Cryptocurrencies and E-commerce

ADCOM 2017:
Annual Conference of the Advanced
Computing and Communications Society (ACCS)
International Institute of Information Technology, Bangalore

C.E.Veni Madhavan

Informatics Laboratory
Department of Computer Science and Automation
Indian Institute of Science, Bangalore

10 September 2017

Contents

1. Money, money - It's a Blockchain World
2. Science - cashstats, cryptonomics, cryptomath, cryptocurrencies
3. Engineering - Distributed Ledgers
4. Technology and Human Factors
5. Economics, Finance, Legislation, Jurisprudence
6. Sociology, Diplomacy, Polity
7. The CC, BC Mystery

1. Money, Money: It's a Blockchain World

- money, money, many monies
- ecash versus cryptocurrencies
- hashcash, primecoin, bitcoin, ethereum, litecoin
- digital signatures, ID-based signatures
- Our Proposal - VSKchains, VMcoins, APhashchains
- proof-of-work, proof-of-stake
- MY PROPOSAL: useful work - SUPW

2. Science - cashstats

- pre-paid instruments (PPI) : value (Rs 213B), volume (314 M) [2014-15] (YoY growth of 70%), [IAMAI, PCI with PwC - Disrupting cash- accelerating electronic payments]
- cost of currency operations - Rs 210 B
- India's preference for cash is high and persistent
- cash is persistent across the world - scale varies!
- of all consumer payments cash volume is from Indonesia (100%), India (98%), China (90%) to USA, UK (50%)
- of all consumer payments cash value is from Indonesia (70%) India (68%), China (45%) to USA, UK (12%)

2. (contd) Cashstats

- India GDP [Wikipedia article] (quite encouraging!)
- $ 2.454 T (Rs. 158.2) (nominal) $ 9.5 T (Rs. 609.3) (PPP) i.e., by PPP ($1 $= 64.13/3.87 =$ Rs. 16.6)
- per capita: $1850 (PPP $7160) $\simeq$ Rs 11670 p.a. *simeq* Rs 950 p.m (*thou shall not divide by infinity in India!*)
- Gini coefficient - 33.9% (is good because of the mathematics of integration!) (12.4% below poverty line $1.9 per day or Rs 121 p.d)
- fastest growing, service sector: 9.2% contributes to 53% of GDP (remaining agriculture 17%, industry 29%) (digitization of the economy has implications in these two sectors as well!)
- currency-to-GDP (India 10.6) China (9.1) , USA, UK, EU (8 to 4)

RBI Currency Statistics
(RBI Report: Sept 2013)

		1	2	5	10	20	50	100	500	1000	
coins	n (Bn)	36	22	11	1						
TOT											70 Bn
	v (Bn)	36	44	55	10						
TOT											145 Bn
notes	n (Bn)		5	7	25	3.8	3.5	14.4	11.7	4.3	
TOT											73 Bn
	v (Bn)		10	35	252	77	173	1442	5359	4299	
TOT											12 Tn

RBI Currency Statistics

(Status: Mar 2016)

		1	2	5	10	20	50	100	500	1000	
coins	n (Bn)	45	30	14	3.7						
TOT											93 Bn
	v (Bn)	45	59	70	37						
TOT											211 Bn
notes	n (Bn)		9	32	4.9	3.9	15.8	15.7	6.3		
TOT											87 Bn
	v (Bn)		45	320	98	194	1578	7854	6326		
TOT											16 Tn

(withdrawn currency: Nov 2016)

	n (Bn)							16.4	7.6		24.0 Bn
	v (Tn)							8.2	7.6		15.8 Tn

(takes a month to get 3 Bn notes!)

(an estimate of black cash: @10% of 20% of GDP is Rs 2.8 Tn!)

(currency returned by 10 Dec: Rs.12.44 Tn of estimated 15.8Tn)

(Jul 2017 estimate Rs 15.46 T of 15.8 T returned!!!)

FRB Currency Statistics
(Status: Mar 2016) (in $ Bn)

	1	2	5	10	20	50	100	500to1000	
notes n (Bn)									
TOT									38.1 Bn
v (Bn)	11.4	2.3	13.7	19.0	171.3	79.8	1082	0.3	
TOT									1.38 Tn

(growing at the rate of $0.1Tn every year since 2010 (faster than before)) (about 9% of GDP)

(expenses for cash operations $578 Mn - growing by about $ 8Mn every ear)

2. (contd) Cashstats

- Aug 29 2017, Bloomberg View
  Reports on Currency Death are greatly exaggerated : bloomberg.com
  (the central nervous system of global finance, since 1981)
  Individuals see paper currency as store of value, as hedge against financial crisis
  Fed Reserve Statistics
  \$1 bill $->$ \$11.7 B; CAGR 3.2%, well above 0.7% population growth
  Total transactional cash (ATM favorite \$20 bills), Dec 2016, \$308 B = \$1000/person
- Similar story holds in Europe (European Central Bank), even higher levels of cash in circulation.
  total transactional cash (E1 to E50) in circulation, Dec 2016, E 585 B (twice value in US), CAGR since 2010 is 7.6% (higher than US)
- cash is easy to make, difficult to manage!
  (MY CASE: ecash SHOULD be easier to make and manage - NOT like Bitcoins)

2. (contd) Cashstats

- (FedRes - note costs 12 cents to produce
  (RBI 31 Aug 2017 - note total cost R 93 B for 20 B notes of value R 12 T)
- consumer preference and NOT central Bank and "state" desiring to ban cash
- storing a few high denom cash is a hedge against crisis in low inflation states
- it is costly to handle cashless transactions
  (US gas stations woo customers by coming to the store to buy food/snacks to ward off the 2 to 5% charges from payments processors)
- Bitcoin genre indicates the desirability of holding store-of-value cash outside the traditional system similar to cash under mattress
  Transaction fees are still a problem
  (MY CASE: proof-of-work is costly to produce!!!)

2. (contd) Cashstats

- Demonetisation: Cash in Rs.2000 now exceeds Rs 1000 value in FY16
  March 2016 currency in circulation Rs 16.4 T, in March 2017 Rs 13.1 T
  Volume of currency goes up by 11 %, but value declined by 20 %
  Volume goes up from 90 B to 100 B and value comes down from 16.4T to 13.1 T
  This explains the cost of printing - 2016 - 2017 Rs 80 B compared to 34 B in 2 015-2016
- Rs 10, Rs 100 rose from 53% to 62%!, Rs 2000, 50% in total value!
  (SIMPLE - large volume of low denom; last year high denom notes were of 86% value, now it is 73%)
  (MY CASE: low denom ecash, for large volume of SVP)

2. (contd) Cashstats

- We skip the socio-political-economics of exercises, such as monetary cleansing, no-cash (to less-cash) steps viewed as "probable" solutions to the problems of
  (i) black wealth, (ii) fake currency (iii) suspicious transactions (iv) tax-net escape (v) societal corruption (v) financial non-inclusion
- (financial inclusion as goal for moving toward an equitable, just society is a great thing!)
  But, we should give the same access, facility, and ease of use for various financial products and services, such as, deposits, funds, insurance, besides direct subsidies and social security and health care, education)
  (MY CASE: Our ecash system can provide these features!!!)

2. (Contd.) Science - ecash, cryptonomics, cryptomath

- D.Chaum [CWI - 1984!], Brandt's cash
- ecash analogs of fiat cash
- hash chains with signatures on terminal coins
- withdrawal, spending, deposit protocols
- blind signatures, double-spending
- anonymity, privacy, fungibility, transferability
- mutual authentication, distributed operations
- implementations unsuccessful - world was not ready
- our earlier paper - transferable ecash [Indocrypt 2000] (cevmecash2000.pdf)
- our previous work - semi-distributed ecash [FIRST Project] (cevmfirstcoin.pdf)
- our recent paper - VSKchains [ADCOM 2017]

2. (Contd.) Science - Cryptocurrencies

- A.M.Antonopoulos, *Mastering Bitcoin: Unlocking digital cryptocurrencies*, O'Reilly, Shroff Publishers, Mumbai, 2015.
- bitcoin transaction - double entry book-keeping - debit-credit (passbook)
- payment or transfer and ownership is vouched by a digital signature
- posting into the ledger (mining) is by a proof-of-work process (mining or minting)
- all transactions transmitted to the bitcoin peer-to-peer network
- mining or posting into the distributed ledger or a system of blockchains is achieved by finding a prescribed hash value from a given value
- mining/minting/generation of proof:
  given a prescribed bit string
  $H =<< b_1, \ldots, b_k > || < b_{k+1}, \ldots, b_{256} >$,
  and beginning with a initial hash h_0, find a nonce x such that $\mathcal{H}(h_0 + x) = H$, for a hash function $\mathcal{H}$.

2. (Contd.) Science - Cryptocurrencies

- probability of finding the solution x, with a *good* hash function $\mathcal{H}$ is $2^{256-k}/2^{256} = 2^{-k} \Rightarrow$, the expected number of trials is 2^k.
- there does not seem to be any better way than, the naive, check the condition for all $i = 1, \ldots, x$
- finding a solution is exponentially hard, verification is poly bounded - the essence of all proof-of-work (one-way computable) functions and also the essence of cryptanalysis work vis-a-vis cryptosystem work
- many candidate problems can be used!
- architecture: keys, addresses, wallets; transactions; clients; network; the blockchain; mining and consensus
- alternative chains, applications; security

3. Engineering: Distributed Ledgers

- distributed databases
- clock synchronization
- crypto algorithms, keys
- central servers, networks
- blockchains as trust zones
- performance and service equity

4. Technology and Human Factors

- many natural applications
- user friendly, devices and interfaces
- coping with legacy systems - ERP, Databases

5. Economics, Finance, Legislation, Jurisprudence

- cash, coupon, card
- mint, vault, till, wallet
- fiat versus private currency
- float, seigniorage, valuation
- stocks, public coin offerings
- GDP (GNP, Gini coefficient),
- taxes (IT, GST), subsidies (DBT)
- exchanges, liabilities, insurance
- banking and fiscal regulations
- State and local fiduciary systems
- IT-Act, Regulation, Audit, Cyberlaws

6. Sociology, Diplomacy, Polity

- parity, exchange
- financial inclusion
- privacy versus security
- citizen, commerce and state
- cybercrimes and cyber-warfare
- digital threats and cyber-ethics
- employment, empowerment and welfare

if blockchains ran the world [The Economist, 15 July 2017]
(trust business, smart contracts, new-born an entry in a blockchain, identity registration, truth services, autonomous vehicles with financial autonomy, central bank issued cryptocurrency,
$\Rightarrow$
minimum to no government and maximum distributed governance!)

7. The CC, BC Mystery

Sequences of chunks of cryptocurrencies and blockchains,
are the ledgers of new kids of blocks from many terrains,
of fiscal transactional and ubiquitous informational data.
These new age chants of business and government cantata
need, for de-mystification, the academic computational refrains.

cevm
10 September, 2017