Blockchain Synthesis

José Carrijo / ITI / CC/ PR

Keywords: Blockchain, cryptocurrency, digital currency, bitcoin, ethereum, Monero, proof of work, elliptic curve, RSA

1. INTRODUCTION

Going deeper into the details of *blockchain* or cryptocurrency leads to an enhanced awareness on how ingenious this technology is, sparking technical reasoning, fostering curiosity, helping to absorb concepts, and allowing to realize that this technology may change the way how interactions take place between people, government agencies, and both public and private companies. Upon focusing on the mathematical theories that enabled safe and efficient applications to be developed, there is no obvious challenge to understanding the mathematical evidence, however curiosity is visibly aroused. ITI seeks to have sufficient technology know-how to discuss with expert technicians on a peer level, propose solutions, review projects, and partner with governmental agencies and private enterprises. Overall, ITI strives to make its technical contribution, spreading the interest in technology with a clear technical message, to foster research towards advances in technology. Having technical knowledge on networks involving *blockchain*, such as cryptocurrency networks, it is possible to envision the reasons for their technological beauty, their subtlety, their acceptance and unfettered adoption by society. The most intriguing is that the entire process – carried out in a sequenced, intermittent, or periodical manner – can be recorded in a sequence to a *blockchain*, the requirement being to measure the strategy relating technical, political, bureaucratic, structural, and financial interests.

Blockchain is a promising technology. It is the framework for diversified applications, such as cryptocurrencies and documental records, arranged in sequenced and linked blocks, in decentralized environments. Linking is done in a way to render it unlikely for records to be altered without such changes being noticed.

It is possible that several other *blockchain*-based applications will come up and, in a short time these will make a difference and become something greater, causing significant social impact, and triggering irreversible changes to everyday life and culture. Fruition of such technology, be it either for the citizen’s convenience or for transparency and control – such as cryptocurrencies that have been revolutionizing and changing forecasts – or applications to record and link documents, their conception, buy-in, and integration to our culture may cause a radical change in human behavior. In this case, it is important to highlight two basic issues: firstly, if it is the case of providing a service whose homologation is performed in a decentralized manner; secondly, whether transparency is the intended goal.

The truth is that *blockchain* is the cornerstone for this dichotomy, the base for cryptocurrency and chained and linked documents recording applications. It is common to see comments on cryptocurrencies, or chained documents recording, highlighting the *blockchain* technology and terminology, however neglecting to quote the application. *Blockchain* has become a label on its own; the most varied applications are overshadowed by the technology principle: chaining blocks with decentralized checking by means of challenges. It must be considered that it would become difficult to consolidate systems having digitally-signed transactions and checks exclusively, considering the source, however perhaps failing to take in the link to their destination.

Document chaining and linking applications are peculiar, maybe not sufficiently differentiated, if compared to those developed for cryptocurrencies, on account of both their use and their users. Applications that are exclusively for linking documents have no reason to be based on ‘Proof of Work’ (PoW) by challenges, and the data or documents are not necessarily saved to record blocks. Furthermore, the definition or development of an application for such purpose depends of the State or company interest, since it requires infrastructure, interest in having transparency, and the availability of data and documents whose access is not necessarily unrestricted.

On its turn, cryptocurrency belongs to an application class much more widespread in the *blockchain* realm. Applications like those used in cryptocurrencies are more than a system; they are topologies on their own for being overly complex and, at the same time, as if there were an assumptions/concepts dichotomy, they are transparent to users. What’s most intriguing is that, from the few major cryptocurrencies, hundreds of others have been derived.

From the *blockchain* applications existing to date, the most impactful, best known, and most enigmatic, are those for cryptocurrencies. The idea of cryptocurrencies – if taken merely as a concept – is quite eccentric: from one system, people begin to buy and sell digital money, something like a ‘virtual asset’, that is valued according to demand, and not as a ‘solid product’, which simply doesn’t exist. Whoever buys them will receive no dividends, they’ll only profit on the demand. Their value possibly fluctuates on account of there being no collateral, perhaps because they are new, and maybe because they have no liquidity. There are hundreds of currencies available, however most of them have trouble in getting established, on account of being comparatively unknown.

For an initially valueless cryptocurrency, certain amounts are offered to random users – under the label of *Initial Coin Offering (ICO)* - upon launching the application, at no cost whatsoever. Then, they await its acceptance, deployment, and trading. This takes place without any visible collateral, without centralized control, based solely on the confidence of users and investors, who learn to trust and believe in the technology, the process, and the system. Such features may be deemed – and subjectively understood – as the collateral for digital currencies.

Among other peculiarities of cryptocurrencies, there is the development and implementation of applications. Their topology is overly complex. For instance, upon their creation, the maximum amount of currency is set, as well as the approximate time for miners to formalize and clear each transaction. They also enable miners to collect service fees from users and, most intriguingly, they reward the first miner to approve a transaction by means of challenges based on the miner’s “processing capacity”. Results are statistically achieved, based on evidence: *Proof of Work, PoW*. To win these challenges, for the most common cryptocurrencies, some minutes of exhaustive computational execution were required, based on usually dedicated hardware and firmware. For some digital currencies, there is also the *Proof of Stake (PoS*), which takes less time, usually one minute or less.

The availability of a sum given to miners, as a reward after the Proof of Work, is evidence that the transaction is valid and unique; this is when the digital currency is created. In the specific case of the *bitcoin* cryptocurrency, this amount is halved every time a preset time period elapses. This computing effort is set on the average computing time required to validate the transaction, in order to properly take into account the currency’s “life span”. This makes the computational effort vary from time to time, always prioritizing the time required to validate the transaction, regardless of the technology used to track the solution considered.

One peculiarity of these cryptocurrencies is that they come to be exclusively from the development of an application, usually based on, and using, the technology framework of pre-established others, allowing users to buy and sell something exclusive, also named “digital currency”, “virtual currency”, or “crypto currency”. The purchase and sale operation is named transaction, which must be validated by third parties, named miners, who are usually rewarded for each validation by the system.

For users, there are possible hurdles to mining. For instance, if the amount in the transaction is next to nothing, or a cryptocurrency offers a higher reward, or holds a better cost-benefit ratio for the miner, this may shift the miners’ preference. On their turn, miners must make some investment in computing infrastructure, and pay their electricity bills. Thus the trade becomes a mix of trusting the system and mining infrastructure, aiming at profits for both miners and users.

2. THEORY AND TECHNOLOGY

Blockchain quickly became a well-known expression, a widely deployed term, a technical benchmark for multiple applications. In a natural and gradual way, it became widespread intrinsically and simultaneously with the massive use of some applications, and the possibility of being implemented in the most diverse technology segments. Nowadays, the *blockchain* technology is seen as a synthesis of its own technical framework.

Blockchain technology is used in applications that consider the use of chaining blocks containing linked data records, traceable and unchangeable. It further enables decentralized or otherwise tracking and clearance, linking each records block – *flat file* –

to its predecessor. Applications using *blockchain* and having relevant impact on society are digital currencies. They are conceived for decentralized clearance of each transaction, recording it on files, thus allowing transparent tracking of the transactions, albeit not necessarily its users. Just a few years were enough for hundreds of cryptocurrencies to come up. User IDs are preferably kept anonymous, while transaction records are unchangeable. It’s quite common to see comments on the *blockchain* technology associated to cryptocurrencies, and vice-versa.

Blockchain applications, upon providing services like decentralized clearance and permanent records brought an insight to users provided with more ideology and enthusiasm. They began to credit its use and widespread as a way out to get exempted from overwhelming control exerted by the State, and as an unequivocal manner to secure transparency to services provided by government, institutions, and companies alike. From the most varied stances, an underlying tenet is that making any services available through *blockchain* applications requires their control and clearance to be decentralized. This, however, is neither an assumption nor a major feature in this technology. Furthermore, conservative users also allege that, in case applications with contrary rules - such as decentralized clearance - would necessarily undermine processes aiming for transparency. This line of thought is so biased, that the simple option to purchase something different - like centralized clearance - automatically evokes the feeling of its being a backwards attitude, like going back to transparency, bad use of technology, and deception as well. This is not necessarily the case.

Blockchain is a subject that, when discussed, tends to demystify its technical complexity. In order to achieve a better understanding of the idea’s grounds, it is handled here with a technical, informative, and contextual stance. Part of the observations may be redundant, merely elucidative, or technically more conservative. Technical terms and expressions are used only when strictly necessary. The discussion of the techniques in this technology may bring about some better understanding of many of the reasons for its massification, which involves, and at least causes, some curiosity.

Such views and remarks on *blockchain* are based on the compilation and sequencing of ideas laid-out in different study and research sources. Essentially, they explore the stated perception of both the technological and contextual components. Some definitions expressed here in a rather simplistic manner are intended to mitigate doubt, when quoted upon commenting on processes involving *blockchain*.

2.1. CRYPTOGRAPHIC HASH

First, a ‘binary sequence’ should be understood as the digital content stored in some memory area, or digital content such as digital documents, images, audio, or video files.

The *Hash Function* found no standard translation into Portuguese. At first, professors in the São Paulo State – at Unicamp and USP – defined it as *“função resumo”*. On its turn, they also defined *“hash”*, the univocal correspondence to a binary sequence, as a “cryptographic hash”. This concept is important, because it’s at the core of block chaining.

Technically, there are security assumptions made for a hash function, which will ensure the uniqueness of the outcome, and the consequent security in the *blockchain* sequence. Given the x and y binary sequences, of any length |x| e |y|:

- It is [computationally] impossible to have the same cryptographic hash, i.e. HASH(x) = HASH(y)

- Once a cryptographic hash has been provided h = HASH(x), it is impossible to recover the binary sequence x that defined it.

Breaking a hash function is understood as when an attacker is able to ascertain that one or the other of these assumptions is not met; even if partially, however in a meaningful manner. Breaking a hash function is a term used in a different way when it’s about breaking the security of a signature or algorithm. Breaking a hash function occurs when two cryptographic hashs are found, regardless of their entries, with a high collision level: the quantity of coinciding bits in the cryptographic hash is significantly above 50%. The security of criptographic algorithm is broken when it is possible to retrieve the secured information or its key. Breaking a digital signature system, sometimes named signature break, takes place when an attacker manages to sign a document as a third party, either adulterating the document itself or not.

Given an input bit sequence of any length, a secure hash function outputs is statistically well-distributed bit sequence. So each miner, upon receiving the details of a transaction, and a “nonce”, an equally well-distributed bit sequence, plus a counter, executes exhaustive computing and cryptographic hash operations, until there are at least “k” zero-bits at the beginning of the string. This is why the challenge is fair, since it is impossible to know beforehand that a certain “nonce” will cause a larger or smaller number of calculations.

2.2. DIGITAL SIGNATURE

Having the intent of providing a better discussion on *blockchain* without recurring to technical cryptography principles, it is unavoidable to cover digital signature schemes. It is a principle required to ensure integrity and trustworthiness in systems based on this block chaining methodology, to have records signed and checked by public and private key pairs, or by digital certificates issued by PKI-type structures.

For *blockchain* applications, ITI considers it important to have digital certification based on Public Key Infrastructures (PKI), though most of the currently available applications use public and private key pairs. The use of such pairs is aimed to preserve the users' anonymity, generating them from the application, making the public key the basis for their address. ITI deems it important to have these two business models, the possibility of digital certificates in the ICP-Brasil standard, as they are legally valid.

Digital signature processes come from cryptography techniques and methods, specific protocols, from cryptographic primitives. On their turn, the best-known schemes are those based on the RSA system and elliptic curves. A digital certificate is basically the public (user) key encapsulated in a certain format with additional information as the user name and its validation, irrelevant in the mathematical process for ascribing the signature, however important for control and credibility.

It is worth noting that digital signature includes the integrity and non-repudiation service, as the user has no way of denying a signature if it was made using their private key. On its turn, the user's digital certificate, which includes their public key, does such check.

2.3. PROOF OF WORK (PoW)

The Proof of Work measurement comprises the repeated calculation of *hashes*, until the *hash* obtained has its first "k" positions filled with zeros.

The system defines as “target” a measurement forwarded to the miner, so that they may determine a cryptographic hash smaller than this metric sent. For instance, for the target 0xc7ea4f82, the hash result of a transaction, to which a nonce is added – a random sequence for each miner – enchained with a number that is increased step by step, corresponds to determine a *hash* that is smaller than:

```
PoW = 0xea4f82 * 2**(8*(0xc7 - 3)) =
0x0000000000ea4f82000000000000000000000000000000000000000000000000
```

3. SCENARIO

It is important to understand that the efficiency and credibility of the *blockchain* protocol will be the reason for other protocols and applications to be made available in the near future.

Blockchain comes up in the global scenario as an innovative and promising tool, on its own fostering research and development in countless environments. Applications make the key pairs generation service available for the self-identifying users. ITI considers that, for specific applications, such as those used by government, they may use ICP-Brasil standard digital certificates, which are legally valid, over key pairs.

Blockchain technology features block chaining, decentralized clearance, and digital signature check. As a rule, the protocols proposed so far ensure non-repudiation, however not necessarily data security nor thwarted tracking.

ITI understands as essential to build an aligned line of thought, to provide technical know-how and an actual contribution in *blockchain* technology for purposes where government is a stakeholder. In this context, the use of legally valid digital certification is deemed important. One example of *blockchain*-based applications is cryptocurrencies. Though these were proposed recently, since 2009, with support and investment from large corporations, they progressed quickly, and in a way that pleased their users. As a consequence, hundreds of other currencies were born in this short time span.

The countless *blockchain*-based protocols proposed require transposing challenges regarding privacy, scalability, and lacking governance – users control and the generated public and private keys.

Scalability is a hurdle for some applications that use - or that may use - the *blockchain* technology. There are applications requiring previous registration – licensing - of their users, while others don't – non-licensed. In these applications, performance in transaction clearance is low, on top of lacking governance. In applications with licensed users, performance is higher however the number of users is small. Furthermore, organizations and corporations are not necessarily democratic in their behavior, requiring control of their systems, operations, and policies, while this technology features transparency.

4. APPLICATIONS

Blockchain applications are based on digital signatures with elliptic curves. Among these, I'd like to comment on the peculiarity of the Monero cryptocurrency, for the subtlety of its protocol: it uses a quite efficient and secure signature method based on elliptic curves, named Ed25519. Its security is equivalent to NIST P-225's elliptic curve, and the 3000-bit RSA system; it provides non-traceability through one-off addresses and anonymous users; it is based on a homeomorphic cryptography scheme; and renders signature revoking impossible. The system implemented was a variation from the proposal by Fujisaki et al., named *ring signature*: the user signs a private transaction with their private key; for checking, this user makes available all public keys for all users in that ring in the registered users group; any group member who checks the signature on the transaction will be convinced that the subscriber is a member of the group, however it will be impossible to determine who signed it, therefore preserving anonymity. If, on one side, the *bitcoin* protocol uses a unique pair of private and public keys, the Monero protocol generates a one-off public key; this latter one is based on the user's access address; only the origin (the node) is able to recover the equivalent single private key.

5. CONDITIONERS

The *blockchain* technology provides data integrity, non-repudiation, and transparency; the transactions are chained and traceable, some are not encrypted. It stands out significantly in financial transactions; its users may make queries and transactions.

There is some concern by institutions and companies to adopt the most suitable application, binding their business model to some basic assumptions, such as different restrictions to licensed users or otherwise, centralized databases or otherwise.

For example, *Bitcoin* and *Ethereum* are *blockchain* instances for non-permissioned users, having decentralized databases. Any user may log in to the network to perform tasks or not, without any entity supervising them.

Cryptocurrency is just one of the applications for this technological innovation, having specific rules to validate transactions in an independent and decentralized manner.

Each block of transactions is enchained by the cryptographic hash of the preceding block in a unique way. Every transaction is signed by the user, and the most commonly used cryptographic hashs are 256 bits in length.

The *blockchain*-based protocols’ technical base refers to deployed resources which are public, not exchangeable, and sorted.

Technology develops in the details of each one of its parts. Specifically, the *bitcoin* core includes wallets, requirements for a transaction, block validation, and a complete peer-to-peer nodes network. It is an open source project for any purpose, there is a user community optimizing it, based on technical documents describing each service, feature, or functionality.

In order to better understand the *bitcoin* core, for those who are familiar with the installation of operating systems and applications, it might be interesting to install the development environment from the technical documentation, noticing the tools, libraries, software support, and the widely varied directives.

6. CRIPTOCURRENCY

Applications chaining and linking documents are differentiated from those used for cryptocurrencies, on account of both their use and their users. Applications exclusively for linking documents have no reason to be based on Proof of Work - PoW (challenges). Demand comes from the private sector, from government, or from citizens. The first two seek transparency and the availability of documentation, the latter focuses on investment and profit.

Each application, upon being made available to users, each currency, has a preset life span, the maximum amount in currency, the approximate time for miners to validate each transaction by means of winning challenges named [computational] Proof of Work, PoW, which is continuously adjusted, or Proof of Stake, PoS, and its associated reward.

Cryptocurrency belongs to an application class widely spread in the *blockchai*n technology. The cryptocurrency systems are topologies themselves, overly complex ones. As if there were a concepts vs. assumptions dichotomy, they are transparent to the users. What’s most intriguing is that, from the few central cryptocurrencies, hundreds of others are derived.

From the *blockchain* applications existing to date, the most impactful, best known, and most enigmatic, are those for cryptocurrencies. If taken merely as a concept, is quite eccentric: from one system, people begin to buy and sell digital money, and not a ‘solid product’, which simply doesn’t exist. Whoever buys them will receive no dividends, they’ll only profit if demand increases. Their value possibly fluctuates on account of there being no collateral, perhaps because they are new, and maybe because they have no liquidity. There are hundreds of currencies available, however most of them have trouble in getting established, on account of being comparatively unknown.

7. SUBTLETIES OF THE BITCOIN CURRENCY

Having created a measurement named “Proof of Work” to validate transactions is at least an ingenious idea. In the case of bitcoin, at every 2016 blocks, this computational effort is re-dimensioned. In average one block takes a few minutes to get validated. If the average time to clear increases beyond what was predicted, the computational effort will be lower, and vice-versa. This metric is directly linked to the stipulated life span of the currency. In this way, independently from new hardware and technology, the system controls it so that each clearing occurs as conceived.

For every clearing act there is a reward. In the case of bitcoin, in 2009 it was 50 bitcoins. Every four years (or every

210,000 validated blocks), the reward is halved. Currently, it is 12.5 bitcoins, in 2056 it will be 0.01 bitcoin, and in 2140, only 0.000000003 bitcoin. This reward amount dropping to its half at every time span may cause an adjustment to the fees stipulated by miners.

The Proof of Work measurement comprises the repeated calculation of hashes, until the hash obtained has its first “k” positions filled with zeros.

The hash resulting from a transaction, added to a ‘nonce’ – a random sequence, different for each miner and incremented one step at a time – corresponds to determining a hash having at least “k” initial bits filled with zeros, in a 256-bit sequence. Currently, the hash to be found must have 60 initial bits equal to zero, k = 60. This means that the probability of discovering a hash by luck with so many initial zeros makes it at least one trillion less likely than winning the Brazilian Mega Sena lottery: $2^{61}/2^{26}=2^{40}$. For this reason, a secure hash function must be chosen, with a statistically well-distributed resulting sequence.

8. KEYS and ADDRESSES

A cryptocurrency relies on methods, protocols, and cryptography algorithms that provide transaction security, authorship, and integrity; critical services for the blockchain technology. Keys, addresses, and digital signature schemes make up the core of this protocol. Public keys are employed as user addresses for receiving funds, private keys serve to sign for transactions. The key pairs are created by users and stored in their portfolios, generation parameters are saved by the system to - if required - generate the corresponding public keys from the private keys. Each user enables different services with an ownership certificate, a model of trusted cryptographic test and decentralized control.

The bitcoin protocol uses the elliptic curve sec256k1, NIST standard (National Institute of Standards and Technology) (Y^2 = X^3 + 7 mod p, with prime p defined as p = $2^{256}+2^{32}+2^9+2^8+2^7+2^6+2^4-1$), with 256 bits. To generate keys, a preset point on the G-curve is used. The public key is a point on the curve, comprising an ordered pair (x,y) that solves this equation. In order to cut to half the storage space for the public key, only the variable “x” is stored on wallet. To secure the private key, it is encrypted with the AES cryptography algorithm and a user password, and it is saved encrypted on wallet.

An wallet may hold a collection of key pairs, public (K) and private (k), encoded on 'Base58'. The private key is a 256-bit randomly generated binary sequence, often represented as a QR code. From the private key, the corresponding public key is determined. This user’s address (A) is generated with the functions SHA256 and RIPEMD160, and their public key. In every portfolio, the triad (k, K, A) is stored.

9. PORTFOLIO

The ‘Wallet’ term for cryptocurrencies may have different meanings and structures. Wallets don’t store user credits, as these remain on the blockchain network. Such terminology may refer to the user interface application, to making the service available while preventing undue access, to the management of keys and addresses, or to transaction tracking and signature. These applications provide the process core, ease of operation, security, and flexibility. ‘Wallet’ also refers to the data structure – files – used to store and manage keys, which may be deterministic or otherwise. These are generated from random sequences, and used one at a time. Those are hierarchically generated, by means of seeds in a tree structure. Thus they can be re-generated, which provides ease of use and portability: migration to another Wallet. In practice, security was made flexible, at the expense of user-friendliness and portability. Understanding the keys as a tree structure, certain branches may have specific purposes, such as making or receiving payments, or creating public key sequences without having to access private keys, generated from word sequences in English, made available by the application, which renders the generation process user-friendly, thanks to its mnemonics. Bitcoin technology has matured, causing the development of standards, making it interoperable, user-friendly, secure, and flexible.

10. TRANSACTIONS

Referencing one or another technique could be boring; when necessary, brief comments on concepts, terminology or definitions will be included. Cryptocurrency systems like bitcoin have improved in their security and resilience, their power going far beyond digital currency transactions, as they allow storing data unrelated to digital funds transfers. However this trend is controversial, since it clashes with the primary scope of this protocol.

Transactions are the most important part of the cryptocurrency protocols. The entire system is designed to ensure transactions validated within data structures, with sums being transferred between users, encoded and recorded on the blockchain, as if it were an accounting entity. Since blockchain is a recent and developing technology, allowing for the prospection towards creating many other applications, it is important to understand the content of a transaction, the details in its creation and checking, and how it becomes a permanent part of the records in the blockchain structure.

The most important part of the block is the output, comprising indivisible elements, recorded on the blockchain, organized and validated on the network, tracked by nodes organized in a decentralized manner.

For the cryptocurrency application, the digital signature has the purpose of defining and unconditionally guaranteeing the origin, the integrity, and the non-repudiation of the transaction. Every transaction is independently signed; it may even involve different users, when part of the credits comes from other transactions. As a requirement, a signature implies a commitment of the signing user to the transaction. For this purpose, it relies on the generation of random number strings, which should be different for each signature. The reuse of strings may cause a breach to the signature, and thus enable the Wallet to be hijacked, allowing for cryptocurrency embezzlement.

11. FINAL THOUGHTS

Getting familiar with the blockchain technology requires knowing cryptocurrency technology, the best known and most widespread. Systems using blockchain structure can change the relationships in the world, as it is exhaustively said about cryptocurrencies, linking them to blockchain, and vice-versa. What’s most surprising is that it can be applied to any process that results in procedures and their intermittently or regularly generated outcomes. For this intent, the dimension of the scenario to be implemented is paramount, and the outcomes and impacts must be measured.

12. RECOMMENDED READING:

1. AlTawy, Riham; ElSheikh, Muhammad; Youssef, Amr M.; Gong, Guang – Lelantos: A Blockchain-based Anonymous Physical Delivery System

2. Antonopoulos, Andreas M.: Mastering Bitcoin - Programming the Open Blockchain,

3. Chou, Tung – Sandy2x: New Curve 25519 Records

4. Kumar, Amrit; Fischer, Clément; Tople, Shruti; Shaxena, Prateek - A Traceability Analysis of Monero’s Blockchain

5. Li, Ming; Weng, Jian; Yang, Anjia; Lu, Wei – CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourincin

6. Li, Wenting; Sforzin, Alessandro; Fedorov, Sergey; Karame, Ghassan - Towards Scalable and Private Industrial Blockchains

7. Lin, Huijia; Tessaro, Stafano – Indistinguishability Obfuscation from Bilinear Maps and Block-Wise Local PRGs

8. Rivest, R. L; Shamir, A.; Tauman, Y. - How to leak a secret

9. Su, Borching - MathCoin: A Blockchain Proposal That Helps Verify Mathematical Theorems In Public

10. Wüst, Karl; Gervais, Arthur – Do you need a Blockchain?

11. https://eprint.iacr.org

12. https://monero.org

13. https://www.ethereum.org

14. https://bitcoin.org

15. https://www.rsa.com/