TALK: BLOCKCHAINS

ALAN BRACE

Contents

1. Orientation

(1) Keep **The Vision (TV)** in mind - verifiable electronic contracts (PKC) - open or encrypted - about transfer of assets (cash, houses, bonds, shares, dividends, margins) - contracts to be recorded, filed and secured in a public and distributed database (blockchains) - contracts to self-actuate transferring assets according to the contracts (in wind)
(2) **Why** did it all **start with Bitcoin**?? - Glib answer is because its easiest way to implement The Vision!! - inventor anonymous Satoshi Nakamoto - Aussie Craig Wright claims - but lot doubt exists - **NB** Bitcoin uses blockchains, but **blockchains ARE NOT Bitcoin**
(3) The Vision statement is cute - lot of wuffy mission statements out there - but whatever eventuates will involve PKC and blockchains - and probably much else besides
(4) A **blockchain** is a public database comprising blocks of (open or encrypted) contracts added **sequentially** with a timestamp in a **secured verifiable** fashion - blockchain **essential** to prevent **signature aging** i.e. cryptography now underlying signatures probably easy to crack in a hundred years
(5) Participants can be **declared and legal** with blocks added by the **permission** of a regulated legally established central **exchange** (relevant to NAB) - **OR** - participants can be **anonymous** with blocks added in a **distributed** fashion by **consensus** among participants (Bitcoin) - hot with academics, anarchists, drug dealers etc
(6) **Assets** can be **off-chain** (like houses, bonds, shares) - regulated, legal constraints - suited permissioned blockchain (this would be NAB) - **OR** - **assets** (cash) can be **on chain** (like Bitcoin) - light regulation - suited distributed blockchain
(7) There is a lot of debate going on around blockchains - spurred by at least $600M venture capital - so its definitely going somewhere - author reckons gonna be important technology - revolutionary, disruptive (like browser to internet) - **merits serious attention**
(8) Good book on bitcoin is [1] - written at good level - info on how bitcoin works without getting totally bogged down in detail

Date: Wed 8 June 2016 *Email*: alan.brace@nab.com.au.

2. Hash functions

Hashes used in signatures - secure blockchains - stop spam emails - stop website being overwhelmed - plus many other uses! - here's how

2.1. **Byzantine Generals problem.** Five generals A,B,C,D,E each with 100 men face the enemy Z with 300 men

(1) General A prepares line-1 *"attack at 10.00"* of a message and sends to B
(2) General B agrees and adds line-2 *"attack at 10.00"* to message and gives to C
(3) Traitor C changes lines-1&2 adds line-3 all to *"attack at 8.00"* and gives to D
(4) General D agrees adding line-4 *"attack at 8.00"* to message and gives to E

Result D&E attack at 8.00, get wiped out, then C+Z wipe out A&B - how to avoid???

2.2. **Proof-of-work solves the problem.** Don't write one line messages - use skilled artist to sketch a portrait of General A with *"attack at 10.00"* woven in and repeated many times - hard to do and must complete in 10 minutes - General B then adds his portrait with *"attack at 10.00"* similarly woven in and has to do it in 10 minutes - now traitor C has to duplicate portraits of A,B and add himself C with *"attack at 8.00"* woven into all 3 but can't do all that in 10 minutes

2.3. **Definition hash function.** To secure blockchains we use hash functions for proof-of-work - a **hash function** takes a message of any length and produces a fixed length *digest* or *fingerprint* of that message - the standard hash function designed by NSA and published by NIST in 2001 is SHA256, it produces a 256-bit hash (Bitcoin applies SHA256 twice) - properties include

(1) One-way function - if $H(x) = y$ then can't find x from y - but many x go to y and they evenly and seemingly randomly distributed
(2) Slight change in x gives totally different y
(3) Weak collision resistance - given $H(x) = y$ not easy find $H(x_1) = y$
(4) Strong collision resistance - not easy find any x_1 and x_2 with $H(x_1) = H(x_2)$

E.g. no weak collision resistance - Alice sends x to Bob signed with $d(H(x))$ i.e. $\langle x, d(H(x))\rangle$ - Oscar intercepts and replaces with $\langle x_1, d(H(x))\rangle$ - Bob takes as legitimate

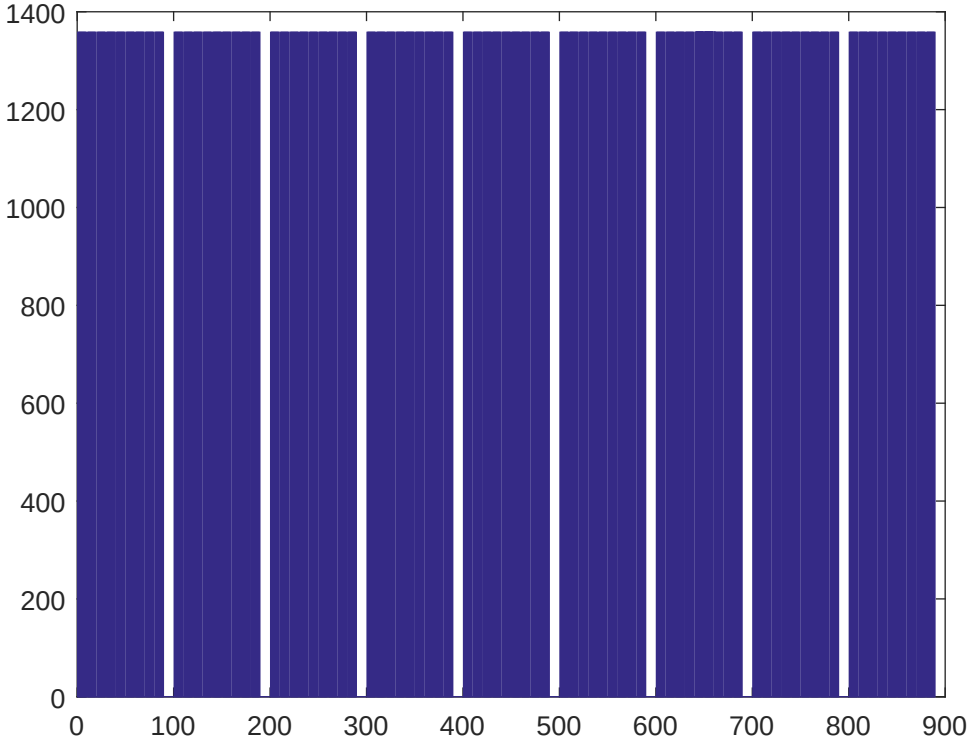
2.4. **Toy hash function.**

Divide message number by 9 three times and put remainders in order

$$9/48973 = 5441 + 4, \quad 9/5441 = 604 + 5, \quad 9/604 = 67 + 1$$

$$H(48973) = 154 \qquad \text{also} \qquad H(49702) = 154 \qquad \text{but} \qquad H(49973) = 485$$

Even distribution of $H(x)$ for messages x ranging over 10000 to 999999 - hash $H(x)$ hits every number between 0 and 888 without a 9 same number 1358 times



Hard go back - but no collision resistance (hey, its a toy hash!)
For **proof of work** - find a **nonce** such that $H(48973 + nonce) = 7$ - search by incrementing from 1, the first $nonce = 606$ giving

$$H(48973 + 606) = H(49579) = 7$$

3. BitCoin

3.1. **Roughly how it works.**

(1) The assets i.e. bitcoins $\mathcal{B}$ are all on-chain, were always on-chain, will always be on-chain - they now **mined** at rate of $\mathcal{B}25$ for each block added to the blockchain to reward **miner** who produced latest block - every valid $\mathcal{B}$ got a *paper trail* through transactions from when mined to now - else *lost*
(2) Now about $\mathcal{B}14M$ on chain - $1M$ to $2M$ users - 5580 active mining **nodes** (1854 in US, 789 Germany, 242 UK, 100 in Oz, 94 China, rest spread around world) - 25 people own 25% of all bitcoin - 75% of bitcoin is inactive - total **hash rate** (mining power) of all nodes now about $30,000TH/sec$ - ATO says bitcoin like barter so **no GST** but **subject** to capital gain tax **CGT**
(3) Alice gets a bitcoin **wallet** app on her iPad - wallet **key-generator** produces a **public key** e with corresponding **private key** d - note $\mathcal{B}$ uses ECC elliptic curve cryptography - wallet also hashes out a **public address** $a = H(e)$ from her public key - wallet automates much of this - warning!! lose iPad, lose wallet, lose $\mathcal{B}$ with no legal recourse - best spread around

(4) Alice goes to bitcoin exchange to get $\mathcal{B}100$ - forks out $\$50k$ (problem!! exchange gotta pay CGT in Oz so not many here) - exchange executes a transaction sending $\mathcal{B}100$ to her address a - bitcoin is then **'stored' at that address** a - Alice must unlock with her private key d before she can spend it

(5) Alice gonna buy car worth $\mathcal{B}100$ from Bob - she (or her wallet) constructs a message x concatenating $\oplus$ the public address a where her $\mathcal{B}100$ is stored, her public key e and an instruction sending $\mathcal{B}100$ to Bob's address b

$$x = a \oplus e \oplus 100 \oplus b$$

She then hashes x, signs with $d(H(x))$ and sends the whole transaction $\langle x, d(H(x))\rangle$ to the *nearest* **mining node** - Bob **does not yet give Alice the car keys**

(6) Node checks the transaction - is the signature valid $e(d(H(x))) = H(x)$?? - is the address Alice's $H(e) = a$?? - does the address a contain enough funds?? i.e. does a previous valid transaction stored on the blockchain send at least $\mathcal{B}100$ to a?? - if transaction valid, node sends it to all the other nodes - takes about 10 seconds to propagate

(7) Each node concatenates the group G of valid transactions accumulated over the past 10 minutes (queued while mining previous block B_0) - adds a hash $H(B_0)$ of the previous block (plus timestamp, to lock it sequentially in the blockchain) - adds a **nonce** N (*number only once*) - and then hashes the lot with SHA256 to give a 256-bit Z like

$$H\{G \oplus H(B_0) \oplus N\} = Z$$

(8) The nodes then **vary the nonce** N (sequentially, randomly, whatever) until a nonce N_1 is found that gets Z under a target T like

$$Z < T = 0000000000000006e1163.....$$

On account the way a hash is constructed, finding N_1 is just brute force and depends mostly on computer power - the target T constantly adjusted to ensure process takes 10 mins

(9) **First node to solve** collects $\mathcal{B}25 \approxeq \$12,500$ reward - that's $\$1.8M$ a day, so attracts miners - and adds the next block B_1 in the blockchain constructed as

$$B_1 = \langle G + H(B_0) + N_1, \quad H\{G \oplus H(B_0) \oplus N_1\}\rangle$$

i.e transaction, hash previous block, nonce, and hash of the lot

(10) Then all nodes go on to the next block B_2, and so on - anyone wanting to alter a contract in G has to rehash B_1 and also keep up with hashing the next block B_2 - **certification through proof-of-work**

(11) If two nodes solve simultaneously, have got a **bifurcation** - two branches to blockchain - miners take their pick and mine a next block - the branch that adds the next block first, will be the branch all other nodes will follow (or they waste time and effort) - contracts in the discarded **orphan** block are broken out and recycled into a later block

(12) Bob waits until transaction **confirmed** i.e. transaction with Alice included in block B_1 and then hands over car keys - if he very careful, he might wait for half-an-hour and confirmation of a few blocks B_1, B_2, B_3 - then zero chance changing B_1

3.2. **Double spending and 51% attack.**

(1) Long ago Oscar bought lots of $\mathcal{B}$ when they were \$0.10 each - in his malevolent old age he sets himself up in a mining node with a super super computer that has more hashing power than all other nodes combined - so he can be sure of being able to mine the next block first
(2) He blows $\mathcal{B}10,000$ on a private plane - the transaction T_1 is verified and added to the pending group of transactions G_1 - the vendor waits for confirmation through inclusion of $T_1 \in G_1$ in the next block B_1 before letting Oscar take off
(3) Oscar simultaneously mines $G_1 \setminus T_1$ i.e. G_1 without T_1 as $B_1^*$and has it ready (he can always get there first) when the other node mines G_1 including T_1 as B_1
(4) Oscar releases B_1^* as an alternative to B_1 creating a bifurcation in the blockchain - recall that the branch of the bifurcation to be followed depends on which branch adds the next block first, and Oscar can mine fastest
(5) Oscar now mines B_2^* from pending group G_2 fastest, and while that is happening blows $\mathcal{B}10,000$ on diamonds sending this transaction T_3 to his node where it will be verified for inclusion in the pending group G_3^* following the bifurcation B_1^* because along this chain the $\mathcal{B}10,000$ is still available to be spent
(6) Once B_2^* is mined, confirming the $*$ branch as the one to follow, Oscar then presses on to mine B_3^* from G_3^* (with the diamond trade T_3) - all other nodes also switch to mining G_3^* following on from B_2^* but Oscar gets to B_3^* first
(7) With the diamond purchase T_3 confirmed in B_3^* Oscar takes the diamonds and gives them to his girlfriend
(8) While B_3^* is being mined, unbooked transactions in the orphaned block B_1 like the plane purchase T_1 are now broken out and added to pending transactions G_4 - but T_1 is not now verified because the $\mathcal{B}10,000$ has been spent in T_3 as documented in B_3^*
(9) Oscar has **double spent** and the plane vendor is unhappy!!

It is not likely that any one miner can acquire 51% of the network hash power - but **mining pools** (i.e. a cooperating group of nodes) can and have done so - it is this uncertainty (and the potential for anonymity) that makes distributed blockchains unsuitable for bank use

4. BlockChain Miscellaneous

4.1. **FOR BANKS.** Transparency, certainty, need to know customer, off-chain assets all point to banks needing permissioned blockchains - if permissioning exchange *nuked* (hacked, sabotaged), can default to distributed blockchain - contracts need be written cover that default?? - need research between scripting language for contracts and legal interpretation - scripting language should be *Turing complete* i.e. capable of reproducing any programming language??? - bitcoin script not Turing complete, not got loops to avoid somebody crashing with infinite loop - how to contracts deal with off-chain assets?? role and scope of exchange?? - how can self-actuating contracts interact with off-chain assets??

R3 CORDA [2] worth reading as system aimed at banks - got some practical ideas - they say they different because

(1) Not build a blockchain - starting point is what matters for banks is individual agreements between firms - reject notion everything be copied to everybody even if encrypted
(2) Focus is on agreements and how to link with legal prose

(3) Take account of reality managing financial agreements - easy write business logic - integrate existing systems and how banks presently choreograph arrangements

4.2. **DTCC & REPOS.** See [3, 4, 5, 6, 7] - Depository Trust & Clearing Corp. (DTCC) - firm at center Wall Street's trading infrastructure, about launch test of blockchain technology, see can provide workable solutions for $2.6 trillion repo market - regulators require clearing members of DTCC contribute $50 billion to liquidity facility CCLF - repos done overnight, often repeated, clearing both legs not super fast - e.g someone does same transaction two days in a row, when first trade comes should be able to offset it against new trade, can only do that if have intra-day netting, which current technology not allow - blockchains could reduce amount of liquidity needed because help DTCC maximize netting of overnight repos reduce risks - not lot detailed info but permissioned blockchains favored (WSJ & Risk)

4.3. **DRUG PROTOCOLS.** Google ¡economist better with bitcoin¿ - In pharmaceutical industry selective reporting of data from trials is rife - how to guard against such things - researcher Dr Irving at Cambridge came up with way to improve reporting of clinical trials using bitcoin - US drugs regulator require all clinical trials registered - Dr Irving saved copy study protocol to text file - then hashed file using SHA256 - then used as private key in bitcoin - his wallet produce corresponding public key - then transferred small sum bitcoin to another wallet - the transaction, public key, time-stamp all entered on bitcoin blockchain - anyone with copy protocol able reproduce steps and check get same public key - prove copy of protocol matched original - reckon stop "hidden outcome switching", practice of secretly changing focus of a clinical trial to fit results

4.4. **IBM DREAMER.** Jerry Cuomo IBM Fellow testifying before U.S. House of Representatives' Energy and Commerce Subcommittee on Commerce, Manufacturing & Trade - see [8]

"Take the U.S. Social Security system, for instance. It involves the federal government, millions of employers, their payroll service providers, and more than 200 million beneficiaries and working individuals who are paying into the system. This is a model scenario for blockchain. There are many parties, many rules, many steps in the process of administering the system, and a critical need for very high levels of privacy protection and security from breaches"

Great sentiments - little info

4.5. **MORINI.** See [9] - Morini gives his take on blockchains and financial derivatives

Imagine a derivatives contract that could value itself in real time, automatically calculate and perform margin payments, and even terminate itself in the event of a counterparty default. Though it sounds like science fiction, it may soon be a reality. The technological advances behind cryptocurrencies such as bitcoin, which combine novel applications of cryptography with the computer science of consensus algorithms for distributed networks, can be used to create these 'smart' derivatives, eliminating many of the operational complexities found in today's over-the-counter market. e.g. High-frequency collateral flows will dramatically reduce credit risk between counterparties, as well as the amount of required initial margin.

4.6. **STANDARDIZATION.** See [10] - soon see different blockchains, different blockchain companies, banks using different blockchains - important have common protocol, so can communicate - as the technology evolves, there won't be one blockchain for everything - be like markets and exchanges and depositories - blockchain ecosystems will be created that must work together and

live together, with assets that are moved across these ecosystems - so development of a protocol and a set of standards becoming the main topic of discussion at industry events and conferences

References

[1] Franco P (2015) Understanding Bitcoin: Cryptography, Engineering and Economics, Wiley ISBN 978-111-901-916-9 (available on Kindle)
[2] Introducing R3 Corda a Distributed Ledger Designed for Financial Services (May 2016) WeekendRead
[3] DTCC and Digital Asset Holding test BlockChains fo the Repo Market (Mar 2016) BitcoinMagazine
[4] DTCC Bets on BlockChain to Slash CCP Liquidity Needs (April 2016) Risk Magazine
[5] DTCC to use Digital Asset Tech for BlockChain PostTrade Trial (May 2016) CoinDesk
[6] Options to Build BlockChain Technology IBM DTCC SWIFT(Feb 2016) BitcoinMagazine
[7] Why Wall Stree is Embracing the BlockChain (Feb 2016) Wired
[8] How Business and Governments can Capitalise on BlockChain (Mar 2016) Forbes
[9] Morini M, Sams R (May 2016) Smart Derivatives can Cure XVA Headaches, Risk
[10] Standards Crucial to Future of BlockChain (May 2016) WatersTechnology