

FIA Operations Americas Webinar:

Efficient technology, not disruptive technology

An Introduction to Bitcoin, Blockchain, Ledger Technology, and potential implementation in Listed/Cleared Derivatives

Nick Solinger, President, FIA Tech

Ray Kahn, Managing Director, Barclays

June 22, 2016



The next big thing?

Tremendous media coverage about Bitcoin, Blockchain and Ledgers. What is it?

“It’s a cost saving device, it’s an error reducing device. ... The post trade processing of financial services really hasn’t been revolutionized in any meaningful sense in decades ”

- Blythe Masters, CEO of Digital Asset Holdings

“The great promise of distributed ledgers for central banks is their potential to enhance resilience”

- Mark Carney, Governor of Bank of England

“Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value”

- Eric Schmidt, CEO of Google

“I am a big believer in the ability of blockchain technology to effect fundamental change in the infrastructure of the financial industry”

- Bob Greifeld, CEO of Nasdaq



Topics

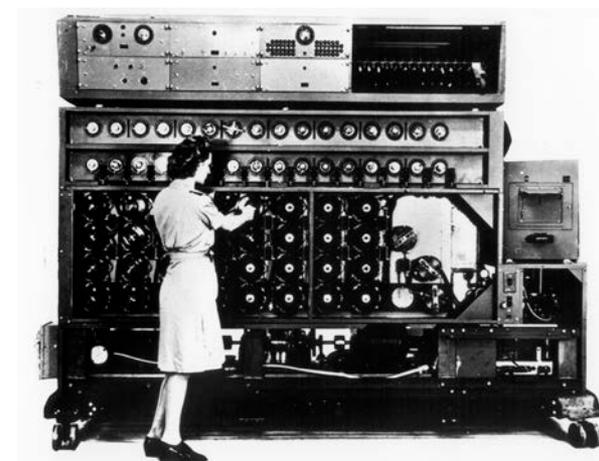
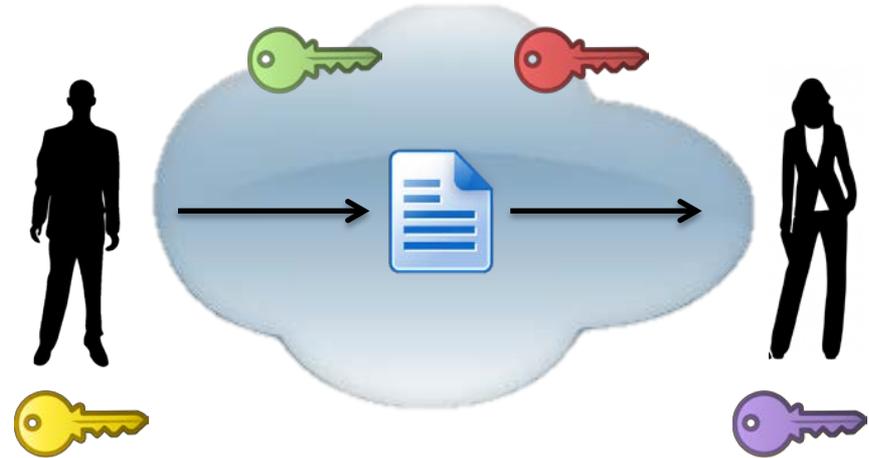
- **Overview of bitcoin and the technologies it has inspired**
- **How bitcoin-inspired technologies are being used**
- **How it may be introduced in Futures/Clearing**
- **Q&A**

Bitcoin History



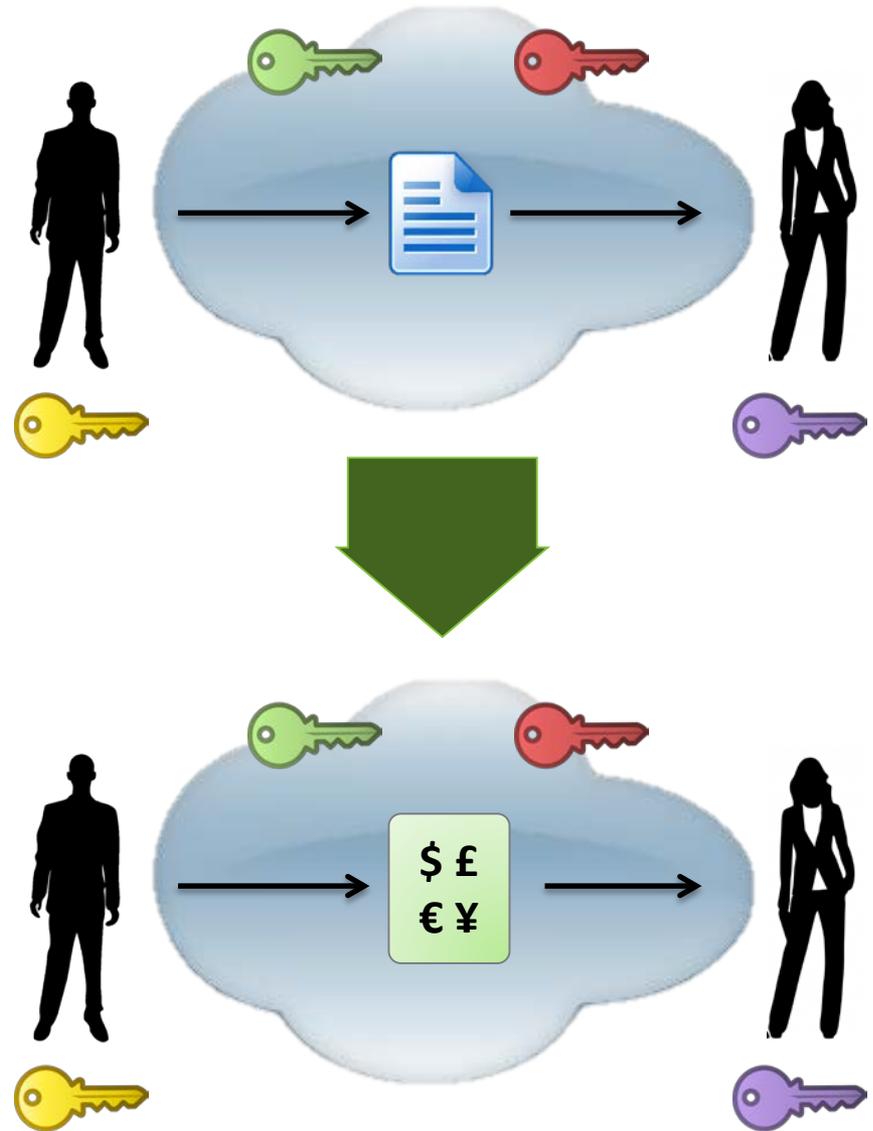
Bitcoin Origins: Cryptography

- Post-war US and UK Intelligence agencies wanted codes which didn't require sharing passkeys in advance
- Public key cryptography was ultimately born
 - Invented by UK intelligence staff in the early 1970s and shared with NSA
- Publicly invented by RSA in the US in the 1970s



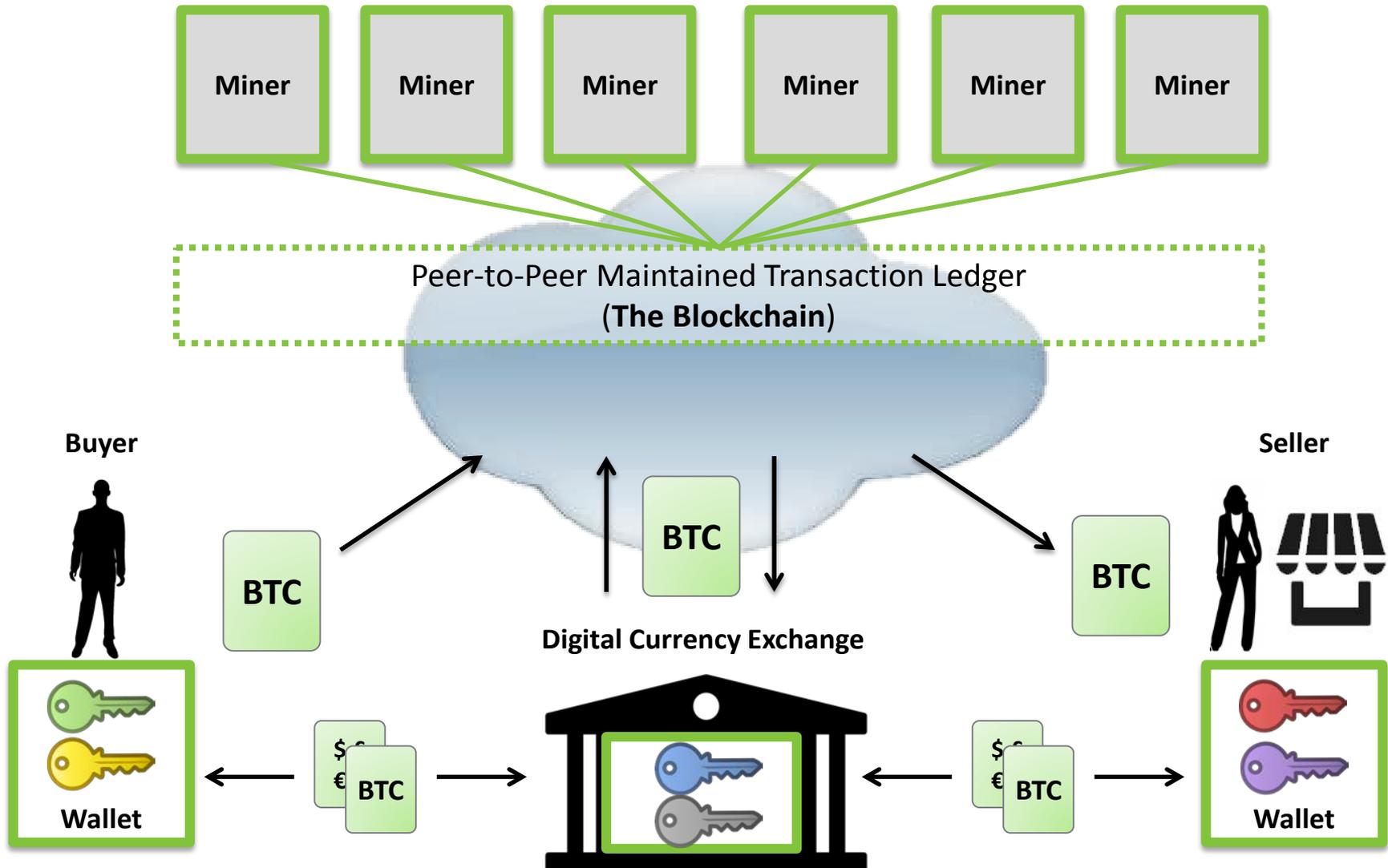
The search for a crypto-currency

- Multiple attempts were made to “invent” a digital payments or currency scheme using cryptography
- In 2008, Bitcoin whitepaper released
 - Incorporated much of the earlier work
 - Packaged it all together in a practical way



Bitcoin Ecosystem & Architecture

Bitcoin Ecosystem



Key elements of the Bitcoin invention

- Open source software vs. the public bitcoin network
 - Related but different things entirely!
- Distributed ledger maintained in the cloud (Blockchain)
 - *Can store any type of data or records*
- Peer-to-peer transaction protocol
 - *Could be used for anything – and is!*
- Model for transaction verification without trusted intermediaries
 - *Transactions cannot be forged or duplicated*
 - *Verification using consensus models and by tracking chain-of-custody*
 - *Doesn't require trusted intermediaries, but can work with them*
 - *Bitcoin mining was only one example, there are already others*
- Exchange of virtual for physical at endpoints (Exchanges)
 - *Ledgers can interoperate with existing trading, clearing and settlement infrastructures in a range of models –*

Potential Implementations



Bitcoin-inspired technologies

- In the institutional and regulated space, private/permissioned ledgers are the focus (DLT)
- Trading, processing and clearing of securities and derivatives are key areas of focus
- Wide range of firms exploring the application of bitcoin-derived technologies.

Bitcoin

Public Ledger



Anonymous
Miners verify
consensus



Replace/disrupt
existing currency
and payments



Simple
Transactions



DLT

Private or
Permissioned
Ledgers

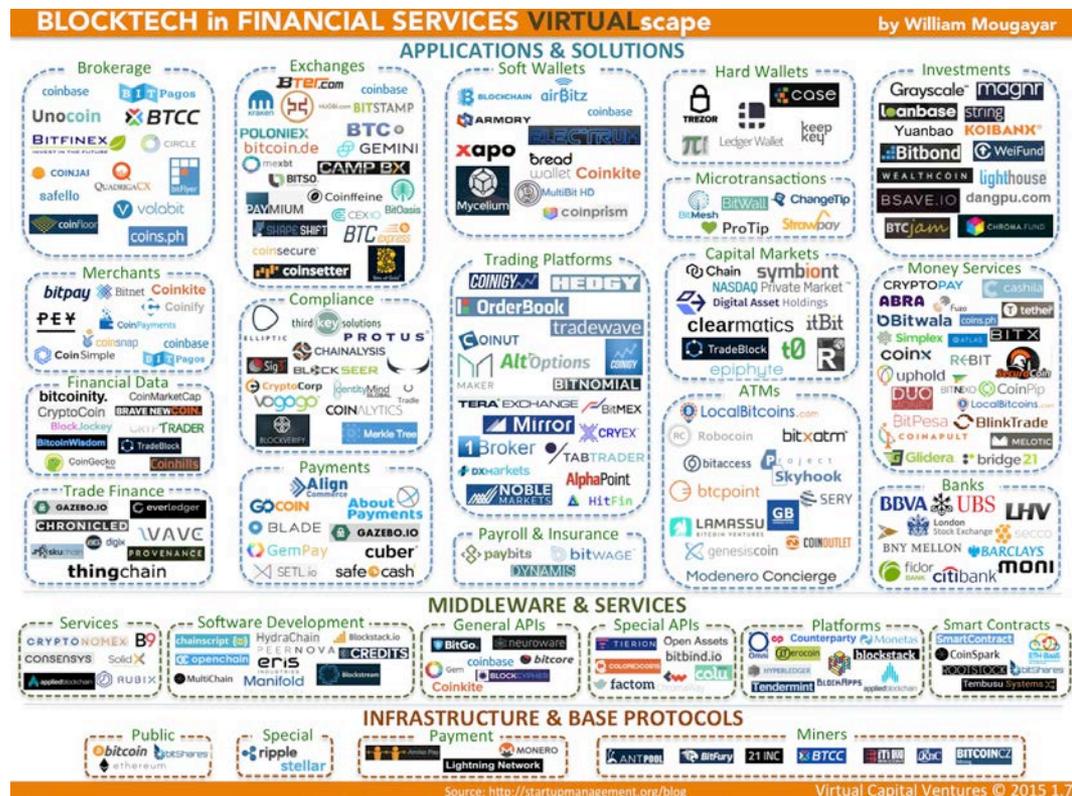
Systems tailored
to use case, with
trusted parties

Interoperate with
existing payment
models and
currencies

Smart
Contracts

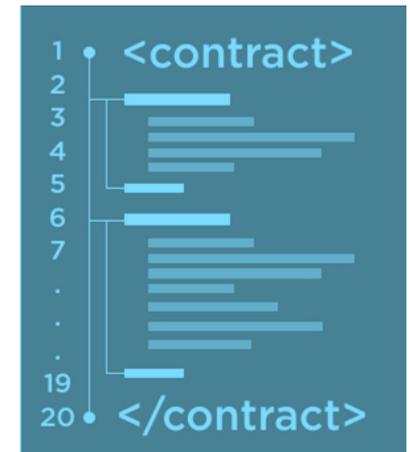
Ledger Technology

- Hundreds of firms (Over 250 according to Crunchbase)
- Testing Ledgers in use cases like post-trade notifications, matching and other transaction lifecycle events
- Complex transactions *could* effect clearing, settlement or record the actual movement of financial instruments, payments or risk
- Firms are experimenting and driving the technology closer and closer to reality every day.
- Better known firms: R3. DAH. Ripple. Axoni. Circle. Chain.com



Smart Contracts

- *If the Ledger is the Operating System, these are the Apps*
- Bitcoin transactions were simple payments, but the transaction protocol allows for more complex transactions and processes: **Smart Contracts**
- The 'Ledger' keeps the historical record of transactions, but if the transactions are Smart Contracts, they can automatically spawn future events/transactions
- Examples:
 - If a payment is missed, revert ownership
 - If terms are met, trigger an exercise of an option
- Firms are looking at using Smart Contracts to model everything from terms of derivatives and securities to post-trade processes and lifecycle events on trades



Landscape for Listed/Cleared Derivatives

Digital Post Trade Process

Fully Open Future State

- Owner Agnostic Network
- Anonymous
- Open Source
- Smart Contract based

Digital Payments

“Virtual Digital Currencies (Bitcoin, Ether, etc.) *
“Fiat Digital Currencies (Fedcoin, BOEcoin, etc.)**

* presently non-regulated network with limited recourse
** central bank issued digital currencies conceptual & a subject for more research

Institutional Post Trade Process

Potential Future State

- Standardized
- Industry Controlled
- Permission Layer

Process Efficiencies
(Improved ledger process)

Current State

- Decentralized
- Bilateral
- Firm Specific

Traditional Institutional Payments

Improved Payment Infrastructure
Improved Security
Improved protocols and time

Payment Efficiencies
(Improved payment rails)

Traditional Currencies (G-20 & beyond)
Existing Bank Payment Infrastructure
Bilateral Payment Protocols (SWIFT etc.)

Example use cases

Focus Areas	Potential Efficiencies
Standardized contracts	Standardization of data structure and terms. Futures requires improved symbology & reference data for post-trade efficiency
Record keeping & Reporting	Rather than execution, clearing, client and CCP all maintaining separate records, opportunity to use ledgers as golden source(s)
Regulatory transparency	Golden source data could also be used to satisfy regulatory reporting obligations more easily
Risk management	Ledger paradigm ensures chain of custody and improved access to real-time data for reporting, monitoring and limit checking
Payment rails	Improved payment applications would allow money to move more efficiently between existing regulated market participants
<i>Clearing and settlement</i>	<i>By starting with the practical, the industry would evolve toward more efficient paradigms for clearing and settlement</i>

Vast potential, but caveat emptor

Ledger Technology and Smart Contracts are very generic new technologies



They will be applied to a vast range of problems – from the mundane to the transformational

The pace of innovation is increasing – more firms, labs, projects, consortia every week



Not all will succeed. Adoption dynamics will begin to be more important than tech

Like with many exciting new technologies, it will happen fast, but take longer than many hope



Fully vetting new technology in regulated/institutional sectors is a high bar

Q&A SESSION

