Bitcoin, Blockchain and Cryptoledger

Dexter Senft
(dexter.senft@morganstanley.com)

September, 2015

THIS IS SALES AND TRADING COMMENTARY PREPARED FOR INSTITUTIONAL INVESTORS; it is NOT a research report; tax, legal, financial, or accounting advice; or an official confirm. The views of the author may differ from others at MS (including MS Research). MS may engage in conflicting activities -- including principal trading before or after sending these views -- market making, lending, and the provision of investment banking or other services related to instruments/issuers mentioned. No investment decision should be made in reliance on this material, which is condensed and incomplete; does not include all risk factors or other matters that may be material; does not take into account your investment objectives, financial conditions, or needs; and IS NOT A PERSONAL RECOMMENDATION OR INVESTMENT ADVICE or a basis to consider MS to be a fiduciary or municipal or other type of advisor. It constitutes an invitation to consider entering into derivatives transactions under CFTC Rules 1.71 and 23.605 (where applicable) but is not a binding offer to buy or sell any financial instrument or enter into any transaction. It is based upon sources believed to be reliable (but no representation of accuracy or completeness is made) and is likely to change without notice. Any price levels are indicative only and not intended for use by third parties. Subject to additional terms at http://www.morganstanley.com/disclaimers/productspecific.html.
Bitcoin: Fad? Foundation? Forerunner?

“It’s a bubble.”
—Dr. Alan Greenspan
Chairman of the Federal Reserve 1987-2006, Bloomberg Television, December 4, 2013

“It is btw a Ponzi game and a conduit for criminal/illegal activities. And it isn’t safe given hacking of it.”
—Dr. Nouriel Roubini
Chairman of Roubini Global Economics, tweet (@Nouriel) dated March 9, 2014

“It’s a bubble.”
—Marc Andreessen

“Personal computers in 1975, the Internet in 1993, and — I believe — Bitcoin in 2014.”
—Paul Buccheit
Creator of Gmail, tweet (@paultoo), dated April 29, 2013

“Bitcoin may be the TCP/IP of money.”
—Dr. Susan Athey
Stanford Graduate School of Business, interview at CoinSummit San Francisco, www.coindesk.com, April 1, 2014

“The ability to move value electronically without counterparties and without IOUs and promises is very useful. If people use it, it will have value.”
—Warren Buffett
Chairman & CEO of Berkshire Hathaway, CNBC interview, March 14, 2014

“The idea that it has some huge intrinsic value is just a joke in my view.”
—Dr. Susan Athey
Stanford Graduate School of Business, interview at CoinSummit San Francisco, www.coindesk.com, April 1, 2014

Please see additional important information and qualifications at the end of this material.
Objectives for Today

• Introduce basic vocabulary of cryptocurrencies and cryptoledgers
• Show bitcoin as both a currency and a technology
• Give a quick peek into the technology of cryptoledgers
• Assess bitcoin pros and cons
• Consider financial market opportunities and threats
• Discuss potential use cases

Please see additional important information and qualifications at the end of this material.
Types of Money

Political money is money created and authorized by a political body, and includes:

- **Commodity money**
- **Representative money** – a note or receipt evidencing commodity money held elsewhere but available on demand
- **Fiat money** – notes or coins backed by no material asset

Please see additional important information and qualifications at the end of this material.
Types of Money

Political money is money created and authorized by a political body, and includes:

- Commodity money
- Representative money – a note or receipt evidencing commodity money held elsewhere but available on demand
- Legal tender – money that must be accepted in payment of a debt

Please see additional important information and qualifications at the end of this material.
Some Forms of U.S. Dollars

Physical Notes and Coins

Other Physical

Non-Physical

Please see additional important information and qualifications at the end of this material.
### Attributes of Various Currencies

<table>
<thead>
<tr>
<th>Type of Money</th>
<th>Physical / Virtual</th>
<th>Digital?</th>
<th>Centralized?</th>
<th>Convertible?</th>
<th>Limited?</th>
<th>Legal Tender?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verbal promise</td>
<td>Fiat</td>
<td>Virtual</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Barley grains</td>
<td>Commod</td>
<td>Physical</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Ancient Chinese coins</td>
<td>Fiat</td>
<td>Physical</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2014 U.S. cent</td>
<td>Fiat</td>
<td>Physical</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>2014 U.S. $50 gold coin</td>
<td>Commod</td>
<td>Physical</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>1981 U.S. cent</td>
<td>Commod</td>
<td>Physical</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>U.S. gold certificate</td>
<td>Rep</td>
<td>Physical</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>U.S. Fed Reserve note</td>
<td>Fiat</td>
<td>Physical</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MTA MetroCard</td>
<td>Fiat</td>
<td>Physical</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Video arcade token</td>
<td>Fiat</td>
<td>Physical</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Electronic boarding pass</td>
<td>Fiat</td>
<td>Virtual</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Frequent flier program</td>
<td>Fiat</td>
<td>Virtual</td>
<td>Yes</td>
<td>Yes</td>
<td>Some</td>
<td>No</td>
</tr>
<tr>
<td>Korean won</td>
<td>Fiat</td>
<td>Physical</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitcoin</td>
<td>Math</td>
<td>Virtual</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Please see additional important information and qualifications at the end of this material.
The Bank knows everyone’s balance and transaction history.

Customers know only their own records.
The Bitcoin Concept

Balances can be reconstructed if you have all transactions ever made.

In Bitcoin, all transactions are public!

<table>
<thead>
<tr>
<th>From</th>
<th>Date/Type</th>
<th>To</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>May 4 Check</td>
<td>Charlie</td>
<td>($37.19)</td>
</tr>
<tr>
<td>Bob</td>
<td>May 7 ATM W/D</td>
<td>Cash</td>
<td>(100.00)</td>
</tr>
<tr>
<td>Charlie</td>
<td>May 7 Deposit</td>
<td>Savings</td>
<td>453.50</td>
</tr>
<tr>
<td>Deborah</td>
<td>May 11 Auto-Pay</td>
<td>Bob</td>
<td>275.12</td>
</tr>
<tr>
<td>Bob</td>
<td>May 1 Xfer MMA</td>
<td>Bob</td>
<td>200.00</td>
</tr>
<tr>
<td>Bob</td>
<td>May 1 ATM W/D</td>
<td>Cash</td>
<td>(150.00)</td>
</tr>
<tr>
<td></td>
<td>May 2 Wire xfer</td>
<td>MMA</td>
<td>(75.00)</td>
</tr>
</tbody>
</table>

Please see additional important information and qualifications at the end of this material.
The Bitcoin Concept

Balances can be reconstructed if you have all transactions ever made.

In Bitcoin, all transactions are public!

But they are pseudonymous (no real names).

Morgan Stanley

Please see additional important information and qualifications at the end of this material.
## Simplified Bitcoin Transaction Ledger

<table>
<thead>
<tr>
<th>From Address</th>
<th>BTC</th>
<th>To Address</th>
<th>BTC</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>a173f9</td>
<td>101.001</td>
<td>4k885p</td>
<td>1.000</td>
<td>Acquired 1 BTC for my petty cash address and 100 BTC for my &quot;main&quot; address</td>
</tr>
<tr>
<td>4k885p</td>
<td>1.000</td>
<td>r4h0t2</td>
<td>0.745</td>
<td>Lunch for 2 at La Maison and change</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4k885p</td>
<td>0.253</td>
<td>My change</td>
</tr>
<tr>
<td>gr739w</td>
<td>100.000</td>
<td>fpu02r</td>
<td>0.813</td>
<td>At the silent auction, I bought a work of art and a day at the spa and a fine wine and change</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11am95</td>
<td>1.006</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>w63429</td>
<td>0.337</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>gr739w</td>
<td>97.841</td>
<td></td>
</tr>
<tr>
<td>4k885p</td>
<td>0.253</td>
<td>n9776y</td>
<td>0.315</td>
<td>Theater tickets</td>
</tr>
<tr>
<td>gr739w</td>
<td>97.841</td>
<td>4k885p</td>
<td>1.000</td>
<td>Refill my petty cash address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gr739w</td>
<td>96.777</td>
<td>Change goes to my main address</td>
</tr>
</tbody>
</table>

Difference of .001 = Transaction Fee
Peer-to-Peer Networks

• A Peer-to-Peer (P2P) computer network is one in which:
  - there are multiple computers working on a common task
  - the work load is shared by all of the computers
  - all computers work as equals (peers) – i.e., no central authority

• Examples of applications using P2P networks include:
  - Napster
  - BitTorrent
  - Skype
  - Bitcoin (and many other cryptocurrencies)

Please see additional important information and qualifications at the end of this material.
Public Key Cryptography (PKC)

- PKC provides every user with two keys:
  - a public key known to everybody, and
  - a private key known only to the user

- Anybody with your public key can send you an encrypted message that only you will be able to read

- Using your private key, you can sign messages with a digital signature that proves* to the recipient(s) that the message was sent by you

* With very high probability if your private key wasn’t stolen
How To Send Bitcoins

• You send a message to at least one machine in the bitcoin network
• You specify the input and output addresses
• For each output address, you specify the number of bitcoins
• You sign with your digital signature
• After sending the message, you wait for your transaction to be validated and confirmed by the Bitcoin network

Please see additional important information and qualifications at the end of this material.
Engaging in bitcoin transactions requires special software, known as a **wallet**. Some of the functions performed by a good wallet include:

- Creation of public and private keys
- Sending and receiving bitcoins
- Signing transactions
- Converting bitcoins to other currency (physical and virtual)
- Statements of balances and transactions
- Additional or substitute security measures
Recap

- Bitcoins are represented by addresses
- Addresses are pseudonymous, based on public keys
- You can have as many addresses as you want
- Transactions occur between addresses
- Bitcoins are “pushed” from input addresses to output addresses
- Transactions can have multiple inputs and/or outputs
- Transactions usually return change to the sender
- Wallets take care of the dirty work for you
- Transactions are public
- Any difference ($\Sigma$ inputs $-$ $\Sigma$ outputs) is a transaction fee
Validation

When your transaction message is received by a machine in the bitcoin network (a node), it:

• Checks to see whether it already processed the transaction
• Checks that all addresses are legitimate
• Checks the digital signature to ensure that the original sender is the rightful owner of the input address(es)
• Checks that the input bitcoins were not already spent elsewhere
• Checks that the input bitcoins are at least as much as the output bitcoins (Any difference is a transaction fee)

If all is well, the node marks the transaction as valid, enters it onto its list of unconfirmed transactions, and passes it on to one or more new nodes.

Please see additional important information and qualifications at the end of this material.
Bitcoin P2P Network In Action

Transaction

Please see additional important information and qualifications at the end of this material.
Bitcoin P2P Network In Action

Transaction 1  
Transaction 4

Transaction 3

Transaction 2

Error Message

Please see additional important information and qualifications at the end of this material.
The nodes may disagree on the order of transactions.
SHA-256

- **Secure Hash Algorithm** with 256-bit (32-byte) output
- Takes any text string as input
- Easy to compute the output from the input
- Very difficult* to compute the input given the output
- Very difficult* to find two inputs with the same output
- Small change to input typically results in big change in output

\[
\text{Input} \quad \text{Output} = \text{SHA256(Input)}**
\]

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello, World</td>
<td>03675ac5 3ff9cd15 35ccc7df cdfa2c45 8c521837 1f418dc1 36f2d19a c1fbe8a5</td>
</tr>
<tr>
<td>Hello, World.</td>
<td>02b5dcd5 f0ef1a39 cffec5f8 b625ec20 bffcf918 e4efd3f5 4babec4e ae03b347</td>
</tr>
<tr>
<td>Hello, World!</td>
<td>dffd6021 bb2bd5b0 af676290 809ec3a5 3191dd81 c7f70a4b 28688a36 2182986f</td>
</tr>
</tbody>
</table>

* Not solvable in asymptotic polynomial time

Translation: Not worth the time and effort

CompSci: Proof of Work

- Challenge: Find a number which, when appended to “Hello, World!” gives an SHA-256 hash beginning with leading zeros.
- These can only be found by trial and error.
- But anyone can easily check that you did the work.
- The appended number is called the **Proof of Work**.

<table>
<thead>
<tr>
<th>Input</th>
<th>Output = SHA256(Input)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello, World!</td>
<td>dff6021 bb2bd5b0 af676290 809ec3a5 3191dd81 c7f70a4b 28688a36 2182986f</td>
</tr>
<tr>
<td>Hello, World!1</td>
<td>b3e6153a 3ce901e2 769b77d7 96b0aeea 68ab0344 a98b94b7 84f9e2b7 94487540</td>
</tr>
<tr>
<td>Hello, World!2</td>
<td>d469e19a ae363334 35190ccc f4800a33 9ecc6b46 7bfdaa3b 4e6f757f 2dd0853f</td>
</tr>
<tr>
<td>Hello, World!3</td>
<td>b91abd0f c9eb7aeb 78ef3cd5 f5b9b5a9 139fb2fb 0c452e76 4e9639a6 c089c5ba</td>
</tr>
<tr>
<td>Hello, World!4</td>
<td>0f3af36d 81b5efc4 8feec2b5 f6484868 92699c64 5d8ad569 0c7bdfcf 8e6e0778</td>
</tr>
<tr>
<td>Hello, World!229</td>
<td>00b92f46 05232084 7022a3c8 21f8e830 8ce3a66b 9aaf9de6 f83572b5 babc9f8d</td>
</tr>
<tr>
<td>Hello, World!741</td>
<td>000c5644 054b75e9 5e220856 dbb4a8ce bf3923f7 848c5108 76c5df33 cce20f2d</td>
</tr>
<tr>
<td>Hello, World!280635</td>
<td>0001ed4 bc824777 27b6d2cd 4a991e92 b6d9b7d1 cf55c4a6 a24dc3d4 76ba80f8</td>
</tr>
<tr>
<td>Hello, World!1558215</td>
<td>00008fb 67e78dee 225c2bea 554b989b 164c1db4 cbc5d281 d00ffa81 724a83b3</td>
</tr>
<tr>
<td>Hello, World!12320463</td>
<td>0000080 883ee61b b729275d 87fc0491 b7f6c8b4 06af8928 aa4879a4 fb0c78de</td>
</tr>
</tbody>
</table>

Please see additional important information and qualifications at the end of this material.
Confirmation

1. Nodes collect valid but unconfirmed transactions
2. These are assembled into groupings called blocks
3. The node tries to solve the Proof of Work problem
4. If it succeeds, it adds its PoW to the block
5. The block and PoW are published to the Bitcoin network; the first node with a valid PoW wins

This process is called mining. Miners get paid via transaction fees and newly issued bitcoins. The current reward for each accepted PoW is 25 bitcoins.
The first block is mined and sent to the network

The second block is mined, sent to the network, and linked to the first block

The third block is mined, sent to the network, and linked to the second block

The resulting data structure is known as the blockchain. It is a distributed cryptoledger.

Transactions are confirmed once they appear in the blockchain

The confirmation level is the number of blocks that refer to the transaction

The deeper the transaction is "buried" in the chain, the less likely it is to be changed by the network

Many bitcoin users will not consider a transaction to be "final" until it is confirmed to six levels.
Issues Handled By The Blockchain

1. Prevents the same bitcoins from being spent twice by the same owner

2. Establishes a universally agreed order in which transactions occurred

3. Resolves any controversy over the rightful owner of a bitcoin

4. Makes it extremely difficult to counterfeit bitcoins

5. Makes it extremely difficult to plant non-existent transactions

Please see additional important information and qualifications at the end of this material.
Where Are The Bitcoin Nodes?

As of September 14, 2015 there were 5,995 nodes in the Bitcoin network. Each of them has the complete bitcoin history (approx. 83mm transactions).

Source: Bitnodes (https://getaddr.bitnodes.io)

Please see additional important information and qualifications at the end of this material.
# Top 10 Cryptocurrencies by Market Cap

Data as of 9/14/2015

<table>
<thead>
<tr>
<th>Rank</th>
<th>Name</th>
<th>Genesis</th>
<th>Market Cap</th>
<th>Price</th>
<th>Symbol</th>
<th>Current Supply</th>
<th>Max Supply</th>
<th>Logo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>2009</td>
<td>$3,385,269,054</td>
<td>$231.67</td>
<td>BTC</td>
<td>14,612,525</td>
<td>21,000,000</td>
<td><img src="image" alt="Bitcoin Logo" /></td>
</tr>
<tr>
<td>2</td>
<td>Ripple</td>
<td>2011</td>
<td>$277,461,653</td>
<td>$0.0085</td>
<td>XRP</td>
<td>32,488,247,336</td>
<td>100,000,000,000</td>
<td><img src="image" alt="Ripple Logo" /></td>
</tr>
<tr>
<td>3</td>
<td>Litecoin</td>
<td>2011</td>
<td>$120,527,873</td>
<td>$2.8500</td>
<td>LTC</td>
<td>42,283,360</td>
<td>84,000,000</td>
<td><img src="image" alt="Litecoin Logo" /></td>
</tr>
<tr>
<td>4</td>
<td>BitShares</td>
<td>2014</td>
<td>$10,262,936</td>
<td>$0.0041</td>
<td>BTS</td>
<td>2,511,953,117</td>
<td>No maximum*</td>
<td><img src="image" alt="BitShares Logo" /></td>
</tr>
<tr>
<td>5</td>
<td>Dogecoin</td>
<td>2013</td>
<td>$12,591,184</td>
<td>$0.0001</td>
<td>DOGE</td>
<td>100,984,764,499</td>
<td>No maximum*</td>
<td><img src="image" alt="Dogecoin Logo" /></td>
</tr>
<tr>
<td>6</td>
<td>Stellar</td>
<td>2014</td>
<td>$10,422,907</td>
<td>$0.0022</td>
<td>STR</td>
<td>4,837,356,606</td>
<td>100,804,168,101</td>
<td><img src="image" alt="Stellar Logo" /></td>
</tr>
<tr>
<td>7</td>
<td>Dash</td>
<td>2014</td>
<td>$13,445,606</td>
<td>$2.3200</td>
<td>DSH</td>
<td>5,784,499</td>
<td>184,460,000,000</td>
<td><img src="image" alt="Dash Logo" /></td>
</tr>
<tr>
<td>8</td>
<td>Ethereum</td>
<td>2014</td>
<td>$65,358,410</td>
<td>$0.8931</td>
<td>ETH</td>
<td>73,177,990</td>
<td>No maximum*</td>
<td><img src="image" alt="Ethereum Logo" /></td>
</tr>
<tr>
<td>9</td>
<td>BanxShares</td>
<td>2014</td>
<td>$12,567,312</td>
<td>$1.7600</td>
<td>BANX</td>
<td>7,140,721</td>
<td>12,000,008</td>
<td><img src="image" alt="BanxShares Logo" /></td>
</tr>
<tr>
<td>10</td>
<td>MaidSafeCoin</td>
<td>2013</td>
<td>$9,637,285</td>
<td>$0.0213</td>
<td>MAID</td>
<td>452,552,412</td>
<td>4,000,000,000</td>
<td><img src="image" alt="MaidSafeCoin Logo" /></td>
</tr>
</tbody>
</table>

*Supply is technically unlimited but growth rate is constrained

Source: coinmarketcap.com

**Total cryptocurrencies: 685**

**Total market cap: $4.02 billion (BTC = 84%)**

Please see additional important information and qualifications at the end of this material.
Bitcoin Price History (in US$, as of September 14, 2015)

- Genesis block was in 2010
- Value in US$ exploded in 2013
- Rocky downhill ride since peaking at over $1,000/BTC
- 2015 price has been highly volatile
- Average daily change was ±2.3%
- 7 days had >10% move
- Not a good store of value

Source: coindesk.com

Please see additional important information and qualifications at the end of this material.
Sample Businesses Accepting Bitcoin

**Businesses**

- Dell
- Expedia
- Dish
- Sandman
- Intuit
- Overstock.com
- The King's College
- 50 Cent
- Okcupid
- Holiday Inn Express
- Kings
- Quakes
- Morgan Stanley

**Payments & e-commerce**

- Braintree
- Square
- Stripe
- Shopify
- WordPress
- Revel
- TigerDirect.com
- Newegg
- Overstock.com
- Intuit
- Expedia
- Dell
- Sandman
- The King's College
- 50 Cent
- Okcupid
- Holiday Inn Express
- Kings
- Quakes
- Morgan Stanley

**Alt-currency processors**

- Bitpay
- Coinbase

Sources: www.bitpay.com, coinbase.com, company reports

Please see additional important information and qualifications at the end of this material.
Bitcoin: Ten Pros

1. True 24x7 market; knows no holidays
2. Send or receive money any time, fairly quickly and at modest cost
3. No personal information need be revealed
4. It’s easy to establish a wallet and get involved
5. Bitcoins cannot be seized by any authority without the owner’s cooperation
6. Bitcoins are accepted by a large and growing number of businesses
7. You may have as many addresses (pseudonyms) as you like
8. Businesses can be hacked by a small group with modest budget; blockchain cannot be.
9. Inflation-proof: no central authority and limited bitcoin supply
10. First mover advantage; market cap 5x greater than the sum of competitors

Please see additional important information and qualifications at the end of this material.
Bitcoin: Ten Cons

1. Widespread skepticism: “Bitcoins have no real value” “They’re not legal tender”
2. Transactions are irreversible; there is no authority to appeal to
3. Lack of infrastructure exposes users to counterparty risk
4. If your wallet program is hacked, you could lose all of your bitcoins
5. Too volatile to be a reliable store of value
6. Bitcoin is a currency of choice for some criminal elements seeking stealth
7. Legal barriers exist in many jurisdictions
8. Small market cap creates potential for abuse
9. Fixed supply creates potential for hoarding and deflation
10. Despite all the pseudonyms, the NSA can probably determine your identity

Please see additional important information and qualifications at the end of this material.
And The Winner Is …

**Blockchain**

Instead of bitcoins …
think *any asset or record*

No need for trusted third parties!

Instead of unlimited nodes …
think *licensed, highly secure nodes*

Instead of proof of work …
think *proof of stake, consensus, …*

The Potential Losers Are …

- Depositories
- CCPs
- DCOs
- Payment / settlement systems
- Title companies
- Securities reference data
- Land records
- Escrow agents
- Medical records
- Copyrights
- Software licenses
- Reservation systems
- Crowdfunding contracts

Please see additional important information and qualifications at the end of this material.
What Next?

- Sidechains
  - Represent any asset(s)
- Smart contracts
  - Embed Turing-complete scripts capable of making decisions about future events
- Scripted cash
  - Within a trusted, semi-trusted or non-trusted network
- Colored coins or tokens
  - Securely
  - With near real-time confirmation
- Alternative proofs

Bitcoin 2.0

Please see additional important information and qualifications at the end of this material.
Use Case #1: Overstock.com

“We may decide to offer securities as digital securities, meaning the securities will be uncertificated securities, the ownership and transfer of which are recorded on a cryptographically-secured distributed ledger system using technology similar to (or the same as) the distributed ledger technology used for trading digital currencies. For example, we may decide to offer shares of our capital stock as digital securities, in which case the shares of stock would be the same as any other shares of the same class of stock except that such shares would be uncertificated and represented exclusively as book-entries on a cryptographically-secured distributed ledger. Digital securities are designed to enable trades to settle immediately or nearly immediately, unlike traditional securities, such as shares of our common stock, trades of which settle on the third day following the day the money is exchanged.”
Use Case #2 (Hypothetical): Universal SecRef Database

**Syndicate** creates proto-entry based on information in red herring

Upon issuance, **syndicate** updates with final terms and pricing

**S&P and Capital IQ** supply ISIN and Cusip codes

**Markit** supplies RED code

**Rating agencies** supply initial ratings

**Issuer** or its agent updates with corporate actions: mergers, calls, puts, sinkers

**Rating agencies** update ratings

**Index providers** (S&P, Markit, Russell, ...) provide and update index inclusions

**Portfolio managers** update holdings

**Intex** supplies rules for tranche payments

Please see additional important information and qualifications at the end of this material.
Use Case #3 *(Hypothetical)*: Tokenized Commercial Loan

- Each bitcoin trades in units of .00000001 (1 satoshi)
- Commercial loan borrower acquires 1 satoshi (cost ≈ .0002p)
- Borrower agrees to pay principal and interest to the holder of the satoshi
- Buyer acquires satoshi from borrower
- Buyer pays in bitcoin
- The blockchain records this and all subsequent transactions
- The price of each transaction is visible to all
- Buyer and seller identities are pseudonymous

The satoshi is a “token” for the loan. It is a **digital representative** currency.
Player to Watch: Digital Asset Holdings

“Our Mission is to Reduce Settlement Latency and Counterparty Risk”

<table>
<thead>
<tr>
<th>Who</th>
<th>Role</th>
<th>Known for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blythe Masters</td>
<td>CEO</td>
<td>JPM Commodities, CFO, Credit</td>
</tr>
<tr>
<td>Don Wilson</td>
<td>Board</td>
<td>DRW Trading Group</td>
</tr>
<tr>
<td>Sunil Hirani</td>
<td>Board</td>
<td>trueEX, CreditEx</td>
</tr>
</tbody>
</table>

Sources: digital-asset.com, Morgan Stanley

Please see additional important information and qualifications at the end of this material.
Player to Watch: itBit

“itBit is elevating bitcoin trading to meet the high regulatory, service and security standards set by leading financial institutions.”

<table>
<thead>
<tr>
<th>Who</th>
<th>Role</th>
<th>Known for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chad Cascarilla</td>
<td>CEO</td>
<td>Cedar Hill Capital</td>
</tr>
<tr>
<td>Sheila Bair</td>
<td>Board</td>
<td>FDIC Chair, Amherst, CFTC</td>
</tr>
<tr>
<td>Bill Bradley</td>
<td>Board</td>
<td>Allen &amp; Co., U.S. Senate, NBA</td>
</tr>
<tr>
<td>Robert Herz</td>
<td>Board</td>
<td>FASB Chair, PwC</td>
</tr>
</tbody>
</table>

Sources: itbit.com, Morgan Stanley

Please see additional important information and qualifications at the end of this material.
Player to Watch: Symbiont

“Symbiont is building the first issuance and trading platform for smart securities on blockchain technology”

<table>
<thead>
<tr>
<th>Who</th>
<th>Role</th>
<th>Known for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark Smith</td>
<td>CEO</td>
<td>Counterparty, MathMoney f(x)</td>
</tr>
<tr>
<td>Duncan Niederauer</td>
<td>Board</td>
<td>NYSE, GS Equities</td>
</tr>
<tr>
<td>Matt Andresen</td>
<td>Board</td>
<td>Citadel, Island ECN</td>
</tr>
</tbody>
</table>

Sources: symbiont.io, Morgan Stanley

Please see additional important information and qualifications at the end of this material.
Disclaimer

The information in this material was prepared by sales, trading, or other non-research personnel of Morgan Stanley for institutional investors. This is not a research report, and unless otherwise indicated, the views herein (if any) are the author’s and may differ from those of our Research Department or others in the Firm. This material is not independent of the interests of our trading and other activities, which may conflict with your interests. We may deal in any of the markets, issuers, or instruments mentioned herein before or after providing this information, as principal, market maker, or liquidity provider and may also seek to advise issuers or other market participants.

Where you provide us with information relating to an order, inquiry, or potential transaction, we may use that information to facilitate execution and in managing our market making and hedging activities.

This material does not provide investment advice or offer tax, regulatory, accounting, or legal advice. By submitting this document to you, Morgan Stanley is not your fiduciary, municipal, or any other type of advisor.

This material is not based on a consideration of any individual client circumstances and thus should not be considered a recommendation to any recipient or group of recipients. This material is an invitation to consider entering into derivatives transactions under CFTC Rules 1.71 and 23.605 (where applicable) but is not a binding offer to buy or sell any instrument or enter into any transaction.

Unless otherwise specifically indicated, all information in these materials with respect to any third party entity not affiliated with Morgan Stanley has been provided by, and is the sole responsibility of, such third party and has not been independently verified by Morgan Stanley, our affiliates or any other independent third party. We make no express or implied representation or warranty with respect to the accuracy or completeness of this material, nor will we undertake to provide updated information or notify recipients when information contained herein becomes stale.

Any prices contained herein are indicative only and should not be relied upon for valuation or for any use with third parties.

All financial information is taken from company disclosures and presentations (including 10Q, 10K and 8K filings and other public announcements), unless otherwise noted. Any securities referred to in this material may not have been registered under the U.S. Securities Act of 1933, as amended and, if not, may not be offered or sold absent an exemption therefrom. In relation to any member state of the European Economic Area, a prospectus may not have been published pursuant to measures implementing the Prospectus Directive (2003/71/EC) and any securities referred to herein may not be offered in circumstances that would require such publication. Recipients are required to comply with any legal or contractual restrictions on their purchase, holding, sale, exercise of rights, or performance of obligations under any instrument or otherwise applicable to any transaction. In addition, a secondary market may not exist for certain of the instruments referenced herein.

The value of and income from investments may vary because of, among other things, changes in interest rates, foreign exchange rates, default rates, prepayment rates, securities, prices of instruments or securities, market indexes, operational, or financial conditions of companies or other factors. There may be time limitations on the exercise of options or other rights in instruments (or related derivatives) transactions. Past performance is not necessarily a guide to future performance. Estimates of future performance are based on assumptions that may not be realized. Actual events may differ from those assumed, and changes to any assumptions may have a material impact on any projections or estimates. Other events not taken into account may occur and may significantly affect any projections or estimates. Certain assumptions may have been made for modeling purposes only to simplify the presentation or calculation of any projections or estimates, and Morgan Stanley does not represent that any such assumptions will reflect actual future events or that all assumptions have been considered or stated. Accordingly, there can be no assurance that any hypothetical estimated returns or projections will be realized or that actual returns or performance results will not materially differ. Some of the information contained in this document may be aggregated data of transactions executed by Morgan Stanley that has been compiled so as not to identify the underlying transactions of any particular customer.

Morgan Stanley
This information is not intended to be provided to and may not be used by any person or entity in any jurisdiction where the provision or use thereof would be contrary to applicable laws, rules, or regulations. This communication is directed to and meant for sophisticated investors, including specifically, institutional investors in the U.S and/or those persons who are eligible counterparties or professional clients in the European Economic Area. It must not be re-distributed to or relied upon by retail clients. This information is being disseminated in Hong Kong by Morgan Stanley Asia Limited and is intended for professional investors (as defined in the Securities and Futures Ordinance) and is not directed at the public of Hong Kong. This information is being disseminated in Singapore by Morgan Stanley Asia (Singapore) Pte. This information has not been registered as a prospectus with the Monetary Authority of Singapore. Accordingly, this information and any other document or material in connection with the offer or sale, or invitation for subscription or purchase, of this security may not be circulated or distributed, nor may this security be offered or sold, or be made the subject of an invitation for subscription or purchase, whether directly or indirectly, to persons in Singapore other than (i) to an institutional investor under Section 274 of the Securities and Futures Act, Chapter 289 of Singapore (the “SFA”), (ii) to a relevant person pursuant to Section 275(1) of the SFA, or any person pursuant to Section 275(1A) of the SFA, and in accordance with the conditions, specified in Section 275 of the SFA or (iii) otherwise pursuant to, and in accordance with the conditions of, any other applicable provision of the SFA. Any offering of this security in Singapore would be through Morgan Stanley Asia (Singapore) Pte, an entity regulated by the Monetary Authority of Singapore.

This information is being disseminated in Japan by Morgan Stanley MUFG Securities Co., Ltd. Any securities referred to herein may not have been and/or will not be registered under the Financial Instruments Exchange Law of Japan (Law No. 25 of 1948, as amended, hereinafter referred to as the “Financial Instruments Exchange Law of Japan”). Such securities may not be offered, sold, or transferred, directly or indirectly, to or for the benefit of any resident of Japan unless pursuant to an exemption from the registration requirements of and otherwise in compliance with the Financial Instruments Exchange Law and other relevant laws and regulations of Japan. As used in this paragraph, “resident of Japan” means any person resident in Japan, including any corporation or other entity organized or engaged in business under the laws of Japan. If you reside in Japan, please contact Morgan Stanley MUFG Securities for further details at +813-6836-5000.

This material may not be redistributed without the prior written consent of Morgan Stanley.

© 2015 Morgan Stanley