HEADS UP: BITCOIN

AN INTRODUCTORY CASM BRIEFING PAPER

Jamie Bartlett
Carl Miller
James Smith
Louis Reynolds

17 December 2013

DEMOS

PARTNERS CREDITS

This paper was produced in partnership with Elliptic.

Published by Demos 2013

Third Floor
Magdalen House
136 Tooley Street
London SE1 2TU

T 0845 458 5949
F 020 7367 4201

hello@demos.co.uk
www.demos.co.uk

"The internet is going to be one of the major forces for reducing the role of government. The one thing that is missing but that will soon be developed is a reliable e-cash, a method by which on the internet you can transfer funds from A to B without A knowing B or B knowing A... of course it has its negative side; it means that the gangsters, the people who are engaged in illegal transactions, will also have an easier way to carry on their business."

Milton Friedman, 1999[i]

Introduction

Vires in Numeris – 'Strength in Numbers' – is the motto printed on minted Bitcoins. Of course, these gleaming little discs of metal are symbolic. The real Bitcoin (and the meaning of the motto) is hidden on the back. Under a sticker is a string of numbers and letters, a private key that, in a system involving cryptography, 'blockchains' and community authentication, allows you to hold and exchange units of value.

Bitcoin is a decentralised peer-to-peer digital crypto-currency. It has the potential to ensure a high degree of anonymity. It is also only the most famous of a growing breed of digital currency that rely upon secure, encrypted peer-to-peer exchange. Its trust, worth and constant use lie entirely outside of the 'fiat' of our conventional financial and institutional system. Its legitimacy derives from the community that uses it.

In its initial years – Bitcoin was introduced in 2009 – users were mainly drawn from the niche tech and online community. It is now making the transition from the margin to the mainstream. For a number of months, the sector has attracted significant venture capital investment, and its exchange with offline currencies is growing more intense. Coinbase (an international 'digital wallet') sold $1 million worth of Bitcoins in February 2013.

Governments have struggled to respond to its rapid rise, and integrate it into existing monetary systems. The US Financial Crimes Enforcement Network has classified US 'Bitcoin miners' as Money Service Businesses, subject to regulation and legal obligations. In August, Germany accepted Bitcoin for tax and legal purposes. In December, Norway ruled it was subject to tax. Thailand has banned it, and China has banned its banks from dealing in it.

Crypto-currencies pose a number of challenges and opportunities for our online and offline worlds. In 2014, Demos will be conducting a project on the fuller implications of crypto-currencies, for business, consumers, law enforcement, financial services and more. In this short paper marking the beginning of that series, we set out what a Bitcoin is, how the currency operates, and some of the possible futures of digital currencies.

History

Bitcoin is now the best known crypto-currency, but it is not the first. In 1982 computer scientist David Chaum wrote a ground-breaking paper on the concept of a cryptologically secure digital currency. Chaum subsequently founded Digicash and developed E-cash, one of the first electronic money systems. However, the system failed, principally because it depended on existing credit card and government infrastructure. After Ecash, other electronic currencies such as 'bit gold', 'RPOW' and 'b-money' also tried and failed to replace fiat currency.

Bitcoin itself has a mysterious origin. The decentralised crypto-currency concept that forms the basis of Bitcoin was first described in an October 2008, published by an anonymous and enigmatic individual under the pseudonym "Satoshi Nakamoto". Bitcoin was further developed in an open-source project in 2009, and quickly developed a dedicated online community of users, investors, developers and supporters.

Unlike these early attempts, Bitcoin is the first crypto-currency to become widely adopted, both online and offline. As the Eurozone financial crisis began to bite around April 2013, and especially when accounts in Cyprus were threatened with painful 'haircuts', the mathematical rigour of cryptographical guarantees began to look like a more secure way to protect wealth than this form of Governmental, centrally controlled fiat.

Around that time, Bitcoin began to then radically increase in use, worth and prominence. It soon attracted significant venture capital investment, and its exchange with offline currencies grew more intense, and its value began to radically increase. However, Bitcoin was also closely associated with illicit activities: being the currency of choice for a number of online drugs market places, most infamously Silk Road. When Silk Road was subject to a series of FBI raids – and ultimately shut down in October 2013 – the value of Bitcoins fell, and some commentators believed this would seriously undermine the currency's future. However, soon afterwards the Department of Justice and the Securities and Exchange Commission told a US Senate Committee investigating the currency's risks and benefits that Bitcoin represents a legitimate financial service. The value of a single Bitcoin increased to $1,200 in early December 2012: a five-fold increase from six months earlier. It is now trading at between $800-1,000.[ii]

Authorities have now begun to react, and not entirely negatively. Although Thailand has banned their use, Germany has recognised it as a 'unit of account'. Ben Bernanke, the Chairman of the Federal Reserve has carefully said they 'may hold long-term promise' and a number of other organisations, from The Department of Justice, the FBI, even the Royal Mint, have begun to admit they are not intrinsically illegal.

How Bitcoin Works

Early digital currencies suffered from a number of problems. One of the most lethal was 'double spending'. Very little prevented the information that makes up a unit of digital currency being copied,

pasted and spent multiple times. The ease with which this could be done made fraud a major problem, and confidence in the currency impossible to sustain.

Bitcoin was able to overcome this problem in a unique manner. By distributing the transaction record - referred to as a ‘block chain’ - among its users, Bitcoin is able to ‘crowdsource’ fraud protection in a powerful and unique manner. Individuals dedicate part of their computer processing power to the verification of transaction records and in doing so contribute to crytopgraphical fraud prevention. By participating in this system, individuals generate new currency in a process known as ‘Bitcoin mining’; essentially, therefore, the process of anti-fraud development and the gradual and controlled release of currency into the Bitcoin economy are mutually supportive. Bitcoin mining today is an increasingly competitive business, with Bitcoin miners using massive, sophisticated computer rigs in order to mine coins.

This decentralised system, where the minting of digital coins, the regulation of the currency and the prevention of fraud is based on mass participation, makes Bitcoin independent from traditional financial mechanisms, or indeed any centralised control, in a way that other electronic cash systems never could be. Bitcoins are guaranteed by the quality of the confidence of its users, and stored in digital ‘Bitcoin wallets’ on personal computers. Bitcoins operate independent of any psychical location, government control, state-based regulation or oversight.

Yet the Bitcoin community has developed its own complex economic system. Bitcoin exchanges allow users to exchange Bitcoins for fiat currencies and vice versa. The Bitcoin Foundation lobbies on behalf of Bitcoin users, representing and promoting the nascent currency. While the development of Bitcoin as a day-to-day currency is still a relatively distant prospect, a latent probability rather than a certainty, its use as an investment commodity has been evolving quickly.

Philosophy of Bitcoin: a challenge to the status quo?

For some, Bitcoin is more than a currency, it is a political project. Crypto-currencies have emerged from a quite distinct internet community of cryptographers and cipher-punks, who follow a distinct philosophy – digital libertarianism – that holds the internet as a fragile opportunity to rise above our current system of nation-states to become autonomous, self-governing communities.

The 'fiat' of nation-states is therefore regarded as a blocking force for progress, and its many institutions – including currencies and the financial system - something to wrestle free of. Crypto-currencies – based on the free, consensual use of peer community and governed not by people but by mathematics – is a vital way to do this.

Consistent with this vision, some of the most savvy and longtime users of Bitcoin have, and will, continue to make it exempt from state control. It is possible they will build technologies and offer services like Bitcoin laundries that make it difficult for Bitcoin to be, whether through law, regulation or enforcement, accommodated within the financial systems that we have today.

Challenges and opportunities: politics, society and economy

Bitcoin is currently used more as a store of value – similar to a commodity like gold – than a way of buying and selling. But the possibility of secure, encrypted peer to peer currency at practically zero cost has potentially huge benefits for both consumers and business. For example, it could potentially insulate against international political instability such as the Eurozone crisis and political macroeconomic decisions, such as intentional devaluation. Above all, it provides almost free transaction costs. Buying something using a credit card can cost 3 even 5 per cent for the buyer, and sellers stump up merchant fees, usually around 2.75 per cent. In addition, it is computationally infeasible to counterfeit.

If Bitcoin steps over the threshold and begins to be used as a currency – starting with online purchasers and then migrating into the offline world, it will present increasingly difficult challeges to existing institutions. In our series exploring these opportunities and challenges, we consider the following to be critical to ensuring Bitcoin can become a source of individual and social good – for businesses, consumers and society – rather than for ill.

- **For individual consumers:** It has no basis in law, only in use – its value is only buttressed by its continual acceptance by an, up to now, relatively small community of users. So – how can you trust a currency that is not guaranteed by a government or backed by a central bank?

- **For business:** Bitcoin allows a user to bypass banks, and all the charges they levy. Transaction costs can be up to 3 per cent for smaller vendors even more. Bitcoin may simply be a very compelling value proposition for small merchants, although with still limited use, a volatile exchange rate, lack of regulatory clarity, use is also risky.

- **For banks:** Bitcoin poses a significant challenge to banks. Allowing large multinational corporations to globally transfer money cheaply, or even freely, could incentivise these organisations to operate largely outside of the traditional banking sector.

- **For money transfer:** According to the World Bank, international remittances cost an average of 9 per cent, often affecting the poorer parts of society the most. Bitcoin enables such international payments at a fraction of the cost. Furthermore, merchants accepting Bitcoin can do so from a wide range of international customers for very low cost, in contrast to more established payment networks. Bitcoin also makes possible new payment models, such as micropayments which are more difficult to implement with fiat currencies. One could imagine seamless per-second billing for video in place of

advertising, for example.

- **For the financial sector:** Integrating Bitcoin into the financial structure will be a major challenge. This will require industry and regulators to mutually agree upon a categorisation of Bitcoin. The way Bitcoin becomes a part of the financial landscape will depend largely on whether it is treated as a true currency, or as a potentially volatile and tradable commodity. This will also inform the regulatory and tax frameworks that apply to all crypto-currencies.

- **For central government:** Peer to peer currencies reduce the ability of central banks to manipulate the money supply; have significant implications for how to track illegal transactions, and may erode tax raising powers. The challenge for central government is how to ensure the currencies encourage innovation, business freedom, consumer choice, without losing control over key functions of the state.

Conclusion

The future may not be Bitcoin. Peercoin, Anoncoin, Zerocoin, Litecoin all bring different strengths and benefits, from privacy and anonymity to the efficiency of the transaction. In truth, no-one can be sure what will happen. The task now is to ensure that if crypto-currencies creep into our lives, they make them better; that they encourage innovation, business freedom, consumer choice, without undermining the key functions of the state; to promote basic social goods without washing this promising and fragile new asset away in a sea of regulation.

Demos – Licence to Publish

C If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works,You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

A By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:

i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;

ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

B except as expressly stated in this licence or otherwise agreed in writing or required by applicable law,the work is licenced on an 'as is'basis,without warranties of any kind, either express or implied including,without limitation,any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental,consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination

A This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence,however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.

B Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

A Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.

B If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

C No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

D This Licence constitutes the entire agreement between the parties with respect to the Work licensed here.There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You.This Licence may not be modified without the mutual written agreement of Demos and You.

NOTES

[i] https://www.youtube.com/watch?v=j2mdYX1nF_Y#!, accessed 27/11/13
[ii] https://gold.net/chart/currency/BTCUSD/, accessed 27/11/13