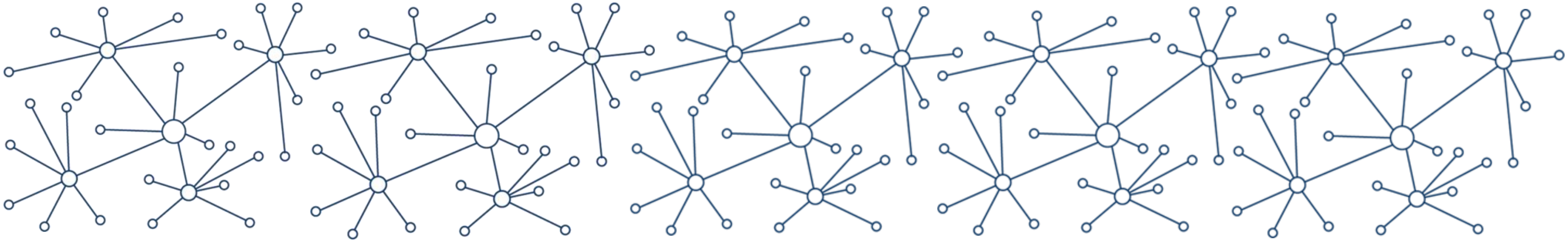


Blockchain Technology

Open Elective @ VJTI - Fall 2019

Lecture#1 (22 July 2019)

Dhiren Patel

VJTI Mumbai

Know the game (Course)

- Course scheme (5 credits)
- Schedule (Monday 1115 - 1315, Thursday 1115 - 1315, Thursday 1415-1515 (1615), Saturday (if required))
- Curriculum / Syllabus (next 3 slides)
- Teaching methodology (Interactions)
- Book(s), Reference(s), PPTs, Study material, Reading (ACM, IEEE, etc..)
- Course website (MooC/Moodle/EdX??)
- Evaluation - Mid-sem, End-sem, Assignments (coding?), Quiz/Tests, Presentations, Attendance requirement (?)
- Relative Grading
- Let’s start with the course pre-test (of 20 minutes)…
- Bitcoin, Record, DLT, Blockchain, (Smart) Contract
- (e.g. Pothole complaint and resolution in Metropolitan area)….

Course objectives

- Let us learn with the mindset "How could Blockchain technology potentially benefit us instead of fitting problems in?"
- Decentralized computing, Distributed ledger technology, Blockchain and its applications.
- Understand technology foundations of Blockchain through protocols, security primitives, token economics, smart contracts, attacks and advances.
- Design and implement new ways of using blockchain for applications with cryptocurrency and beyond.
- Explore platforms to build applications on blockchain

Course outcome

1. Understand blockchain architecture and requisite crypto foundations
2. Understand various consensus protocols and their usage for specific applications
3. Understand and Resolve security concerns in blockchain
4. Explore blockchain advances and upcoming platforms
5. Learn to write smart contracts
6. Understand distributed application and design use-cases
7. Solve problems and create solutions.. (Capacity building)

Micro details (flexible)

- Introduction and Crypto foundations: Elliptic curve cryptography, ECDSA, Cryptographic hash functions, SHA-256, Merkle Trees, Crytpocurrencies (4 hrs)
- Bitcoin: Bitcoin addresses, Bitcoin's blockchain, block header, mining, proof of work (PoW) algorithms, difficulty adjustment algorithm, mining pools, transactions, double spending attacks, the 51% attacker, block format, pre-SegWit transaction formats, Bitcoin script, transaction malleability, SegWit transaction formats, smart contracts (escrow, micropayments, decentralized lotteries), payment channels, Lightning network (8-10 hrs)
- Ethereum: Overview of differences between Ethereum and Bitcoin, block format, mining algorithm, proof-of-stake (PoS) algorithm, account management, contracts and transactions, Solidity language, decentralized applications using Ethereum (4-6 hrs)
- Smart Contracts (4-6 hrs)
- Different Blockchains and Consensus mechanisms (4-6 hrs)
- Blockchain and Security: Attacks and countermeasures (4-6 hrs)
- R3, CORDA and Hyperledger System architecture, ledger format, chaincode execution, transaction flow and ordering, private channels, membership service providers, case studies (4-6 hrs)
- dApps – (6 hrs)
- Blockchain use cases and advanced topics (4-6 hrs)

Know the players

- Students - Groups
- Disciplines/Departments/Compartments??
- Boundary-less, Flexible, Autonomous education ecosystem
- Instructors (Fall 2019) –
  - Dhiren Patel (VJTI),
  - Yann Busnel (IMT Atlantique),
  - Jay Bothra (HSBC),
  - Deven Shah (TCET),
  - XXX(tba) ….

Cryptocurrency (Wikipedia)

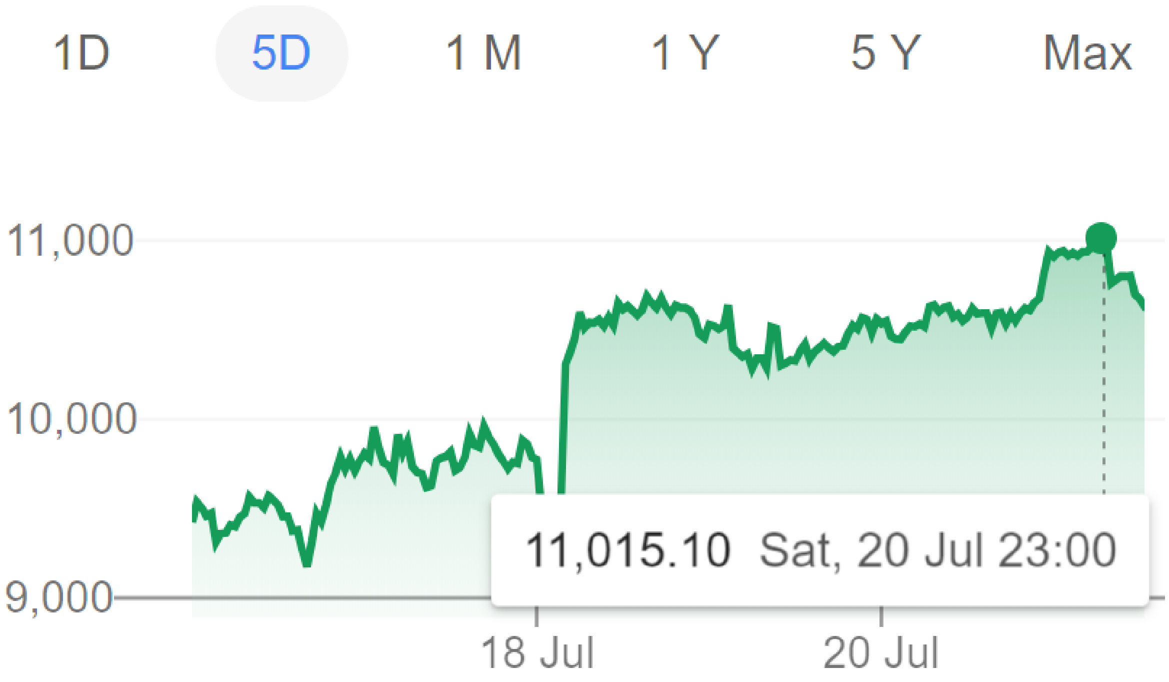
- It is a digital asset designed to work as a medium of exchange
- that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.
- (normal currency example – exchange, storage, ownership, value, purchase power, trust, production, interoperability..)
- It uses decentralized control as opposed to centralized digital currency and central banking systems
- The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database

Cryptocurrency – Bitcoin invention philosophy

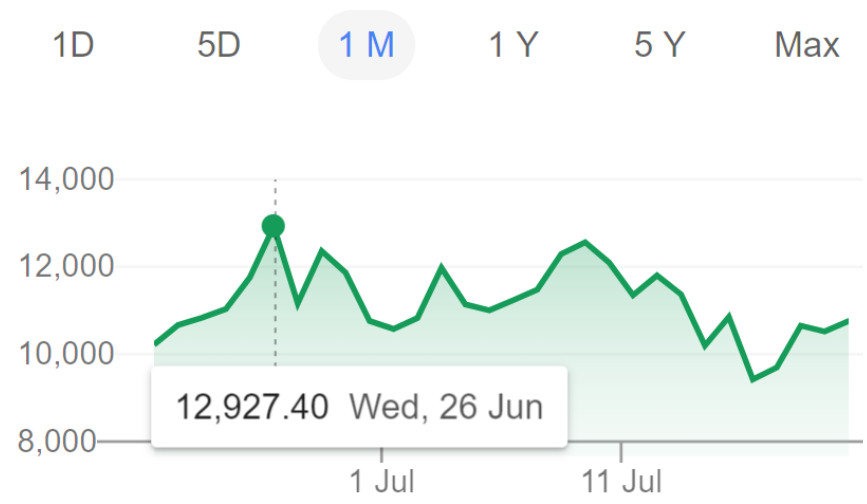
- encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank
- Bitcoin – Satoshi Nakamoto 2008/2009
- Banking the Unbanked, De-banking All, Stable digital currency
- Crypto-currency-based payments system could be especially useful in countries with high inflation/unstable banking systems and for cross-country remittances
- control over finance that cannot be seized, frozen, or censored by Governments, Banks, Financial Institutions
- Value to Bitcoin, Total supply – 21M, Exchanges and Wallets
- Craig Wright (Aus) – claiming to be Nakamoto
- Filed 95 patents on Blockchain in the last 3 years

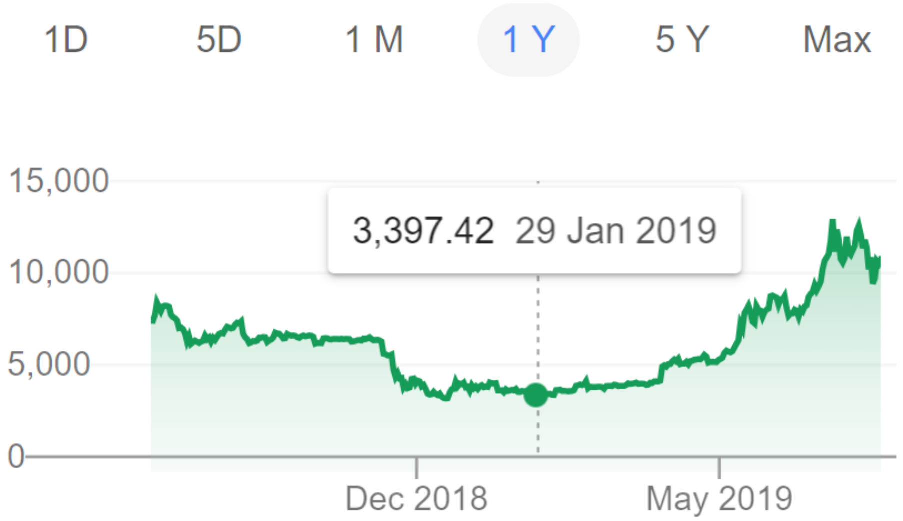
Lets dive in further

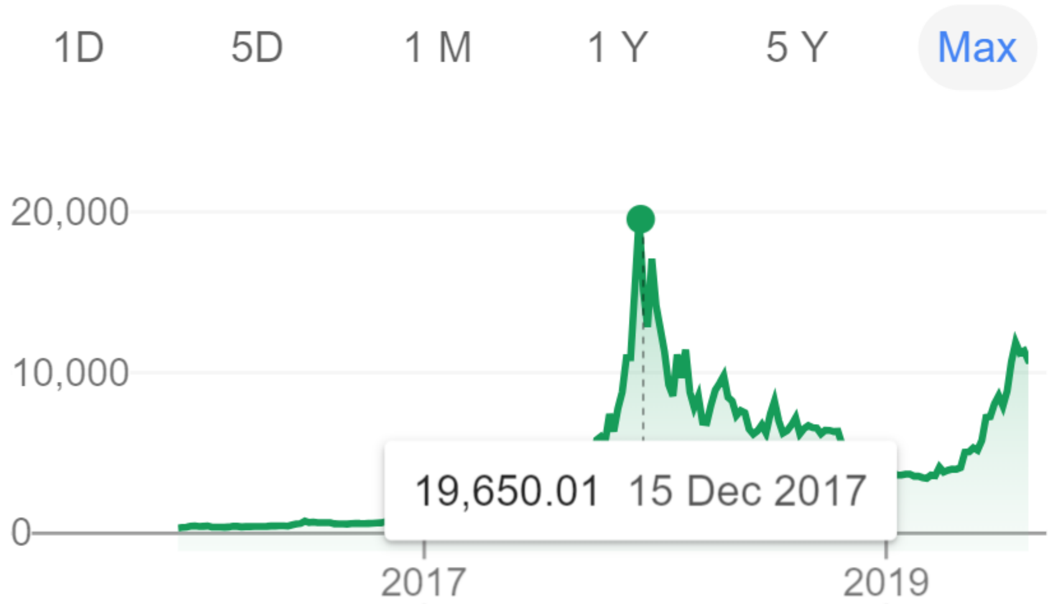
- Bitcoin, crytpocurrency, Blockchain
- Bitcoin price in USD



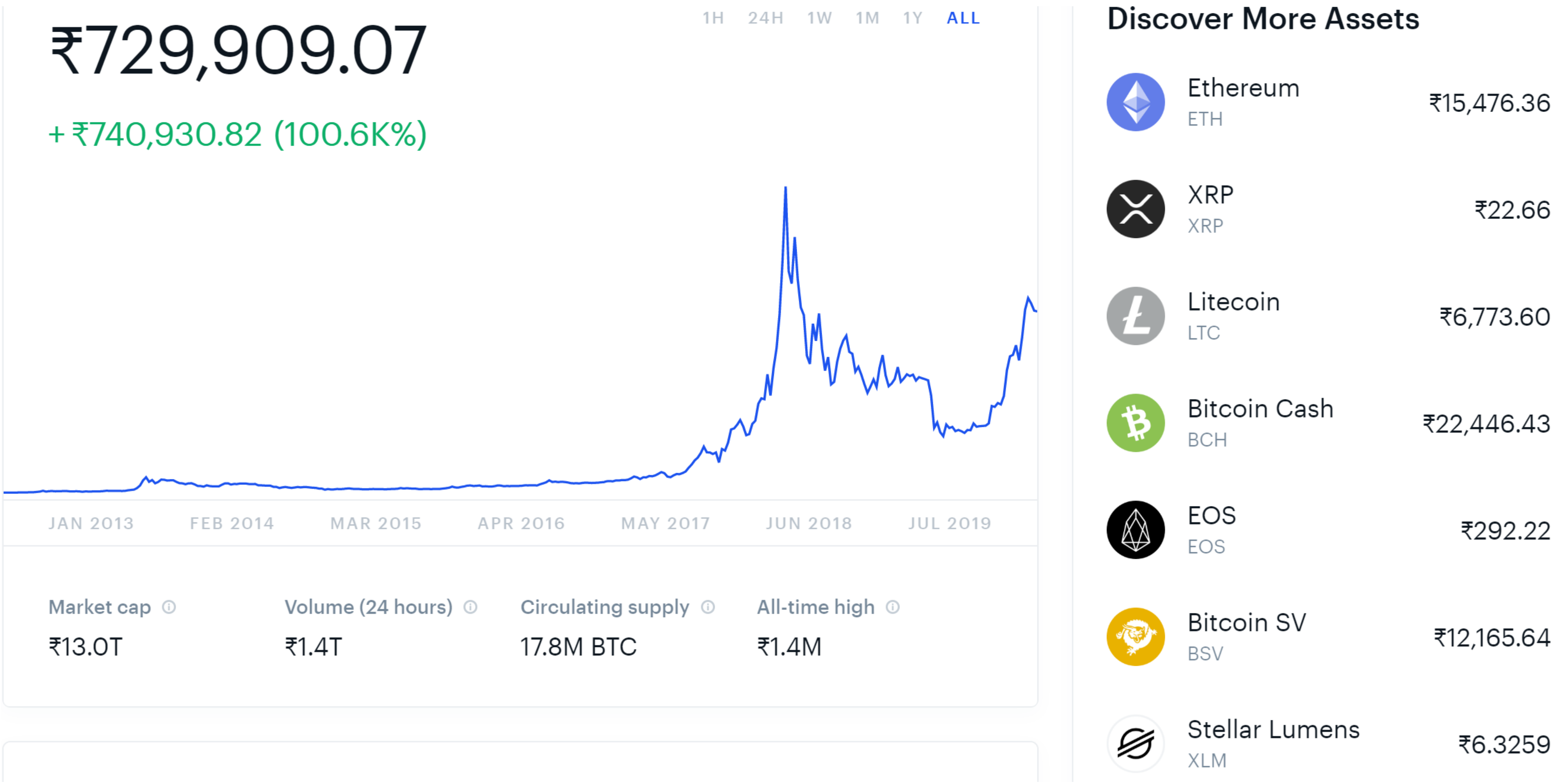
Bitcoin price (historical)







Bitcoin and other cryptocurruncies



₹729,909.07

+ ₹740,930.82 (100.6K%)

Market cap	Volume (24 hours)	Circulating supply	All-time high
₹13.0T	₹1.4T	17.8M BTC	₹1.4M

Discover More Assets

Ethereum ETH	₹15,476.36
XRP XRP	₹22.66
Litecoin LTC	₹6,773.60
Bitcoin Cash BCH	₹22,446.43
EOS EOS	₹292.22
Bitcoin SV BSV	₹12,165.64
Stellar Lumens XLM	₹6.3259

Cryptocurrencies – revisiting

- US President Donald Trump declares himself “not a fan” of cryptocurrencies, “whose value is highly volatile and based on thin air”.
- Bitcoin’s Price Could Rise if Facebook’s Crypto (CaLibra) Survives Congress Hearings
- Banning of Cryptocurrency & Regulation of Official Digital Currency Bill 2019, India

What (Govt of India stance)?

- ~~The draft bill proposes banning cryptocurrency-related activities in India~~

  ~~(Terror funding, money laundering, black money)~~
- ~~Heavy penalty and punishment of up to 10 years jail has also been proposed~~
- ~~it proposes a jail term of one to 10 years for those who mine, hold, transact or deal with cryptocurrencies in any form, whether directly or indirectly through an exchange or trading~~

~~‘cryptocurrency’ defined (in draft Bill)~~

- ~~any information or code or number or token (not being part of any official digital currency),~~
- ~~generated through cryptographic means (or otherwise),~~
- ~~providing a digital representation of value which is exchange with or without consideration,~~
- ~~with the promise or representation of having inherent value in any business activity~~
- ~~which may involve risk of loss or an expectation of profits or income,~~
- ~~or functions as a store of value or a unit of account~~
- ~~and includes its use in any financial transaction or investment~~

Other interpretations (cryptocurrency)

- This clearly separates cryptocurrency from digital rupee and digital foreign currencies
- The definition seems to be targeting digital currencies not backed by any central banks
- [**Australian Anti-Money Laundering and Counter-Terrorism Financing Act**] - cryptocurrency is defined
- as a type of currency that only exists in digital rather than physical form (not coins or notes) and
- can be exchanged for goods, services or physical currency and
- is not issued by or under the authority of a government
- [**Financial Instruments and Exchange Act of Japan**] - categorises and recognises cryptocurrencies as crypto-assets

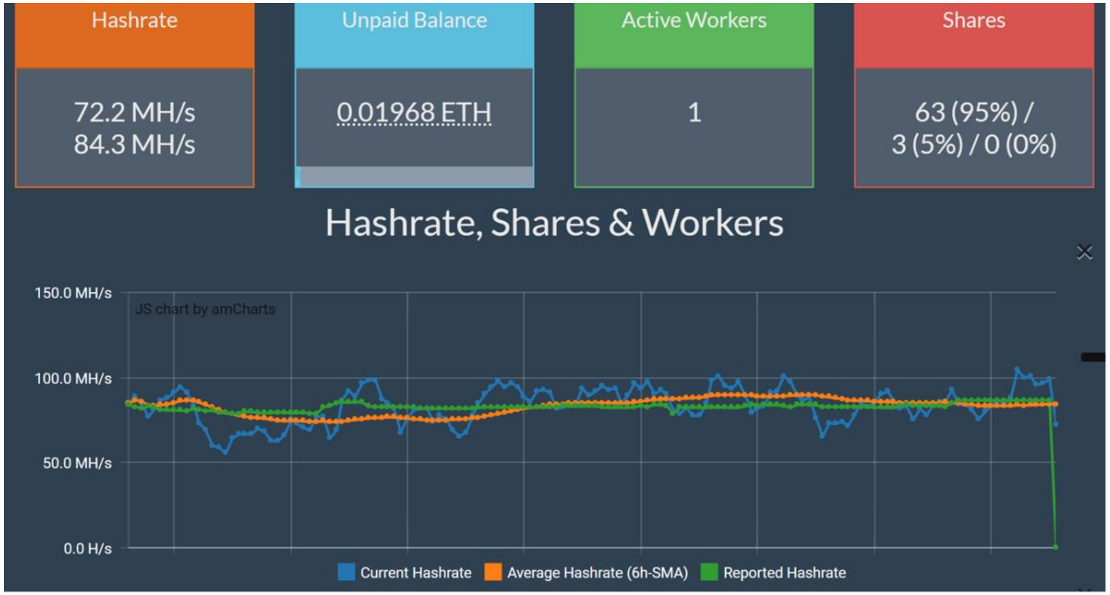
Research and Education

- No person shall mine, generate, hold, buy or sell or deal in, issue, transfer, dispose of or use cryptocurrency in the territory of India
- (The draft clarifies that certain terms will not apply to any person using technology or processes underlying any cryptocurrency for the purposes of experiment or research including education provided that no cryptocurrencies are used for making or receiving payment in such activity)
- (It also clarifies that any law would not target blockchain or the use of Distributed Ledger Technology (DLT) for creating a network for delivery of any financial or other services or for creating value, without involving any use of cryptocurrency for making or receiving payment)

~~India Government Stance~~

- ~~Amid rising uproar over the leaked and reported draft bill,~~
- ~~the Indian government which recently in parliament had stated that the draft Bill is still under development,~~
- ~~one can expect changes in some of the proposed regulations in the final draft.~~

Mining experiment (Don’t do it!!)



Hashrate

72.2 MH/s
84.3 MH/s

Unpaid Balance

0.01968 ETH

Active Workers

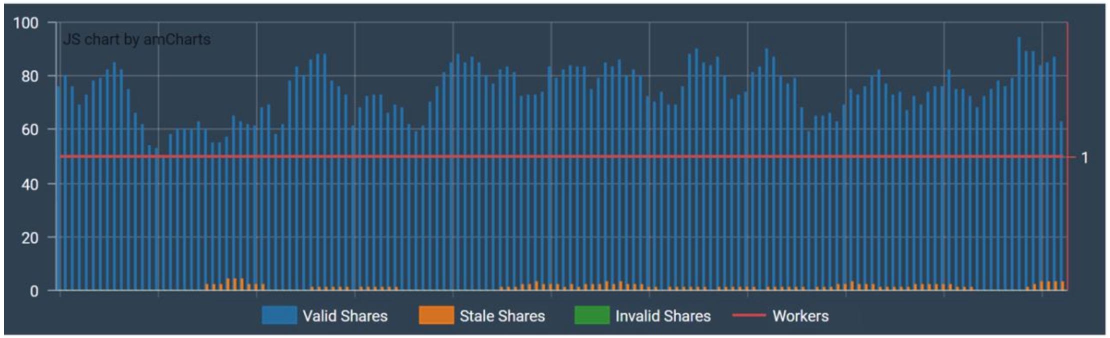
1

Shares

63 (95%) /
3 (5%) / 0 (0%)

Hashrate, Shares & Workers

68h50m, Tesla V100 GPU – 100% (stopped on 22 May 2019 1340)



Yield ~ 0.02 ether (~5 USD)

Concluding Remarks

- Never gets into mining
- Ethics and integrity – Capacity building for Global good
- We all have a responsibility to help advance financial inclusion, support ethical actors, and continuously uphold the integrity of the Blockchain ecosystem….