Bitcoin, blockchain and the future economy

By Terry Levin

19 Aug 2016

Speaking at Cape Town's Bandwidth Barn on 17 August 2016, The Blockchain Academy training director and Bitcoin evangelist Lorien Gamaroff unpacked the basics of new digital currencies and blockchain technologies to an audience of curious professionals and students - ranging from financial, engineering, clean energy and social media disciplines to a mixed bag of entrepreneurs and investors.

Image by Terry Levin

Contextualising his topic, Gamaroff, a Gauteng-based Rhodes University computer science graduate and “geektrepreneur” answered every question you never thought to ask about Bitcoin and blockchain trends, beginning that no new technology mysteriously comes out of nowhere, but is usually the result of decades of intense research, pointing out how completely new things are historically met with doubt, fear and suspicion. Citing the PC in 1975, the internet in 1993 and Bitcoin in 2009 as examples and the quote by Economic Nobel Prize winner Paul Krugman that stated categorically, “By 2005 or so, it will become clear that the internet’s impact on the economy has been no greater than the fax machine’s.” Which just goes to show that trend forecasting is not everybody’s game, but I digress.

Lorien goes on to explain how new technologies such as Uber are usually born out a “pain point” or an attempt to eliminate inconvenience or other identified problems within a system.

So what were the “pain points” that prompted Bitcoin inventor Santoshi Nakamoto to develop the nine-page Bitcoin whitepaper that started it all in 2008?

Pain point 1: The internet’s fundamental flaw

With regard to finance, the internet’s fundamental flaw and blind spot that has never really been addressed has been to do with payment trust. The credit card, invented in 1950, was never meant to be combined with internet technology. Apart from the risks of fraud and hacking of sensitive personal information, additional expenses involved in trying to mitigate these issues are exacerbated when institution-to-institution or cross border transactions are involved compounding delayed payments, waste and expense.

Pain point 2: State of money in the world today

Gold, Gamaroff enlightens us, derives its value from being the rarest finite commodity on earth and as such has proved itself a good store of value for over 2000 years. By contrast, because there is no restraint on the store of currencies in the world, global markets have been in a hyperinflationary phase for decades. This is cited as one of the reasons Nakamoto was prompted to invent the Bitcoin system.

Bank bailouts

Factors such as the January 2009 *Times* headline “Chancellor in brink of 2nd bailout for banks”, referring to then UK Chancellor of the Exchequer Alistair Darling and similar accounts of the 2008 US sub prime mortgage crisis and subsequent bank bailouts which caused chaos in the world, inspired Santoshi to invent a currency that would be able to emulate the rarity and resilience of gold. The fact that even the mighty dollar has been in continual decline since its invention in 1913 points to a real need for stability and renewed trust in global markets.

An unabated increase in money supply due to unrestrained printing of fiat currency, the resultant need by countries to competitively devalue, negative or close to 0% interest rates and global recessions have given economies little room to manoeuvre. In the last 100 years, 55 countries have hyper-inflated with Nigeria, Zimbabwe, Yugoslavia, Venzueula and the Weimar Republic potentially foretelling the potential demise of even more resilient monetary systems such as Japan, US and Europe. As economies shrink, currency should be removed from circulation, but as this doesn’t happen, the peak of financial systems as we know them could be a reality.

The current unit of 15-million Bitcoins in the world is expected to achieve its capacity of 21-million units by 2140. If that sounds like a ridiculously small number by comparison with billions and trillions of units of global currencies we are used to hearing about, Gamaroff explains that Santoshi intended the 21,000,000 cap, with divisibility, to be key. The potential to divide down into hundreds of millionths if necessary, by adding zeros ensures that by never having to run the risk of inflating supply, units become more valuable, not less valuable over time. With a gloomy predicted global GDP of approximately 2%, the system begins to make sense.

Right now 1 Bitcoin will buy you 10,000 worth of stuff, but that might become worth 100,000 or 1-million due to built in rarity.

Bitcoin the tipping point

Bitcoin evangelists believe critical mass might be imminent thanks to remarks issued in 2014 by UK's Chancellor George Osborne that the "once dismissed" alternative or “digital currencies may now well play a big part in our financial future."

So how does blockchain work?

Gamaroff shared with us that Bitcoin has its origins in earlier versions of anonymous, digital systems such as E-cash, AAEC, Bitgold, Hashcash and B-money. Beginning to paint a picture of how the tech that makes Bitcoin work can be expanded to any asset such as shares, certificates of ownership, land titles, car etc. Theoretically, you could sell your

house, trade shares on the JSE and buy and sell any asset via blockchain. Many sectors are looking at how to create cool, new businesses models for the future, passports and IDs for example might disappear on the blockchain.

One database

Using his preferred example of the fictitious characters Alice and Bob, Lorien creates scenarios. For example with current systems if Alice wants to transfer assets to Bob she has to notify bank, whose database needs to be updated and transferred to Bob's Bank, where their info and database will need to be verified, a time consuming and inefficient system of multiple intermediaries for which we are paying in both time and money.

To fix this, one source of truth, the one database, instantly updated, to which everyone has access, which blockchain has been designed to provide, would be an optimum situation. Another benefit of the Bitcoin/blockchain database is that the data never goes away, allowing provenance and a foolproof tracking trail. Blockchains' decentralised model, means there is no one managing it. The database itself provides the records or rows of data – which is how they may come to signify the serial number of any asset be it a car, share or house.

Bitcoin mining for beginners

The Bitcoin mining process is about transaction processing. Only one server gets to process a block or Proof of Work, which is like a difficult to solve maths puzzle, guessing a "magic number" and is how new bitcoins get created.

New transactions happen every 10 minutes, with the processors that identify the winning numbers earning 12,5 new Bitcoins as well as any fees on the transaction. The mining process is non deterministic and correlating to processing power, in a similar way to how buying 1000 lottery tickets would give you a better chance of winning than buying one lottery ticket.

Thus computers become nodes, doing what they do best, processing, validating transactions and in doing so, earning money and adding to the security of the network with no human input.

People are making a living from this and forging new business models, with processors popping up in China, Iceland and elsewhere, especially in places where electricity is cheap, such as hydro electricity projects.

The system is apparently self-regulating, in that every two weeks the difficulty is adjusted - the blockchain - software that is running checks to see what the average amount of time taken to process blocks - keeps the system stable. As new data centres start mining transactions, more numbers are being guessed and it gets quicker to process blocks, so network checks and balances are automatically in place to maintain equilibrium.

Like Linux or Ubuntu, the open source systems, Bitcoin is a project that anyone can contribute to, with groups of people assigned the role of project "maintainers" in a similar way to which Mark Shuttleworth has governance of Ubuntu Open Source.

Up till now Bitcoin has grown and grown, because everyone has agreed, with quality checks, feedback and difficult debates or decisions getting consensus from its community.

Visions of liberation

There is a lot of excitement globally on the opportunities that digital currencies such as Bitcoin and its underlying technology, the blockchain, offer for financial and non-financial institutions. In South Africa, The Blockchain Academy was established to help companies and individuals understand the systems, application processes, conversions and opportunities offered by this revolutionary new disruptive technology.

The Blockchain Academy can tailor courses to specific needs and runs beginner and advanced training and at the

Bandwidth Barn in Woodstock, Cape Town and the AlphaCode Club in Sandton, Johannesburg.

Follow them on @BlockchainAcad and @gamaroff.

ABOUT TERRY LEVIN

Brand and Culture Strategy consulting | Bizcommunity.com CCO at large. Email terry@offtheshelf.co.za, Twitter @terrylevin, Instagram, LinkedIn.

- Raising the flag on threats and opportunities - 18 Oct 2016
- Going, going Gordhan - 17 Oct 2016
- Bitcoin, blockchain and the future economy - 19 Aug 2016

View my profile and articles...