MONERIUM

Blockchains and the future of financial services

Technology overview, financial markets relevance, market trends and a likley future endgame.

Jón Helgi Egilsson & Sveinn Valfells, PhD

March 8, 2017

Commit 6b20e21

monerium@monerium.com

Monerium ehf.
Klapparstígur 16
101 Reykjavík
Iceland

Contents

Executive summary

> The distributed ledger is a genuine technological innovation that demonstrates that digital records can be held securely without any central authority.
>
> Bank of England [1]

Bitcoin is the first blockchain

Blockchain distributed ledger technology opens up new ways of building commercial and social networks without the intermediation of central authorities. The first and most notable example of blockchains to date is Bitcoin which is designed for online payments *without going through financial institutions* [2]. The Bitcoin blockchain is a ledger which consists of blocks of transactions of a native digital currency, bitcoin. Transactions are authenticated and transmitted on a peer-to-peer network using public key cryptography. Specialized service providers called miners compete to assemble and calculate cryptographic watermarks for new transaction blocks, receiving new bitcoins and transaction fees as reward when successful. The computational power invested in the resulting chain of interlinked transaction blocks removes the need of a trusted centralized entity to update and store the ledger.

In seven years, Bitcoin transaction turnover has reached $65 billion per annum. It follows a similar hypergrowth trajectory in online payments as PayPal which had $353 billion in turnover in 2016 and is still growing at over 25% year-over-year. Unlike PayPal, however, the Bitcoin protocol is open and free. Participation is also permissionless, anyone can join the network and transact bitcoins or compete to mine new ones. Through combination of clever design and built-in incentives, Bitcoin has become a global payments network which bypasses existing financial service providers and defines an entirely new class of financial assets, digital virtual currency.

Blockchains are driving innovation in financial services

Bitcoin has inspired a wave of innovation in transaction platforms based on the decentralized and distributed blockchain architecture. The community counts millions of users and thousands of developers and entrepreneurs. A new category of blockchains pioneered by Ethereum supports smart contracts, protocols which enable the creation of digital assets and contracts. In principle, almost any form of security currently traded in capital markets can be issued and transacted as a smart contract on a blockchain. Smart contract blockchains also support programmable transactions which enable new forms of automated financial services.

Incumbents are actively exploring blockchains

Incumbents in financial services have started adopting blockchain technology, both individually and through alliances. A key business goal is to increase the efficiency of their operations. One example is the recently launched transaction platform Corda developed by the technology company R3 in collaboration with over seventy of the world's leading banks. Arguably the leading distributed ledger solution for financial incumbents, Corda is designed to manage legal agreements on an automatic and

enforceable basis using an open, enterprise-grade, shared platform to record financial events and execute smart contract logic. Corda and comparable solutions may with time substantially reshape the way existing financial service providers operate.

Blockchains may influence central banking

Finally, a growing number of central banks have initiated research into the economic implications of blockchains. It is too early to tell what systemic impact blockchains may ultimately have on central banking, but strong arguments have been made to support the notion that blockchains may ultimately change how central banks issue currency and conduct monetary policy. Researchers at the Bank of England have even suggested that issuing central bank digital currency via distributed ledgers could permanently raise GDP by as much as 3% and substantially improve central banks' ability to stabilize the business cycle [3].

Blockchains are a transformational technology for finance

It is still early in the adoption cycle for blockchains, and the direct economic impact of blockchains in global trade and finance is small, as yet. But only eight years after Bitcoin was launched, it is already clear that the blockchain distributed transaction and data storage architecture is a transformational technology for finance which could fundamentally change how money is issued, held on deposit and exchanged.

Blockchains

> The notion of shared public ledgers may not sound revolutionary or sexy. Neither did double-entry book-keeping or joint-stock companies. Yet, like them, the blockchain is an apparently mundane process that has the potential to transform how people and businesses cooperate.
>
> The Economist [4]

Introduction

For centuries ledgers have been used to keep track of financial transactions of individuals, institutions and governments. Ledgers are essential and indispensable tools for organizing many aspects of civilization. The success of the Medici, the British Empire or Microsoft would have been impossible without the accurate tracking on various ledgers of how each of these institutions used their resources . A new ledger technology can therefore have fundamental implications for many industries or even entire societies.

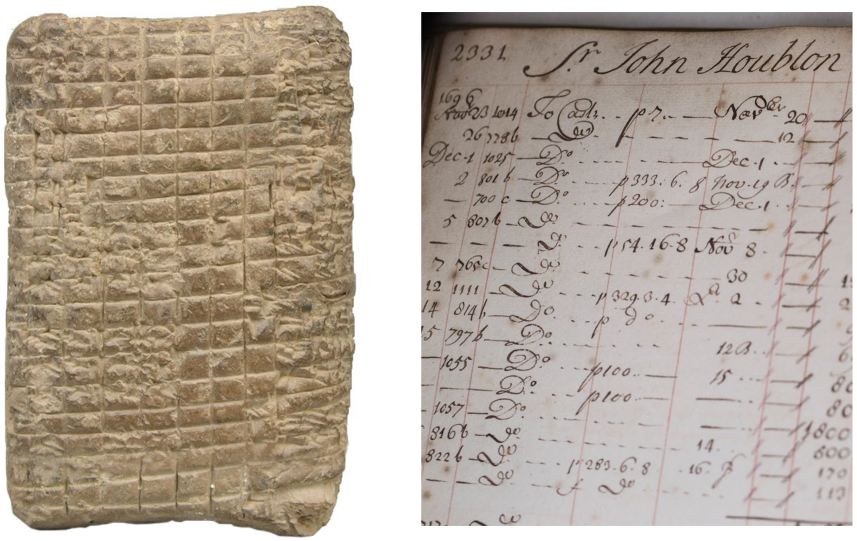

Figure 1: Two examples of transaction ledgers. On the left (ca. 1800 BCE), a Mesopotamian clay tablet recording the disbursements of food to various individuals. On the right (1696), the Bank of England's Private Drawing Ledger Number 1 which lists in ink on paper the financial accounts of the Bank's first customers including Sir John Houblon, the Bank's first governor [5].

Dictionaries define ledger as "the principal book in which the commercial transactions of a company are recorded". The origin of ledger is traced to Middle English from the Dutch "leggen", to lay [6]. Regardless of whether a ledger was kept by a country, a company or a person, it maintained a single, central record of transactions, sometimes with controlled access so only specific individuals were allowed to read the ledger or write into it.

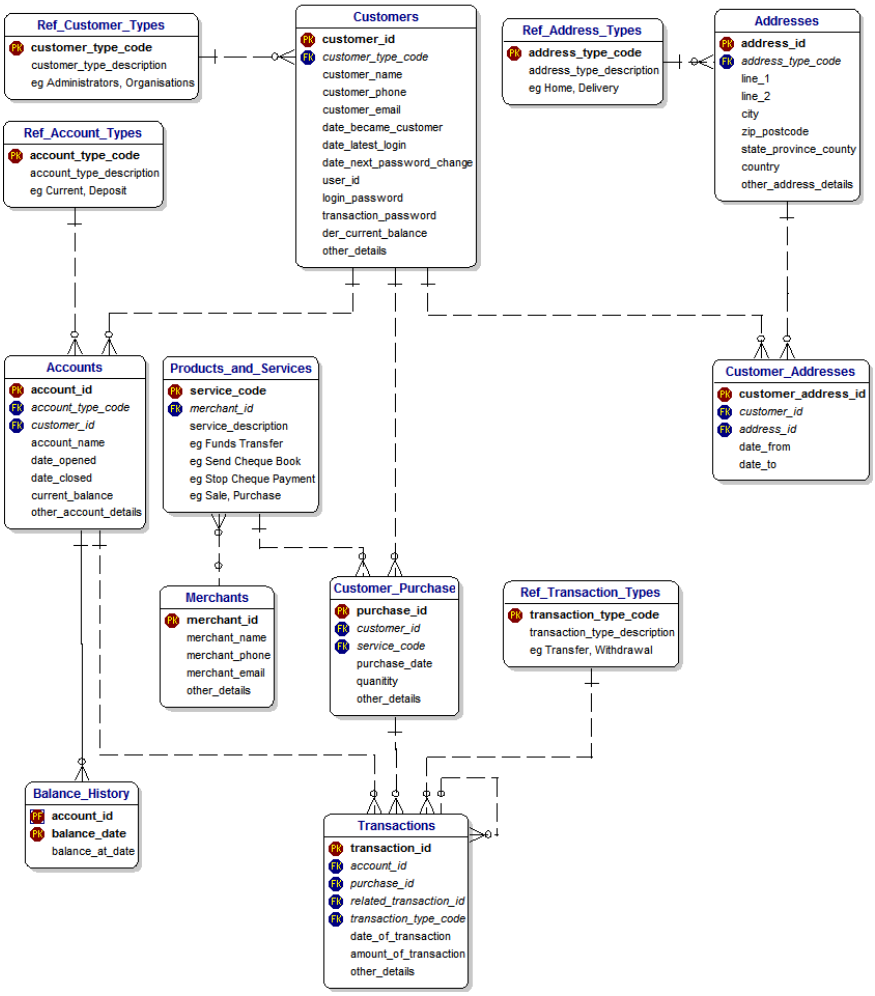

Figure 2: A modern banking data model (2010) [7]. The model consists of multiple linked ledgers stored in digital form in a central database.

In the late 20th century, digital technology transformed the medium of the ledger from paper to binary form. Nevertheless, a ledger maintained in a modern relational database (Figure 2) is essentially centralized although it can be replicated and searched more easily than older ledgers maintained on physical form (Figure 1).

Blockchains

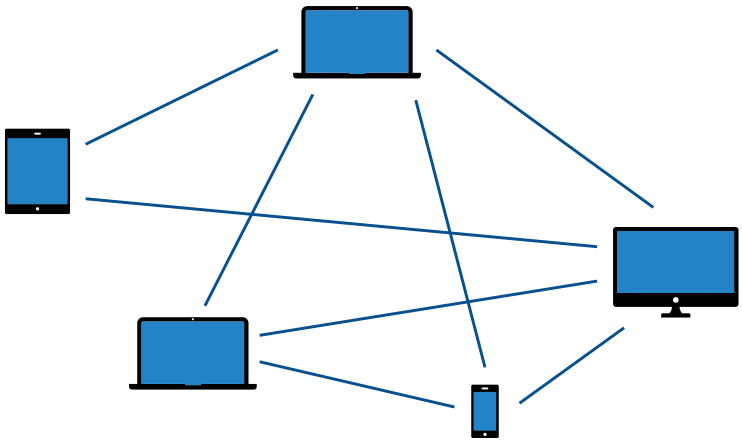

Figure 3: A Peer-to-Peer (P2P) network has no central server, clients connect with each other freely to broadcast and relay transactions [8].

A blockchain is a new form of digital ledger which does not need to be maintained by a central authority. Instead, it can be distributed or shared between multiple participants or nodes on a Peer-to-Peer (P2P) network. A user joins a P2P network by connecting to one or more nodes and broadcasts a transaction (Figure 3). Each receiving node relays the transaction to its connections until eventually all nodes have a copy of the transaction. Some or all of the nodes regularly assemble new transactions into timestamped transaction blocks. The new blocks are broadcast through the network. Consensus is established when all the nodes or a supermajority of the nodes have received a valid block of new transactions which is appended to the previous blocks. Each new block is digitally signed and includes the signature of the preceding block. The linked digital signatures guarantee the integrity of the transactions registered in the blockchain, and there is no need to maintain a central copy.

Blockchain P2P network
On a blockchain P2P network, nodes perform three main types of functions:

- Send and relay transactions
- Update blockchain with new transaction blocks (consensus)
- Relay transaction blocks

The Bitcoin blockchain is permissionless, anyone can join or leave the Bitcoin network and perform any function without authorization. In contrast, permissioned blockchain deployments allow administrators to control access and function of network nodes (page 25). Consenus can be established proof-of-work, calculating cryptographic signatures of new blocks as in Bitcoin mining (page 15). Consensus can also be established by collective agreement of validating nodes or some subset of them. Validators are chosen based size of cryptocurrency holdings (proof-of-stake), trust levels, or a range of other criteria determined by the network architects. New blocks which receive the support of the designated number of validators are added to the blockchain.

The first blockchain to gain wide use and attention is Bitcoin. Launched as an open source project in January of 2009, Bitcoin is designed as a peer-to-peer online payment network with its own native virtual cryptocurrency, bitcoin.[1] There are now dozens of public blockchains in use globally. Currently, Bitcoin, Ethereum and Ripple are the most valuable blockchains based on the value of the respective embedded cryptocurrencies. In addition to cryptocurrency blockchains, new types of blockchains are emerging which are designed primarily as transaction platforms for traditional securities, for example Chain, Corda and Hyperledger. In many respects, Bitcoin serves as template with which almost all other blockchain projects are compared, open source or proprietary. We therefore begin by describing Bitcoin.

The key innovation
The distinguishing feature of blockchain-based digital currencies is that they are *both currencies and payment systems to settle financial transactions*

Sveriges Riksbank [9]

The key innovation of blockchain-based digital currencies is the 'distributed ledger' which *allows a payment system to operate in an entirely decentralized way, without intermediaries such as banks*

Bank of England [1]

[1] A list of special terms and acronyms, such as cryptocurrency, digital currency and virtual currency, is located in the Special terms section, page 49.

Bitcoin

The rapid rise of Bitcoin

Bitcoin was announced in a whitepaper published in October 2008 on an Internet cryptography mailing list [10]. The identity of the author or authors is still unknown, he, she or they are are listed under the pseudonym Satoshi Nakamoto. The purpose of Bitcoin as described in the original whitepaper is, however, very clear:

> A purely peer-to-peer version of electronic cash [to] allow online payments to be sent directly from one party to another without going through a financial institution [2]

Three months later, in January 2009, the first version of Bitcoin was published on the open source code repository SourceForge. The first block of Bitcoin transactions, the genesis block, contains a quote of a headline of an article published in The Times on January 3, 2009:

> The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

The first public price quote for the bitcoin cryptocurrency was published in November, 2009, $1 for 1,309.03 BTC [11].[2] The first bitcoin exchange opened in July, 2010, with bitcoin trading at $0.05/BTC. The market cap and turnover have since grown at average annual rates of 170% and 105%, respectively. Seven years after Bitcoin was launched, there are now over 16 million bitcoin in issue trading at $1188/BTC. The market capitalization is $19 billion, and the annual turnover of bitcoin-to-bitcoin transactions is $65 billion (Figure 4).[3]

For comparison, PayPal was started ten years before Bitcoin and helps consumers and merchants receive and send online payments. Unlike Bitcoin, however, PayPal uses banks as intermediaries [13]. In 2016, the total payment volume of PayPal was $353 billion, growing at 25% year-over-year; PayPal's market cap on December 30, 2016, was $48 billion [14, 15].

While Bitcoin is growing fast and commands a sizable fraction of PayPal's value and volume, it is still small compared to the industry payment leaders VISA, MasterCard and American Express. At year end 2016, VISA, MasterCard and American Express had market cap of $181, $112 and $67 billion, respectively [16]. In 2014, the largest credit and debit card networks led by VISA, MasterCard and American Express processed $24 trillion in 196 billion transactions for an average transaction size of $122 [17].

Bitcoin architecture

Bitcoin's success is predicated on a well-designed, secure architecture which presents low barriers of entry for users, service providers and third-party developers [19]. Users' balances are controlled by public key cryptography which is widely used for secure online communication, e.g. for SSL certificates (Figure 5). The distributed ledger is updated by a network of timestamp servers called miners. Every 10 minutes on average, a miner calculates a cryptographic signature or watermark of the

[2] The virtual cryptocurrency of the Bitcoin blockchain is called bitcoin, abbreviated as BTC or XBT.

[3] Unless otherwise noted, all calculations relating to bitcoin are performed by the authors and based on data published by `http://www.blockchain.info` [12].

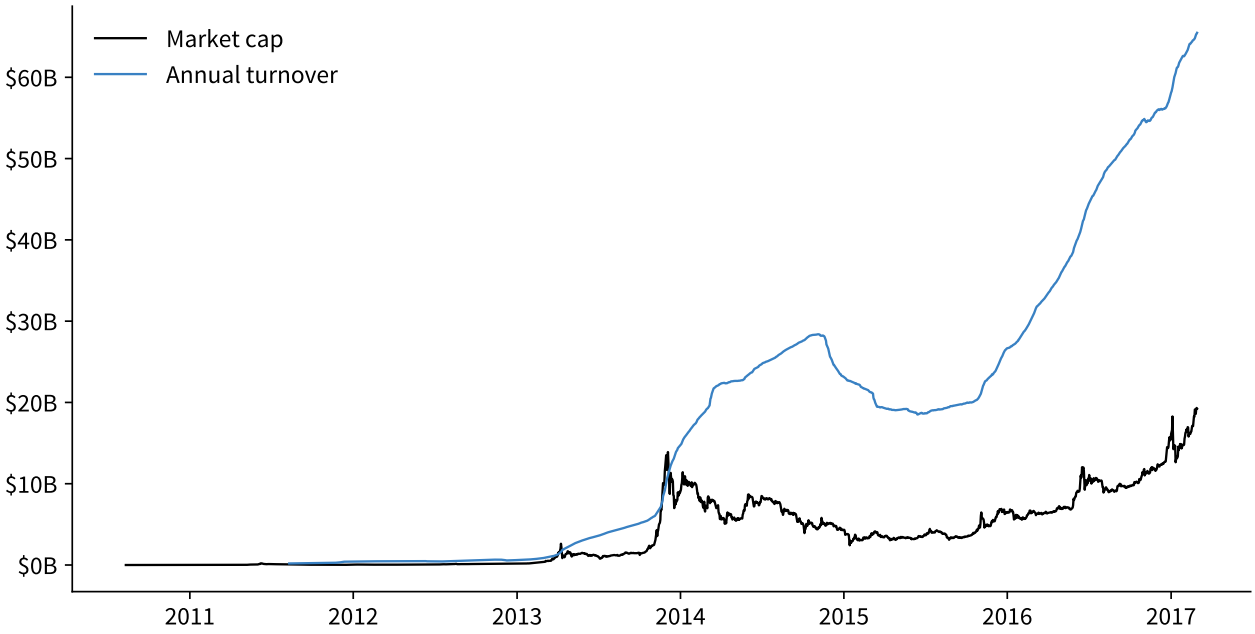

Figure 4: Bitcoin market cap and turnover (trailing 365 days).

latest block of transactions. Bitcoin uses standard hash functions as watermarks, the longest chain of transaction blocks with valid hashes provides the consensus for the Bitcoin transaction history (Figure 6). A more detailed explanation of hash functions and Bitcoin mining is included on page 12 and page 15, respectively.

Because Satoshi chose secure and widely used technologies as the main building blocks for his payments system, Bitcoin is highly reliable and secure. Several bitcoin exchanges and wallets containing users private keys have been hacked through negligent administration or vulnerabilities in supporting systems. To date, however, no fundamental security flaw has been identified in Bitcoin.

Each Bitcoin transaction refers to a previous input transaction to establish the source of the bitcoins to be sent. The sender creates and signs a transaction script with the output amounts and addresses of the recipients. The sender broadcasts the transaction onto the P2P network. Receiving nodes check and relay the transaction to their peers. A transaction can include a short message of up to 80 bytes. The release of the outputs can be delayed until a specified time and date. Multi-signature addresses are supported, requiring M of N keys, for example 2 of 3, to release funds. Miners claim new bitcoins in a special transaction called a coinbase transaction. All bitcoins in circulation can be traced back to a miner coinbase transaction. An example of a Bitcoin transaction script is shown on page 16.

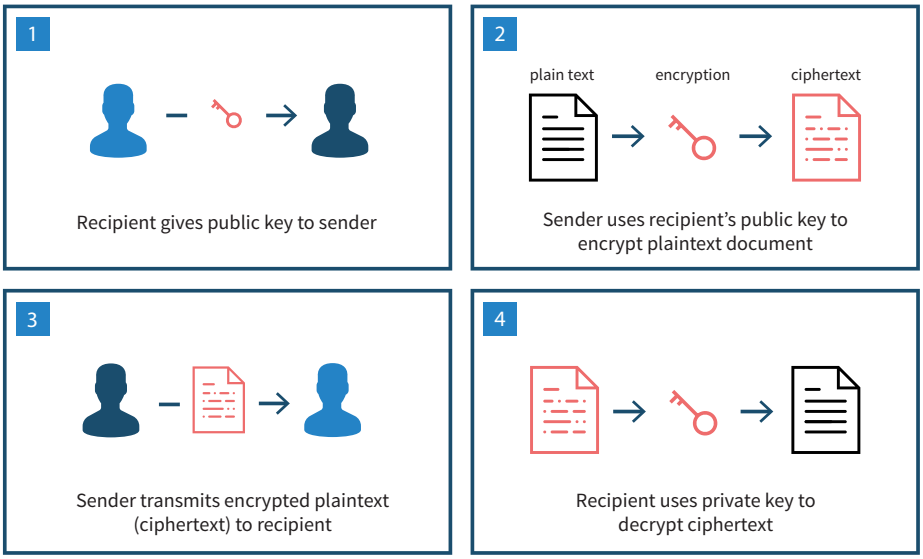

Figure 5: An illustration of how public key encryption is used to exchange information confidentially [18]. The sender uses the recipient's public key to encrypt a message which can only be decrypted by the recipients private key. Bitcoin and other blockchains platforms use same technology to authorize and send payments. The payer uses his private key to sign and authorize a release of funds from his address; the payee's public key serves as the receiving address.

Hashing with SHA256
A strong cryptographic hash function results in an output which can not be used to guess the original input message. Bitcoin uses the hash function SHA256 [21]. When applied to the input message "The quick brown fox jumps over the lazy dog(.)", SHA256 produces two very different outputs depending whether or not the full stop (.) is included:

```
"c03905fcdab297513a620ec81ed46ca44ddb62d41cbbd83eb4a5a3592be26a69"
"(b47cc0f104b62d4c7c30bcd68fd8e67613e287dc4ad8c310ef10cbadea9c4380)"
```

As illustrated by this example, it is practically impossible to guess the input message from the output hash value. Hash functions are frequently used to encrypt passwords.

The cryptographic hashes which serve as watermarks of the transaction blocks play a key role in securing the Bitcoin ledger, the blockchain. Each valid new transaction block includes the hash of the previous block in the blockchain (Figure 6). A new block n is linked to the preceding block $n-1$. The next valid block $n+1$ will, in turn, include a link to n. Any attempt at changing a transaction in the blockchain therefore requires recalculating not only the hash for the target block but also the hashes of all subsequent blocks. Unless the attacker commands 51% or more of the miners it is practically impossible for him to recalculate an alternative blockchain with the

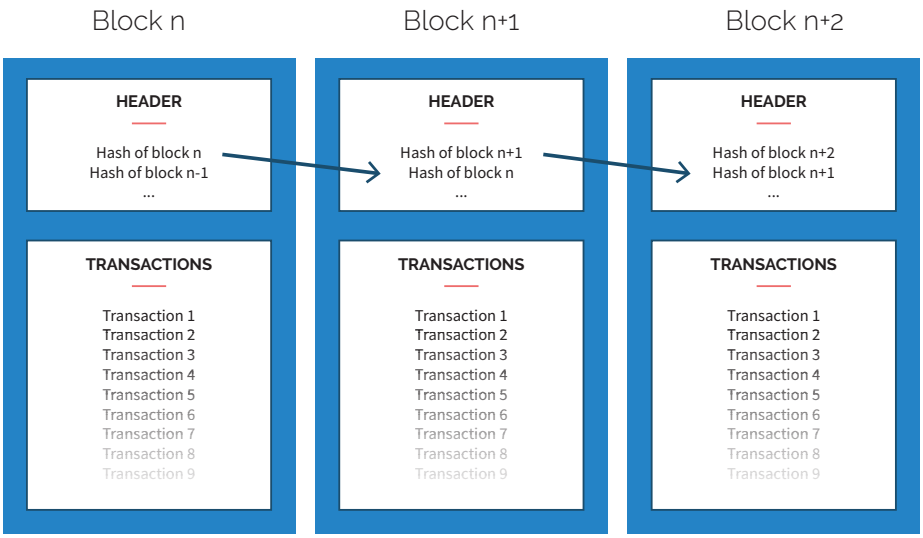

Figure 6: The Bitcoin transaction ledger is a chain of interlinked transaction blocks, secured and timestamped with cryptographic hashes of the block header (Table 1). The process of calculating a valid hash is known as mining (page 15).

modified transaction. The linked hashes guarantee the integrity of the blockchain and remove the need for a trusted authority to keep a central transaction ledger.[4]

[4]We estimate the replacement cost of the current mining capacity of 3.5 petahash/second at over $3 billion; the marginal cost of operating that capacity for a year is about $300 million dollars, and the power consumption is roughly 400 MW [19].

Field	Purpose	Updated when …	Size (B)
Version	Block version number	New protocol version	4
Prev. block hash	256-bit hash of the previous block header	A new block comes in	32
Merkle root hash	256-bit hash based on all of the transactions in the block	A transaction is accepted	32
Time	Current timestamp as seconds since 1970-01-01T00:00 UTC	Every few seconds	4
Bits	Current target in compact format	The difficulty is adjusted	4
Nonce	32-bit number (starts at 0)	A hash is tried (increments)	4
Transaction count	Number of transaction entries	If new block is started	1

Table 1: The data fields of a Bitcoin block header, the total size is only 81 bytes [20].

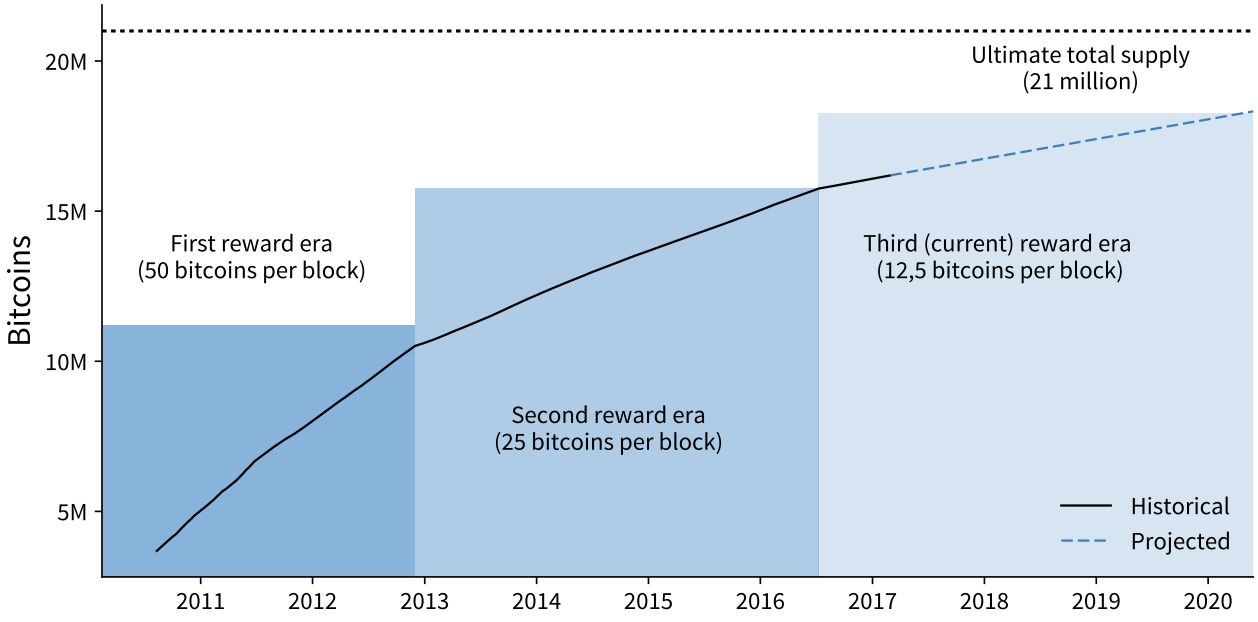

Figure 7: TOTAL SUPPLY OF BITCOINS. The new bitcoin block reward started at 50 BTC per block and halves every 210,000 blocks. The ultimate total supply is therefore limited at 21 million, the last new bitcoins are projected to be issued in late 2040 [23].

It is important to keep in mind that the success of Bitcoin relies on more than just clever technology. Some of the key attributes of Bitcoin which drive its success are:

Architecture	Reliable and tested technologies used for key components.
Incentives	Built-in incentives for users and miners.
Marketing	Good choice of brand name, release targeted at early adopters.
Permissioning	Permissionless participation for users and miners.
Secure	Strong cryptography protects users balances and ledger integrity.
Trust	Bitcoin mitigates the need for trust by not relying on a central authority or existing financial infrastructure.
Value proposition	A radically different approach to online payments over prior alternatives with potential for significant cost and performance improvement.

Bitcoin mining
The Bitcoin blockchain consensus process called mining. Bitcoin miners compete to calculate a valid double SHA256 hash (page 12) of the Bitcoin block header (Table 1). The hash serves as proof-of-work for the Bitcoin blockchain. If the hash meets a target difficulty the successful miner is rewarded with all the transaction fees of the included transactions and a fixed number of new bitcoins. If the hash does not meet the target difficulty, a random field called nonce is changed and the hash is recalculated until a valid hash meeting the target difficulty is found. The target difficulty is adjusted every 2016 blocks to aim for an average 10 minute interval between new blocks. A valid hash has a certain number of leading zeros defined by the target difficulty.
Shown below is the hash of Bitcoin block 345,981 which was mined on March 3, 2015, for a block reward of 25 BTC and transaction fees of 0.09805807 BTC [22]. The block included 710 transactions and was mined by KnCMiner. The double SHA256 hash of the header of block 345,981 is:

```
"000000000000000003e560d227c225b5cdf7bcee3358d53222d5d0af6240db4d"
```

Bitcoin transaction example

Bitcoin transaction `90b18aa54288ec610d83ff1abe90f10d8ca87fb6-411a72b2e56a169fdc9b0219` took place on February 19, 2014, and was included in block 286,731. The transaction has a single input of value BTC 1,684, the sender address `1GqpaRR` acquired the bitcoins in the previous transaction `18798f8`. The two outputs of BTC 1,678.069 and BTC 5.931 were sent to addresses `18mZn5V` and `17rfobS`, respectively. The voluntary transaction fee was zero. The gross value of the transaction at the time was just over one million dollars [12, 24].


```
{
  "hash":"90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219",
  "version":1,
  "lock_time":0,
  "size":226,
  "inputs":[
    {
      "previous_transaction_hash":"18798f8795ded46c3086f48d5bdabe10e1755524b439
                                   12320b81ef547b2f939a",
      "output_index":0,
      "amount":168400000000,
      "script":"3045022100c1efcad5cdcc0dcf7c2a79d9e1566523af9c7229c78ef71ee8b63
                00ab59aa63d02201fe27c3e6374dd3a5425a577d9ca6ad8ff079800175ef9a4
                4475bc98bcef21cf01 023b027d54ce8b6c730e0d5833f73aec6a5bae4efe04
                f57d2864a6a7df2af56e46",
      "addresses":[
        "1GqpaRRvdX8HpqRUzg42v5GMPEoFDXV27Q"
      ]
    }
  ],
  "outputs":[
    {
      "amount":593100000,
      "spent":true,
      "script":"OP_DUP OP_HASH160 4b358739fc7984b8101278988beba0cc00867adc
                OP_EQUALVERIFY OP_CHECKSIG",
      "script_hex":"76a9144b358739fc7984b8101278988beba0cc00867adc88ac",
      "script_type":"hash160",
      "addresses":[
        "17rfobSZ8Dj61c8sanhzzR76ADMjWYYpCP"
      ]
    },
    {
      "amount":167806900000,
      "spent":true,
      "script":"OP_DUP OP_HASH160 55368b388ccfe22a3f837c9eee93d053460db339
                OP_EQUALVERIFY OP_CHECKSIG",
      "script_hex":"76a91455368b388ccfe22a3f837c9eee93d053460db33988ac",
      "script_type":"hash160",
      "addresses":[
        "18mZn5VXoxcb6MbNKQj17bX4qYxNEU7SDe"
      ]
    }
  ],
  "amount":168400000000,
  "fees":0,
  "confirmations":122442,
  "block_height":286731,
  "block_hash":"00000000000000000bf3856e067ec21f4c30a8a859cc7ed7f2de9a2b579200639",
  "block_time":"2014-02-19T16:47:08Z",
  "block_branch":"main"
}
```


Miners' incentives play a key role in Bitcoin's success. Mining is capital intensive,

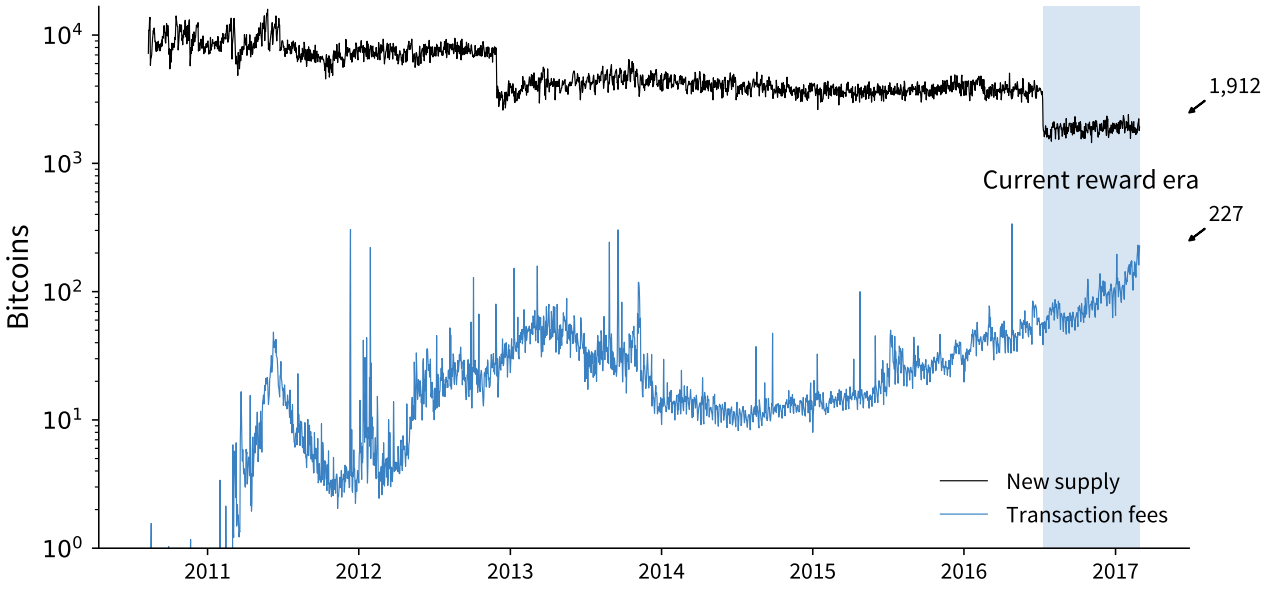

Figure 8: THE BITCOIN BLOCK REWARD: NEW SUPPLY AND TRANSACTION FEES (DAILY). NEW SUPPLY IS CURRENTLY 8× GREATER THAN TRANSACTION FEES [12].

the replacement cost of the Bitcoin network now stands at an estimated $500 million [19]. The miners are rewarded by new issue of bitcoin and block transaction fees (Figure 8) which currently generates annual revenues of $592 million. New issue of bitcoin declines over time, ultimately miners will derive most of their revenues from transaction fees (Figure 7). Early miners are rewarded for providing consensus services by a subsidy of new bitcoins (Figure 8).

Because miners' revenues in the early stages of the ecosystem are predominantly derived from new supply, miners can process transactions with zero fees which encourages user adoption. Other properties also facilitate user adoption. Importantly, bitcoin has all the qualities required of money. The bitcoin cryptocurrency is fungible, each bitcoin is the same as another one. Bitcoin is divisible, each bitcoin can be subdivided into 100 million units, called satoshi, for a total of 21^{14} satoshi. With global population approaching 10 billion, the ultimate supply of bitcoin in terms of satoshi is approximately 210,000 satoshi per person, enough to price even the least expensive goods and services in terms of satoshi for some time to come. Bitcoin relies on proven cryptographic technologies which makes it impossible to counterfeit. And bitcoin has predictable and finite supply, as the ecosystem matures it is likely to retain value. Because of these qualities, bitcoin has the potential to provide the same function as traditional currencies and serve as means of payment, as store of value, or as unit of account.

Bitcoin has been described as a "big deal" (Dan Kaminsky) and "a technological tour de force" (Bill Gates) [25, 26]. Currently, it is on a growth track comparable to that of PayPal, it's value and volume as a payments network are likely to continue to grow. Bitcoin is also a catalyst and a model for a whole new category of commercial and social networks, in finance and in other sectors.

Ethereum

Ethereum, a blockchain for distributed applications

The second most valuable blockchain by market cap is Ethereum, currently valued at $1.4 billion. First proposed in 2013 by Vitalik Buterin, and further described by Gavin Wood in 2014, the Ethereum blockchain was launched on July 30, 2015 [27, 28, 29]. Like Bitcoin, Ethereum has a native cryptocurrency called ether which currently trades at $15.88. The current supply is 89 million whereof 72 million was pre-sold in July of 2014 for bitcoin then valued at $18.5 million in order to fund development [30, 29].

Figure 9: The price of ether (ETH) [31].

Like Bitcoin, Ethereum can be used to make online payments using ether. The stated purpose of Ethereum extends, however, far beyond online payments. It is designed to run distributed applications, Dapps, also referred to as smart contracts. Vitalik Buterin described Ethereum in his original whitepaper as follows:

> The intent of Ethereum is to create an alternative protocol for building decentralized applications, providing a different set of trade offs that we believe will be very useful for a large class of decentralized applications, with particular emphasis on situations where rapid development time, security for small and rarely used applications, and the ability of different applications to very efficiently interact, are important [27].

The online guide accompanying Ethereum's first release, Frontier, describes Ethereum in the following words:

> Ethereum can be viewed as a single computer that the whole world can use …anybody can upload programs to the Ethereum World Computer and anybody can request that a program that has been uploaded be executed …every program has its own permanent storage that persists between executions [32].

Broadly speaking, Ethereum is Bitcoin with the addition of distributed applications. Ether is intended as means of payment for services requested by users or distributed applications deployed on the Ethereum network. Resource requirements of user transactions and Dapp are measured in special units called gas. Users pay for transactions with ether, and the Dapp are funded with ether which is used to pay for their execution:

$$\text{transaction fee (in ether)} = \text{transaction cost (in gas)} \times \text{gas price (in ether)}$$

Users and distributed applications can specify the maximum price they are willing to pay for gas, and miners can specify the lowest price. The goal of the design is to let user demand for services and miner supply of resources determine the price of ether.

Consensus in Ethereum is provided by a mining algorithm. The Ethereum mining algorithm hashes not just the new block header but also a dataset generated from previous block headers. Miners are rewarded by new supply of ether and transaction fees, the supply of new ether will increase at a constant annual maximum amount of 18 million ether which is 25% of the ether sold in 2014 to fund initial development [33, 34]. Ethereum mining is scheduled to change in 2017 with the introduction of bonded validators which would require miners to hold a deposit of ether in order to mine [35].

Because Ethereum is more recent than Bitcoin and has a much broader remit, it is difficult to predict how adoption will evolve. But the success of Bitcoin in global payments suggests that Ethereum has considerable potential to serve as distributed ledger for various types of transactions not addressed by Bitcoin. Ethereum adoption was given further boost by the announcement on February 27, 2017, of an Enterprise Ethereum Alliance of thirty leading companies from finance and information technology, including Microsoft, JP Morgan, and Intel [36].

Ethereum architecture

Ethereum has two types of accounts, one comparable to a Bitcoin account and another for use with smart contracts or distributed applications:

External account — Controlled by private keys, has ether balance and can send and receive messages.

Contract account — Controlled by contract or Dapp code, has ether balance, can send and receive messages, run internal code, read and write to internal storage and create other contracts.

A sample Ethereum contract account is shown on page 20; Table 3 compares the features of Bitcoin and Ethereum accounts.

Feature	Bitcoin	Ethereum external	Ethereum contract
Holds balance	Yes	Yes	Yes
Messages	Yes	Yes	Yes
Holds code	No	No	Yes
Stores data	No	No	Yes

Table 2: Comparison of the features of Bitcoin and Ethereum accounts.

Ethereum contract
Ethereum includes a high-level language for creating smart contracts, Solidity. The contract shown here demonstrates how to create a coin which can be transacted on the Ethereum blockchain [37]. Ethereum contracts defined in high-level languages such as Solidity are compiled into byte code which runs on a virtual machines deployed on the Ethereum network.

```
contract token {
  mapping (address => uint) public coinBalanceOf;
  event CoinTransfer(address sender, address receiver, uint amount);

  /* Initializes contract with initial supply
     tokens to the creator of the contract     */
  function token(uint supply) {
    coinBalanceOf[msg.sender] = supply;
  }

  /* Very simple trade function */
  function sendCoin(address receiver, uint amount)
                                    returns(bool sufficient) {
    if (coinBalanceOf[msg.sender] < amount) return false;
    coinBalanceOf[msg.sender] -= amount;
    coinBalanceOf[receiver] += amount;
    CoinTransfer(msg.sender, receiver, amount);
    return true;
  }
}
```

Like Bitcoin, new Ethereum blocks contain transactions broadcast since the last block, including transactions rewarding successful miners with new ether and transaction fees. Unlike Bitcoin, Ethereum transaction blocks also include a hash of the new state of all accounts after applying the new transactions.

The last notable difference between Bitcoin and Ethereum is the transaction scripting language. The Bitcoin transaction language includes basic instructions, or scripts, required to transfer bitcoin balances from one account to another. Bitcoin scripts are deliberately restricted in order to keep execution time finite, for example they

Feature	Bitcoin	Ethereum
Consensus	Mining (double SHA256)	Mining (Ethash)
Stores	Transactions	Transactions & state (account balances, code, data)
Block time	10 min	14 sec
Maximum block size	1 Mb (2 Mb proposed)	None
Blockchain size	77 Gb	15 Gb

Table 3: Comparison of the features of Bitcoin and Ethereum blockchain.

can not loop. The Ethereum transaction scripting language extends scripting functionality to include such features as adjustable transaction sizes, loops (iterations) and ability to include additional blockchain data as inputs. Each step in the execution of the scripts accrues a computational charge in gas which must be paid for with ether. The Ethereum scripts are therefore restricted by economic constraints instead of technical ones. In terms of computer theory, the Ethereum scripting language is Turing complete but the Bitcoin scripting language is not.

Ripple

Ripple, a blockchain for global payments and settlements

Ripple is a P2P payment and settlement network developed and promoted by a private company called Ripple Labs, Inc, founded in 2012 [38, 39]. Ripple uses a distributed open ledger, but the architecture and intended use differs in many important respects from Bitcoin.

Like Bitcoin, Ripple has a native cryptocurrency, XRP, which is used to pay transaction fees. The supply of XRP is 100 billion XRP all issued at launch. The two cofounders of Ripple Labs received 10 billion each, and Ripple Labs received 80 billion XRPs of which approximately 15 billion have been distributed to various other parties. Each XRP can be divided into million subunits called drops.

In the period from February 2016 to February 2017 XRPs traded from $0.0055 to $0.0084 (Figure 10). On March 1, 2016, the XRP price was $0.0055 corresponding to a market cap of $203 million, ranking fourth behind Bitcoin, Ethereum and Dash.[5] On March 1, 2017, the trailing 12 month payment volume of Ripple was $1.2 billion.

Unlike Bitcoin, the Ripple network is designed to support transactions of IOUs issued by network participants, for example currency certificates of deposits. XRPs are required to pay transaction fees on the Ripple network. XRPs spent on transaction fees can not be re-spent, they are destroyed. The purpose of the XRPs is to provide a mechanism for Ripple Labs to charge for access to the network and at the same time impose a cost on spamming attacks.

The main actors on the Ripple network are [38]:

[5] XRP market cap is calculated based on supply of XRP not held by Ripple Labs, 37 billion units to date. The market cap based on the full supply of 100 billion was $547 million [41].

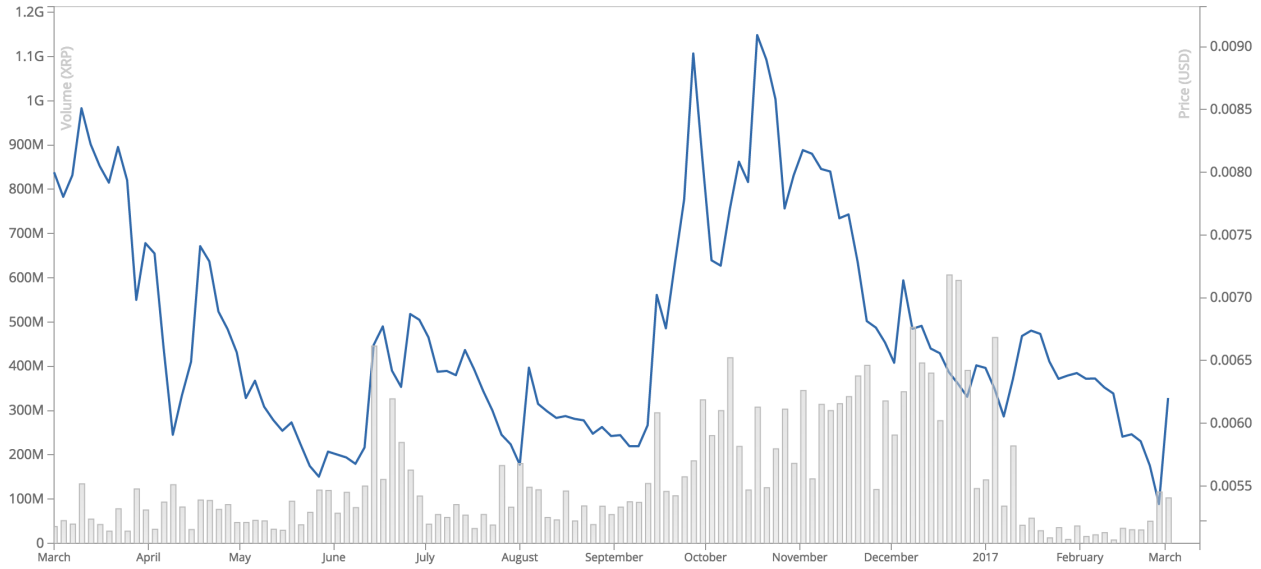

Figure 10: The one year price and volume history of XRP on March 1, 2017 [40].

Issuing gateways	Issuing gateways create IOUs to represent assets they hold on behalf of users, for example USD IOUs.
Private exchanges	Private exchanges provide a venue for users to trade XRP. There is also a currency exchange built into the Ripple protocol itself.
Merchants	Merchants accept payment within the Ripple consensus network in exchange for goods and services.
Users	Users use Ripple network to transfer IOUs between each other, paying transaction fees in XRP.

The original goal of Ripple was to build transaction volume of the IOUs thereby generating demand for XRPs. As of April 25, 2015, there were 23 issuing gateways listed on the Ripple Labs website, the greatest IOU balance was in USD-denominated IOUs, total value was approximately $6 million issued by four gateways [40].

In spite of the modest volume and balances on its payment network, at the time of this writing Ripple Labs is still operating its global payments network. In Q4 of 2015, however, Ripple Labs announced software solutions for banks involved with cross-border payments and FX trading, and the revenue model of the company has changed to include software licensing. Ripple Labs claimed on its website that it was working with “10 out of the top 50” banks [38].

Ripple architecture

The Ripple ledger contains not only transactions but also account states or balances. Like Bitcoin and Ethereum, authorized transactions are broadcast on a P2P network.

Nodes which participate in consensus are called validators [42]. Validators decide which other validators they trust and then vote on which transactions to include in a ledger update. Notes keep voting on new transaction lists until a supermajority of trusted validators agrees on a new version of the ledger. The transactions in the new transaction block are then added to the previous version of the ledger, and the account states of all balances are changed to reflect the new transactions. Participation in the validation process is voluntary and does not require permission; validators are not rewarded for participating in forming consensus. The native transaction scripting language of Ripple is restricted, a contract language has been outlined but not implemented [43].

Ripple transaction
Below, a Ripple transaction showing payment of $1 from account `rf1BiGe` to `ra5nK24` using an USD denominated IOU issued by account `rf1BiGe`. The transaction fee is 10 drops [38].

```
{
  "TransactionType" : "Payment",
  "Account" : "rf1BiGeXwwQoi8Z2ueFYTEXSwuJYfV2Jpn",
  "Destination" : "ra5nK24KXen9AHvsdFTKHSANinZseWnPcX",
  "Amount" : {
     "currency" : "USD",
     "value" : "1",
     "issuer" : "rf1BiGeXwwQoi8Z2ueFYTEXSwuJYfV2Jpn"
  },
  "Fee": "10",
  "Flags": 2147483648,
  "Sequence": 2,
}
```

The Ripple ledger is several terabytes in size, Ripple Labs keeps an official copy but nodes on the Ripple network do not necessarily maintain the full transaction history, only the most recent state of the ledger.

Corda

Developed by R3 in partnership with over seventy international banks, Corda is a distributed ledger platform designed to record, manage and synchronize financial agreements between regulated financial institutions. First released on November 30, 2016, at the time of this writing Corda has not yet been tested in the marketplace to the same extent as other blockchain technologies. It deserves mention, nevertheless, because of several factors:

Architecture While inspired by blockchains, transactions are shared selectively between transacting parties and not published on a blockchain, consensus is established by "predetermined observers" which are independent of transacting parties [44].

Partnerships The Corda platform is developed in close partnership with over seventy leading international banks.

Team — The Corda team includes experienced business executives and Bitcoin developers.

Some of the key features of Corda are listed in Table 11.

Hyperledger

Launched on September 13, 2016, Hyperledger is an "umbrella" project for open source blockchain and smart contract technologies hosted by the Linux Foundation [45]. The stated goal of Hyperledger is:

> …to advance blockchain technology by identifying and addressing important features for a cross-industry open standard for distributed ledgers that can transform the way business transactions are conducted globally.

Hyperledger is new in the market but deserves mention nevertheless as an open source cross-industry collaborative project with participants from automotive, consulting, IT, financial services and other sectors.

Initially, Hyperledger focuses on three sectors: finance, health care and supply chain management. There are currently five business blockchain projects listed on the Hyperledger website, three of which are in "incubation". To date, the Hyperledger project which has arguably captured the most mindshare is Sawtooth, a modular blockchain suite contributed by Intel. Among notable features is a new consensus algorithm, Proof of Elapsed Time (PoET). PoET relies on trusted execution environments in Intel processors to pseudo-randomly select a leading validator for new block assembly each time a blockchain is updated. As with Corda, the Hyperledger projects have not yet been tested in the marketplace to a comparable extent to other blockchain technologies. Some of the key features of Hyperledger are listed in Table 11.

Open source blockchain summary

Key properties of main open source blockchains are summarized in Figure 11, the comparison reflects current feature sets. Many proposals have been published which aim evolve each of the protocols. Some of the most notable ones include:

Bonded validators — It has been proposed to change the Ethereum consensus protocol and require miners to be bonded, i.e. to hold ether deposits, starting in 2017 [46].

Confidential transactions — Confidential transactions is a new method for keeping the amounts transferred in any blockchain transaction visible only to participants in the transaction [47].

Merged mining — Merged mining is a process for mining non-Bitcoin blockchains at the same time as the Bitcoin blockchain, including blockchains supporting smart contracts [48, 49].

Sidechains — Sidechains is a proposed set of procedures and standards for linking non-Bitcoin blockchains to the Bitcoin blockchain [48].

	Bitcoin	Ethereum	Ripple	Hyperledger	Corda
Targeted use	Online payments (P2P)	Smart contracts (P2P)	Global settlement (financials)	Cross-industry platform	World's largest financial institutions
Author(s)	Anonymous	Vitalik Buterin, Gavin Wood,*et al*	Ripple Labs	Multiple	R3
Licensing	MIT	MIT (proposed)	ISC	Apache 2.0	Apache 2.0
Governance	Core developers, companies	Core developers, companies	Ripple Labs	Consortium	R3
Native token	Bitcoin (BTC)	Ethereum (ETH)	Ripple (XRP)	None	None
IOUs	No	Yes	Yes	Yes	Yes
Transaction script	Restricted	Turing complete	Restricted	Turing complete	Turing complete
Smart contracts	Limited (as yet)	Yes	Limited (as yet)	Yes	Yes
Consensus	Mining	Mining (revised in 2017)	Trusted validators	Trusted validators	Trusted validators
Block interval	10 min	14 sec	< 10 sec	2-3 sec	Arbitrary
Private blockchains	Possible	Possible	Possible	Only	Possible
Derivatives	Litecoin, Namecoin, others	None yet	Stellar	None yet	None yet

Figure 11: Comparison of the key features currently supported by five leading open source blockchain technologies, Bitcoin, Ethereum, Ripple, Hyperledger and Corda.

Public or private blockchains

Bitcoin, Ethereum and Ripple all operate as open, permissionless transaction networks. There is only one Bitcoin blockchain which participants agree on, the same applies to Ethereum and Ripple. The protocol on which these blockchain technologies are based and the code base which powers many of the nodes does, however, allow anyone to set up their own network with a separate blockchain. The terms "permissionless", "permissioned", "public" and "private" are variously used to define different blockchain configurations [50]:

Public blockchains
: A public blockchain is permissionless, anyone can send transactions and read the transaction ledger, and anyone can participate in the consensus. There is no central authority which maintains an official copy of the ledger. Public blockchains are "fully decentralized".

Consortium blockchains
: A consortium blockchain is a blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, a consortium of several financial institutions, each of which operates a node and the majority of which must sign every block to form consensus. The right to read

	and write the blockchain may be restricted in part or full. Consortium blockchains are “partially decentralized”.
Private blockchains	A private blockchain is a blockchain where all permissions are controlled by a single entity, they are effectively “centralized”.

Blockchain companies

Parallel to the open source blockchain initiatives, a number of private companies have announced blockchain products or services, both open source and proprietary. Some of the more prominent ones are:

Blockstream	A pioneer in evolving blockchain technology that has proposed sidechains architecture for linking blockchains and confidential transactions.
Chain.com	Developing blockchain solutions for financial markets.
Clearmatics	Developing proprietary decentralized clearing solutions based on blockchains.
ConsenSys	Blockchain application developer founded by key contributors to the Ethereum project.
Digital Asset Holdings	Developing blockchain solutions for financial markets.
Elliptic	Developing analytic tools for blockchains.
Eris Industries	Developing blockchain platform supporting smart contracts.
Multichain	Developing proprietary blockchain solutions based on Bitcoin.
R3 CEV	R3 leads a consortium of over forty global banks developing blockchain solutions for financial markets.
Symbiont	Developing proprietary blockchain solutions with focus on smart contracts.
T0	Developing blockchain solutions for trading and settlement.

Blockchains and existing digital data storage

When comparing blockchains with existing data storage technologies, the two main question to consider are differences in structure and usage.

Structure	How are blockchains different from existing data storage technologies?
Usage	When is it appropriate to use blockchains instead of existing data storage technologies?

Because blockchains are relatively new, a small but growing number people are attempting to explain, define and use them, ranging form academics to entrepreneurs

to CTOs of established companies. New papers, presentations and demos appear almost daily. Although a general understanding is emerging of what blockchains can and can not do, it is unlikely that the full implications of blockchain technology will be understood for some time yet.

Traditional data storage structures

Broadly, traditional digital data storage fall into six categories [51]:

Relational Relational database management systems (RDBMS) are implemented as two-dimensional tables which are queried and managed using Structured Query Language (SQL). RDBMSs exist in a number different closed source and open source implementations, two of the best known include Oracle RDBMS and PostgreSQL.

Key-value Key-value databases are structured as look-up tables. A key is used to look up a value similar to how a file name is used to locate a document on a file system. Examples include LevelDB and Berkeley DB.

Columnar A database structure similar to RDBMS which organizes data by column. Cassandra is one example.

Document Document databases are designed to store documents. MongoDB is one example.

Graph Graph databases structure data in terms of nodes and relationships between nodes. Neo4J is one example.

Polyglot Polyglot systems are systems which use two or more categories of databases.

Seven out of the ten most popular database engines in the world are relational, one is document, one is columnar and one is key-value [52].

Database deployment can either be centralized or distributed. To avoid conflict in distributed deployments, rules are established and imposed on data modifications. A common configuration for distributed databases is referred to as "master-slave" where one database has ultimate say over data content and others replicate. Databases support flexible data definition, manipulation and queries by means of standards and languages, such as SQL for RDBMS.

Two features of blockchains which distinguish them from existing data storage systems are [53]:

Conflict resolution Conflict resolution rules for modifying data which protect transaction integrity without need for "master" nodes.

Smart contracts Embedded support for contracts that modify the blockchain data in complex transactions.

Bitcoin is a good example of the former, it has run for over seven years without any central nodes. Ethereum which launched in mid-2015 is holds the promise to be a good example of a blockchain with the latter property, which is limited in Bitcoin. Together, Bitcoin and Ethereum serve as useful starting points for evaluating when

blockchains can be used instead of existing databases.

When are blockchains better?

The practical, short answer to the question of when to consider using blockchains is simple: Whenever other data storage systems don't meet design goals. To date, Bitcoin serves as the primary example of a successful blockchain architecture and use case. Bitcoin is an open and decentralized transaction network which would have been impossible to implement using existing data storage technologies. The data storage is in the blockchain according to predefined data definition rules. Manipulation of data is restricted to writing irreversible transactions which must conform to predefined rules. Queries are not supported, they must be run on separate systems. Bitcoin fulfills its own design and blockchain selection criteria which is to make trusted financial intermediaries irrelevant.

When considering other possible use cases for blockchains, it is useful to ask where open and decentralized transaction networks with distributed ledgers may be useful for social or commercial transactions. In addition to Bitcoin, some notable applications of blockchains are:

Ethereum Ethereum extends the features supported by Bitcoin to include more sophisticated and complex transactions.

Litecoin Litecoin is an open and decentralized payment network based on Bitcoin but with a different mining algorithm and shorter block interval.

Namecoin Namecoin is an open and decentralized key-value data storage blockchain based on Bitcoin.

Twister Twister is an open and decentralized P2P micro-blogging blockchain based on Bitcoin.

As the above examples show, there already exist modifications of Bitcoin (Litecoin), radical extensions of Bitcoin in terms of features (Ethereum), and extensions of Bitcoin into alternate domains (Namecoin, Twister). Only time will tell which of these networks and technologies will grow beyond small communities of early adopters.

We think that it is highly probable that new commercial and social networks based on blockchains will emerge over the next decades. Much of the architecture and code is in the open domain, it is easy for individuals and institutions to fork and experiment. It is impossible to anticipate all the future use cases for blockchains. Successful blockchains are most likely to emerge where there is either demand for a completely new type of network or demand for an alternative to an existing centralized closed configuration vulnerable to censorship with low levels of service, high fees or other features undesirable to end users.

Financial services

> Get closer than ever to your customers. So close that you tell them what they need well before they realize it themselves.
>
> Steve Jobs

Stakeholder analysis

New emerging business models, based on distributed ledgers, can potentially alter significantly how financial services will be offered in the future. In the process, tens of billions of dollars of capital may be saved, new services offered with increased efficiency and value. Such a change will obviously change the competition landscape, stakeholders roles and their relationships. In order to evaluate such a likely financial services endgame it is helpful to map the stakeholders, likely trends and the value chain.

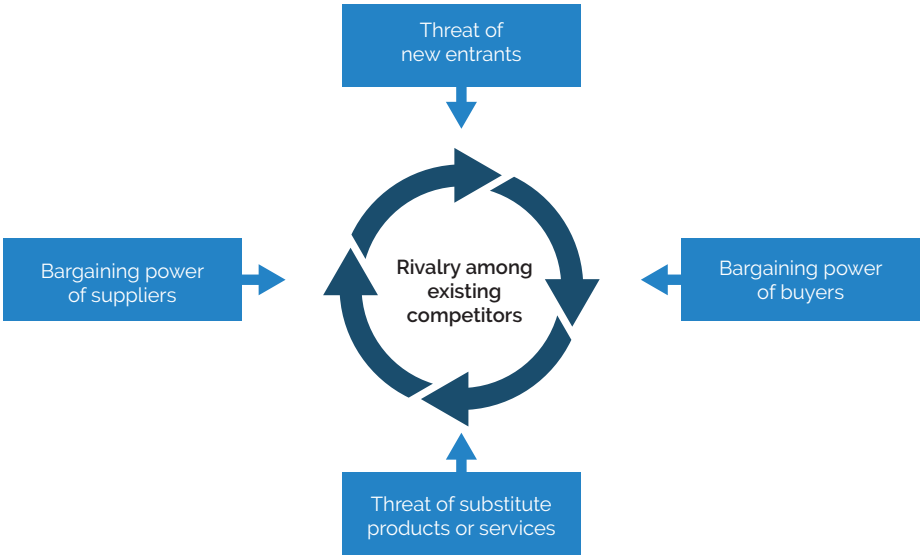

Figure 12: Porter's five forces of competitive position. See Porter, M.E., (1979), "How Competitive Forces Shape Strategy", HBR, March 1979.

In this chapter we conduct a stakeholder analysis for a future blockchain-based financial sector. The analysis is based on Porter's five forces of competitive position analysis, see figure 12.

Threat of new entrants

In banking it is sometimes stated that: "Payments are, after all, the glue that holds customers, both depositors and borrowers, to the bank" [54]. Currently deposits are mostly kept at banks that control, safeguard, and provided centralized deposit services. However, the promise of distributed ledgers is that deposits don't need to be centrally controlled; deposits can be stored on a distributed transaction ledger

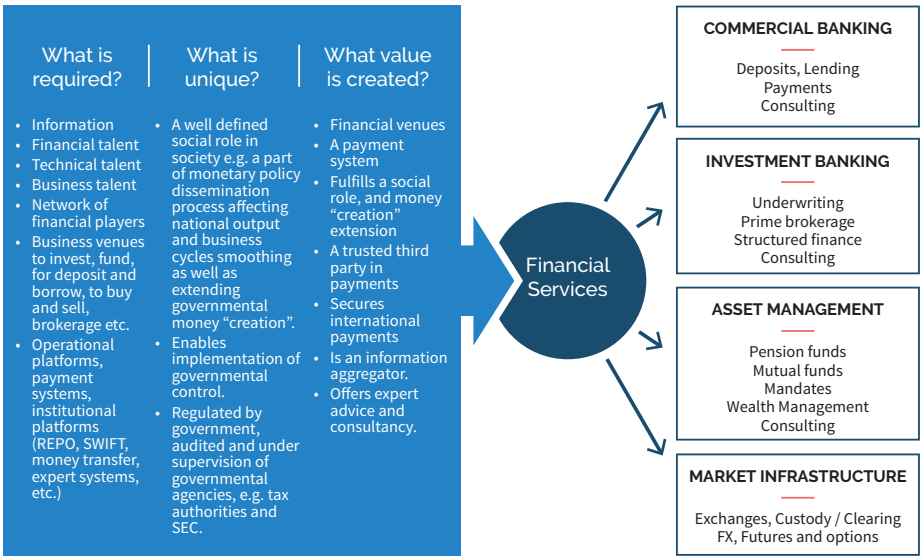

Figure 13: What is financial services? What value is created and how? What enters into the value creation process? What constitutes the difference between financial services and other businesses?

network. In that case, the bank's "glue" will loose its grip. "The degree to which the payments industry has changed in just a decade is off the scale. We've witnessed the arrival of new currencies, technologies, business models and forms of transactions; all within an environment of global economic upheavals and increasingly comprehensive regulation. The most significant change has been the arrival of new players; non-bank financial institutions that bring a groundswell of innovation and are turning market models on their head" [55].

The list of potential new fintech entrants is long and growing, see Figure 14. Global investment in financial services-related startups has soared, and increasingly established large firms invest in blockchain related technology and ventures. The landscape of new entrants is rapidly changing and a good overview is provided by William Mougayar in figure 14, see further [56].

Threat of substitutes

Threat of substitutes occurs when companies within one industry are forced to compete with industries producing substitute products or services. In financial services, Apple and Samsung are good examples how tech giants came up with substitute mobile based payment services. But although Apple- and Samsung Pay offer new ways to pay, they are currently based on a centralized payment processing network operated by the banks. However, this infrastructure is likely to be temporary and soon to be replaced by leaner, better and less costly upcoming infrastructure of distributed payment transaction networks, see figure 15. When that happens, the end-customer is unlikely to notice such a change except in the form of increased efficiency, more options, and better services and value. But, when the payment infrastructure has been converted future global players can offer payment services, independent of

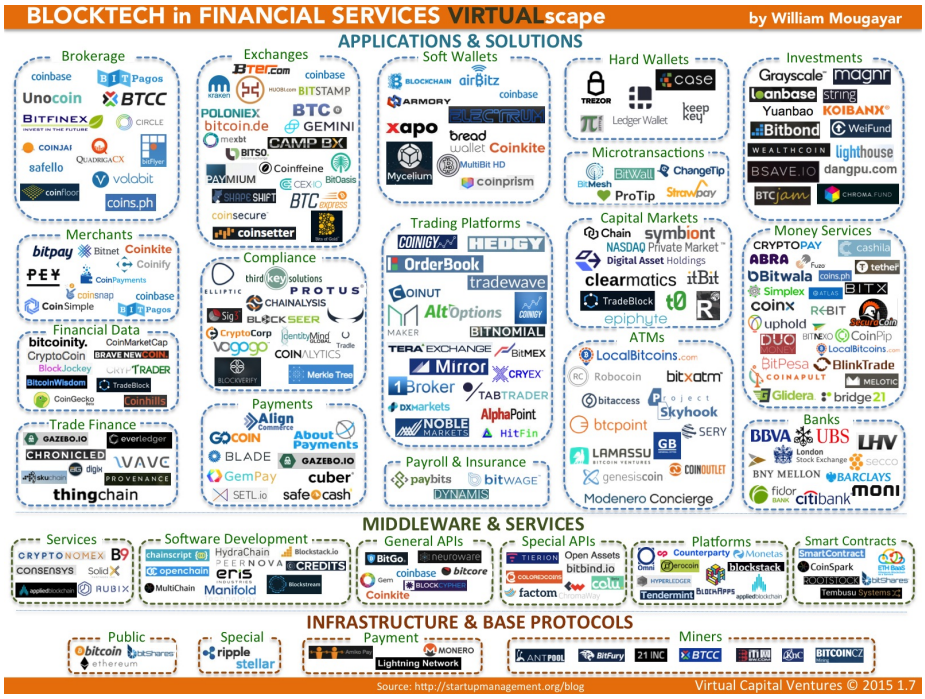

Figure 14: An overview of the rapidly changing landscape of new entrants entering into the fintech blockchain-based ecosystem [56].

banks and embed it into additional functionality and further increase its value. We already see signs of new value propositions where payments are embedded into social media, such as the one promoted by status.im where payments and chat is integrated. Payment services are likely to be embedded into future functionality in ways we cannot imagine today.

Another source for potential substitutes of contemporary financial services are central banks. The central banks of Sweden, Denmark, Finland, the UK, Russia, China and India, have all expressed their interest to investigate the feasibility of issuing Central Bank Digital Currency (CBDC) based on the distributed ledger technology. CBDC would complement other forms of central bank money currently in circulation. A monetary regime with CBDC has never existed anywhere, mainly because the technology to make it feasible has not been available. In a recent report, researchers at the Bank of England claim that a CBDC regime could offer economic benefits; for example, it could increase output, help stabilize the business cycle, and foster financial stability [3]. But, CBDC would fundamentally change the role and value proposition for traditional banks. Central banks could offer retail customers the opportunity to deposit their money directly at the central bank at some interest rates. This would be in a direct competition to bank's deposits and raises various political questions as marked by Mark Carney, the Governor of the Bank of England [57]:

> Looking ahead, it is possible that virtual currencies and fintech-based providers, particularly where they gain direct membership to central bank payment systems, could begin to displace traditional bank-based pay-

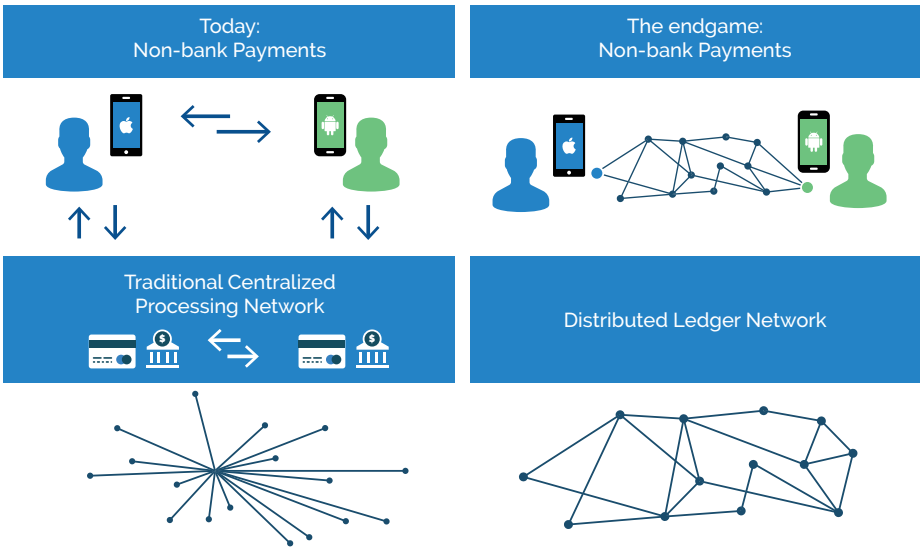

Figure 15: The non-bank payment infrastructure has already changed but is likely to be radically different when, a secure, trusted, and decentralized blockchain based payment network is available for most fiat currencies.

ment services and systems.

On some levels this is appealing; people would have direct access to the ultimate risk-free asset. In the extreme, however, it could fundamentally reshape banking including by sharply increasing liquidity risk for traditional banks.

Central banks have strong incentives to embrace the new technology. For example, it offers the possibility to eradicate cash. Negative interest rates could also be imposed, and tax avoidance would be practically eliminated when payments are fully traceable. Via central banks, the government would get direct access to the retail funding market, and eliminate the middlemen and lower cost. The operation of a payment system where payments, clearing and settlement are all in one can increase efficiency and lower cost as well. But, a central bank taking over fundamental contemporary banking roles, such as offering deposits, is likely to push other traditional banking roles out as well and invite potential new risks such as increased likelihood of a bank run. Would a central bank take over those roles as well such as customer relationship and creation of money through lending? The possibilities and incentives are in place are, but are likely to be political sensitive an debated for some time.

Threat and bargaining power of suppliers

When suppliers have bargaining power, they can apply pressure to affect prices, adjust quality or control availability. Contemporary global financial players have already taken a proactive approach to increase the value of their financial services to respond the new emerging technology. Just as non-financial players are likely to move into the space of traditional financial services, current players are increasing

quality by embedding and expanding their service offers. As an example, credit card companies are responding with new payment solutions, and seem to be determined to utilize the blockchain-based technology.

Threat and bargaining power of customers

Current customers can cut costs by participating in blockchain-based distributed networks such as via P2P lending platforms. Another example is the retailer shop Overstock which is an early adopter of the technology using it to issue own private bonds [58]. The US Securities and Exchange Commission (SEC) has approved the company's issued public stocks based on a blockchain platform [59]. Contemporary financial services buyers have now the option of boycotting traditional financial services channels with leaner and more cost-efficient platforms. The new technology equips customers with new operational platforms for funding, issuing stocks and the like.

Industry rivalry

Industry rivalry usually takes the form of competing for position using various tactics, for example, price competition, advertising battles, new products or innovation. Rivalry tends to increase in intensity when companies either feel competitive pressure or see an opportunity to improve their position with new technology. The nature of a distributed system is that it has a global reach and global operational potentials. Markets are becoming ever more integrated where global social media, collaborative tools, and businesses are intertwined. The customer is increasingly likely to demand a globally scalable financial solution. Strictly local financial services may suffer. Strong global brands, with economy of scale potential, might be in a key position to expand across national borders as financial services seems bound to become more global.

Public institutions are also paving the way to facilitate innovation and glottalization with new regulations spanning jurisdictions. The European PSD2 directive aims to facilitate innovation and to lower barriers to entry for new players across European borders. As a result, services in payments, funding, investment and asset management are likely to become more competitive. A more crowded field is likely to negatively impact margins. If earnings are not to suffer, firms must make up for this with increased volume, specialization, or both. Higher volumes translate into expanding products and service offerings across national borders.

Market expectations

In March 2016, 42 of the world's biggest financial institutions, tested a blockchain-based system under the umbrella of R3CEV (R3) [60]. In 2017 R3 had 92 members and some of its founding members had left the consortium. R3's aim is to lead the way for standardization of blockchain based services in banking. Such a development demonstrates at least two facts. First, the major financial service providers felt the need to collectively form a consortium to respond to external non-bank treat, based on the new technology. Second, there are internal conflicts in the consortium due to rivalry and a likely conflict of interests, and coordinating problems. Some financial services institutions have decided to leave the organization and seek to harness the opportunity on their own.

Figure 16: The R3CEV consortium of 92 major financial institutions was formed in 2015 as a response to the threat/opportunity of the blockchain technology. Its aim is to develop standards and protocols for blockchain-based financial services.

The very existence of R3, as a consortium of the worlds biggest and most progressive global banks, is a testament of the industry's expectations of up and coming imminent disruptive changes. Such expectations were also echoed in Oliver Wyman's report[61]: "The blockchain vision is clearly a massive change to the structure of capital markets". The stakeholders expectations include:

- Central banks, are now re-evaluating their traditional role as a central authority. Authority that partly relies on a banking controlled and centralized payment- and settlement systems.
- Regulators are designing new rules that are supportive of the new emerging distributed trustless technology. The goals include:
  - Fostering innovation, economic growth and job creation.
  - Lowering barriers for new entrants into financial services.
  - Mitigating risk associated with few big centralized financial institutions. A single point of failure (SPOF) system is undesirable where the goal is high availability and reliability. It is better business for society to decentralize financial services.
- Customer expectations and demands change. New solutions, new business models, coupled with ever more ambient technologies in a more integrated world is a catalyst for change.
- New entrants include Bitcoin, Ripple, Tether, BitPesa, SoFi, KickStarter, Dwolla, P2P lending and crowd-funding platforms, Lending club, TransferWise, Square, PayPal, Alipay, Venmo, Circle, Payoneer, Apple pay, Samsung pay, Google Wallet, Facebook payment, Starbucks payments, etc.

Banks

The Economist's intelligence unit surveyed 203 senior retail banking executives around the world about customer expectation[6] Some of their key findings for 2020 are [62]:

- P2P lending will be available via banking platforms (65%) and P2P lenders attract dissatisfied borrowers and savers (21%).
- More money will flow via fintech firms than traditional retail banks (57%). Robo-advisers could lure away more clients (17%).
- Investment, and life-based investment products, discretionary wealth management and consumer finance faced the biggest threat of losing most market share to new entrants.

Central banks

In 2015, prior to becoming the R3's CTO, Richard Brown shared his thoughts on how a general public access to central bank money would completely change the premises for the payments infrastructure. Mr. Brown wrote "pretty much all of the payment infrastructure in the world exists because most money isn't central bank money. If you imagine a world where everybody holds central bank money, suddenly the picture begins to look a lot simpler" [63], see Figure 17.

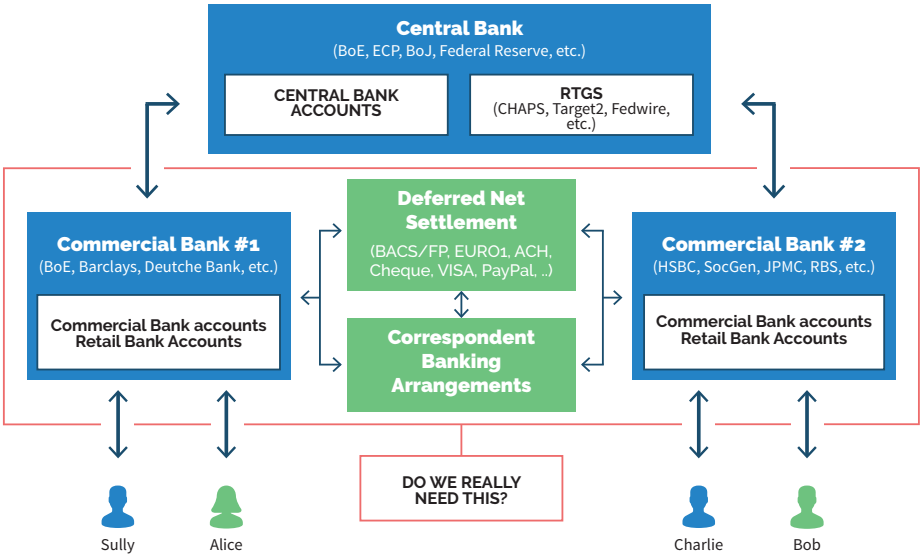

Figure 17: In March 2015, an IBM employee asked on his bloc if current banking payment infrastructure was really necessary. He is now the CTO of R3CEV, a consortium of major global financial institutions responding jointly to the new emerging technology.

[6] Of which 61 was from Asia Pacific, 62 from Europe, 60 from North America and 20 from the rest of the world. Over one-half (135) of the respondents work for banks with assets of less than $50bn. Some 44 have assets of $250bn or more.

Browns thoughts are certainly relevant for a potential endgame, but are a part of a bigger debate on banks future role in society as noted by the Deputy Governor for Monetary Policy at the Bank of England when he noted: “If it were a close substitute for bank deposits, a Central Bank Digital Currency (CBDC) would represent a shift towards a “narrower” banking system. This too is an old debate in economics, i.e. should banks be prevented from creating liquidity, or is maturity transformation an inevitable and necessary feature of market economies?” [64].

Bank of England and the Swedish central bank have both stated that nothing should stop central banks from issuing a new digital liability onto a blockchain based transaction network. Such a digital central bank issued currency could strengthen macroeconomic policy. In 2016, central bank issued digital currency formed a core part of BoE research agenda [65]. Central bankers find the technology appealing since it allows the banks to charge negative interest rates which is not possible for physical currencies [66]. The Dutch [67] and the Irish [68] central banks have both been reported testing blockchain-based systems, as is the Federal reserve which purportedly is exploring blockchains in collaboration with IBM [69].

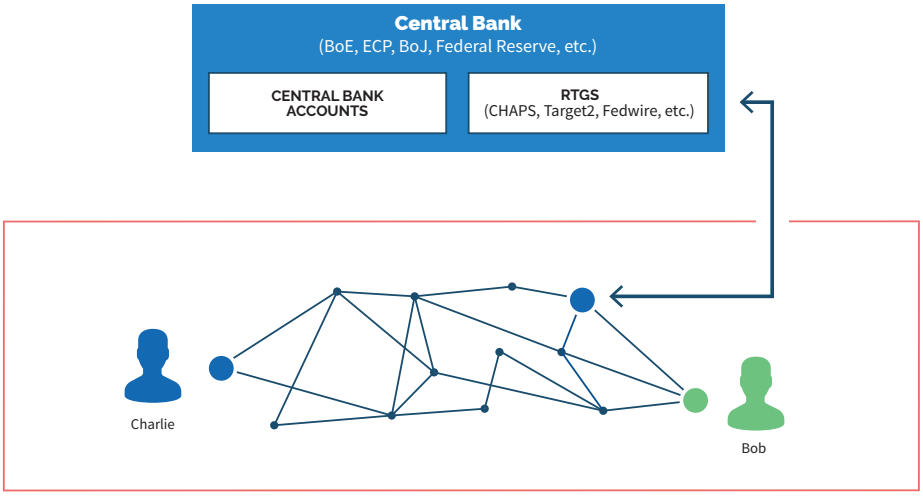

Figure 18: Central banks could issue their currencies directly to end users via distributed ledger technology. However, such a change raises fundamental questions about the roles of private and central banks, and about macroeconomic and financial stability.

The European Central Bank wrote in a 2016 report[70]: “…the Eurosystem intends to assess their relevance for the different services it provides to the banking communities (payments, securities settlement as well as collateral). This investigation will identify opportunities that these new technologies, such as blockchain, may provide, as well as the challenges that they create”.

With the right design, a blockchain based currency processing network can help reduce tax avoidance, and money laundering. The BoE chief economist has entertained the thought of simply banning paper money altogether. The BoE chief economist has also stated: “What I think is now reasonably clear is that the distributed payment

technology embodied in Bitcoin has real potentials. On the face of it, it solves a deep problem in monetary economics': How to establish trust, the essence of money, in a distributed network. Bitcoin's "blockchain" technology appears to offer an imaginative solution to that distributed trust problem"[66].

Bank of England's Deputy Governor Minouche Shafik declared in 2016 that "The emergence of various forms of distributed ledger technology (DLT) poses much more profound challenges because it enables verification of payments to be decentralized, removing the need for a trusted third party"[71]. If central banks will issue central bank money on blockchains it will also affect macroeconomic- as well as financial stability issues. That is why central bank now emphasis research in this area. Although the new technology has great potentials it also evokes policy challenges and questions as marked by Mark Carney, the governor of Bank of England in 2017 [57]:

> On some levels this [central bank digital money on blockchains] is appealing; people would have direct access to the ultimate risk-free asset. In the extreme, however, it could fundamentally reshape banking including by sharply increasing liquidity risk for traditional banks."

Number of consultants and scholars had published their thoughts on the pros and cons of central bank money on the blockchain (e.g. [72], and [73]).

Regulators

Payment systems are subject to regulatory scrutiny. A public effort is now made to promote competition and innovation in the field, as can be seen by a recent EU PSD2 directive. The EU's directive's aim is to facilitate innovation in payments solutions that can later evolved to broader service offering. PayPal is an example of a company that started in payments and has now evolved into other areas, such as funding through PayPal Credit[74]. Banks within the European Economic Area (EEA) have to comply with the PSD2 directive. Given certain premises retailers and aggregators can access banks account information for client-approved payments and data-mining.

Customers trust

Keeping customer's money safe, ensuring system integrity, legal and regulatory compliance, may be key in securing banks future role. However this world is fast changing and increasingly social media is trusted to store and keep personal information records. At the beginning of 2017, Facebook had almost 2 billion monthly active users [75]. Facebook offers payment services and the convenience of free peer-to-peer payments through its Messenger application. This followed the 2014 launch of Snapchat's Snapcash, a similar feature. Another well known global consumer technology company, Samsung, announced its acquisition of LoopPay (Samsung Pay), a mobile wallet that competes with Apple Pay and Google has Android Pay.

Strategic options

> If you don't know where you're going, any road will take you there.
>
> Alice in Wonderland

A blockchain-based future in financial services brings number of opportunities as well as threats. Some banks are likely to respond with a survival strategy to stay relevant, others with ignorance or indifference, while other will view this as an opportunity to strengthen their position. Based on potential endgame scenarios, current status and the stakeholders analysis, each financial institution can choose between at least four general strategies:

- Wait and see.
- Open up platforms to others.
- Build own proprietary solution.
- Partnership.

Trust and customer experience is vital for future sustainable financial services. Today, established financial institutions have the upper hand when it comes to trust but more tech savvy global and more flexible players may be better suited to offer a different and sometimes better customer experience. Keeping customers money safe, ensuring systems integrity, legal and regulatory compliance, may be key securing a successful path towards the endgame. Regulators may initially lag behind but will press for tougher “know-your-client” and anti-money laundering rules, as new non-bank solutions gain ground.

The “wait and see” strategy might turn risky since non-bank consortiums can respond by moving their business elsewhere or even building their own financial solutions. In some sense a bank revolves around a centralized ledger of payments and capital transactions. A blockchain is however a technology of a decentralized ledger and accordingly benefiting where decentralized systems are of more value. In this sense, blockchain based solutions compete with banks, rather than being a complementary technology to banks. Banks will have to rethink their business if it is believe that a decentralized blockchain based approach is the endgame.

To open up platforms to third parties is questionable. For a small financial institution, with limited technical know-how and resources, a carefully crafted partnership with key businesses could be a strategy worth considering. Such a partnership could create value and be beneficial for both parties. Global banks and non-banks are a threat to smaller local banks, but a partnership with a global player focusing on core competitive advantage should be an option considered.

The endgame

A blockchain-based future for the financial market holds the promise to revolutionize, streamline and improve how people will conduct finance. Smart contracts can simultaneously trade, carry out payments and settlements across financial markets and national borders. They allow automatic and decentralized execution of covenants on open and interconnected platforms and enable real time audit and surveillance possibilities. Bank roles and core business functions may shift, change or move to new and better positioned players. A framework for analyzing the possible impact of blockchains is included in an appendix on page 47.

In the blockchain ecosystem, new alliances are still being formed and traditional market participants are scrambling to straddle the two worlds of traditional financial services and the new one. New players include fintech companies (e.g. Ripple,

Ethereum, ConsenSys, Symbiont, Digital Asset Holdings, etc.), big global tech players (e.g. Google, Apple, Samsung, IBM, Intel, Facebook), various global businesses (e.g. Overstock, Starbucks, Vodafone, Amazon etc.), traditional financial players and newly formed consortiums (e.g. R3CEV, Project Ledger, Nasdaq, VISA, SWIFT etc.), central banks (BoE, Bank of Ireland, the Fed, etc.). Blockchain based financial services are still in the design mode and as such, characterized by uncertainty. The legal- and regulatory framework is also lagging behind. Therefore it is of value to draw up the likely endgame for a blockchain-based financial service future. One way to do so is to use a robust decision-based approach, "The Improvement Cycle": An iterative decision analytic framework (see figure 19). For a business not only to survive, but to thrive, a continuous improvement cycle is beneficial. Such an approach rests on an assumption of some endgame scenario, to design realistic options to respond to such future scenarios, and position the effort accordingly.

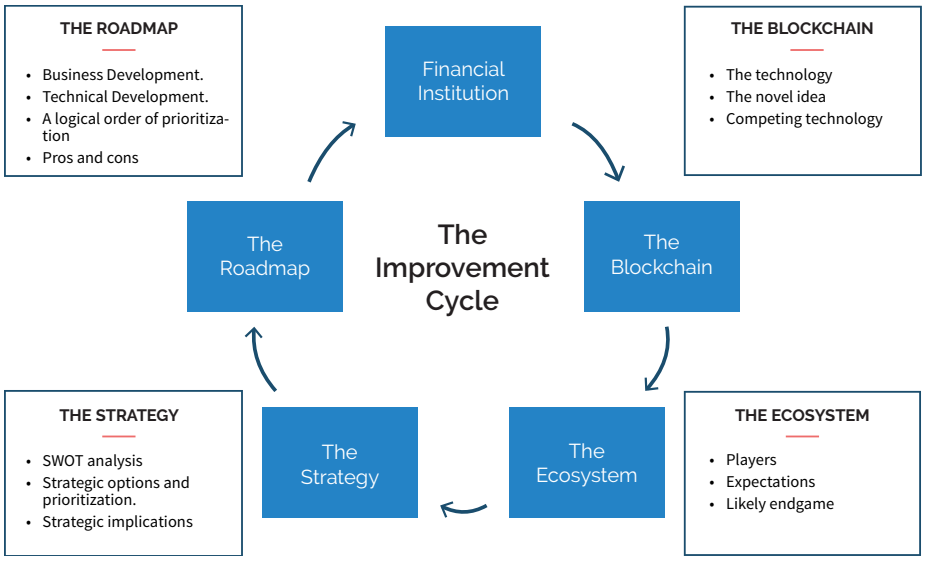

Figure 19: The improvement cycle is a continuous re-evaluation process of business- and technological development.

Financial services

For a business to secure itself a role in a new market it is common to focus on being first to market, i.e. to secure the "first mover advantage". Peter Thiel, the seasoned entrepreneur, cautioned however that it's actually better to start slowly and identify clear goals [76]. Thiel quotes "you must study the endgame before everything else" and emphasizes working backwards. To study the endgame and work backwards is a common practice in OR theory [77] since a key challenge of sustainability is to examine the range of plausible future pathways under conditions of uncertainty, surprise, human choices and complexity. Scenario analysis provides a powerful tool to do so and in this report we draw up one possible endgame scenario (see Figure 20 and for further analysis [61]).

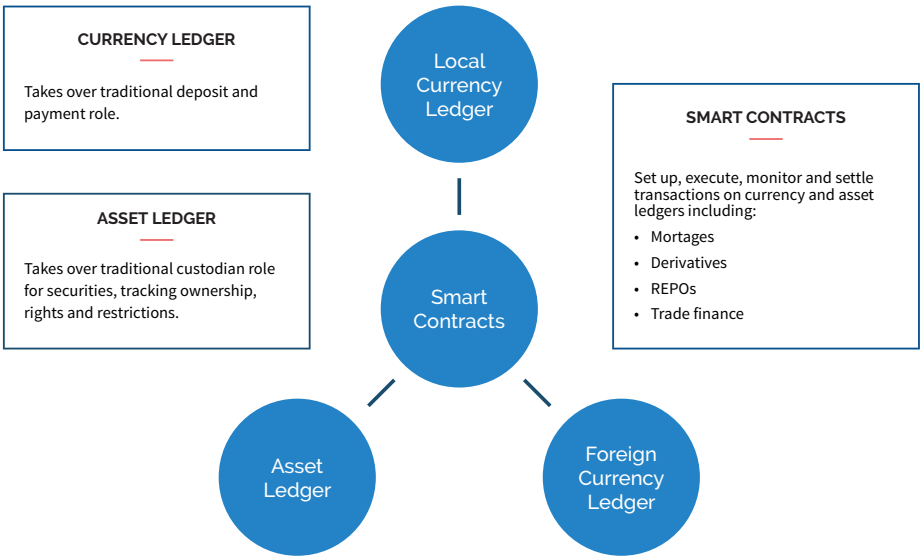

Figure 20: One possible endgame scenario assuming smart contracts dominating financial services, a regulatory framework supporting it, and a growing base of more sophisticated tech literate customers interacting directly.

Payment transactions

According to the endgame scenario (see figure 20), clients exchange payments directly between themselves regardless if it is local or foreign digital currency. Funds are redeemable at a bank, at the central bank or non-bank financial services institution. Clients make use of wallets to make and track payments, make use storage services that have largely replaced banks deposits. Identification is either by fingerprints, passwords, through global service providers e.g. Facebook or Microsoft identification services. The endgame scenario assumes the change due to the following factors:

- Customer preferences and options have changed.
- The blockchain technology is a trust-less solution that has changed the core of client-banking relationship.
- The blockchain technology solved the old double spending problem.
- Regulation facilitated changes through new initiatives and regulations.
- Deposit guarantee schemes are no longer necessary since claims are on sovereign funds and central bank money.

Deloitte [74] identified three likely emerging scenarios for payments in addition to status-quo, see Figure 21.

- New oligopoly. Payment systems are open, but customer trust in non-banks is limited. As a result, the non-bank newcomers will be restricted to a handful of big players with brand and scale.

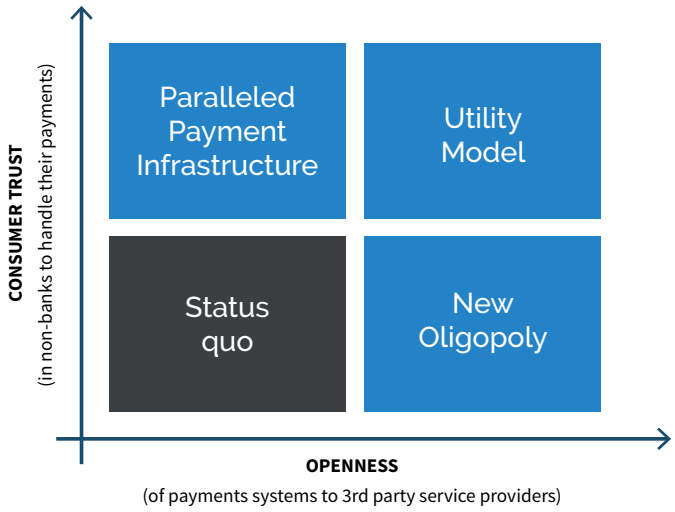

Figure 21: Three potential payments systems endgame scenarios, depending on trust and payment openness [74]

.

- Utility mode. If customers are more willing to experiment, both banks and non-banks will offer payments applications that run on banking payment "rails" which are low-margin, high volume utilities.
- Parallel payments infrastructure. Should customer desire for change to outpace regulatory pressure to open up payments systems, completely new methods of payment could take hold. For now, the likeliest candidates are cryptocurrencies that use block-chain technology to bypass central banks, traditional currencies, centralized clearing and settlement systems.

Payment services will be offered by the private sector, competing for customers, ensuring innovative and technological development. Whatever solution wins the support of customers, has always to fully comply with central banks legal- and regulatory demands. It is unlikely that future central bank role will be considered to promote innovation, drive technical development, or serve the developers community.

Funding and investing

In the endgame scenario, funding is through various venues where clients can issue their IOU without any intermediary, identify collateral and credit history that is available on-line from a trusted source. Clients can search and find appropriate investments options to choose from or use asset management service providers. In 2016, over ten major stock and commodities exchanges had voiced their enthusiasm for the technology [78].

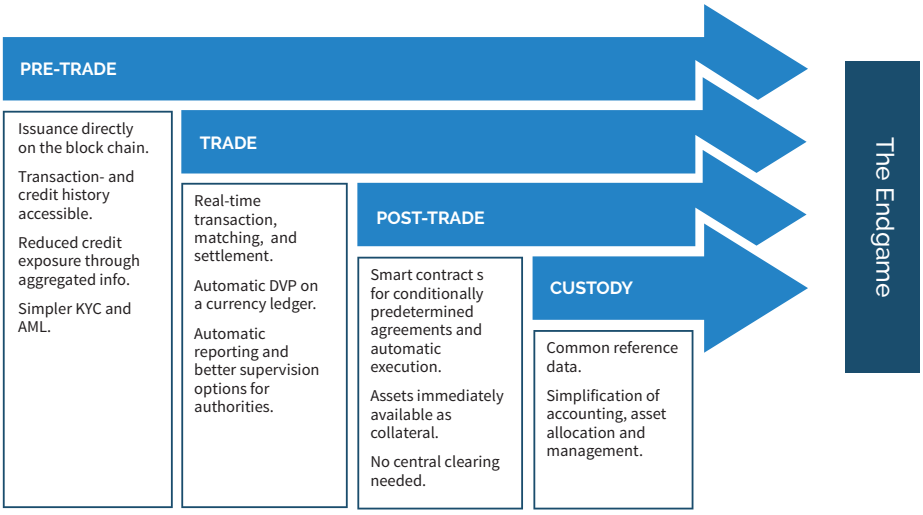

Figure 22: The endgame scenario affects financial services at all levels from back- to front office activity.

Mortgages and derivatives

In the endgame scenario, mortgages and derivatives are created as preprogrammed smart contracts, capturing the obligations of counterparts. Collateral, margin rules, margin calls and swap conditions are pre-programmed. Collateral is provided directly as cash on a currency ledger or an asset on an asset ledger. Inter-operable derivatives and collateral ledgers automatically allow the contract to call additional collateral from asset ledgers. At maturity, a final net obligation is computed by the smart contract, and a payment instruction automatically generated in the currency ledger, closing out and settling the deal.

Asset and fund management

In the endgame scenario, new securities are issued directly onto an IOU- or asset ledger. Mandatory events and payment distributions are managed via smart contracts embedded within the securities. Complex events can be structured as simple Delivery Versus Payment (DVP) transactions between issuers and investors.

The new technology is not changing financial services main value proposition, i.e. asset and fund management. There will always be demand for expert advice and acting on behalf of the customer in financial markets. However, the new technology will make clients more mobile and independent if they so choose. It will become easier for new non-bank financials to offer the assets and funding intermediaries services as clients are more “mobile”. Consumers will have more selection and ability to change service providers. Expectations about easy client mobility will increase and becomes a part of the selection criteria when choosing a service provider. This is in addition to increased efficiency in trading, execution, settlement, clearing, automation, information access and quality of service.

Towards the endgame

The path towards the potential endgame will take time. A practical strategy must factor in the necessary order of the underlying blockchain building blocks. This can be thought of as a kind of a technical hierarchy, see Figure 23. As an example it is not possible to build a smart contract loan contract triggering some fiat currency remittances based on some defined covenants on mortgage conditions if the currency- and/or asset ledgers are missing. A technical solution has a logical technical hierarchy order to be followed.

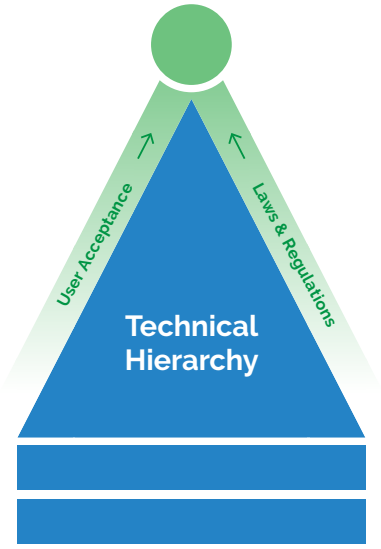

Figure 23: Any blockchain based business strategy must factor in the time lag of an appropriate legal- and regulatory framework, user acceptance rate, as well the logical technical hierarchy order.

The technical hierarchy's basic building block is the blockchain itself, see Figure 24. The second building block is the ledger type, i.e. one of three types of ledger consensus arrangements. Bitcoin is an example of a public distributed ledger, whereas Ripple is a hybrid between a public and consortium operated ledger. The third block is a currency ledger used for payments, settlement and clearing. The forth block is an asset ledger where an issuers issues an IOU and transactions are recorded. A part of an asset ledger has to be an issuer system. The fifth block is a venue, e.g. to match needs of debtors and investors. A smart contract system might be contingent on all of these building blocks.

Any strategy proposed has also to factor in the likely time lag due to legal and regulatory framework catch-up as well time to allow for customer acceptance rate, i.e.:

- Legal and regulatory framework. A necessary prerequisite for a successful and generally accepted blockchain-based financial solution is a supporting legal and regulatory framework. Are smart contracts and assets on the blockchain legally supported? Is a blockchain ledger legally equivalent as current reg-

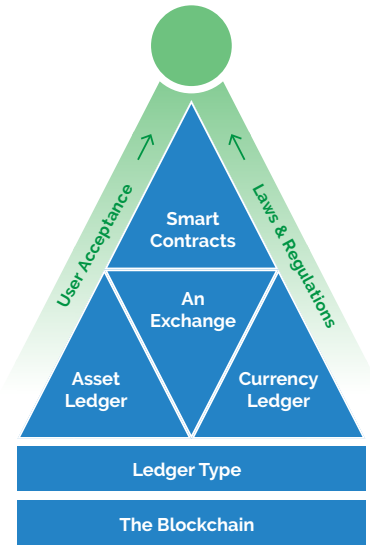

Figure 24: The technical hierarchy is broken down into six blocks forming a logical order when developing blockchain-based financial solutions.

istries? Are smart and traditional contracts legally equal? What about regulatory reporting requirements? Is a distributed blockchain ledger history sufficient for auditing purposes?

- Users acceptance rate. Time is needed for a new solution to catch on. Technology savvy individuals might be both willing and able to revolutionize finance. However, it will take time and longer for the general public. This translates into a time lag between a fully fledged technical solution and customer acceptance.

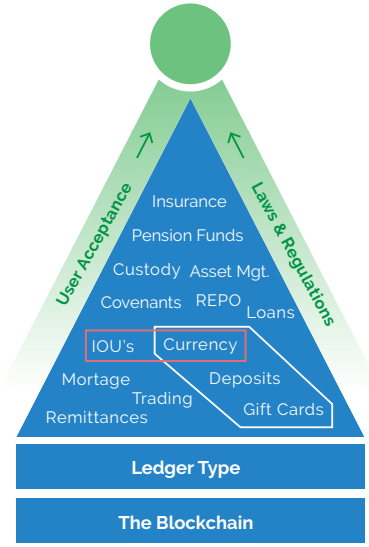

Figure 25: Once fiat denominated digital currency is issued blockchains, a logical next step is to add IOU's on the asset ledger.

Appendices

Blockchain feasibility analysis

Financial services providers need to evaluate both “if” and “when” it is feasible to utilize blockchain based solutions for their service offerings. In this appendix we outline a simple method for analyzing if parts of financial services can benefit from blockchain based technology. A schematic figure of the proposed feasibility analysis is put forward in figure 27.

1. The financial service should by descried by a project team. The description should include the value chain, the market size, frequency of trade, type and number of participants etc.

2. Having debated pros and cons of all the use cases, a questionnaire evaluation criteria can be applied, see figure 27. Such a questionnaire can be used to grade and evaluate selected use cases, see an example of a questionnaire below.

3. Based on the evaluation criteria a priority order is revealed. If the team agrees on the priority, a more detailed analysis is conducted for those use cases scoring the highest.

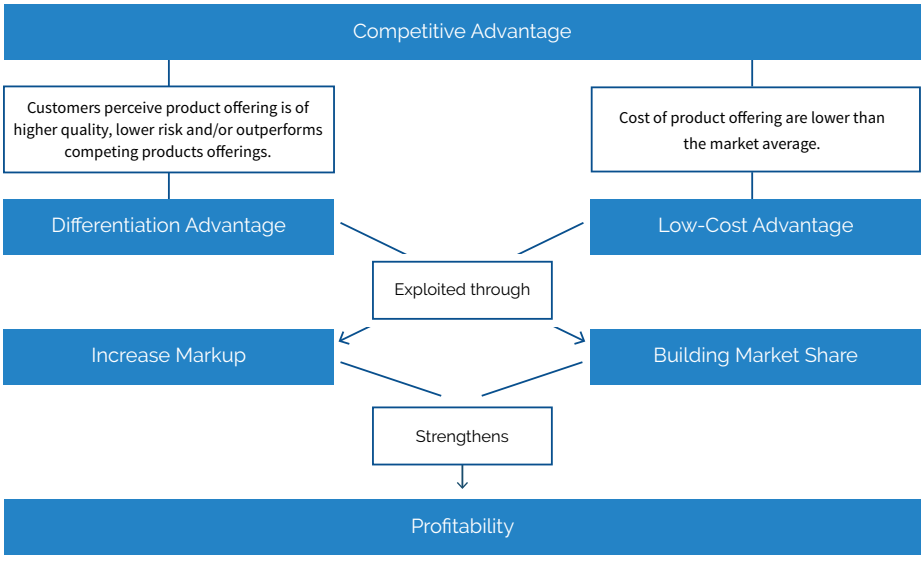

Figure 26: Whether some parts of financial services can benefit from utilizing the blockchain technology, is like any other business feasibility study. It has to make business sense, and be based on some competitive advantages affecting the bottom line.

An example of an evaluation questionnaire is put forward below. The questions are categories into three parts. Each question is comprised in such a way that a

positive YES answer gives maximum score, whereas a positive NO, gives a minimum score. Ambiguous answers fall somewhere in between. Questions are weighted according to relative importance agreed by the team. By summarizing the weight times the score for all the questions among all team participants, a total score is established.

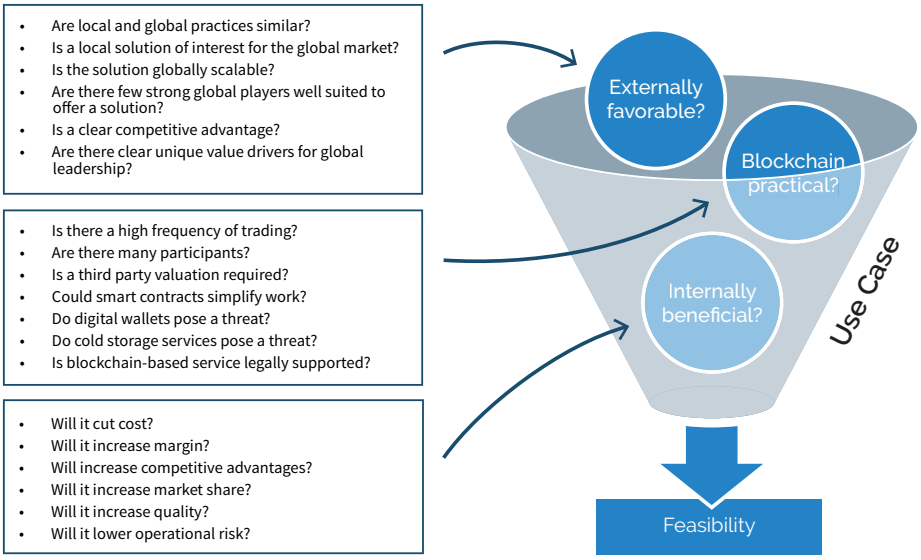

Figure 27: The use cases were filtered by evaluating i) how practical an analogous blockchain service would be, ii) if external factors are favorable and iii) how beneficial it is for current operation.

Special terms

Acronyms

BTC A widely used abbreviation for bitcoin.

CBDC Central Bank Digital Currency.

DVP Delivery Versus Payment.

ETH A widely used abbreviation for ether.

P2P Peer-to-Peer.

RDBMS Relational database management system.

SQL Structured Query Language.

XBT The unofficial ISO currency code for bitcoin [79].

XRP The unofficial ISO currency code for ripple [79].

Glossary

billion One thousand million or 1,000,000,000.

Bitcoin A blockchain for online payments with an eponymous built in payment token, bitcoin.

bitcoin The payment token of the Bitcoin blockchain.

chain Chain is a blockchain protocol for a shared, multi-asset, cryptographic ledgers designed and developed by Chain Inc.

coinbase The first transaction in each block of the Bitcoin blockchain used by miners to claim new coins and include messages.

consensus The process of updating a blockchain with new transactions.

Corda Distributed ledger technology developed by the R3CEV consortium.

cryptocurrency Digital currency which uses cryptographic methods.

Dapp Decentralized application which run on a distributed ledger.

digital currency Any digital form of money.

drop One millionth of an XRP.

ether The native token of the Ethereum blockchain.

Ethereum A blockchain for smart contracts with a built in native token, ether.

gas Gas is an internal unit of computational cost in Ethereum used to price actions performed by users or contracts.

hash A function which takes an input message and returns a fixed sized output message.

hyperledger A consortium for cross-industry blockchain technology development.

miner An individual or company operating computers which calculate hashes to update the bitcoin blockchain.

mining The process of calculating hashes to update the bitcoin blockchain; a form of proof-of-work.

proof-of-stake A blockchain consensus process where the validator of each new block block is chosen in a deterministic way commensurate to the validator's stake.

proof-of-work A blockchain consensus process based on performing computational work to secure and timestamp blocks, such as mining.

Ripple A blockchain for online payments with an eponymous built in payment token, ripple.

ripple The payment token of the Ripple blockchain.

satoshi The smallest unit of bitcoin, $1/10^8$ bitcoins or one hundredth million of a bitcoin.

Solidity A programming language for creating contracts on Ethereum.

trillion One million million or 1,000,000,000,000.

Turing complete A programming language is Turing complete if it can simulate any computer algorithm.

virtual currency "unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" [80, 81].

virtual machine An emulation of a computer system.

wallet software client which controls the private keys of a blockchain user.

References

[1] Robleh Ali (Bank of England). *Innovations in payment technologies and the emergence of digital currencies*. 2014. URL: http://www.bankofengland.co.uk.

[2] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: http://www.bitcoin.org.

[3] John Barrdear and Michael Kumhof. *The macroeconomics of central bank issued digital currencies*. 2016. URL: http://www.bankofengland.co.uk.

[4] The Economist. "The trust machine". In: *The Economist* (October 31, 2015).

[5] David Levene. *Inside the Bank of England*. 2015. URL: http://www.theguardian.com.

[6] The Free Dictionary. *ledger*. Retrieved, April 2016. URL: http://www.thefreedictionary.com.

[7] Barry Williams. *Online Banking Data Model*. 2010. URL: http://www.databaseanswers.org.

[8] Wikipedia. *Peer-to-peer*. Retrieved April, 2016. URL: http://en.wikipedia.org.

[9] Paola Boel. "Thinking about the future of money and potential implications for central banks". In: *Svergies Riksbank Economic Review 2016:1* (2016).

[10] Wikipedia. *Satoshi Nakamoto*. Retrieved April, 2016. URL: http://en.wikipedia.org.

[11] Bitcoin Wiki. *History*. Retrieved April, 2016. URL: https://en.bitcoin.it.

[12] Blockchain. *Bitcoin Developer API's*. Retrieved April, 2015. URL: http://www.blockchain.info.

[13] Wikipedia. *PayPal*. Retrieved April, 2016. URL: http://en.wikipedia.org.

[14] Google. *Paypal Holdings Inc (NASDAQ:PYPL)*. Retrieved, April 2008. URL: https://www.google.com/finance.

[15] PayPal. *PayPal Reports Fourth Quarter and Full Year 2016 Results*. January 26, 2017. URL: https://investor.paypal-corp.com.

[16] Google. *Google Finance*. Retrieved, April 2008. URL: https://finance.google.com.

[17] The Nilson Report. *Global Cards 2014*. 2014. URL: https://www.nilsonreport.com.

[18] Wikipedia. *Public-key cryptography*. Retrieved April, 2016. URL: http://en.wikipedia.org.

[19] Sveinn Valfells & Jón Helgi Egilsson. *The future of bitcoin mining*. Preprint, under review.

[20] Bitcoin Wiki. *Protocol documentation*. Retrieved, 2016. URL: http://en.bitcoin.it.

[21] Wikipedia. *SHA-2*. Retrieved, April 2016. URL: http://www.wikipedia.org.

[22] Blockchain. *Block # 345981*. Retrieved April, 2015. URL: http://www.blockchain.info.

[23] Bitcoin Wiki. *Controlled supply*. Retrieved, 2016. URL: http://en.bitcoin.it.

[24] Toshi. *Toshi*. Retrieved April, 2016. URL: https://toshi.io.

[25] Dan Kamnisky. *Let's Cut Through the Bitcoin Hype*. May 3, 2013. URL: http://www.wired.com.

[26] Fox Business News. *Munger/Buffett Disagree on Corporate Tax Rates*. May 6, 2013. URL: http://www.foxbusiness.com.

[27] Vitalik Buterin. *A Next-Generation Smart Contract and Decentralized Application Platform*. 2014. URL: https://github.com.

[28] Gavin Wood. *Ethereum: A secure decentralised generalised tranaction ledger (Homestead draft)*. 2014. URL: http://gavwood.com/.

[29] Wikipedia. *Ethereum*. Retrieved April, 2016. URL: https://en.wikipedia.org.

[30] Etherscan. *Total Ether Supply*. Retrieved, April 2016. URL: https://etherscan.io.

[31] Etherscan. *Etherscan APIS*. Retrieved, April 2016. URL: http://www.etherscan.io.

[32] Ethereum. *Ethereum Frontier Guide - What is Ethereum?* Retrieved, April 2016. URL: https://www.gitbook.com.

[33] Ethereum Foundation. *Ether*. Retrieved, April 2016. URL: http://www.ethereum.org.

[34] Joseph Lubin. *The issuance model in ethereum*. April 10, 2014. URL: https://blog.ethereum.org.

[35] Vlad Zamfir. *Introducing Casper "the Friendly Ghost"*. August 1, 2015. URL: https://blog.ethereum.org.

[36] Anna Irrera. *JPMorgan, Microsoft, Intel and others form new blockchain alliance*. URL: http://www.reuters.com/.

[37] go ethereum. *Contract Tutorial*. Retrieved, April 2016. URL: http://www.github.com.

[38] Inc Ripple Labs. *Ripple*. Retrieved, April 2016. URL: http://www.ripple.com.

[39] Wikipedia. *Ripple (payment protocol)*. Retrieved, April 2016. URL: http://en.wikipedia.org.

[40] Inc Ripple Labs. *Ripple Charts*. Retrieved, April 2016. URL: http://www.ripplecharts.com.

[41] Coinmarketcap. *Crypto-Currency Market Capitalizations*. Retrieved, April 2016. URL: https://coinmarketcap.com/.

[42] Ripple Wiki. *Consenus*. Retrieved, April 2016. URL: https://wiki.ripple.com.

[43] Ripple Wiki. *Contracts*. Retrieved, April 2016. URL: https://wiki.ripple.com.

[44] "Richard Gendal Brown *et al*". *Corda: An Introduction*. August, 2016. URL: https://www.r3cev.com.

[45] Hyperledger Project. *Hyperledger Project*. Retrieved, April 2016. URL: http://hyperledger.org.

[46] go ethereum. *Introducing Casper "the Friendly Ghost"*. August 1, 2015. URL: https://blog.ethereum.org.

[47] The Elements Project. *Confidential Transactions*. Retrieved, April 2016. URL: https://elementsproject.org.

[48] et al. Adam Back. *Enabling Blockchain Innovations with Pegged Sidechains*. October 22, 2014. URL: https://www.blockstream.com.

[49] Rootstock. *Rootstock*. Retrieved April, 2016. URL: https://rootstoc.io.

[50] Vitalik Buterin. *On Public and Private Blockchains*. August 7, 2015. URL: https://blog.ethereum.org.

[51] Eric Redmond & Jim R. Wilson. *Seven Databases in Seven Weeks: A Guide to Modern Databases and the NoSQL Movement*. 2012.

[52] DB Engines. *DB-Engines Ranking*. Retrieved April, 2016. URL: http://www.db-ranking.com.

[53] Gareth William Peters & Efstathios Panayi. *Understanding Modern Banking Ledgers through Blockchain Technologies*. November 18, 2015. URL: http://arxiv.org.

[54] *Business Knowledge for IT in Global Retail Banking*. Essvale Corporation Limited, 2011.

[55] *FinTech 2.0*. 2015. URL: http://www.gtb.db.com/docs_new/GTB_FinTech_Whitepaper_A4_SCREEN.pdf.

[56] Startup Management SUM. *Update to the global landscape of blockchain companies in financial services*. December, 2015. URL: http://startupmanagement.org/2015/12/08/.

[57] Mark Carney. *The Promise of FinTech – Something New Under the Sun? Speech given by Mark Carney, Governor of the Bank of England, Chair of the Financial Stability Board, Deutsche Bundesbank G20 conference on "Digitising finance, financial inclusion and financial literacy", Wiesbaden*. Bank of England. Jan. 2015. URL: http://www.bankofengland.co.uk.

[58] Wired business. *SEC Approves Plan to Issue Stock Via Bitcoin's Blockchain*. December, 2015. URL: http://www.wired.com.

[59] TO. *Banks Are Right To Be Afraid of the FinTech Boom*. July 8, 2015. URL: https://t0.com/home.

[60] Jemima Kelly Reuters. *Forty big banks test blockchain-based bond trading system*. Mar. 2, 2016. URL: http://www.reuters.com/article/idUSL8N16A30H.

[61] Oliver Wyman and Euroclear. *Blockchain in Capital Markets. The Prize and the Journey*. February, 2016. URL: http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/feb/BlockChain-In-Capital-Markets.pdf.

[62] The Economist Intellegence Unit. *Retail Banking. In tech we trust*. 2016. URL: http://www.eiuperspectives.economist.com/sites/default/files/Retai\l%20Banking.pdf.

[63] Richard Gendal Brown. *A Central Bank "CRYPTOCURRENCY"?* 2015. URL: https://gendal.me.

[64] Ben Broadbent. *Central banks and digital currencies*. 2016. URL: http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech886.pdf.

[65] Bank of England. *One Bank Research Agenda. Discussion Paper | February 2015*. 2015. URL: http://www.bankofengland.co.uk/research/documents/onebank/discussion.pdf.

[66] Andrew G Haldane. *How Low Can You Go, a Speech by BoE's Chief Economist, Portadown Chamber of Commerce, Northern Ireland)*. 2015. URL: http://www.bankofengland.co.uk/publications/Documents/speeches/2015/speech840.pdf.

[67] CoinDesk. *Dutch Central Bank to Create Prototype Blockchain-Based Currency*. March 24th, 2016. URL: http://www.coindesk.com/.

[68] Finextra. *Bank of Ireland and BNP Paribas announce blockchain breakthroughs*. April 16th, 2016. URL: https://www.finextra.com/newsarticle/28698/.

[69] Gertrude Dreyfuss Reuters. *Exclusive: IBM looking at adopting bitcoin technology for major currencies*. Mar. 12, 2016. URL: http://www.reuters.com/article/idUSKBN0M82KB20150312.

[70] The European Central Bank Eurosystem. *Eurosystem's vision for the future of Europe's financial market infrastructure. RTGS services — consultative report.* 2016. URL: http://www.ecb.europa.eu/paym/t2/shared/pdf/professionals/RTGS_services_consultative_report.pdf.

[71] Minouche Shafik. *A New Heart for a Changing Payments System*. 2016. URL: http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech878.pdf.

[72] Deloitte. *State-Sponsored Cryptocurrency: Adapting the best of Bitcoin's Innovation to the Payments Ecosystem*. 2015. URL: http://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-cons-state-sponsored-cryptocurrency.pdf.

[73] George Danezis & Sarah Meiklejohn. *Centrally Banked Cryptocurrencies*. 2016. URL: https://eprint.iacr.org/2015/502.pdf.

[74] Deloitte Ltd. UK. *Payments disrupted | The emerging challenge for European retail banks*. 2015.

[75] Statistica. *Number of monthly active Facebook users worldwide as of 4th quarter 2015*. 2016. URL: http://www.statista.com/statistics/264810/.

[76] Peter Thiel. *ZERO TO ONE*. 2004.

[77] Jon Helgi Egilsson. *Soft systems approaches in strategic planning*. Danmarks Tekniske Universitet, DTU, 1994.

[78] CoinDesk. *10 Stock and Commodities Exchanges Investigating Blockchain Tech*. April 14th, 2016. URL: http://www.coindesk.com/.

[79] Wikipedia. *ISO 4217*. Retrieved November, 2015. URL: http://en.wikipedia.org.

[80] European Central Bank. *Virtual Currency Schemes*. Report. European Central Bank, October 2012.

[81] Wikipedia. *Virtual currency*. Retrieved, April 2016. URL: http://www.wikipedia.org.