What’s in the Blocks?
Can we really use the blockchain for identity?

David G.W. Birch
Keynote Presentation, EEMA (London, July 2017)
David G.W. Birch

Global thought leader in digital identity and digital money;
Global top 15 favourite sources of business information (Wired);
London FinTech Top 10 most influential commentators (City A.M.);
Top 20 Fintech Influencer (JAX London);
Top five Leaders in IDentity (Rise);
Top 10 Twitter accounts followed by innovators, along with Bill Gates and Richard Branson (PR Daily);
Top 10 most influential voices in banking (Financial Brand);
Top 50 blockchain insider (Richtopia);
Europe’s most influential commentator on emerging payments (Total Payments).
Available at all good bookshops…
There are real problems out there and it would be good to use new technology to fix them
What can the blockchain do for us?

Because… Blockchain!
Finance Industry

Blockchain to become ‘beating heart’ of global financial system

More than 90 central banks considering using bitcoin software, says report

Charlie Taylor

Swift has launched a proof of concept (PoC) to explore whether blockchain/distributed ledger technology (DLT) can be used by banks to improve the reconciliation of their nostro databases in real time.

Under the current correspondent banking model, Swift says banks need to monitor the funds in their overseas accounts via debit and credit updates and end-of-day statements. The maintenance and operational work involved represents a “significant portion of the cost” of making cross-border payments. This PoC will test whether distributed ledgers may be able to help banks reconcile those nostro accounts “more efficiently and in real time, lowering costs and operational risk”.

As part of Swift’s global payments innovation (GPI) initiative, which seeks to deliver a “new standard” in cross-border payments, the new PoC was scoped in collaboration with “leading” correspondent banks. Swift GPI member banks can apply to participate in this PoC, set to launch in early 2017.

According to the study, blockchain technology could lead to lower fees for consumers, improved regulatory oversight and better preparedness against financial bubbles.

The blockchain is the solution to our problems

No Poverty

Blockchain-based systems will lower the barrier to entry to the global financial system. According to the UN and the ID2020 project, currently 2.5 billion people lack identity in a way that allows them access to financial and government services. M-Pesa is an example of a digital platform that enables people without such access to claim a financial identity. It was quickly adopted in Kenya because of the vacuum there for government-provided identity.
Every Industry

In fact, it’s the solution to most industries’ problems
Example: Supply Chain

How The Salad Oil Swindle Of 1963 Nearly Crippled The NYSE

Health warning over boom in fake Viagra pills bought online after more than £11m of counterfeit and unlicensed pills are seized in a year

- Britain being flooded with dangerous fake Viagra pills from criminal gangs
- Gangs exploiting a growing market for cheap online drugs that can be fatal
- Officials seized more than £11m of counterfeit treatments in last 12 months
- That is three times value of erectile dysfunction drugs seized year before

Texas. The assassination not shocked the nation, but shook stock market as well. However, very few people have heard of The Great Salad Oil Swindle which nearly crippled the New York Stock Exchange that

The blockchain will keep meat out of burgers or something like that
I'm forming “Evil Geniuses for Blockchain” If any of you want to join me
What’s wrong with DB2?
It was good enough for my father and his father before him

There are reasons to use shared ledger even a double-permissioned ledger with known participants and central co-ordination

Why Use a Shared Ledger?
Wait, What is a “Blockchain”? 

Yes, I know it’s wrong but hey it’s the Financial Times
Consensus Computers

How can we animate the immutable record so that events trigger actions?

How do we agree the immutable record of transactions?

What kinds of assets will be in the transactions?

Which entities create and propagate transactions?

A different way of thinking
RBS fined £56m over 'unacceptable' computer failure

© 20 November 2014 | Business

Bank of England payment system crashes leaving homebuyers in limbo

Bank apologises for failure of system used for large transfers as governor Mark Carney orders urgent investigation

Royal Bank of Scotland (RBS) has been fined £56m by regulators after a 2012 software issue left millions of customers unable to access accounts.
Content: Innovation

What’s in the blocks?

- hashes of data
- data
- encrypted data
- proofs about data

What’s in the Blocks?
Why is it in the Blocks?

- time stamping
- global consensus
- coordination within trust group
- auditable privacy

with acknowledgement to Maya Zahavi, QED-it
Consensus: Integrity

Recommenations to the Group of 20
February 2010

And then it happened. For over a week, there had been a run on the assets of three structured investment vehicles (SIVs) of BNP Paribas. The run was so severe that on August 9, BNP Paribas had to suspend redemptions. This event informed investors that the asset-backed commercial papers (ABCPs) and SIVs were not necessarily safe short-term vehicles. Instead, these conduits were supported by subprime and other questionable credit quality assets, which had essentially lost their liquidity or resale options.

BNP Paribas’ announcement caused the asset-backed commercial paper market to freeze, an event that most succinctly highlights the next major step to a financial crisis, namely the lack of transparency and resulting counterparty risk concerns.

Consider the conduits of BNP Paribas. For several years, there had been huge growth in the development of structured products, ABCPs and SIVs being just two examples. However, once pricing was called into question as subprime mortgages defaulted, the conduit market faced:

Lessons from the Last Financial Crisis
I the Future Role of Institutional Investors

by Lars Rohde

The dynamics of the financial crisis were driven by underpricing of risk and lack of transparency, which led to a loss of confidence when the bubble finally burst. Massive government interventions that caused a permanent transfer of losses to the public sector as well as sovereign-debt crises that may involve painful solutions. Letting banks fail is a necessary disciplinary factor, but it requires a well-defined “game plan” which did not exist in the crisis. Regulatory reforms underway aim at restoring confidence, but they may hamper the institutional into perhaps even deeper developments. It is important to further these go transparent bond initiatives for private-public sector cooperation.

JEL Classification: G21

Keywords: Financial institutions, long-term
"Contracts" are just software – that’s why they are so flexible
Shared Ledgers

Can anyone use the ledger?

Yes
- anyone can use it

No
- only a selected group

why do they maintain the integrity?

They are given rewards on the ledger itself
- double permissionless

They are given incentives off the ledger
- permissionless

who maintains the integrity?

All group members
- permissioned

Privileged group members
- double permissioned

Public Shared Ledgers

Private Shared Ledgers

Stuff like Bitcoin

Stuff like R3
The Identity of Things in General

Things as consensus applications running on a consensus computer
Reputation of things as proofs stored by those applications
Can You Trust My Things?

Decentralized Blacklistable Anonymous Credentials with Reputation

Rupeng Yang$^{1,2}$ *, Man Ho Au$^2$ **, Qiuliang Xu$^1$ **, and Zuoxia Yu$^2$

1 School of Computer Science and Technology, Shandong University, Jinan, 250101, China
orbbyrp@gmail.com, xql@sdu.edu.cn
2 Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong
csallen@comp.polyu.edu.hk. zuoxia.yu@gmail.com

Abstract. Blacklistable anonymous credential systems provide service providers with a way to authenticate users according to their historical behaviors, while guaranteeing that all users can access services in an anonymous and unlinkable manner, thus are potentially useful in practice. Traditionally, to protect services from illegal access, the credential issuer, which completes the registration with users, must be trusted by the service provider. However, in practice, this trust assumption is usually unsatisfied. Besides, to better evaluate users, it is desired to use blacklists, which record historical behaviors of users, of other service providers, but currently, this will threaten the security unless a strong trust assumption is made. Another potential security issue in current

Maybe, just maybe, shared ledger technology can help you
OK, so it’s not just me….

JPMorgan taps Zcash privacy feature for blockchain platform

J.P. Morgan Taps Zcash to Add Security to Quorum Blockchain Platform

Press release: Zero-knowledge Security Layer to be Added to Quorum Blockchain Platform

There are some genuinely new ways to do things
Case Study: Salad Days

- Translucent transactions and ambient accountability
Can we use the blockchain for identity?

Yes, depending on what you mean by identity
(and depending on what you mean by a blockchain)
in the future, everyone will be famous for fifteen megabytyes

engage dgwbirch limited
post 1 Armadale Road, Woking, Surrey GU21 3LB, UK
call +44 7850 863168
contact mail@dgwbirch.com
visit www.dgwbirch.com
follow @dgwbirch
comment blog.dgwbirch.com
connect https://www.linkedin.com/in/dgwbirch/
order amazon.co.uk “Before Babylon, Beyond Bitcoin”