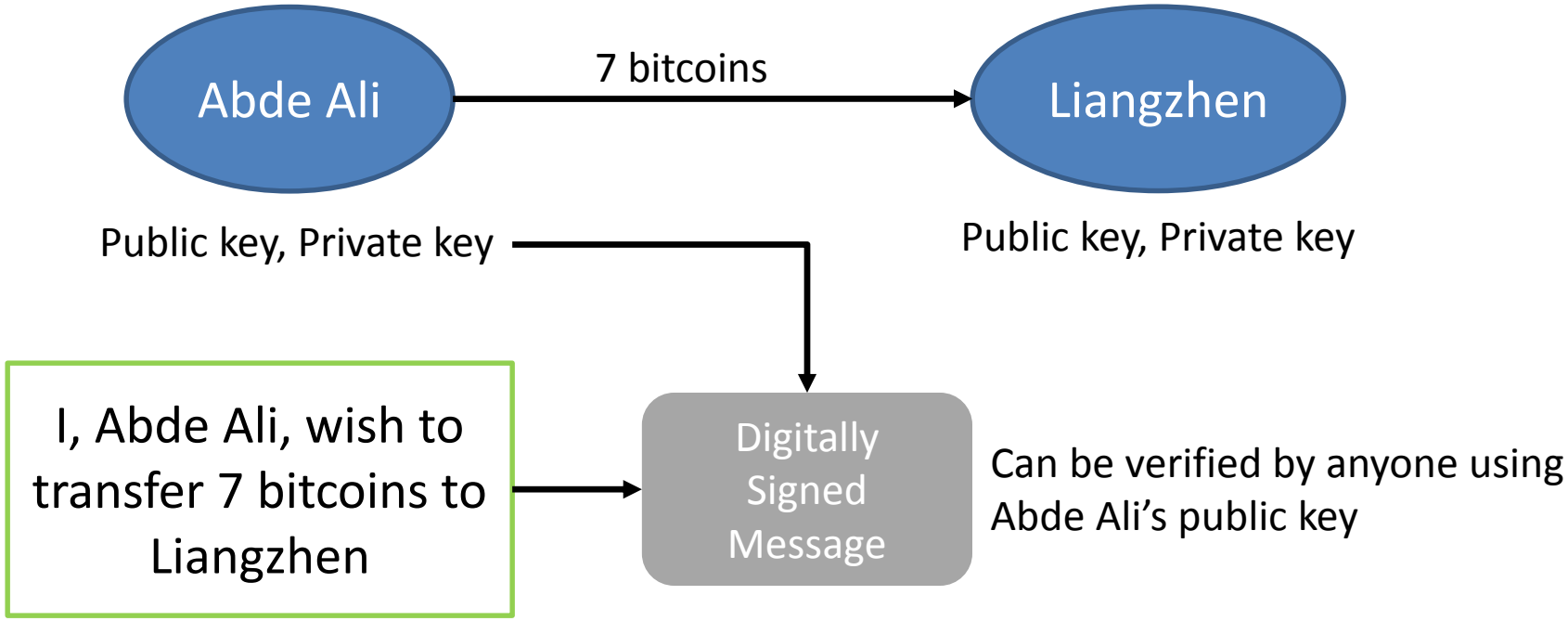
Valuation of bitcoin



Digital Signature (Image Source: Wikepedia)



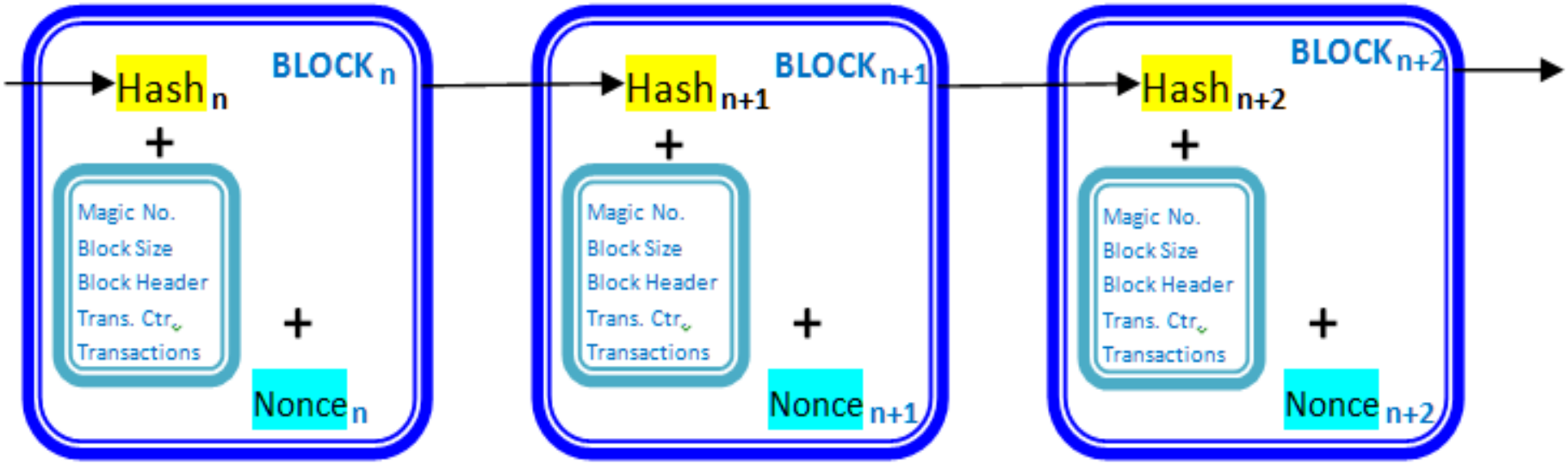
Bitcoin Transactions via Digital Signature



- Online transactions currently verified by a bank
  - Does Abde Ali own enough bitcoins ?
  - Double spending: Abde Ali should not be able to use the same bitcoins to pay Weiche
- Can a bank be completely eliminated from the online payment transfer protocol ?
  - → Ingenuity of Bitcoin

Decentralized Transaction Verification: Block Chain

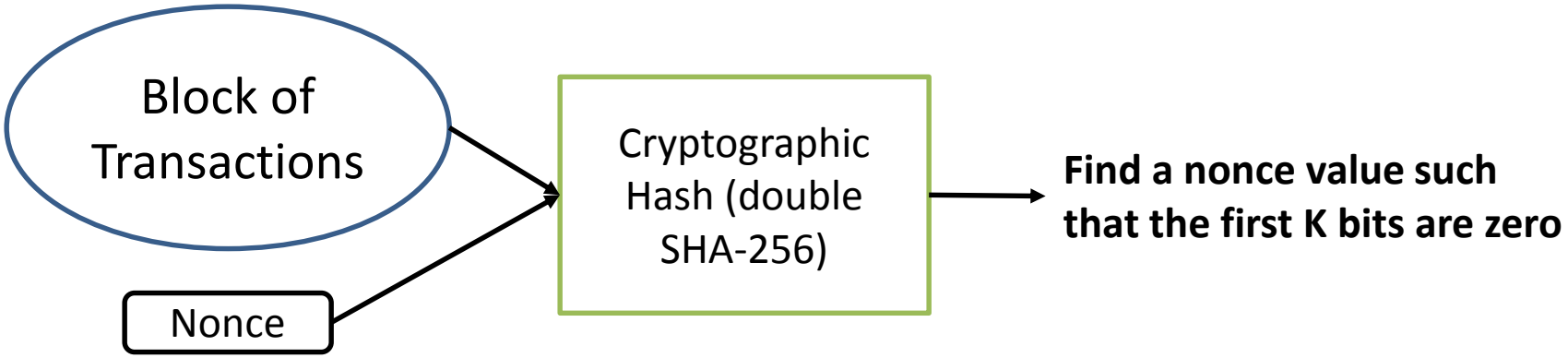
- Public ledger of transactions
- A set of transactions referred to as a ‘block’
- All verified blocks are added to the global block chain
- Liangzhen can look at the block chain and check if Abde Ali is not cheating
- Problem: What if Abde Ali tries to pay both Liangzhen and Weiche at the same time ?



Prevent Double Spending: Computationally Intensive Verification

- Potential Solution: Both Liangzhen and Weiche publicly release the digital message and request all users to verify
- Problem: Abde Ali can create millions of users that will validate both transactions
- Bitcoin solution is to make verification computationally expensive using a proof-of-work protocol
  - Solve a artificially challenging puzzle to verify a block chain
  - Reward users who verify blocks with new ‘mined’ bitcoins
  - This verification is done by bitcoin miners

Bitcoin Mining Challenge Puzzle: Proof-of-Work



- Since hash function is 'almost' random, 2^K attempts are required to solve the challenge
- On average blocks are verified in 10 minutes
- The successful miner is rewarded with 25 newly generated bitcoins
  - Number of bitcoins generated will be halved after every 210,000 validated blocks
  - Bitcoin generation will stop once the reward less than 10^{-8} (Minimum unit called Satoshi)
  - Miners also receive transaction fees

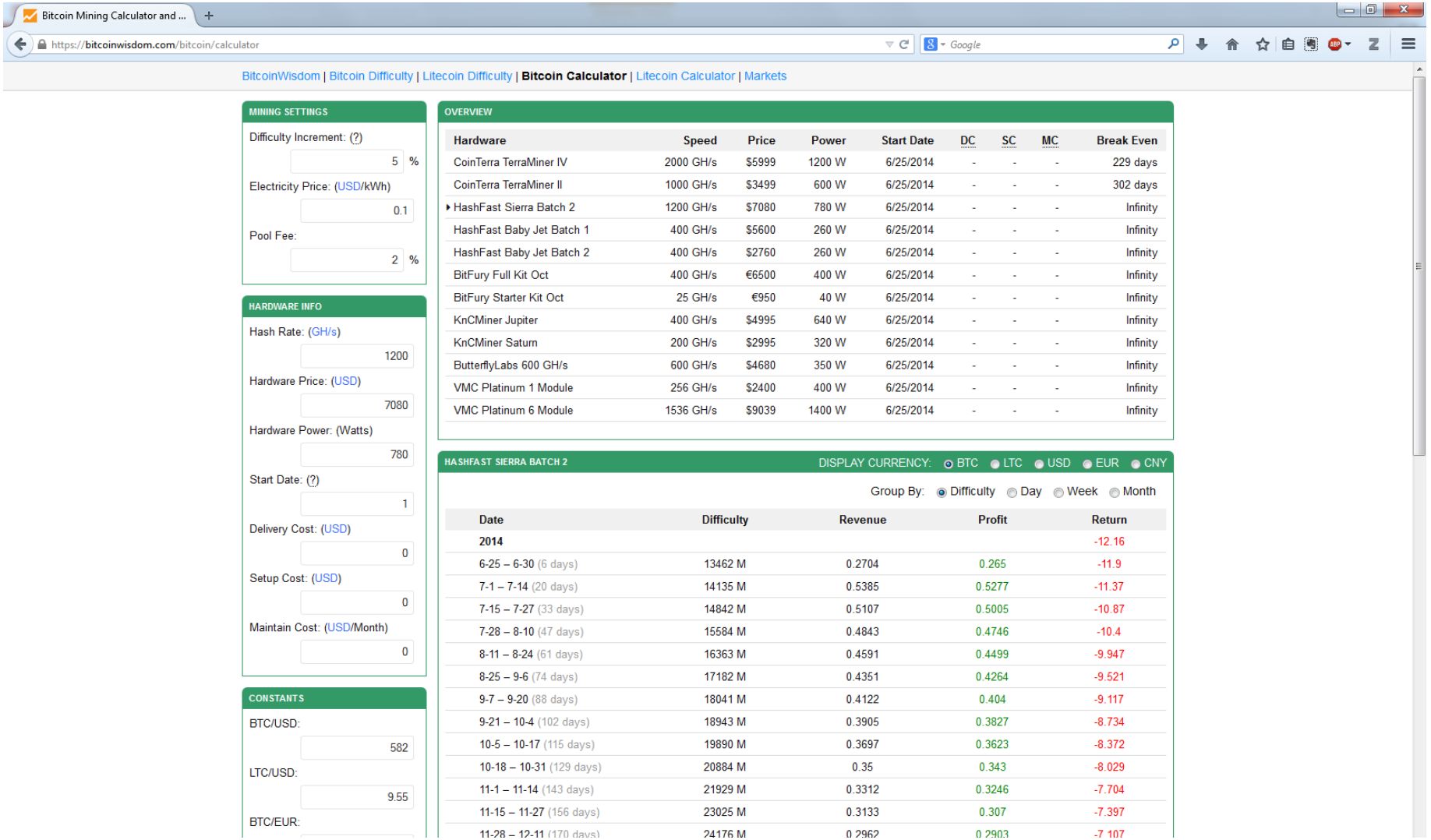
Bitcoin Mining Infrastructure

- Initially Satoshi's open source software could be used on any CPU → No longer viable
- GPU and FPGA based mining is fairly popular
- ASIC solutions are the most viable option now

Comparison of FPGA and ASIC Chips

	Spartan6-150	BFL Single	BFL miniRig	Avalon	BFL	ASICminer
Type	Xilinx FPGA	Altera FPGA	FPGA	ASIC	ASIC	ASIC
Process	45 nm	45 nm (?)	45 nm (?)	110 nm	65 nm	130 nm
Hash Rate Per Chip	210 MH/s	415 MH/s	650-750 MH/s	280 MH/s	4 GH/s	300 MH/s
Power Draw	15 W	40 W	35 W	2.8 W	30 W	2.5 W
Efficiency (MH/s per W)	14	10	20	100	133	120
US$ / MH/s	1 to 2.5	0.75	0.6	Varies	Varies	Varies
Notes	Typically 1 to 4 FPGAs Per Board	2 FPGAs Per Board	2 FPGAs Per Board, 17 to 18 Boards	Priced In BTC (prices increase)	BFL Anticipates A Slight Reduction In Power Draw	Priced In BTC (prices increase)

Comparison of Bitcoin Mining Hardware:https://bitcoinwisdom.com/bitcoin/calculator



Bitcoin Mining Calculator and ...

https://bitcoinwisdom.com/bitcoin/calculator

BitcoinWisdom | Bitcoin Difficulty | Litecoin Difficulty | **Bitcoin Calculator** | Litecoin Calculator | Markets

MINING SETTINGS

Difficulty Increment: (?) 5 %

Electricity Price: (USD/kWh) 0.1

Pool Fee: 2 %

HARDWARE INFO

Hash Rate: (GH/s) 1200

Hardware Price: (USD) 7080

Hardware Power: (Watts) 780

Start Date: (?) 1

Delivery Cost: (USD) 0

Setup Cost: (USD) 0

Maintain Cost: (USD/Month) 0

CONSTANTS

BTC/USD: 582

LTC/USD: 9.55

BTC/EUR:

OVERVIEW

Hardware	Speed	Price	Power	Start Date	DC	SC	MC	Break Even
CoinTerra TerraMiner IV	2000 GH/s	$5999	1200 W	6/25/2014	-	-	-	229 days
CoinTerra TerraMiner II	1000 GH/s	$3499	600 W	6/25/2014	-	-	-	302 days
HashFast Sierra Batch 2	1200 GH/s	$7080	780 W	6/25/2014	-	-	-	Infinity
HashFast Baby Jet Batch 1	400 GH/s	$5600	260 W	6/25/2014	-	-	-	Infinity
HashFast Baby Jet Batch 2	400 GH/s	$2760	260 W	6/25/2014	-	-	-	Infinity
BitFury Full Kit Oct	400 GH/s	€6500	400 W	6/25/2014	-	-	-	Infinity
BitFury Starter Kit Oct	25 GH/s	€950	40 W	6/25/2014	-	-	-	Infinity
KnCMiner Jupiter	400 GH/s	$4995	640 W	6/25/2014	-	-	-	Infinity
KnCMiner Saturn	200 GH/s	$2995	320 W	6/25/2014	-	-	-	Infinity
ButterflyLabs 600 GH/s	600 GH/s	$4680	350 W	6/25/2014	-	-	-	Infinity
VMC Platinum 1 Module	256 GH/s	$2400	400 W	6/25/2014	-	-	-	Infinity
VMC Platinum 6 Module	1536 GH/s	$9039	1400 W	6/25/2014	-	-	-	Infinity

HASHFAST SIERRA BATCH 2 DISPLAY CURRENCY: BTC LTC USD EUR CNY

Group By: Difficulty Day Week Month

Date	Difficulty	Revenue	Profit	Return
2014				-12.16
6-25 – 6-30 (6 days)	13462 M	0.2704	0.265	-11.9
7-1 – 7-14 (20 days)	14135 M	0.5385	0.5277	-11.37
7-15 – 7-27 (33 days)	14842 M	0.5107	0.5005	-10.87
7-28 – 8-10 (47 days)	15584 M	0.4843	0.4746	-10.4
8-11 – 8-24 (61 days)	16363 M	0.4591	0.4499	-9.947
8-25 – 9-6 (74 days)	17182 M	0.4351	0.4264	-9.521
9-7 – 9-20 (88 days)	18041 M	0.4122	0.404	-9.117
9-21 – 10-4 (102 days)	18943 M	0.3905	0.3827	-8.734
10-5 – 10-17 (115 days)	19890 M	0.3697	0.3623	-8.372
10-18 – 10-31 (129 days)	20884 M	0.35	0.343	-8.029
11-1 – 11-14 (143 days)	21929 M	0.3312	0.3246	-7.704
11-15 – 11-27 (156 days)	23025 M	0.3133	0.307	-7.397
11-28 – 12-11 (170 days)	24176 M	0.2962	0.2903	-7.107

Bitcoin Mining Pools

- Bitcoin mining is a very risky venture
  - As soon as one miner solves the puzzle, all others must restart on the next block
- Typically done in pools
  - All miners in pool share rewards for a successful mine
  - Miners who contribute more ‘partial’ solutions get greater share of reward
  - Several different miners with different protocols for joining, sharing, etc.

References

- Good Explanation of Bitcoin: http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/
- Tutorial videos on Khan Academy: https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it
- Hardware for Mining: http://www.tomshardware.com/reviews/bitcoin-mining-make-money,3514-3.html