Public versus Private Blockchains

Part 1: Permissioned Blockchains

White Paper

BitFury Group
in collaboration with Jeff Garzik (jeff@bloq.com)

Oct 20, 2015 (Version 1.0)

Abstract

Blockchain-based solutions are one of the major areas of research for institutions, particularly in the financial and the government sectors. There is little disagreement that backbone technologies currently used in these sectors are outdated and need an overhaul to conform to the needs of the times. Distributed or decentralized ledgers in the form of blockchains are one of the most discussed potential solutions to the stated problem. We provide a description of permissioned blockchain systems that could be used in creating secure ledgers or timestamped registries. We contend that the blockchain protocol and data should be accessible to end users to provide a higher level of decentralization and transparency and argue that proof of work could be effectively used in permissioned blockchains as a means of providing and diversifying security.

Version History

Version	Date	Change description
1.0	Oct 20, 2015	Initial version

Although most of settlement work between trading companies could be automated, the corresponding financial operations are nowadays performed by hand partially due to law regulations and partially because of tradition and inertia [1]. Similarly, there are multiple registries operated by governments with a lengthy and resource-consuming process of their reconciliation. Thus, there is a demand on automated registry systems, that could supersede existing registries and form a single interconnected environment.

Bitcoin [2] is a peer-to-peer digital currency system, with the blockchain being the core innovation behind the currency. In essence, a blockchain is a type of a distributed database specifically suited for processing time-ordered data such as financial transactions. The key design element of blockchains – embedded security – makes them different from ordinary horizontally scalable distributed databases such as MySQL Cluster, MongoDB and Apache HBase. Blockchain security makes it practically impossible to modify or delete entries from the database; furthermore, this kind of security is enforced not through the central authority (as it is possible with the aforementioned distributed databases), but rather through the blockchain protocol itself. The distributed and decentralized nature of blockchains makes them an attractive replacement for the existing solutions utilized by financial institutions. The downsides of blockchains, e.g., comparatively slow transaction confirmation and a lesser degree of scalability, are less important in this case than increased security and absence of a single point of failure. In the words of Nick Szabo [3], the inventor of smart contracts, "proper financial controls are already somewhat decentralized, thanks to a "human blockchain" of accountants, auditors, etc. checking each other's work." Thus, automating the operation of this chain while keeping decentralization intact could be a logical step.

Financial institutions and other companies operating data registries are cautious to use the Bitcoin blockchain (a most developed public permissionless blockchain), or other available public blockchains. There are several reasons behind this, such as compliance. In Section 1, we describe the present state of adoption of blockchain technology. We examine the basis of blockchain technology in Section 2 and argue that institutions operating blockchains should make it at least partially transparent to their clients for security reasons. In Section 3, we review solutions that could leverage permissioned blockchains, such as merged mining and blockchain anchoring, and contend that proof of work is applicable for this kind of chains. In the second part of the paper, we will consider permissionless blockchains, which could form the ubiquitous base layer of blockchain applications, and compare private, permissioned and permissionless blockchain designs.

1 Present State of Affairs

Since 2014, the topic of blockchain-based ledgers has gained much popularity among banks and other financial institutions. Several prototypes and concepts involving blockchain technology have been publicly announced. Some of these prototypes use the Bitcoin blockchain directly:

- Estonia's LHV Bank is testing Cuber (Cryptographic Universal Blockchain Entered Receivables)

based on colored coins on top of the Bitcoin blockchain [4].

- Similarly, the NASDAQ stock exchange plans to use one of the colored coins protocols, Open Assets Protocol, to power the full management cycle of private company securities [5, 6].
- France's largest bank BNP Paribas is reportedly researching the possible ways to incorporate Bitcoin into the bank's currency funds [7].
- The UK bank Barclays partnered with bitcoin exchange Safello to explore possible applications of blockchain technology in the financial services sector [8].
- Goldman Sachs published a report, *The future of finance: redefining the way we pay in the next decade*, which implies Bitcoin and cryptocurrencies could change the payments ecosystem [9]. Goldman Sachs also participated in a $50 million funding round for a bitcoin financial services startup Circle [10].
- Switzerland-based UBS considers Bitcoin derivatives potentially attractive, provided the corresponding legislation is adopted [11].

Several other prototypes involve Ripple or Ethereum:

- The Ripple protocol was integrated with German bank Fidor, as well as Kansas-based CBW Bank and Cross River bank from New Jersey [12]. According to Giles Gade, CEO and president of Cross River, one of the main reasons behind this decision is Ripple's compliance with US laws.
- Three of Australia's banks – Commonwealth Bank of Australia (CBA), Westpac Banking Corporation, and Australia and New Zealand Banking Group – are experimenting with payments using the Ripple protocol [13, 14]. Chief information officer at CBA David Whiteing cited the absence of built-in assets for Ripple as the key reason why Ripple was preferred over Bitcoin.
- UBS announced experiments with Ethereum blockchain aimed to build fully automated bonds [15]. Alex Batlin, a director of innovation and research at UBS, did not rule out using the Bitcoin blockchain for the similar purposes.

However, in most cases, financial institutions are willing to build their own private blockchains or are investigating the unspecified blockchain solutions:

- Three large banks in the Netherlands – ABN Amro, ING and Rabobank – investigate the use of blockchain for payment systems [16].
- Citigroup has built three private blockchains and an internal currency with a prime focus on payments and eliminating counterparty risks when dealing with smaller local banks [17]. Additionally, Citigroup has partnered with Safaricom, a mobile operator in Kenya, to enable transfer services to the unbanked.
- Santander, one of the largest banks in the world according to Forbes [18], has identified 20 to 25 possible applications of blockchain technology in banking, including international remittance, syndicated lending and collateral management [19].

- Similarly, Deutsche Bank has stated that distributed ledgers and particularly blockchains have possible applications in both fiat currency and securities management, creating transparency and facilitating Know Your Customer / Anti-Money Laundering surveillance [20].
- Monetary Authority of Singapore has named blockchains as one of the big trends in technologies affecting financial services, citing lower cost of operation, faster processing and failure resilience as their main benefits compared to the traditional approach [21].

The blockchain-based solutions are not utilized exclusively for distributed ledgers; a related concept – blockchain-powered Internet of Things – is being developed by IBM and Samsung [22]. The project called ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) uses Ethereum as a protocol for smart contracts. Another project by IBM is aimed to create a smart contracts platform and is primarily targeted at unbanked [23].

Blockchain is quite often regarded by financial as a technology that can transform the future of payments:

- Blockchain is referenced in two major shifts expected to occur in the nearest future, according to the survey report by World Economic Forum [24]. The first shift – first tax collected by a government using the blockchain technology – is expected to occur in 2023. The second one – storing more than 10% of global gross domestic product in blockchains – will supposedly have taken place by 2027.
- Bank of England issued a report stating "[d]istributed ledger technology represents a fundamental change in how payment systems could work." [25]
- Blythe Masters, CEO of Digital Asset Holdings, has compared blockchain to e-mail for money [26].
- According to chief innovation officer at Standard Chartered Anju Patwardhan, blockchain-based infrastructure could make financial transactions more secure and traceable, while undercutting their costs for end customers and easing anti-money laundering surveillance [27].
- Usama Fayyad, chief data officer at Barclays, regarded blockchain as a transformative technology for finances [28].

The general stance of financial institutions towards Bitcoin and other public permissionless blockchains remains rather skeptical, while opinions on private / permissioned blockchains are generally much warmer. The major reasons behind the hesitation to use permissionless blockchains in financial environments are as follows:

- Inability to control transaction processors (i.e., miners in the case of Bitcoin) [26]. According to many jurisdictions, identities of transactions processors need to be known, and that directly contradicts Bitcoin's openness (anyone can mine provided they have enough computational resources at their disposal). According to CEO of Metro Bank Craig Donaldson, the lack of definitive financial compliance rules for Bitcoin services inhibits their development potential [28].

- Related to the first problem, there are concerns about clients' confidentiality in a public environment.
- Permissioned ledgers can be more efficient for testing purposes, quickly applying modifications to the protocol, and so on [15].
- Proof of work, which is fundamental to the Bitcoin blockchain, is made largely redundant on private blockchains; this allows the increase of transaction throughput and reduction of the cost of operations [15].

There are a certain number of Bitcoin optimists, such as LinkedIn co-founder and billionaire investor Reid Hoffman [29]: "At least one global cryptocurrency will achieve mass-market adoption. That cryptocurrency will either be Bitcoin or a derivative inspired by it." Similarly, Richard Gendal Brown, CTO of blockchain innovation company R3 CEV, warned against dismissing Bitcoin in favor of permissioned distributed ledgers, as "[Bitcoin's] core design goal of censorship-resistant digital cash has such disruptive potential – good and bad; this possibility alone is reason to keep an eye on it" [30].

1.1 Financial Ledger Innovations

A recent trend in blockchain innovations is companies building solutions specifically aimed at providing support for next generation financial services. We list several of these companies with brief descriptions below; for a more detailed review, one should refer to the *Permissioned distributed ledgers* report by Tim Swanson [31].

- **Digital Asset Holdings** (digitalasset.com) aims to build a layered system for processing securities trades. The middleware layer of the system would enable support of both blockchain-based backends and legacy infrastructure (e.g., FedWire). Digital Asset Holdings plans using both public blockchains (such as Bitcoin) and private ones (built with Hyperledger technology [32]).
- **Chain** (chain.com) offers an enterprise blockchain platform focusing primarily on asset transfer. The company has recently raised $30 million in funding supported by major financial institutions including Visa, Nasdaq, Citi Ventures and Orange [33].
- **R3 CEV** (r3cev.com) is an innovation company building next-generation global financial services. R3 leads a partnership of global banks (including Barclays, Credit Suisse, JP Morgan, UBS, BBVA, and Commonwealth Bank of Australia) to create a distributed / shared ledger technology [34].
- **Clearmatics** (clearmatics.com) builds a decentralized clearing network that would allow users to settle securities trades and automatize financial contracts via smart contracts technology.
- **Eris Industries** (erisindustries.com) provides open source solutions enabling financial operators to build low-cost / high quality infrastructure utilizing blockchain technology and smart contracts.
- **Tembusu** (tembusu.sg) has developed the TRUST (Tembusu Reputation-based Universally Secure Transaction System) framework – a blockchain-powered platform for managing custom assets.

- **Enigma** (enigma.media.mit.edu) project builds a cloud platform with guaranteed privacy by utilizing secret sharing techniques.

Additionally, several companies such as **Factom** (factom.org) are developing infrastructure for financial services on top of the Bitcoin blockchain.

Unlike readymade distributed ledgers used in cryptocurrencies, the aforementioned companies offer solutions that can be crafted to meet the specific needs of financial institutions:

- The proposed solutions generally use a pool of known services to create blocks of transactions. In most cases, integrating blocks into a chain does not involve proof of work as used in Bitcoin and several other cryptocurrencies. Because of this, the proposed blockchains do not generally have a built-in token.
- The access to the blockchain itself can be restricted to the participating institutions and regulators.
- The algorithm of determining valid transactions is more complex than in case of Bitcoin; it is usually flexible to reflect the needs of particular types of financial services. Oftentimes, a Turing-complete [35] language is integrated into the blockchain to allow for complex smart contracts. Note that Bitcoin scripting language is *purposely* not Turing-complete, as a language with limitations prevents the process for validating transactions from being used as a vulnerability.

2 Blockchain Technology

Blockchain is a distributed database for transaction processing. Although most current blockchains operate financial transactions, this is not necessarily the case; in the most generic case, transactions could be viewed simply as atomic changes to the system state. For example, a blockchain may be used to timestamp documents and secure them from alterations.

All transactions in a blockchain are stored onto a single ledger. As transactions are ordered by time, the present state of the system (in the case of a financial blockchain, the collection of all users' balances) is uniquely determined by the ledger. Storing all transaction history has other benefits such as increased regulatory compliance and the ability to determine the state of the system at *any* specified moment of time by "replaying" corresponding transactions.

In the ideal case, transaction processing with blockchain technology satisfies the following properties:

- Transactions should **conform** to the present state of the system: e.g., in the case of financial transactions, if Alice's balance is $1,000, she cannot pay Bob $10,000.
- Transactions should be **authorized**, i.e., only Alice should have an access to perform transactions using her name.
- Transactions should be **unmodifiable**: once transaction has entered the ledger, it should be impossible to modify its information (e.g., if there is a transaction in which Alice pays Bob $10,

a perpetrator should not have the ability to change the sum of payment or its sender, or its recipient).

- Transactions should be **final**: once transaction is recorded in the ledger, it should be impossible to delete it, which would effectively reverse the transaction.
- **Censorship resistance:** if a transaction conforms to a ledger protocol, it should be eventually added to the ledger.

Conformance is enforced by checking transactions against the present state of a system securely stored in memory. As the present state can be restored from the ledger, this assumption does not diminish the security of the system. Rather, it imposes a requirement that the ledger should be organized in a way that the secure verification of transactions takes acceptable amount of time. One way to do this for financial blockchains is to use unspent transaction outputs (UTXOs) as in Bitcoin instead of explicit user balances. In this case, a state of the system is essentially a registry of ownership, which contains information on who is eligible for redeeming each asset circulating in the system.

The authorization problem is solved by using a public key cryptography [36]. Each user of the system is granted a pair of private and public keys; the public key can be safely published to determine the digital identity, because it is impossible to infer the private key from it. For example, if Alice wants to transfer $10 to Bob, she (or a trusted agent on her behalf) can sign the corresponding transaction with a digital signature using her private key. As

- a valid signature can only be made by a person knowing Alice's private key,
- a signature can be verified by anyone knowing Alice's public key,
- a signature is invalidated if any parameters of the transaction are changed,

use of digital signatures solves not only authorization but also modifiability problem. If digital signatures are utilized for all transactions in the ledger, it becomes impossible for a perpetrator having internal access to the system (e.g., a hacker or a former employee) to change any of them.

Immutability and finality of transactions in blockchain systems are achieved by splitting transactions into time-ordered blocks and calculating the cryptographic hash of each of these blocks (Fig. 1). A Merkle tree [37] is an efficient structure for calculating such a hash; to avoid confusion and to be consistent with Bitcoin terminology, we will call hashes inferred from transactions *Merkle roots*. To make it impossible to delete or replace the whole blocks of transactions and to secure Merkle roots, blocks are organized into an ordered chain (a *blockchain*). To simplify blockchain verification, key block features (such as a Merkle root and a time interval the block corresponds to) are extracted into a block header. Each block header contains a reference to the previous block (except for the first block, which is hardcoded into the protocol). Thus, providing immutability of transactions is reduced to providing immutability of block headers. Provided that block headers are secured, to change a single block, an attacker must also change all succeeding blocks in the ledger. An adequate block security mechanism makes it impossible to delete transactions added to the ledger a long time ago; thus, the system possesses a transaction finality property.

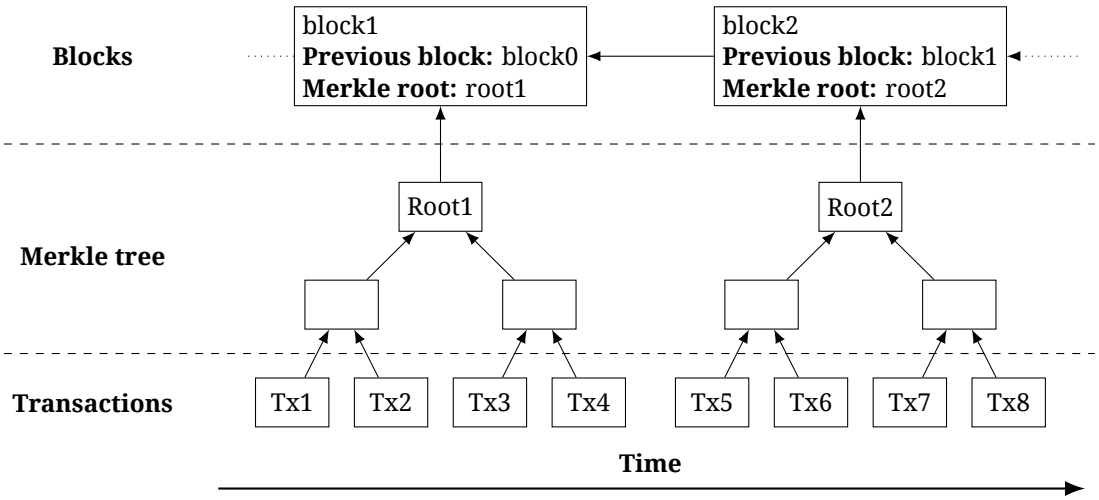

Figure 1: The generic structure of a blockchain with each of two displayed blocks containing 4 transactions. Note that calculated Merkle roots depend on the order of transactions in a block, which means transactions in the blockchain are completely ordered

Immutability of block headers can be achieved in a variety of ways, including proof of work (e.g., as used in Bitcoin), proof of stake (e.g. Nxt), and delegated proof of stake (e.g. BitShares). According to the proof of work protocol, a block header is considered valid only if its hash is less than a specified network-wide value (i.e. *difficulty target*). Due to the properties of hashing functions, there is no known way to create valid blocks other than to change fields in the block header influencing the hash. Examples of such fields are *nonce* (a special integer field), block creation time, and parameters of the *coinbase transaction*[1] (the changes in the transaction result in changes in the Merkle root of the block, which is a part of its header). An alternative block header security protocol is proof of stake. Proof of stake does not rely on extensive computations; on the other hand, this protocol may be less secure than proof of work, as the cost of attacks on a system secured with proof of stake is lower [38].

The organization of transactions into blocks makes it possible to efficiently prove that a certain transaction belongs to the blockchain (using *simplified payment verification* or SPV [2]). A proof consists of a list of block headers from the genesis block up to and including the block containing the transaction, a transaction and a corresponding *Merkle branch* (Fig. 2). The Merkle branch consists of $O(\log N)$ hashes, where N is the number of transactions in a block, and its structure is such that it allows to quickly compute and verify a Merkle root value. It follows from the properties of Merkle trees that it is statistically improbable to forge a Merkle branch for a transaction not present in the blockchain (provided block headers are secured). The implication of using SPV is that clients are not required to locally retain a full copy of the blockchain (or even to have read access to all blockchain data) in order to verify their transactions. In Bitcoin, clients using SPV are more widely deployed than nodes storing the entire blockchain locally. Existing simplified verification schemes require limited trust on information provided by peers and are therefore vulnerable to Sybil attacks. UTXO commitments [39] (a Merkle tree root of the current set of unspent transaction outputs embedded into each

[1] The coinbase transaction is the first transaction in a block, rewarding its miner with newly generated blockchain tokens

block header) would provide a truly trustless SPV implementation.

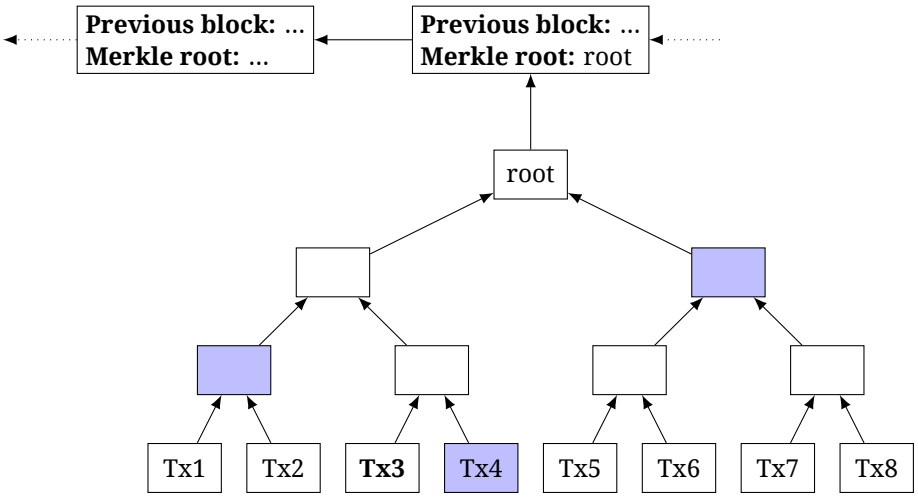

Figure 2: Simplified payment verification scheme for a transaction **Tx3**. Hashes included into the Merkle branch are marked with fill

2.1 Blockchain as Distributed System

According to the CAP theorem [40], no distributed system can simultaneously possess all three of the following characteristics:

- **consistency** – each node sees the same state of the system at each point of time
- **availability** – each request to a system receives a response
- **partition tolerance** – the system performs even if some nodes fail.

Blockchain-based systems are available and partition-tolerant, but not consistent. Indeed, availability of the system dictates that two nodes could accept mutually contradicting transactions. For example, Node A could receive a transaction to send $1,000 from Alice to Bob, while Node B at the same time could receive a transaction to send $1,500 from Alice to Steve, while Alice's balance is $2,000).

In a blockchain environment, the universally agreed upon state is the blockchain; the newest transactions do not initially belong to any block and are therefore *unconfirmed*. A blockchain protocol defines conditions for creating new blocks; after a block is created, it is propagated across the network, and the pool of unconfirmed transactions is updated according to the new state (in particular, transactions contradicting confirmed transactions are removed from the pool). This ensures that while unconfirmed transactions may be contradicting, the transactions in the blockchain are always consistent. A sound blockchain protocol diminishes the possibility for multiple nodes to add a new block at the same time; for example, if there is a known limited number of nodes in the system, those nodes can create blocks in turn with a period several times the duration to propagate a block over the network. Permissionless blockchains, i.e., systems with an open membership allowing every node to create blocks, utilize more complex algorithms out of necessity.

Distributed blockchain systems provide a built-in means of recovery from database corruption. Consider the following example: there are five nodes, two of which contain information about a certain transaction, and the other three do not. In a general case, either the transaction was inserted (perhaps, in an attack) into databases of the two nodes, or it was erased from the databases from the other three nodes; there is no inherent reason to prefer one variant to another. Furthermore, the node would not be able to immediately detect the inconsistency with other nodes. In the case of a blockchain-based database, not only are the corrupted versions of the database immediately obvious, but also they can be corrected as long as a single node with a valid blockchain remains in the network.

In case of Bitcoin, the blockchain is Byzantine fault tolerant [41] except for a negligible probability, i.e., the nodes of the network reach eventual consistency even in the presence of malicious actors or arbitrary failures of network nodes [42]. Blockchain technology is not the only way to create a fault-tolerant communication in a decentralized environment; there exist other consensus algorithms, for example, Paxos [43] and Raft [44]. Blockchains are better specifically for transaction processing, as they provide a built-in mechanism for transaction verification. In a related context, blockchains can be viewed as solving the multi-master replication problem persistent in other distributed databases [45].

2.2 Access to Blockchain Data

Blockchains can be classified based on access to the blockchain data.

Definition 1. A *public blockchain* is a blockchain, in which there are no restrictions on reading blockchain data (which still may be encrypted) and submitting transactions for inclusion into the blockchain.

Definition 2. A *private blockchain* is a blockchain, in which direct access to blockchain data and submitting transactions is limited to a predefined list of entities.

Definition 3. A *permissionless blockchain* is a blockchain, in which there are no restrictions on identities of transaction processors (i.e., users that are eligible to create blocks of transactions).

Definition 4. A *permissioned blockchain* is a blockchain, in which transaction processing is performed by a predefined list of subjects with known identities.

Note that a permissioned blockchain does not need to be private (Table 1). Indeed, there are multiple levels of access to a blockchain including:

1. reading transactions from the blockchain, perhaps with further restrictions (e.g., a user may have access only to transactions that involve him directly)
2. proposing new transactions for the inclusion into the blockchain
3. creating new blocks of transactions and adding them into the blockchain.

While the third level of access in permissioned blockchains is granted to a limited set of institutions (such as banks cooperatively running the blockchain or licensed transaction processors), it is

Table 1: Categories of blockchains based on access to transaction processing (permissioned vs. permissionless) and access to data (public vs. private)

By access to transactions	By access to transaction processing	
	Permissioned	Permissionless
Public	Proprietary colored coins protocols	Existing cryptocurrencies (e.g., Bitcoin)
Regulated	Direct read / transaction creation access for clients (limited; leveraged by client-friendly devices and applications) and regulators	Some colored coins protocols (e.g., Colored Coins Protocol), where ability to create transactions can be regulated
Private	Access limited to transaction processors (i.e., opaque for clients); benefits of blockchain technology are diminished	Not applicable

not immediately obvious that direct access to blockchain data should be restricted. On the contrary, the financial institutions jointly administering a permissioned blockchain could

- grant read access (perhaps, limited) to transactions and block headers to their clients in order to provide a technological, transparent and reliable way of ensuring the safety of clients' funds
- grant full read access to the blockchain to regulators in order to meet the necessary level of compliance
- provide to all entities with access to blockchain data with a rigorous and exhausting description of the blockchain protocol, which should contain explanations of all possible interactions with blockchain data.

These steps would ease independent auditing and verifying consistency of blockchain data, e.g. by regulatory entities. In the ideal case, blockchain protocols and access to blockchain data would be mostly standardized, which would further ease interaction and integration with other blockchains.

If a blockchain database is completely opaque for clients (i.e., they have no access to blockchain data), the security aspect of blockchain technology is diminished. While such system is still protected from attacks on the database itself, interaction with clients becomes vulnerable, e.g. to man-in-the-middle attacks. As a built-in protocol for transaction authorization is one of core aspects of blockchain technology, its potential subversion in favor of centralized solutions could negatively influence the security aspect of the system. Additionally, as transactions are accessible to a limited set of computers, there exists a risk of human factor intervening into the operation of the blockchain with no way for clients to detect such interference. Thus, the opaque blockchain design essentially undermines the core aspects of blockchain technology:

- decentralization (absence of a single point of failure in the system)
- trustlessness (reliance on algorithmically enforced rules to process transactions with no human interaction required).

In general, any interaction with blockchain data not rigorously defined by the blockchain protocol introduces vulnerabilities to the blockchain; as Nick Szabo argues [3], "[T]o remove vulnerability banks also have to remove individual human control and the individuals in charge or with root access. Banks [...] don't have any choice if they want to gain the benefits of having an army of independent computers that rigorously, constantly and securely check each others' work." We provide a more thorough comparison of private, permissioned and permissionless blockchains in the second part of the paper.

While the permissioned nature of blockchains for proprietary applications may be a necessary compromise in the medium term because of compliance and other factors, read access to blockchain data together with the publicly available blockchain protocol would remove most of vulnerabilities associated with opaque blockchain designs and would be more appealing to the clients of the institution(s) operating the blockchain. As evidenced by Bitcoin, simplified payment verification software can be used to provide a direct interface to blockchain data that would be both secure and not resource-intensive.

3 Permissioned Blockchains

Permissioned blockchains may be more attractive for institutions operating timestamped registries and ledgers, as most jurisdictions require registration of registry processors; these permissioned blockchains could form a more controlled and predictable environment than permissionless blockchains. Unlike cryptocurrencies, permissioned blockchains do not generally have native tokens. Native tokens are necessary in cryptocurrencies to provide incentives for transaction processors; in permissioned blockchains, transaction processors are rewarded by other means.

In the simplest case, creating blocks on a permissioned blockchain does not involve computations associated with proof of work. Indeed, consider the following protocol to create blocks similar to delegated proof of stake consensus in BitShares [46]:

Mining rotation

- There are a fixed number of operators N. Each of the operators possesses a private / public key pair; public keys for all operators along with their identities are known. The miner of a block is identified by a compulsory digital signature of a block, which is a part of its header.
- Operators create blocks in turns with a fixed time interval (e.g., 10 seconds) between blocks. The interval is large enough to ensure that a block is propagated and verified by all nodes before a new block needs to be created. The order of block creators may be fixed (e.g., corresponding to numeric order of their public keys), or randomly shuffled after each full cycle of N blocks.
- If an operator for some reason cannot create a block in the specified time interval, he misses a particular round. If this behavior or other sort of malicious mining activity (such as creating incorrect blocks) is repeated, the misbehaving operator is subject to an investigation.

To reverse a transaction with more than N confirmations, an attacker needs to gain access to *all* of the miners' private keys (cf. with 51% attack in Bitcoin). Thus, if transaction processors are the only consumers of the blockchain data, this protocol is theoretically more secure than proof of work.

However, the situation changes if read access to the blockchain data is available to third parties. As the proposed block creation scheme is similar to proof of stake consensus, it suffers from a similar problem that is the bane of proof of stake, "nothing at stake". The outside observer having a read access to the chain can never be sure that the chain he observes is actually the chain used among operators. As the creation of blocks in the proposed scheme (i.e., signing them with digital signatures) is a trivial operation, colluding operators could effortlessly create an unlimited number of alternative blockchains for various purposes: one for internal book-keeping, another to show to regulators, and so on. The problem is somewhat mitigated if the access to block headers of the chain is public and unrestricted; however, convincing tech-savvy clients and regulators that the network would be impervious to attacks could still be a difficult task, as colluding operators have the ability to effortlessly reorganize the arbitrary parts of the blockchain at any given moment. Thus, the above consensus protocol is secure only if there is no chance of collusion among blockchain operators (e.g., operators represent ideal parties with conflicting interests). Proof of work provides a means to ensure absence of collusion *algorithmically*, aligning with the overall spirit of blockchain technology.

The second consideration for making proof of work a viable consensus algorithm for permissioned blockchains is the following: In the protocol proposed above, the effort to reverse a transaction does not depend on the number of confirmations; transactions both 1 hour and 1 year old require from an attacker to obtain the same N private keys. With proof of work, the older the transaction, the greater the amount of computations is required to reverse that transaction; a 1 year old transaction would require approximately 1 year of continuous computations if the attacker's hash rate is twice the hash rate of the honest miners. Indeed, the attacker would need to overtake the honest chain with an initial handicap of one year's worth of computations. Intuitively, the attacker on average creates two blocks for each block created by honest miners; thus, if we denote the time to overtake the network as t,

$$t + 1 \text{ year} = 2t \;\Rightarrow\; t = 1 \text{ year}.$$

A more rigorous assessment can be performed using the Skellam distribution [47]. Let t_0 denote the expected time interval between blocks in the honest network; the attacker can maintain the generation of blocks with the expected interval $t_0/2$. The number of blocks discovered by the honest network over the period t is $n_h(t)$, a discrete random variable having Poisson distribution with mean t/t_0. Similarly, the number of blocks discovered by the attacker $n_a(t)$ is a Poisson-distributed random variable with mean $2t/t_0$. Observe that $n_a(t) - n_h(t)$ has the Skellam distribution; thus, the probability of a successful attack taking time t is

$$P\{\text{Skellam}(2t/t_0, t/t_0) > N\},$$

where N is the initial handicap of the attacker measured in blocks. For example, if $t_0 = 10$ minutes, $N = 1 \text{ year}/t_0 = 52{,}560$ blocks, then the probability of a successful attack taking a year is approxi-

mately 49.9%. For the attack to succeed with the probability of 99%, it needs to last a little longer – approximately 372 days.

The miner rotation protocol discussed above could be accommodated to incorporate proof of work:

Mining rotation with proof of work

- There is still a fixed number of miners with known identities proved by digital signatures in block headers. Note that miners and transaction processors are not necessarily the same entities; in the case that mining is outsourced to trusted companies, block headers should include digital signatures both from a miner and one or more processing institutions.
- Miners create blocks satisfying proof of work condition similar to that used in Bitcoin.
- There is an enforced mining diversity [48]: a miner cannot create more than rW blocks from the latest W blocks, where W is an integer window (e.g., $W = 10$), and r is the diversity parameter (e.g., $r = 0.4$, meaning no miner can create more than 40% blocks in the long term).

The diversity condition somewhat diminishes the hash rate providing network security. However, with the right choice of parameters, W and r, this loss could be minimized. For example, if $W = 10$, $r = 0.4$, and there are 5 miners with $p = 20\%$ hash rate share each, the amount of hash rate lost due to enforced diversity is

$$\sum_{i=\lfloor rW \rfloor+1}^{W} \binom{W}{i} p^i (1-p)^{W-i} = \sum_{i=5}^{10} \binom{10}{i} 0.2^i \cdot 0.8^{10-i} \approx 3.3\%.$$

The proposed protocol solves the problem with the potentially unlimited number of alternative chains. Maintaining multiple versions of a blockchain with proof of work costs resources: electricity and hashing equipment. The hashing power spent to create a blockchain and the hashing power of every miner can be reliably estimated based on difficulty target and period between created blocks; an auditor could compare these numbers with the amount of hashing equipment available to operators and make corresponding conclusions.

The main drawback of mining rotation with proof of work is the exponential distribution of time periods between neighboring blocks. The expected time period between blocks could be reduced to a minute or less; the problem of benign blockchain splits caused by two miners creating a new block at approximately the same time can be mitigated by invertible Bloom lookup tables [49].

For an additional boost in transaction processing speed, a permissioned blockchain system could additionally introduce synchronization of unconfirmed transactions (e.g., using a two-phase commit protocol [50]). This mechanism would be virtually inevitable when a system in question needs to make decisions faster than a minimum achievable interval between blocks; an example is high-frequency trading. The blockchain would still be useful in this case as an immutable storage of transaction history. Using an additional consensus protocol for unconfirmed transactions alleviates most problems associated with occasionally long time intervals between blocks when using proof of work.

As entities maintaining a permissioned blockchain with proof of work do not need to continuously increase their hash rate in order to maximize their profit (cf. with Bitcoin and other cryptocurrencies), the hash rate on a permissioned chain is not required to reach the levels of Bitcoin (order of 10^{17} hashes per second at the time of writing). On the other hand, the hash rate level needs to be set high enough to make outside attacks implausible; this goal can be accomplished if the hash rate level necessitates the use of specialized hardware – application-specific integrated circuits (ASICs) with their design differing from the designs used in existing cryptocurrencies. As there is a limited number of ASIC manufacturers, a chance of a covert attack in this case would be quite low (note that, besides manufacturing hardware, an attacker would still need to obtain private keys of all miners on the permissioned chain).

Consider the estimate of hash rate based on the balance of expenses and profits gained from implementing security relying on proof of work. Assume that operating expenses of proof of work equipment are caused by its electricity consumption. As

- energy efficiency of modern hashing equipment is order of 0.1 kW / (THash / s)[2] [51],
- cost of electricity is order of \$0.1 per kW · h [52],

the operating expenses are approximately equal to $\$0.01H$ per hour, where H is the hash rate measured in THash / s. The cost of hashing equipment is close to \$400 per THash / s [53]; thus, if we assume the amortization period of three years, amortization expenses are equal to

$$\$400H/(3 \cdot 365 \cdot 24) \approx \$0.015H \text{ per hour.}$$

Thus, the total expenses are order of \$0.03 per 1 THash / s per hour, or

$$\$0.03H \cdot 24 \cdot 365 = \$262.8H \text{ per year.}$$

Consequently, \$10 million yearly expenses on proof of work security (which is quite low compared to potential gains from utilizing blockchain technology, estimated at several billion dollars per year [54]) correspond to the hash rate of approximately 38 PHash / s, or a little less than 10% of the total hash rate of the Bitcoin network.

Note that using merged mining technique, all permissioned blockchains operated by the same institution could be secured with the same hashing equipment, thus significantly reducing the price of proof of work security. Moreover, proof of work could be partially or completely provided by existing public blockchains as described in the following sections; collusion attacks on a permissioned blockchain remain implausible regardless of the way proof of work is utilized in blockchain security.

3.1 Merged Mining

Merged mining is a technique that allows for the use of the same proof of work mining equipment to secure more than one blockchain [55]. For example, merged mining is supported in Namecoin [56];

[2] 1 THash / s $= 10^{12}$ hashing operations per second

miners can submit Bitcoin proof of work instead of Namecoin native proof of work to create valid Namecoin blocks. However, as the Bitcoin protocol itself does not currently support the concept of merged mining, it is not possible to submit proof of work from another blockchain for a Bitcoin block.

Merged mining and chain anchoring, which we consider in the following section, both rely on the concept of witness transactions.

Definition 5. A *witness transaction* on Chain A (the supporting blockchain) witnessing a block on the Chain B (the main blockchain) is a valid transaction according to the protocol of Chain A, which contains the unique identifier of the block in question constructed according to the protocol of Chain B (e.g., a 32-byte cryptographic hash of its header) as a part of transaction data.

In the case Bitcoin is used as the supporting blockchain, a block header hash can be included in a transaction using a **RETURN** instruction of the Bitcoin scripting language or other techniques similar to those utilized in colored coins protocols.

Consider the principles of merged mining with the example of the Bitcoin / Namecoin pair:

1. A miner who wants to create blocks both for Bitcoin and Namecoin processes transactions for both of these systems. The miner creates a Namecoin block template by assembling enough transactions, fills in its header and calculates a hash of the block. Note that the assembled block is not a valid Namecoin block as it most probably does not satisfy Namecoin proof of work.
2. The miner then inserts a witness transaction, i.e. a transaction, which contains the calculated hash of a Namecoin block as a part of its data, into a set of unconfirmed Bitcoin transactions. From the point of view of the Bitcoin protocol, it is an ordinary transaction.
3. The miner assembles a Bitcoin block containing the transaction he created in the previous step, and attempts to solve the block to satisfy a difficulty target either in Bitcoin or in Namecoin.
4. If the miner finds a valid Bitcoin block first, he publishes it in the Bitcoin network.
5. If the miner finds a Bitcoin block header that satisfies the difficulty target for Namecoin, the miner creates and publishes a new Namecoin block based on the previously created template. The new block additionally includes the Bitcoin block header, the witness transaction and the Merkle branch corresponding to it.

Merged mining could be used to accept Bitcoin proof of work for permissioned or private blockchains (Fig. 3). Note that the miner is not required to process transactions on the chain that supports merged mining; he merely needs to know the block header template for this chain. For example, a permissioned blockchain could accept the proof of work protocol based on SHA-256 hashing function [57] as used in Bitcoin. In this case, security of the blockchain could be achieved by cooperating with Bitcoin mining pools; the transaction processors on the permissioned chain could provide the pools with block header templates via established secure channels and receive block headers secured with proof of work.

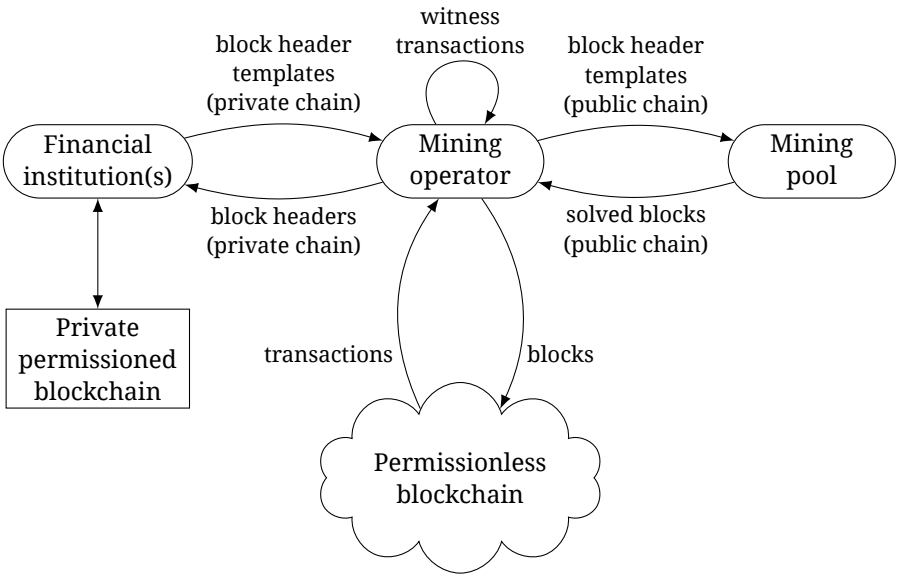

Figure 3: Merged mining for a private permissioned blockchain and a public blockchain (e.g., Bitcoin)

Merged mining could also be used to aggregate security of multiple permissioned blockchains (Fig. 4). With this setup, local network nodes corresponding to multiple chains maintained by an institution all submit block header templates to a local specialized proof of work data center. The center builds a specialized *metachain* with submitted block header templates entirely replacing transactions (i.e., the only goal of the metachain is securing other blockchains; it does not have tokens and does not process value transfer). When a new metachain block is discovered, it is submitted to all connected permissioned blockchains. Thus, all connected blockchains are secured with the hash rate of the metachain, which can be set sufficiently high to correspond to the total value transfer rate. Furthermore,

- the described approach is scalable, as it decouples security and transaction processing and can be adapted to hundreds of permissioned blockchains
- maintenance of the metachain could be outsourced to a trusted security provider without compromising confidential transaction details.

3.2 Blockchain Anchoring

A similar concept to merged mining is *blockchain anchoring* (a term used, e.g., in the Factom white paper [58]). In blockchain anchoring, those who maintain the permissioned blockchain would periodically submit hashes of block headers for inclusion into a supporting permissionless blockchain in the form of witness transactions; then, the included information can be verified manually by users of the permissioned chain by providing a simplified payment verification proof similar to those used in merged mining (Fig. 5). Anchoring provides additional guarantees of blockchain immutability, while the primary source of immutability is still internal to the permissioned blockchain (e.g., it is provided by the mining rotation algorithm described earlier). On the other hand, in merged mining, the use of

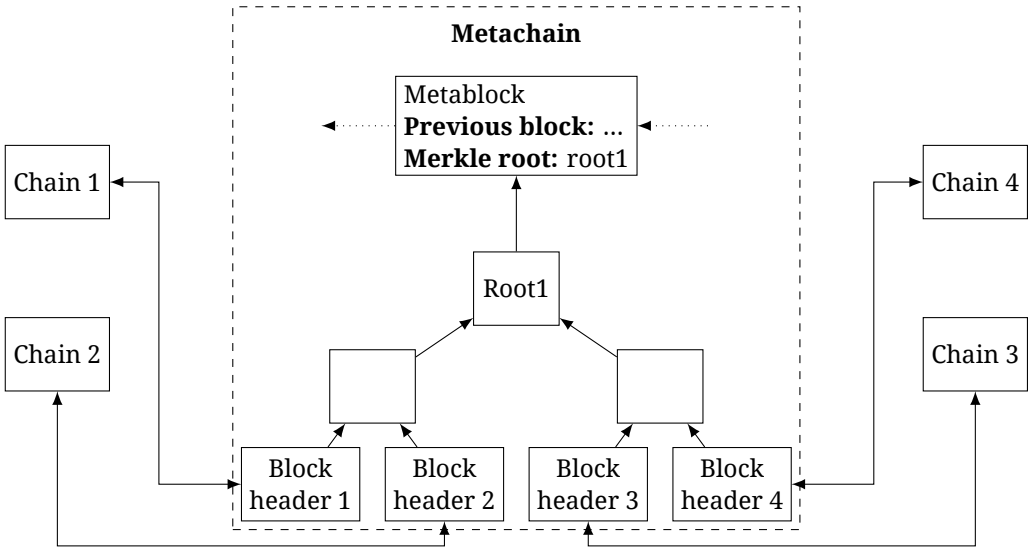

Figure 4: Merged mining used to secure multiple permissioned blockchains with a single dedicated metachain

an external blockchain is one of the primary sources of immutability; most of blocks on the chain supporting merged mining could be secured with external proof of work, as it is the case for Namecoin. Compared to merged mining, anchoring has advantages:

- Anchoring can be used for blockchains that do not rely on proof of work as an internal consensus mechanism; for example, anchoring can be successfully implemented for a mining rotation protocol.
- Unlike merged mining, anchoring does not require cooperation with miners on the permissionless blockchain. While merged mining is virtually effortless for miners in theory, its adoption can still be slowed down due to various factors. In the case of anchoring, the cooperation between those who maintain the permissioned blockchain and miners on the supporting chain is entirely optional.
- Anchoring utilizes the full hash rate of the supporting blockchain, whereas merged mining typically uses a small fraction of its hashing power, which is equal to the fraction of miners performing merged mining among all miners on a supporting blockchain.

An anchoring protocol needs to allow for the fact that blocks on the supporting blockchain containing a block header hash are typically created at irregular intervals that are substantially greater than the interval between blocks on the permissioned blockchain. For this reason, the anchoring protocol may specify that a block header on the permissioned blockchain may (but does not need to) include an SPV proof for a witness transaction of one of preceding blocks on the permissioned chain. For example, if blocks on the permissioned blockchain are created each 10 seconds:

1. A witness transaction could be submitted to the supporting chain for one block in 180 (i.e., every 30 minutes).
2. The witness transaction corresponding to this block header would need to gain a necessary number of confirmations (e.g., 4 or 6) such that a reorganization that would exclude the transaction

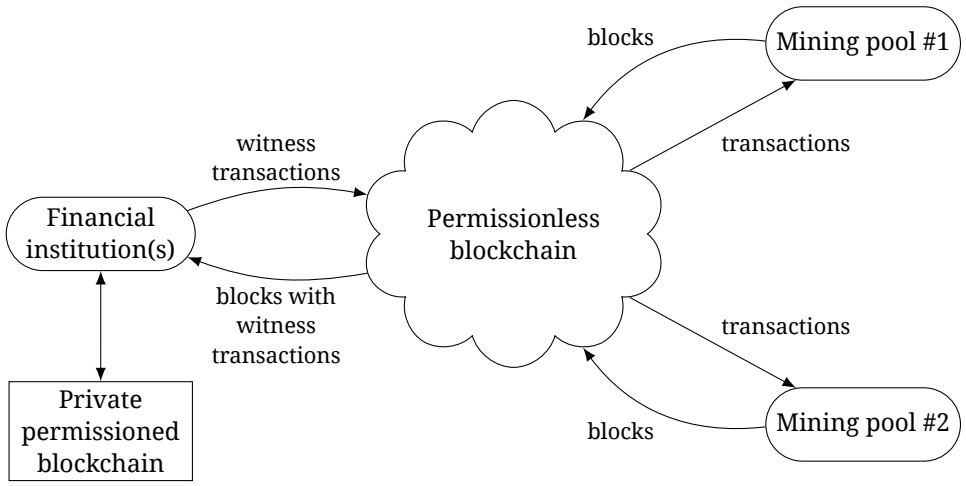

Figure 5: Anchoring a private permissioned blockchain with the supporting public blockchain (e.g., Bitcoin). Unlike merged mining, anchoring requires no or limited cooperation with mining pools

from the supporting chain to be statistically unlikely.

3. Then, the SPV proof corresponding to the witness transaction would be included into the header of a block on the permissioned chain.

In the case of Bitcoin, the whole process would take a couple of hours. The probability for a witness transaction to gain the necessary number of confirmations can be calculated using Poisson probability distribution:

$$P_c(C) \stackrel{\text{def}}{=} P\{\langle\text{confirmations in 2 hours}\rangle \geqslant C\} = 1 - \sum_{k=0}^{C-1} \frac{\lambda^k e^{-\lambda}}{k!}, \tag{1}$$

where $\lambda = 12$ is the expected number of confirmations over the span of 2 hours. Equation (1) yields $P_c(4) \approx 99.8\%$ and $P_c(6) \approx 98.0\%$.

For a chain secured with anchoring, an attacker would need to target consensus mechanisms of both the permissioned blockchain and the supporting public chain. For example, if the permissioned blockchain is secured by mining rotation and it is anchored to the Bitcoin blockchain, one would need to obtain all private keys of miners on the former blockchain and control 50% of the Bitcoin hash rate in order to reverse a transaction. Thus, anchoring is an efficient mechanism for diversifying security of a blockchain system.

4 Conclusion

Blockchain-based databases provide a secure and naturally decentralized framework for transaction processing. One of major advantages of blockchains compared to other distributed databases is integration of data processing, consistency and security into an algorithmically enforced blockchain protocol, which removes the human factor from the equation. Due to legal and technical concerns, institutions that operate financial ledgers or registries may be inclined to utilize permissioned blockchains, at least in the short run. However, permissioned does not necessarily mean private; two core

aspects of blockchain technology – decentralization and trustlessness – are fully leveraged only if access to the blockchain protocol and contents is provided to the end users.

Permissioned blockchains could form a the basis for blockchain innovations for services that operate ledgers or timestamped registries. Although permissioned chains do not require to use proof of work, this consensus protocol can still be utilized as an additional level of security and to increase auditability and attractiveness of chains for customers, especially if blockchain data is partially or completely public. In proof of work-enabled blockchains, merged mining can be used as an effective tool to cut the costs of the mining equipment or outsource it without compromising the security of the system. Blockchain anchoring has a similar goal of diversifying blockchain security and could be used for permissioned blockchains that do not rely on proof of work internally. Both approaches are not mutually exclusive and could be utilized together to achieve the optimal level of security in a permissioned environment.

Bitcoin in particular could be appropriate for use in blockchain innovations as a supporting blockchain in merged mining or anchoring due to the following factors:

- relatively small number of mining pools with established identities, which allows them to act as known transaction validators by cooperating with institutions
- high level of security provided by the hash rate of the Bitcoin network.

References

[1] *Matt Levine* (2015). Blockchain for banks probably can't hurt. In: Bloomberg View
URL: http://www.bloombergview.com/articles/2015-09-01/blockchain-for-banks-probably-can-t-hurt

[2] *Satoshi Nakamoto* (2008). Bitcoin: A peer-to-peer electronic cash system
URL: https://bitcoin.org/bitcoin.pdf

[3] *Ian Allison* (2015). Nick Szabo: If banks want benefits of blockchains they must go permissionless. In: International Business Times
URL: http://www.ibtimes.co.uk/nick-szabo-if-banks-want-benefits-blockchains-they-must-go-permissionless-1518874

[4] *Leon Pick* (2015). Estonia's LHV Bank Testing Colored Coins-Based 'Cuber'. In: Finance Magnates
URL: http://www.financemagnates.com/cryptocurrency/news/estonias-lhv-bank-testing-colored-coins-based-cuber/

[5] (2015). Nasdaq launches enterprise-wide blockchain technology initiative
URL: http://www.nasdaqomx.com/newsroom/pressreleases/pressrelease?messageId=1361706&displayLanguage=en

[6] (2015). Nasdaq and Chain to partner on blockchain technology initiative
URL: http://www.nasdaqomx.com/newsroom/pressreleases/pressrelease?messageId=1373282&displayLanguage=en

[7] *Ian Allison* (2015). The French bitcoin revolution: BNP Paribas testing crypto on its currency funds. In: International Business Times
URL: http://www.ibtimes.co.uk/french-bitcoin-revolution-bnp-paribas-plans-add-crypto-its-currency-funds-1512360

[8] *Grace Caffyn* (2015). Barclays trials Bitcoin tech with pilot program In: CoinDesk
URL: http://www.coindesk.com/barclays-trials-bitcoin-tech-with-pilot-program/

[9] *Joon Ian Wong* (2015). Goldman Sachs report says Bitcoin could shape 'future of finance'. In: CoinDesk
URL: http://www.coindesk.com/goldman-sachs-report-says-bitcoin-could-shape-future-of-finance/

[10] *Emily Spaven* (2015). Circle raises $50 million with Goldman Sachs support. In: CoinDesk
URL: http://www.coindesk.com/circle-raises-50-million-with-goldman-sachs-support/

[11] *Pete Rizzo* (2014). UBS: Banks could 'absorb the benefits' of Bitcoin. In: CoinDesk
URL: http://www.coindesk.com/swiss-bank-ubs-banks-absorb-benefits-bitcoin/

[12] *Stan Higgins* (2014). US banks announce Ripple protocol integration. In: CoinDesk
URL: http://www.coindesk.com/us-banks-announce-ripple-protocol-integration/

[13] *Jon Southurst* (2015). Australia's Commonwealth Bank latest to experiment with Ripple. In: CoinDesk
URL: http://www.coindesk.com/australia-commonwealth-bank-ripple-experiment/

[14] *Grace Caffyn* (2015). Australian banks Westpac and ANZ experiment with Ripple. In: CoinDesk
URL: http://www.coindesk.com/australian-banks-westpac-and-anz-experiment-with-ripple/

[15] *Ian Allison* (2015). UBS reveals its interest in Sidechains as well as Ethereum. In: International Business Times
URL: http://www.ibtimes.co.uk/ubs-reveals-its-interest-sidechains-well-ethereum-1519706

[16] *Diana Ngo* (2014). ING, other major Dutch banks take interest in blockchain tech
URL: http://cointelegraph.com/news/113033/ing-other-major-dutch-banks-take-interest-in-blockchain-tech

[17] *Ian Allison* (2015). Codename Citicoin: Banking giant built three internal blockchains to test Bitcoin technology. In: International Business Times
URL: http://www.ibtimes.co.uk/codename-citicoin-banking-giant-built-three-internal-blockchains-test-bitcoin-technology-1508759

[18] *Liyan Chen* (2015). 2015 Global 2000: The world's largest banks. In: Forbes
URL: http://www.forbes.com/sites/liyanchen/2015/05/06/2015-global-2000-the-worlds-largest-banks/

[19] *Oscar Williams-Grut* (2015). Santander is experimenting with bitcoin and close to investing in a blockchain startup. In: Business Insider
URL: http://www.businessinsider.com/santander-has-20-25-use-cases-for-bitcoins-blockchain-technology-everyday-banking-2015-6

[20] *Deutsche Bank Group* (2015). Re: Deutsche Bank's response to ESMA's call for evidence on virtual currencies and distributed ledgers
URL: http://scribd.com/doc/273151640/Deutsche-Bank-Letter

[21] *Ravi Menon* (2015). A smart financial centre (keynote address at Global Technology Law Conference 2015)
URL: http://www.mas.gov.sg/news-and-publications/speeches-and-monetary-policy-statements/speeches/2015/a-smart-financial-centre.aspx

[22] *Stan Higgins* (2015). IBM reveals proof of concept for blockchain-powered Internet of Things. In: CoinDesk
URL: http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/

[23] *Stan Higgins* (2015). IBM developing new blockchain smart contract system. In: CoinDesk
URL: http://www.coindesk.com/ibm-developing-new-blockchain-smart-contract-system/

[24] *Global Agenda Council on the Future of Software & Society* (2015). Deep shift: technology tipping points and societal impact
URL: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[25] *Robleh Ali, John Barrdear, Roger Clews, James Southgate* (2014). Innovations in payment technologies and the emergence of digital currencies
URL: http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf

[26] *Edward Robinson, Matthew Leising* (2015). Blythe Masters tells banks the blockchain changes everything. In: Bloomberg Business
URL: http://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything

[27] *Anju Patwardhan* (2015). Blockchain – a disruptive force for good? In: LinkedIn Pulse
URL: https://www.linkedin.com/pulse/blockchain-disruptive-force-good-anju-patwardhan

[28] *Emily Spaven* (2015). Barclays data officer praises blockchain tech at SWIFT forum. In: CoinDesk
URL: http://www.coindesk.com/barclays-data-officer-praises-blockchain-tech-at-swift-forum/

[29] *Reid Hoffman* (2015). Why the block chain matters. In: Wired.
URL: http://www.wired.co.uk/magazine/archive/2015/06/features/bitcoin-reid-hoffman

[30] *Richard Gendal Brown* (2015). Blockchain is where banks have the most obvious opportunity. But you ignore Bitcoin at your peril
URL: http://gendal.me/2015/05/12/blockchain-is-where-banks-have-the-most-obvious-opportunity-but-you-ignore-bitcoin-at-your-peril/

[31] *Tim Swanson* (2015). Permissioned distributed ledgers
URL: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

[32] (2015). Hyperledger summary
URL: http://d1iohkh6wgqugq.cloudfront.net/static/resources/hyperledger-summary.pdf

[33] (2015). Chain raises $30 million from financial industry leaders
URL: http://www.prnewswire.com/news-releases/chain-raises-30-million-from-financial-industry-leaders-300140260.html

[34] *Justin OConnell* (2015). Nine major banks partner on block chain initiative. In: CCN: Financial Bitcoin & Cryptocurrency News
URL: https://www.cryptocoinsnews.com/nine-major-banks-partner-block-chain-initiative/

[35] Turing completeness. In: English Wikipedia
URL: https://en.wikipedia.org/wiki/Turing_completeness

[36] Public-key cryptography. In: English Wikipedia
URL: https://en.wikipedia.org/wiki/Public-key_cryptography

[37] *Ralph Merkle* (1988). A digital signature based on a conventional encryption function. In: Advances in Cryptology – CRYPTO '87 (Lecture Notes in Computer Science), Vol. 293, pp. 369–378
URL: http://link.springer.com/chapter/10.1007%2F3-540-48184-2_32

[38] *BitFury Group* (2015). Proof of stake versus proof of work
URL: http://bitfury.com/content/4-white-papers-research/2-proof-of-stake-vs-proof-of-work/pos-vs-pow-1.0.2.pdf

[39] *Andrew Miller* (2012). Storing UTXOs in a balanced Merkle tree (zero-trust nodes with $O(1)$-storage). In: BitcoinTalk Forums
URL: https://bitcointalk.org/index.php?topic=101734.0

[40] *Seth Gilbert, Nancy Lynch* (2002). Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. In: ACM SIGACT News, Vol. 33 (2), pp. 51–59

[41] *Leslie Lamport, Robert Shostak, Marshall Pease* (1982). The Byzantine generals problem. In: ACM Transactions on Programming Languages and Systems, Vol. 4 (3), pp. 382–401
URL: http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf

[42] *Andrew Miller, Joseph J. LaViola, Jr.* Anonymous Byzantine consensus from moderately-hard puzzles: a model for Bitcoin
URL: https://socrates1024.s3.amazonaws.com/consensus.pdf

[43] *Leslie Lamport* (1998). The part-time parliament. In: ACM Transactions on Computer Systems, Vol. 16 (2), pp. 133–169
URL: http://research.microsoft.com/en-us/um/people/lamport/pubs/lamport-paxos.pdf

[44] *Diego Ongaro, John Ousterhout* (2013). In search of understandable consensus algorithm
URL: https://ramcloud.stanford.edu/wiki/download/attachments/11370504/raft.pdf

[45] *Gideon Greenspan* (2015). Ending the bitcoin vs blockchain debate. In: MultiChain blog
URL: http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/

[46] *Daniel Larimer, Charles Hoskinson, Stan Larimer* (2014). BitShares: a peer-to-peer polymorphic digital asset exchange
URL: http://scribd.com/doc/173481633/BitShares-White-Paper

[47] Skellam distribution. In: English Wikipedia
URL: https://en.wikipedia.org/wiki/Skellam_distribution

[48] *Gideon Greenspan* (2014). MultiChain private blockchain
URL: http://www.multichain.com/download/MultiChain-White-Paper.pdf

[49] *Gavin Andresen* (2014). O(1) block propagation
URL: https://gist.github.com/gavinandresen/e20c3b5a1d4b97f79ac2

[50] Two-phase commit protocol. In: English Wikipedia
URL: https://en.wikipedia.org/wiki/Two-phase_commit_protocol

[51] *Pete Rizzo* (2014). BitFury raises $20 million to power new ASIC chip development. In: CoinDesk
URL: http://www.coindesk.com/bitfury-raises-20-million-asic-development-mining-output/

[52] Average price of electricity to ultimate customers by end-use sector, July 2015 and 2014. U.S. Energy Information Administration
URL: http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_06_a

[53] Antminer S7 batch 1. Bitmain
URL: https://bitmaintech.com/productDetail.htm?pid=000201508270840214710HYdwd9D06A0

[54] *Yessi Bello Perez* (2015). Santander: blockchain tech can save banks $20 billion a year. In: CoinDesk
URL: http://www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year/

[55] Merged mining specification. In: Bitcoin Wiki
URL: https://en.bitcoin.it/wiki/Merged_mining_specification

[56] Namecoin
URL: http://namecoin.info/

[57] SHA-2. In: English Wikipedia
URL: https://en.wikipedia.org/wiki/SHA-2

[58] *Paul Snow, Brian Deery, Jack Lu, David Johnston, Peter Kirby* (2014). Factom: business processes secured by immutable audit trails on the blockchain
URL: https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper.pdf