International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 12 Issue 05 May 2024, Page no. – 4231-4237

Index Copernicus ICV: 57.55, Impact Factor: 8.316

DOI: 10.47191/ijmcr/v12i5.07

# In the Era of Blockchain Technologises as the Ultimate Solution for Bank Transfer Security

**Bernard KABUATILA Kabuatila[1], Dieudonné NGALAMULUME Lumbala[2]**

[1,2] University of Our Lady of Kasayi (U.KA), Kananga, DRC

[1] University President Joseph Kasavubu(UKV), Boma, DRC

**ARTICLE INFO**

**Published Online:**
**18 May 2024**

Corresponding Author:
**Bernard KABUATILA Kabuatila**

**ABSTRACT**

*Blockchain* technology is a distributed network on decentralized machines that allows transactions to be carried out and validated. The term *blockchain* has been used in various ways in the banking market for several years. By considering the architecture of the *blockchain* and the banking infrastructure, we can attest that the blockchain is a solution par excellence for securing banking transactions. In this study we will sketch the existing banking transaction security protocols, their vulnerabilities, then we will present the blockchain and finally go through a practical case of its mode of use.

**KEYWORDS:** blockchain, transaction, banking security, computer network.

## I. INTRODUCTION

According to a study by the global data and business intelligence platform ' *Statista'* , in 2023, the number of online shoppers is estimated at 2.64 billion , or 33.3% of the world population [1] . The process of dematerialization of exchanges and transactions between banks and client mobile applications is intensifying. The issues of securing and making document exchanges and flows more reliable are central. Blockchain provides strong answers by positioning itself as a single source of reliable information between BtoB partners .

Today there is marked confusion between Bitcoin and blockchain. The general public is gradually discovering this technology with great potential and its first applications, namely cryptocurrencies, but without fully understanding how it works and its consequences on the economy. Indeed, this revolutionary technology with disruptive potential became known to the general public in 2008 during the creation of the cryptocurrency Bitcoin and after the publication of a document entitled “Bitcoin: A Peer-to-Peer Electronic Cash System”. Blockchain, although complex to define, can be characterized as a distributed, decentralized and shared database that allows values or assets to be transferred and stored via the Internet. The strength of this technology comes mainly from a virtue allowing the removal of trust in an intermediary since the blockchain has a decentralized mode of governance and operates peer-to-peer. Blockchain is both a technology arousing interest and fear on the part of financial institutions, and more particularly banks which are experiencing a certain cumbersome operation due to strict regulation and a crisis of confidence on the part of economic agents as a consequence of the financial crisis of 2008. However, it is these elements of regulation and trust in a third party which initially proved the reliability and stability of these institutions. This situation of questioning of the banking sector has notably allowed the emergence of new players called “Fintechs”, some of which use this technology in their offer of financial services. However, the application of this technology is not only intended for the banking and financial sector, but also concerns the health sector, insurance, and the automobile sector.

## II. THEORETICAL SKETCH

### A. *Terminologies*

- *A bank :* A bank is a financial institution that provides banking services, including deposit, credit and payment. In short, it is a financial institution that accepts deposits and grants credits. By transforming deposits into credit, banks achieve the intermediation mechanism between surplus agents and deficit agents. In the broad sense, the term bank includes commercial banks, mutual or cooperative banks, savings banks and limited financing companies.

- *A* ***Bank transfer*** means the transfer of a sum of money from one bank account to another bank account. These accounts can be domiciled either in the same banking establishment, or in two very distinct banks [ 2] .

  ***Types of transfers***

  - *Occasional domestic transfer: is an order that allows a one-time transfer of funds from one originator account to another. It is free when the accounts of the issuer and the beneficiary are in the same banking establishment, but often chargeable when the beneficiary has his account in a competing establishment;*
  - *Permanent transfer: allows you to automatically transfer a specific sum on a fixed date (generally monthly) from an originator's account to a beneficiary; often used to fund savings accounts or pay monthly rent, for example;*
  - *International transfer: as part of the new SEPA standard (Single Euro Payments Area), the customer can now transfer their assets to any country in the SEPA zone with the same security using the same standards.*

***Role of the bank in the transfer process***

*Agent in the operation, the bank acts "on order". The bank must have the instructions in writing and have precise references of the recipient of the funds to avoid any risk of error. The bank must act diligently: transfers must be processed immediately, as a delay could be detrimental to the issuer and/or beneficiary. The bank has a duty to report and therefore to inform its client of the proper execution of its instructions.*

- *The bank account* : is an accounting instrument on which all transactions carried out between the bank and its client are recorded . The bank records, in a column entitled **credit** , all the sums that its client remits to it or that it receives from other people on behalf of its client. She enters, in another column called **debit,** all the sums that she withdraws from her client's account either to pay to him or to remit them to a third party designated by this client. There are different types of bank account, the main ones are: term account, blocked account, collective account, current account, suspense account, deposit account, savings account [ 3] .

### ***B.*** *Security threats linked to banking transactions*

As we highlighted above, this study is intended to be research into the means of security of banking data exchanged in transactions; therefore before presenting the protocols which secure the exchange between clients, it is preferable to list some risks linked to the electronic exchange of banking data. Among which we can cite:

- *Phishing*

Phishing is an attempted online scam which consists of posing as an official organization, often known (such as a bank, the caf, etc.), in an attempt to recover sensitive personal data, such as login credentials or credit card details. These attempts take the form of emails with a generally alarmist tone.

- *Identity theft*

Identity theft occurs when someone illegally obtains and uses your personal information to commit fraud. This often takes the form of unauthorized financial transactions.

- *Insecure websites*

Transactions on unsecured websites are vulnerable to interception by cybercriminals. These sites generally do not use HTTPS encryption, making sensitive data like your banking details easily accessible.

- *Malware and viruses*

Malware and viruses can infect your device, allowing cybercriminals to access personal information and financial details stored on your device.

- *Credit card fraud*

Credit card fraud involves the unauthorized use of your credit card information to make purchases or withdraw funds [ 4] .

### ***C.*** *Secure banking communication protocols*

To constrain the different threats that we have just presented in the form of a non-exhaustive list in the previous section, banks use several protocols which ensure the security of data between two communicating entities, among these protocols we can cite:

- EBICS (Electronic Banking Internet Communication Standard) is a protocol allowing secure communication between banks and their customers. Secure banking exchange protocols have emerged in particular to overcome the risk linked to the exchange of banking data on networks while maintaining the ability to exchange large volumes of information. The objective is therefore to facilitate exchanges between banks and businesses in a secure and standardized framework.
- Indeed, excluding Internet banking (webbanking), the formalized exchange of banking data can also be done via: the SWIFT protocol, an FTP with an sFTP (Secure Shell File Transfer Protocol) type protocol or FTPs (File Transfer Protocol Secure).

For these purposes, SWIFT is aimed at international companies with numerous banking partners around the world. Via the private network SWIFTnet, SWIFT is the global standard for secure communication of banking information. However, there is a charge for access. Unless we increase the number of international banking partners, it is therefore preferable to move towards the EBICS protocol, the operation of which allows same level of security [ 5].

### *D. EBICS reliable in terms of security*

Due to the encryption of the files exchanged, the EBICS protocol is a particularly reliable means of banking communication. Indeed, file encryption makes any form of deliberate alteration or reading of files by unauthorized third parties impossible. So to speak, **only human error could compromise the security of banking transactions.** Among them, two major risks may weigh on the company despite the adoption of the EBICS protocol:

- Obtaining certificates by third parties;
- Fraudulent payment orders from a legitimate payer.

The encryption key guarantees the unalterability of files sent to the bank. Once a crook has the key, they could access the sent files provided they successfully intercept the packets.

### *E. Limitations of banking communication protocols*

That being said, human error still remains very prevalent. Adopting the EBICS protocol does not protect the company against most transfer fraud. Increasing every year, scammers see more opportunity in the delegation of banking powers than in the interception of bank files.

Whether through fake supplier scams, CEO fraud or phishing methods, the company runs a real risk by relying solely on having secure protocols in place to protect against fraud.

In parallel with the EBICS protocol, it therefore appears essential to **raise awareness among all company stakeholders** of the different types of payment fraud. Beyond raising awareness, **the company can equip itself with additional tools** to clean up its supplier repository in order to ensure that the bank details always correspond to the identity of the beneficiaries of transfer orders. For these purposes, the blockchain solution becomes a solution par excellence for ensuring the security of transactions with an emphasis on non-repudiation since the addition of the block is only done by users who have been previously authorized and known in the business. This solution thus strengthens third-party control processes to thwart transfer fraud and allows companies to secure all transactions [ 6] .

## III. BLOCKCHAIN

Starting from the limits noted on the communication ensured by the protocols that we have listed above, we present in this part the solution that we consider excellent for the moment even if in the field of NICT there is not absolute security:

### *A. Definition*

“Blockchain is a technology developed since 2008, specialized in the storage and transmission of information. Each blockchain corresponds to a register, a large database that can be shared with all of its users. Each user has access to this data, and can enter new information, according to the rules set by a very secure computer protocol.

The information is stored in the blockchain without any intermediary. Each modification made by a user is therefore visible to all users in real time. This ensures a single, reliable source of data. »

### *B. How does blockchain work?*

“The blockchain is a distributed database, which will keep the history of transactions between users since its creation. Each computer hosts a copy of the database. Each user has a cryptographic key that identifies them on the network, so we can know who entered each new piece of information.

When a transaction is made, it will be transmitted throughout the network until it reaches the computer of a validator participant called a “miner”. This will check whether the transaction is valid or not. If so, it is included (along with other pending transactions) in the database in the form of a data block (this is the “block” in “blockchain”). Once a block is added in the blockchain, it means that the transaction is irrevocable and tamper-proof [ 7] .

Unlike a “classic” transaction, the data does not circulate through a trusted third party, such as an institution or a bank, but via a peer-to-peer network. »

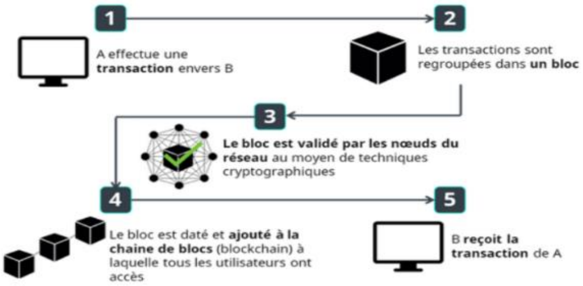
1
A effectue une transaction envers B
2
Les transactions sont regroupées dans un bloc
3
Le bloc est validé par les nœuds du réseau au moyen de techniques cryptographiques
4
Le bloc est daté et ajouté à la chaine de blocs (blockchain) à laquelle tous les utilisateurs ont accès
5
B reçoit la transaction de A

**Figure 1. blockchain shemat**

- *Blockchain*

The blockchain operates on cryptoassets. That is to say from a currency, or token called “token” which ultimately corresponds to an underlying asset. The first module thus corresponds to a chain of computer blocks, which we will compare to a notebook having a beginning but no end, because we can write on it permanently. One particularity is essential: that of the impossibility of modifying the order of the pages of this notebook.

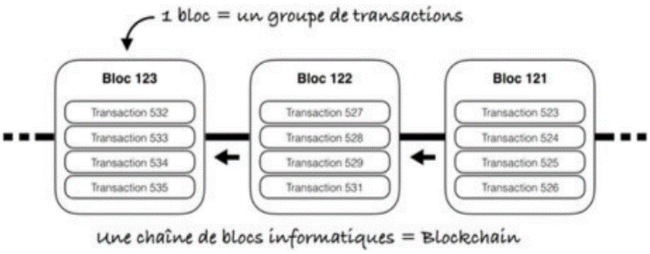

**Figure 2. The blockchain**

The blockchain works in the same way with non-modifiable blocks which correspond to one or more transactions, and linked together by cryptographic hashes. That is to say that each added block has a specific code, called “hash”, which depends on the previous ones. Furthermore, when a data modification occurs, the hash of the block will be modified. These are in fact users or computers called “miners”, who, via the mining process, have the role of validating a transaction. Mining consists of a validation process which takes place in a form of competition between miners, called “Proof of Work” (or “proof of work” in French), and consists of obtaining a hash. Miners who pass this cryptographic test by validating a block are rewarded with new Bitcoins, the emission of which is halved every four years to maintain its aspect of scarcity. In addition to issuing new Bitcoins, miners charge transaction fees on each block. You should know that a block is found every ten minutes, and that the difficulty of solving the mathematical calculation increases every 2,016 blocks, that is to say every two weeks. So, as you will have understood, the level of security of a blockchain using Proof-of-Work depends on the computing power.

### *C. How a blockchain transaction works*

The essential steps of a transaction:

- **A person requests a transaction.** This may relate to cryptocurrencies, contracts, records or other information.
- **The transaction is broadcast to all peer-to-peer (P2P) participating computers in the specific blockchain network.** These computers are called nodes. All transactions are posted to the buffer or “mempool,” where they are considered “pending.” Gas fees are paid by users as part of the transaction to compensate for the computational energy required to process and validate transactions on the blockchain.
- **Miners verify the transaction.** Each computer in the network verifies the transaction against certain validation rules defined by the creators of the specific blockchain network.
- **Validated transactions are stored in a block** and are sealed with a key called Hash.
- **A new block is added to the existing blockchain.** This block becomes part of the blockchain when other computers on the network check whether the key on the block is correct.
- **The transaction is complete.** Now the transaction is part of the blockchain and cannot be modified in any way.

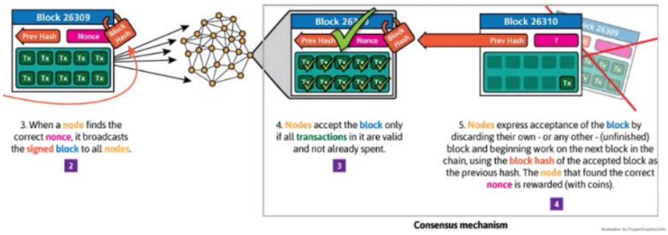
Block 26309
Prev Hash
Nonce
Block Hash
Tx
3. When a node finds the correct nonce, it broadcasts the signed block to all nodes.
2
Block 26309
Prev Hash
Nonce
Block Hash
Tx
4. Nodes accept the block only if all transactions in it are valid and not already spent.
3
Block 26310
Prev Hash
?
Tx
Block 26309
5. Nodes express acceptance of the block by discarding their own - or any other - (unfinished) block and beginning work on the next block in the chain, using the block hash of the accepted block as the previous hash. The node that found the correct nonce is rewarded (with coins).
4
Consensus mechanism

**Figure 3. How a blockchain transaction works**

### *D. Validation of transactions*

There are mainly **two methods to validate transactions: proof of work (PoW) and proof of stake (PoS).** PoW involves solving a mathematical equation, with miners being rewarded for being the first to solve the equation. PoS, on the other hand, involves holders locking up funds (staking) in a smart contract and an algorithm selecting a holder to post the next block.

### *E. What is the impact of blockchain on the banking sector?*

“Blockchain is shaking up the codes of the banking sector and revolutionizing the way we exchange and protect exchanges. It ensures data security during transactions and payments between different users. » confirms Anne-Sophie Luçon, Practice Manager at Michael Page. Blockchain has notably been adopted by banks to secure remote payments or stock trading, and to avoid hacking. It redistributes the cards by proposing a decentralized system, where authority is reassigned to the different users of the network. This multiplication of data allows the systems to be described as virtually inviolable. “It is still difficult today to identify recruitment prospects linked to blockchain. Nevertheless, its impact on the very structure of banks is undeniable. » underlines Anne-Sophie Luçon. Indeed, the various players in the banking sector have gradually joined the R3 consortium, launched by the start-up R3-CEV, to think together about new banking requirements in terms of security, reliability, performance, scalability and control. linked to blockchain. The objective? “Establish the foundations and standards for a blockchain shared between banking establishments in order to enable the development of new financial services and a new form of interbank compensation.” In short, the bank of tomorrow [ 8] .

### ***F.*** *How banks can benefit from Blockchain?*

Blockchain, used for the first time by the cryptocurrency Bitcoin, is characterized by a **“distributed” data structure** . This means that each recorded data exists simultaneously on different computers on the network. This system is deemed to be inviolable and more secure than the traditional databases currently used by banks. In addition, thanks to its peer-to-peer architecture, Blockchain allows transactions to be carried out directly between two parties. We could therefore simply do without banks, while remaining calm about security.

Ironically, it is precisely in its high level of security that banks see the greatest benefit of Blockchain. **The transparency and immutability of data** would allow these institutions to give their customers a guarantee of trust. Indeed, fraud would be practically impossible because the data recorded on the Blockchain cannot be modified.

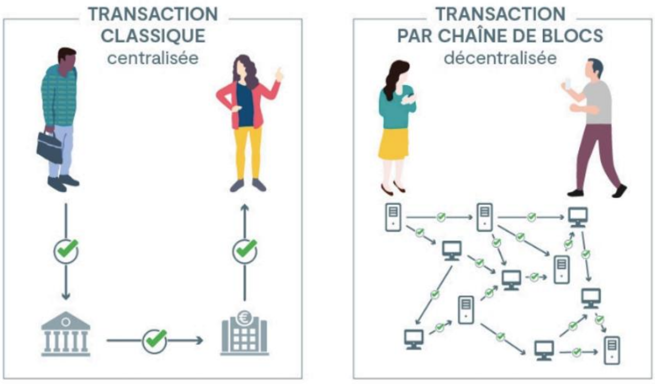

**Figure 4. The blockchain**

In addition, **transactions could be made automatically and without fees**. Finally, Blockchain brings banks what they have always been looking for: efficiency and productivity gains at lower cost!

The blockchain also constitutes an interesting solution for **generating contracts between the bank and the customer** . This is a whole new concept called “smart contracts”. The latter have the ability to perform an action automatically based on the conditions previously defined in the contract.

In addition, researchers are already thinking about building an international currency system, a kind of **global central bank** based on Blockchain. This project presents an undeniable advantage for consumers: we would no longer pay fees for making international transfers. National financial circuits would no longer have as much importance in our daily lives .

### *G. Types of Blockchain*

Now let's talk about the types of blockchains and their security aspects:

1. **Public Blockchains**

   As its name suggests, the public blockchain is open to everyone. As a result, anyone can join and transact on this network without any permission.

   This open variant allows each user to store a copy of the transaction data. This blockchain is therefore entirely transparent to the public.

   Additionally, this transparency creates trust among community members. In addition, this blockchain does not depend on any intermediary for its operation.

   The openness and wide accessibility feature of the public blockchain makes it more secure than other blockchains. For this reason, it is difficult to modify the blockchain with challenges such as the 51% attack.

2. **Private Blockchains**

   Private blockchains operate within a closed network with limited participants. Additionally, this blockchain is managed and controlled by a single entity.

   The smallest number of users allows this blockchain to operate quickly. Additionally, to join a network, users must obtain permission or invitation from higher authorities who operate the blockchain.

   Reliance on a single person or organization weakens the security of private.ate blockchains. It is therefore relatively easy for hackers to attack such blockchain networks.

3. **Hybrid Blockchains**

   Hybrid blockchain involves the combination of twoate and public blockchains. In addition, this blockchain is customizable according to the interest of its central authority.

   This network can regularly change the rules depending on circumstances. Additionally, this blockchain does not disclose transaction data outside its closed perimeter ecosystem.

   Hybrid blockchains use private nodes that provide greater network security and privacy. Additionally, the private nature of this blockchain restricts the network against potential 51% attacks [ 9] .

### *H. Scenario for using blockchain in a banking transaction*

A blockchain is essentially a huge database that is completely transparent to access. It is a digital ledger where every transaction is recorded and distributed across an entire network. Every time a transaction is made, it is added to a block. This block is then recorded using an immutable cryptographic signature. If A gave B $5, the transaction would be recorded in both of their ledgers, as well as in the records of C, D, E, and each ledger user.

As each person has access to the same ledger, a block cannot be easily changed, as a change requires the consensus of each user.

If one block said $4 instead of $5, it would be easy to check the millions of other blocks to see which one is fake. If a hacker wanted to corrupt the system, they would be forced to modify every block on the chain, in every version distributed to users – a hack so costly that the reward would seem unworthy of the risk. Thus, the system is both very transparent and very secure.

Let's take the example of a transaction between Bernard and Dieudonné . Suppose Bernard wants to send bitcoins to **Dieudonné .** Here are the steps they must follow to complete a transaction:

1. **Addresses and keys** : Both Bernard and Dieudonné have a key pair (public and private) and an associated public *Bitcoin address* . The *Bitcoin* public address is an encoded version of the public

key and is used to receive bitcoins. The private key is kept secret and is used to authorize transactions.

2. **Creation of the transaction** : Bernard creates a transaction in which she indicates Dieudonné's address and the amount in bitcoins she wishes to send him. It also adds a small amount (transaction fee) to encourage miners to validate and include this transaction in a block.
3. **Signature of the transaction** : Bernard digitally signs the transaction with his private key. This signature guarantees that the transaction really came from Bernard and that she authorized the transfer of the bitcoins to Dieudonné.
4. **Broadcast of the transaction** : The signed transaction is broadcast on the Bitcoin network. The network nodes (computers participating in the validation of transactions) verify the validity of the transaction and Bernard's signature.
5. **Transaction confirmation** : Miners select unconfirmed transactions and attempt to solve a cryptographic problem to create a new block containing these transactions. Once the problem is resolved, the block is added to the blockchain, which confirms the transaction from Bernard to Dieudonné.
6. **Receipt of bitcoins** : After several confirmations (usually 2 to 6 confirmations are considered sufficient), Bob can consider the bitcoins as received and spendable. One confirmation = 1 block, 6 confirmations = 6 blocks or approximately 60 minutes in the case of a transaction on the Bitcoin network [ 10] .

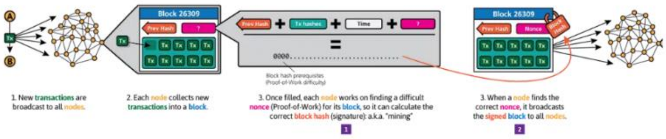
A
Tx
B
Block 26309
Prev Hash
?
Tx
Prev Hash
Tx hashes
Time
?
=
0000.............................
Block hash prerequisites (Proof-of-Work difficulty)
Block 26309
Prev Hash
Nonce
Block Hash
1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Once filled, each node works on finding a difficult nonce (Proof-of-Work) for its block, so it can calculate the correct block hash (signature): a.k.a. "mining"
1
3. When a node finds the correct nonce, it broadcasts the signed block to all nodes.
2

**Figure 5. The blockchain transaction**

The transaction between Alice and Bob is now complete. Alice successfully transferred bitcoins to Bob, and the transaction is permanently recorded on the blockchain. **The network updates its ledger file to reflect changes in account balances.**

## IV. CONCLUSION

Blockchain still has a long way to go before it can truly change the world of finance. Although there is no shortage of financial resources to finance research and infrastructure, the market does not yet have enough experts capable of implementing the new system and carrying out all the projects.

It should also be mentioned that digital currencies are generally exchanged for national currencies. **The high volatility of their prices** scares investors. Fearing falling victim to a sudden devaluation, the latter always prefer euros, dollars or francs, less "fashionable" but more stable.

Finally, it is often said that hackers always find ways to hack even the most sophisticated security systems...

Some experts believe that Blockchain will not survive in the face of so much uncertainty. However, we will not forget that years ago voices were raised to say that the Internet was only a passing fad. And look where we are now! Blockchain has potential, but it remains to be seen what we will do with it. After all, the success of each technology depends not only on its capabilities, but also on everyone involved in its development and its potential users.

It is with this in mind that we carried out this study which had three missions, namely: the presentation of the protocols used in banking transactions and their limits, then we presented blockchain technology to end with a transaction scenario using blockchain.

## REFERENCES

1. https://www.statista.com/outlook/emo/ecommerce/worldwide
2. T. Duclos, Dictionary of banking, 6é Ed. Sefi, Paris, 2013, P80-85.
3. JM Rochi, From online banks to Neobanks, Afranel Edition, Paris, 2020, p19-20.
4. B. Roman and A. Tshibozo, Transforming banking: banking strategy in the digital age, 1st Ed. Dunod, Paris, 2017; p41-45.
5. https://www.neofi-solutions.com/protocoles-interbancaires
6. https://www.cairn.info/revue-d-economie-financiere-2018-1-page-67.htm
7. The Boston Consulting Group, Blockchain White Paper, Medef, Paris, 2016, p25-27. https://bitcoin.fr/blockchain/, https://www.mutualite.fr/actualites/blockchain-mode-demploi/
8. https://coinacademy.fr/academie/transaction-blockchain/
9. Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.
10. Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.
11. Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.
12. Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullende
13. Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

14. Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
15. Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.