Chapter 3 - Technologies underpinning Accounting Information Systems

Gerhard Kristandl

Abstract

For AIS to become the enabling and empowering tools they are expected to be, they require the technological infrastructure or 'underpinnings' that facilitate their smooth operation. Inadequate technologies underpinning AIS can burden the company with extra maintenance and data recovery costs, and issues with data reliability, security and privacy. Thus, inadequate technology can potentially corrupt the very outcomes of an AIS, namely reports and decision-relevant information, leading to incorrect, unreliable decisions. In this chapter, the general relationship between AIS and technology is detailed. Networks are revealed as a necessary technological feature of AIS, and components that are aligned to build and run an AIS are discussed, namely hardware and software. Networks, hardware and software have to work together to provide a reliable basis for any AIS to perform and provide reports and decision-relevant information. Finally, the focus is moved to the emerging technologies of blockchain, the Internet-of-Things and artificial intelligence that have started to heavily impact AIS in recent years.

Introduction

It is now widely accepted that Information Technology (IT) has been, and still is, a major driver for accounting to become a knowledge service profession (Granlund, 2011). Accounting Information Systems (AIS) have grown into complex decision-support systems whilst increasing the speed and accuracy of more traditional accounting tasks (Gelinas et al., 2018). IT impacts the quality of the AIS (measured in terms of scope, timeliness, aggregation, reliability, flexibility and usefulness), which in turn impacts the quality of accounting information (Wisna, 2013). To become the enabling and empowering tools AIS are expected to be, they require the technological infrastructure or 'underpinnings' that facilitate their smooth operation (Ghasemi et al., 2011; Wisna, 2013; Gelinas et al., 2018). Inadequate technologies underpinning AIS can burden the company with extra maintenance and data recovery costs, and issues with data reliability, security and privacy. Thus, inadequate technology can potentially corrupt the very outcomes of an AIS, namely reports and decision-relevant information (Ghasemi et al., 2011), leading to incorrect, unreliable decisions.

In the remainder of this chapter, the general relationship between AIS and technology is detailed. Further, networks are revealed as a necessary technological feature of AIS. Then, the components that are aligned to build and run an AIS are discussed, namely hardware and software. Networks, hardware and software have to work together to provide a reliable basis for any AIS to perform and provide reports and decision-relevant information. Finally, the focus is moved to the emerging technologies of blockchain, the Internet-of-Things and artificial intelligence that have started to heavily impact AIS in recent years. Later chapters may home in on some of the topics covered here in greater detail.

Accounting information systems and technology

Accounting has experienced many improvements due to the computerisation of accounting processes (Ghasemi et al., 2011). Traditional paper-based ledgers and book-keeping processes have been automatized and mirrored in AIS, which eventually morphed into full decision-making systems (O'Donnell & David, 2000). An AIS in this context is a cohesive organisational structure (Boczko, 2007); a set of processes, functions, interrelated activities, documents and technologies (Hurt, 2016) that captures, processes, outputs and stores data, and as such provides information for decision-making and control purposes to internal (Quinn and Kristandl, 2014) and external parties (Hurt, 2016). Historically speaking, an AIS was a specialized subsystem of Management Information Systems (MIS), and thus integrated with other information systems in firms. With the rise of material resource planning (MRP) and subsequently enterprise resource planning (ERP) systems, AIS have become even more integrated with other information systems (Gelinas et al., 2018). This has an important implication for the view taken in this chapter – the technologies that enable AIS to run are the same for other types of information systems. They share the same network technologies, hardware, software and other components that make up the technological basis for them to be efficiently and effectively operated. This view is in line with Gelinas et al. (2018, p.14) who

explain that the distinctions between separate information systems have become somewhat blurred, and a clear differentiation between IS and AIS has been given up today.

As discussed in more detail in other chapters of this handbook, an AIS fulfils not only a decision-oriented, but also a controlling function. The cohesiveness of the AIS structure is achieved through prudent, integrated system design and the interactions of the human actors along a network of computerized resources that capture, process and deliver the required information (Boczko, 2007; Ghasemi et al., 2011; Gelinas et al., 2018). These resources can be determined as a collection of computer hardware and software, connected to one another within a network (Ghasemi et al., 2011; Quinn & Kristandl, 2014), and need to be implemented and maintained to support business processes (Gelinas et al., 2018). Although non-computerized AIS exist (Quinn & Kristandl, 2014), modern businesses that employ such a system can rarely do so without the use of computers. In very simple terms, to capture – ideally – *all* relevant, transaction-based information for accounting purposes in an organisation, the resources need to be linked to one another to input information, send the information to the right addressee (another computer or person) for processing, and finally onwards to the party that requires the processed data for decision-making, reporting, or control (including audit).

Networks

As of the time of writing, almost every business is connected to and uses networks, particularly the Internet. As of 2019, 91% of enterprises in the EU with at least 10 persons employed had used a fixed broadband connection (Eurostat, 2020). Mobile technologies such as mobile payment systems and capturing document data (e.g., via a scan of invoices) and the Internet-of-Things (IoT) have a major impact on AIS and the opportunities to collect and report data in real time (Trigo et al., 2014; Brandas et al., 2015; Romney et al., 2021). This illustrates the importance and – to some extent – implicitness of networks in today's corporate environment. The interconnectedness between devices determines the infrastructure that forms the backbone of any AIS today (Romney et al., 2021).

The technological view on networks is that of a so-called 'hard network' (as opposed to social soft-type, or the logical, more abstract semi-soft type; see Boczko, 2007). A hard network is the physical representation of a group of devices (e.g., computers and servers) connected to one another via a network interface card (NIC) and wired/wireless links, managed by software allowing data exchange (Hall, 2019). Wired connections (e.g., copper wire, twisted pair, coaxial, fibre optic) connect the various computers in a permanent manner, typically via point-to-point links (Tanenbaum & Wetherall, 2021). Wired connections, once set up, are difficult to reconfigure. Physical links provide the infrastructure to enable networking; this includes computer-to-computer, computer-to-server, server-to-server, or computer-to-periphery (e.g., shared network printers; Quinn & Kristandl, 2014) connections. Wireless networks connect via broadcast links, such as high-frequency radio signals, infrared, electromagnetic signals, or laser for short-distance networks; or mobile telephony, microwaves, or satellite for long-distance networks (Boczko, 2007; Richardson et al., 2014; Tanenbaum & Wetherall, 2021). Wireless networks provide the advantages of mobility, rapid deployment, flexibility and scalability, low-cost setup and easy maintenance (Boczko, 2007; Richardson et al., 2014). However, they can

be limited by the distance to the access point, as well as the number of wireless devices using the existing bandwidth at the same time. Wireless network access typically requires access to a wired intranet or internet, linked via a wireless network card (WNIC).

Regardless of their physical connections, all types of networks can be described using the following three attributes (Boczko, 2007):

- Architecture
- Topology
- Protocols

Architecture

The architecture describes the technological and geographical layout and configuration of a network and includes the definition of intra-network and inter-network relationships, the physical configuration, the functional organisation, the operational procedures employed, the data used and the scale of the network (Boczko, 2007; Magal & Word, 2012; Tanenbaum & Wetherall, 2021).

Network architecture can either be described in system or hardware terms. A typical example of the former is a client-server model (C-S) that aims to interconnect and distribute software and hardware efficiently and effectively across a network (Boczko, 2007). Here, a 'client' is a computer or workstation that requests services (programs, applications, data processing), from a 'server', a computer that manages and allocates these services (Curtis & Cobham, 2005; Hall, 2019). The C-S model is an example of a multi-tier architecture (see Figure 3.1), where presentation, data/application processing and data storage/management are separated into different layers (see Chapter 4 - Developing Information Systems for the Contemporary Accounting Profession: Challenges and Recommendations). Information systems such as SAP ERP are based on a C-S architecture, with only the graphical user interface (GUI) running at the user end. The C-S model is widely used in online commerce and forms the underlying idea behind cloud computing with the main difference that the data is stored on a server that is owned by a cloud provider instead of the company, accessed via the Internet (Lin & Chen, 2012; Zissis & Lekkas, 2012).

INSERT FIGURE 3.1 NEAR HERE

Figure 3.1: Client-Server Architecture

An evolution of the standard C-S architecture is Service-Oriented Architecture (SOA), based on the concept of designing and developing inter-operable functions and applications (services) that are reusable without needing to change the underlying application (Magal & Word, 2012; Hall, 2019). Hardware architecture on the other hand supports the distribution of software, data, and processes. Typical examples are LANs, WANs and VPNs.

A LAN (Local Area Network; see Figure 3.2) is a network within geographically close confines, often within the same room or building, privately owned by a single organisation (Quinn & Kristandl, 2014; Tanenbaum & Wetherall, 2021). Within this type of network, computers (*nodes*), servers and peripheral devices, such as printers, are connected either wired or wirelessly (WLAN) (Richardson et al., 2014). Hubs and switches (see Hardware later) interconnect the devices and send packets (formatted, small units of data; Richardson et al., 2014) over the network. LANs allow use of a common network operating system, centralisation of shared data and programs from a central server, as well as their downloading for local processing, communication of personal computers with outside networks (e.g., the Internet), sharing of scarce resources, email, as well as access to and use of a centralized calendar and diary (Curtis & Cobham, 2005). Sharing resources over a network is cost-efficient since there is less need for large-storage hard disks or programs for every computer within the network. Computers may act as both clients and servers in smaller LANs– such a network is then called a peer-to-peer network (Boczko, 2007) due to the equivalent responsibilities that each workstation fulfils. In larger LANs, workstations act as clients only, and are then linked to a server.

INSERT FIGURE 3.2 NEAR HERE

Figure 3.2: Local Area Network

A WAN (Wide Area Network; see Figure 3.3) is a network over a larger geographical area (e.g., a country), connected via public (e.g., phone lines) or private (e.g., leased lines or satellite) communication facilities (Shinder, 2001; Hall, 2019). WANs provide remote access to employees or customers, link two or more separate LANs at sites within a company, and provide the business with access to the Internet (Richardson et al., 2014).

INSERT FIGURE 3.3 NEAR HERE

Figure 3.3: Wide Area Network

Depending on the location of a central hub, there are two types of WAN, namely centralized and distributed. In a centralized WAN, all major functions (e.g., accounting, procurement, sales order processing) are carried out at the central hub. The computers in the network do not process transactions locally but send data processing requests remotely to the central hub (Curtis & Cobham, 2005; Boczko, 2007). All data traffic can be closely monitored, but it puts a heavy burden on the network itself. The central hub needs to queue and prioritize all concurrent requests, rendering the network much more vulnerable to a complete standstill. A distributed WAN, on the other hand, is decentralized in terms of data processing (Curtis & Cobham, 2005; Boczko, 2007), and thus better able to transmit and process individual transactions simultaneously. In a distributed environment, LANs are connected to one another, and/or to larger WANs, via bridges (linking same-type LANs) or gateways (linking different-type LANs; Hall, 2019). The largest distributed WAN to date is the Internet, and the World

Wide Web is a WAN that uses a client/(web) server architecture to transmit data and process tasks (Shinder, 2001).

Variations of WANs are MANs (Metropolitan Area Networks) and CANs (Campus Area Networks) that can be quite large but are confined within a city or campus (Shinder, 2001; Tanenbaum & Wetherall, 2021). A VPN (Virtual Private Network) is created using a secure tunnel between a corporate WAN and (home) offices via virtual links over the Internet rather than leased lines (Richardson et al., 2014; Tanenbaum & Wetherall, 2021). VPNs came to prominence due to the larger bandwidth availability, enabling remote access to corporate WANs from outside the business premises for salespersons, home offices and business partners that require access. Companies that use cloud technology for their networks are particularly in need of secure access points, which a VPN provides. Since they use the Internet, this network type provides a low-cost connection, but suffers a lower Quality-of-Service (QoS) than corporate WANs (Richardson et al., 2014).

Topology

The term *topology* denotes the physical or logical arrangement of network devices (Boczko, 2007). Figure 3.4 shows the most common topologies utilized in networks.

INSERT FIGURE 3.4 NEAR HERE

Figure 3.4: Network topologies

A bus topology is a linear topology where clients share a central line connection (Boczko, 2007; Hall, 2019), either linear or in a daisy chain (see Figure 3.4 a and b). When data is sent along the network, it contains a unique network address for the desired destination and will thus be delivered to the correct network resource. Although a bus topology is easy to set up and extend, the connected devices are competing for connection resources, as only one line is available to them (Hall, 2019). In cases where two or more clients want to use the network at the same time, this might lead to queuing and slow operation of the network – a situation that is exacerbated by every additional node added to the bus. Thus, this topology is limited in size, as it may become difficult to operate and manage (Boczko, 2007).

In a ring topology, each node is connected to two other nodes, and represents a peer-to-peer arrangement (see Figure 3.4 c). As opposed to a bus topology in a daisy-chain configuration, a ring topology creates a closed loop of nodes, meaning that if a signal is sent along the network, and no destination node accepts it, it returns to the sending node (Boczko, 2007; Hall, 2019). Each node has equal status, but only one node can communicate at a time. Unlike a bus topology, the nodes along a ring topology move the signal along rather than ignore it. This improves network speed; the scalability of the network is also superior to a bus topology, as additional nodes do not significantly impact network speeds. It requires more connections however than a bus network, is more costly to implement, and if one single node fails, it will impact the entire network. Both ring and bus typologies have become side-lined in favour of

the more stable star typology (see below; Quinn & Kristandl, 2014). A mesh topology (see Figure 3.4 d) is a variation of the bus topology, where every node is connected to every other node (Boczko, 2007). Although providing a more stable and reliable network for small networks, its complexity increases considerably when the network grows. This can render network management and reconfiguration difficult and costly (Boczko, 2007). Mesh topologies are often used in WANs to connect several LANs to one another.

In a star topology (see Figure 3.4 e), all devices are linked to a central computer which acts as a transmission device (Boczko, 2007; Hall, 2019). In this case, signals are transmitted via the central hub rather than along the entire network. It is relatively easy to implement, extend and monitor, and if a device fails, it rarely impacts the entire network, unless the central hub fails (Quinn & Kristandl, 2014). Other disadvantages are higher costs (maintenance, security) and higher risk of virus infection via the central hub (Boczko, 2007). This topology is often used in both centralized and distributed WANs where the central hub is a mainframe (Hall, 2019).

The topologies above can be combined based on business needs. Examples of such hybrid topologies are star-bus or star-ring topologies (Boczko, 2007) that combine the advantages and eliminate topology-individual drawbacks. Figure 3.4 f shows an example of a star-bus topology that is easier to extend and more resilient than a pure bus topology.

Protocols

Without instructions to manage the communication and flow of data between the devices, networks would merely be physical arrangements of computers and connections. A network requires protocols - formalized and uniform sets of rules and standards that govern the syntax, semantics and synchronisation of communications between nodes to enable them to communicate (Quinn & Kristandl, 2014; Hall, 2019). AIS need to comply with these standards - they define the formals rules of conduct and etiquette to avoid miscommunication and misinterpretation (Hall, 2019). Standardized reference models for network protocols such as the Open System Interconnection (OSI) standard or the more commonly used Transfer Control Protocol/Internet Protocol (TCP/IP) standard provide businesses with a framework to achieve this compliance (Tanenbaum & Wetherall, 2021).[1]

Hardware

Nodes and their periphery addressed when discussing network architectures, topologies and protocols can be summarized as ‘hardware’ in IT. The term comprises all physical devices used to capture, process and store data (Curtis & Cobham, 2005). This includes computers and their components (e.g., keyboards, disk drives, etc.) and servers, but also cloud-enabled devices such as tablets, smartphones (Quinn & Kristandl, 2014) or other smart devices (see ‘IoT’ later in this chapter). A computer is a workstation that provides a network-human interface; an access point to the AIS for both input and output of the required accounting data. The role of a server

[1] The details of OSI v TCP/IP are beyond the scope of this chapter. For a detailed discussion, please see Tanenbaum and Wetherall (2021).

(see also Architecture earlier) in a network is to process and manage the flow of information between the nodes and allocate processing resources to the task at hand.

Typically, a computer comprises (Curtis & Cobham, 2005):

- Input devices that accept, convert and transmit data
- A central processing unit (CPU) that executes program instructions, controls/coordinates data movement, carries out arithmetic and logical operations and stores programs and data
- A secondary storage that maintains a permanent record of data and programs beyond execution and for security
- Output devices that receive information from the CPU and convert it into the required format

These components can be detailed further, as illustrated by Curtis & Cobham (2005). Table 3.1 lists examples of hardware that are typically present in an individual computer. However, from an organisational perspective with elevated technological requirements (processing power and storage), it can be separated into individual devices connected via network links (Quinn & Kristandl, 2014). The connections between nodes and servers require communication devices (see below) that creates and manages these links, e.g., network cards, repeaters and hubs (Boczko, 2007; Richardson et al., 2014), either wired or wireless.

INSERT TABLE 3.1 NEAR HERE

Table 3.1: Examples of computer hardware (Adapted from Quinn & Kristandl, 2014, p.15)

Input devices accept data, convert them into a machine-readable form, and transmit them within a computer system (Curtis & Cobham, 2005). Keyboards are a typical input device, where information is entered into the system and converted into binary code whilst being displayed on a screen. However, keyboards are not the only way to enter data into a system. (see Table 3.1). Further, pointing devices such as a mouse is a commonplace feature in computers. Scanners, for instance, are widely used as input devices. They employ optical character recognition (OCR) or magnetic ink character recognition (MICR) to identify relevant data from a source document. OCR is commonly used by utility companies or government departments. Documents scanned using OCR typically come with specific instructions on how to fill in the data, such as writing in capital letters, black ink and within a confined box, to correctly identify the characters written (Curtis & Cobham, 2005). MICR is mostly used in processing cheques in banks, where the cheque number, account and sort codes are printed in magnetic ink. Barcode readers are another widespread type of input device, particularly in logistical processes to record the movement of goods. A good example of an industry that relies on data input that way is food retailing (e.g., supermarkets). Voice recognition via microphones is also widely used for data entry, for instance in call centres or customer service to screen and route calls. Today, voice inputs are often processed by artificial intelligence, embodied in smart assistants like Apple's Siri, Amazon's Alexa or Microsoft's Cortana. Finally, the IoT uses radio-frequency identification (RFID) tags and GPS to capture data (see discussion later in this chapter). Different input devices show differences in accuracy and cost. Keyboards, for instance, are by and large inexpensive input devices but are subject to human error (Curtis & Cobham, 2005). Also, data entry can be quite slow when keyboards are being used – this is different with scanners or barcode readers where data entry is quick and less prone to error but comes with the disadvantage that they are costlier when acquired and operated.

Processors enable a computing device to decode and execute program instructions, control and coordinate data movements, and perform arithmetic and logical operations (Curtis & Cobham 2005; Quinn & Kristandl, 2014). Examples of processor manufacturers are Intel (i5, i7, i9), AMD (Ryzen series), or Apple (M1 chip). Together with the main memory unit (random-access memory, RAM), used for storage of currently used data/programs, and the operating system, processors are the heart of the computing functions of hardware (Curtis & Cobham, 2005). The history of processors has shown an exponential increase in processing power, which in turn allows for quicker program execution and larger RAM for program-multitasking in computers today.

Storage devices serve to maintain the input, processed data and programs on a permanent basis (Curtis & Cobham, 2005), for immediate or later use or as backup for data in case of security

and integrity issues. Where the CPU only stores data whilst the computer is switched on, storage devices hold the data even if powered off. Different types of storage devices differ in speed of data retrieval, capacity, cost and robustness. Hard disks are a typical storage device in most computers systems. Types of hard disks are magnetic drives (hard drive disk, or HDD), optical disks (Blu-ray, DVD/CD), flash drives (solid state drive, or SSD), or cloud storage where the stored data is accessed via the Internet. The latter type experienced a rapid increase in usage, as it allows not only large, but also small and medium-sized companies to acquire and operate hitherto unaffordable AIS technology (Brandas et al., 2015). Older types of storage devices such as magnetic tapes or floppy disks still exist in some organisations (such as the US Nuclear Weapons Force see BBC, 2016), but nowadays do not feature in modern AIS technology.

Output devices are used to display information in the required format. Typical examples are computer monitors, tablet and smartphone screens, printers, and speakers (Curtis & Cobham, 2005; Quinn & Kristandl, 2014). Screens in general are the most common type. They are used with desktop computers, laptops, tablets, smartphones, machinery, vehicles – in fact, the IoT has had a major impact on screens added to the most unusual devices (Mazhelis et al., 2012). Printers are another output device that issue information by means of laser, ink or thermal printing technology (Curtis & Cobham, 2005). Larger type of printers are plotters, chain and drum printers, but these do not offer the quality and flexibility suitable for AIS. Finally, speakers - in conjunction with screens or as standalone devices - can output information to the user. Particularly when equipped with AI, smart speakers become both input and output devices that can interact with the user (Hart, 2018).

Communication/network devices are hardware that allow network resources to interconnect with one another. As discussed earlier, the actual connection between a node and network is either wired (cabling) or wireless (NIC). However, the cabling or connection alone is not enough – data that is transmitted along the network needs to find the right address. This is done by either hubs, switches or routers. Hubs merely transmit incoming data packets to all other connections, whilst switches and routers intelligently determine an outgoing line for incoming data, choosing the most efficient communication path through a network to the required destination, using the Internet Protocol (IP) addresses of sender and receiver (Richardson et al., 2014; Tanenbaum & Wetherall, 2021).

Networks that use hubs instead of switches are called non-switched networks, where communication links are shared by all devices (Curtis & Cobham, 2005). Typically, switched networks show a better performance than non-switched ones, as there are no data collisions, data can be transmitted simultaneously, and the capacity is used more efficiently (Tanenbaum & Wetherall, 2021). From a data security point of view, switched networks are also preferable, as data traffic is only sent to the address where it is required (Tanenbaum & Wetherall, 2021). They are also more efficient to monitor, as corporate firewalls are a security system comprising hardware like switches, routers, servers and software, to allow or deny a data packet that enters or exits a company LAN to continue on their transmission path (Richardson et al., 2014).

Software

Although hardware and networks are essential in enabling a smooth-running and purpose-driven AIS, without software it would not work. Software is the general term used to describe the instructions that control the operations of hardware (Curtis & Cobham, 2005; Quinn & Kristandl, 2014).[2] Software can either be categorized as operating systems (OS), database systems, or applications software, and requires the use of programming languages to design and create them.

Operating systems software

This type of software comprises programs that enable an efficient and smooth operation of the computer system (Curtis & Cobham 2005) and is considered the 'most important piece of software' (Richardson et al. 2014, p. 242). It is the basis for the hardware to work in the first place and provides the following four functions (Curtis & Cobham, 2005):

- Handling of data interchange between input/output devices and the CPU;
- Loading of data and programs into and out of the main memory;
- Allocating main memory to data and programs as needed (managing processes and memory, so that all programs receive a share of the available resources);
- Handling job scheduling, multiprogramming and multiprocessing.

Examples of OS available on the market are Microsoft Windows, Apple OS, Linux, Unix and Chrome OS for computers, as well as Android and iOS for mobile devices. Not all of these incur acquisition costs – Linux distributions like Ubuntu and openSUSE are free, whereas Windows may have a cost based on the licence model. All these OS provide a Graphical User Interface (GUI) as opposed to text-based interfaces that require the entry of command lines to work with the system – an example was MS-DOS which was eventually superseded by the more user-friendly Windows systems (which in turn had been inspired by Apple's OS in the 1980s).

Its crucial role in the smooth running of an AIS requires the OS to be secured against internal and external threats to its integrity. This includes intended or unintended security threats by users, computers, applications, the OS itself, as well as hacking or data leaks of sensitive information to external parties (Richardson et al., 2014). The OS requires clear IT governance policies (e.g., the COBIT5 framework) that control who can manage and access the system, system and network resources, and actions that are allowed by users. These security features are even more relevant in a cloud-computing environment, where several 'virtual' (rather than actual) OS share the same hardware, and could potentially become permeable, allowing access to resources between two instances of an OS running on the same platform.

[2] The term firmware also exists, indicating an inseparable combination of hardware and software, it being a set of instructions that is permanently encoded on a microchip.

Database systems software

In an integrated AIS, corporate accounting data is typically stored on a central database to ensure that all relevant applications access the same kind of information when processing data. As such, databases are another crucial component in an AIS, and require a database system that is able to record, manage and store a massive amount of day-to-day accounting data. A database system comprises two main software components, namely a data warehouse (a centralized collection of companywide data for a long period of time), and operational databases that draw data from the data warehouse (Richardson et al., 2014). Operational databases contain the data for current/recent fiscal years, updated whenever a transaction is processed. Periodically, data is uploaded from the operational databases to the data warehouse to provide decision-useful information to identify trends and patterns – the process of analysing them as such is called data mining, using Online Analytical Processing (OLAP).

Applications software

Applications software are programs that fulfil specific user functions (Quinn & Kristandl, 2014). In an accounting context, this may mean functions like sales ledger processing, budgeting, forecasting, or reporting (Curtis & Cobham, 2005). Most AIS are offered as application packages that include functional modules such as sales ledgers, accounts receivable/payable, payroll or credit and payment systems. These desktop accounting packages are offered and distributed by ERP software providers such as SAP or Oracle, or mid-level accounting package providers such as Sage or Xero, either as in-house or subscription-based cloud offerings.

If applications packages are unable to fulfil a specific business need, a company could develop it in-house or commission development. However, such specific software developments require lengthy analysis, design and testing phases (Curtis & Cobham, 2005). Commissioned software can become very costly as opposed to application packages; the cost of software development, testing and subsequent updates needs to be absorbed in full by the commissioning business (Curtis & Cobham, 2005). Further considerations stem from the frequent requirement to run the commissioned software on different types of hardware (portability), and the existence of professional documentation that enables adequate IT support. On the other hand, specially commissioned software provides a perfect fit to corporate requirements; this includes the elimination of redundant functions that may not be needed (but paid for), and the compatibility with other existing software (Curtis & Cobham, 2005). Whether a company is able to commission specially designed AIS software is mostly a question of affordability, which typically rules out smaller businesses. Interestingly, it appears that most companies prefer packaged software to self-developed or commissioned ones (Granlund, 2011).

To avoid compatibility issues, businesses often acquire entire software suites, where several programs are integrated and sold together. Suites provide inter-program compatibility in data exchange and user interface – good examples are Microsoft Office (e.g. Word, Excel, Access, Outlook) or the SAP Business Suite (containing ERP, Customer Relationship Management,

Supplier Relationship Management, Supply Chain Management, Product Lifecycle Management).

Programming languages

Software is written as a set of instructions to control computer operations. These instructions are written in a formal language to communicate them to the computer – a programming language. Table 3.2 briefly details the three main categories of programming languages and their characteristics (Curtis & Cobham, 2005):

INSERT TABLE 3.2 NEAR HERE

Table 3.2: Programming language categories

Machine-oriented programming languages have been mostly superseded by higher level ones due to their dependence on the source program and the computer architecture it is written on/for. Task-oriented languages that require compiling can be used repeatedly, are independent of the source program, and provide portability between computer systems and architectures, with a certain level of security against tampering with the compiled code (Curtis & Cobham, 2005). However, programs operate slower due to inefficiencies in the compiling process and the exclusion of the individual CPU structure. Object-oriented programming languages (OOPL) apply a different logic to task-oriented ones, in that they do not define complex operations, but rather the objects and their (changeable) attributes that take part in the operations. OOPLs offer a more natural way of reflecting the real world, objects that are reusable (saving programming time and complexity) and a simpler syntax (Curtis & Cobham, 2005). A good example for an OOPL used in AIS is ABAP Objects for SAP ERP software.

Emerging technologies impacting AIS

In the latter half of the 2010s, a range of disruptive technologies emerged that have already shown an impact on AIS. Blockchain, the IoT and Artificial Intelligence (AI) are chief amongst them (Sandner et al., 2020), all enabled by accelerated growth in computer technology and its processing power (Quinn & Kristandl, 2014). Within just a few years, these three emerging technologies have found purpose in a variety of business processes and functions, such as accounting and AIS. The remainder of this chapter offers a brief overview of blockchain, IoT and AI as well as their impact on AIS, as they are joining the technologies underpinning AIS.

Blockchain

After beginnings in digital time-stamping services in the 1990s, the concept of ‘blockchain’ was popularized in the late 2000s due to the rise of cryptocurrencies, most prominently Bitcoin

(Nakamoto, 2008). Whilst cryptocurrencies have experienced large-scale falls and rises since (Dutta, 2020), blockchain as a technology has emancipated itself from this single focus and found a wide range of additional and diverse uses such as supply-chain management, smart contracts, healthcare, property rights, voting or automated bank books (Wu et al., 2019; Sandner et al., 2020; Romney at al., 2021). Figure 3.5 shows the basic concept behind blockchain:

INSERT FIGURE 3.5 NEAR HERE

Figure 3.5: Blockchain concept (Adapted from Wu et al., 2019, p.3)

In brief, blockchain technology is a database of individual digital records (blocks), linked together in a 'chain'. Blockchain differs from 'traditional' databases in the way it stores data. Each block contains a random number (a 'nonce'), its own hash value (encrypted data on the block) and the hash value of the previous block (Wu et al., 2019; Dutta, 2020; Romney et al., 2021). Once a block is filled, it is chained to the previous block in chronological order. Rather than being stored in a single location, the blockchain is a decentralized database forming a distributed ledger of transactions across all nodes in a peer-to-peer network and made public to each stakeholder therein (Romney et al., 2021). It can store all kinds of transactional accounting data (e.g., bank transfers, sales records, purchases) which get exchanged between contracting parties without the need for intermediaries (such as banks; Romney et al., 2021). The entire peer-to-peer network acts as decentralized monitoring and control authority – a new block gets added only if all previous nodes agree (via a protocol) on its legitimacy and the validity of the data on it. Another key feature of blockchains is that they are immutable (Dutta, 2020), meaning that entries are irreversible and permanently recorded. Any tampering of data by a single entity would alter the hash values of the block header, highlighting the attempt to all other nodes, and increasing the likelihood of not just discovery, but also its origin (Wu et al., 2019).

This robustness of blockchain technology adds accuracy of transaction data and transparency of transaction details (Romney et al., 2021). The data is consistent (as there is only one database) and ensures a higher degree of privacy and security due to the underlying cryptography (Sandner et al., 2020). These advantages are beneficial to the operation and audit of AIS. Most importantly, blockchain technology increases the level of trust in the data/information, as nodes that want to join the blockchain must pass a 'proof of work' test before they can add a new block that is validated by consensus from the other nodes (Dutta, 2020; Romney et al., 2021). This 'proof of work' is basically a test of a new node's processing power. Adding a new block is designed to be difficult and costly (necessary processing power, hardware and electricity) to reduce the gains from fraudulent behaviour (Dutta, 2020). Notable examples for blockchains are Ethereum, Monero, Zcash and Dash.

Internet of Things

The term ‘Internet of Things’ (IoT) was initially coined by Kevin Ashton at the Massachusetts Institute of Technology (MIT) AutoID Labs in 1999 (Kranz, 2017; Ramakrishnan & Gaur, 2019). It describes the linking of sensors embedded in previously non-networked devices, such as vehicles, household and consumer appliances, wearables, medical equipment, even entire buildings, wired or wirelessly, to the Internet (Romney et al., 2021). Physical sensors (like RFID tags, GPS, QR codes or light sensors) ‘connect the unconnected’ (Hanes et al., 2017, p. 21) to create smart devices that collect data and information for transmission over the Internet to a server (Wu et al., 2019). Networked devices can capture, process and communicate data that can be transmitted to and used in AIS for planning, decision-making and control. At the same time, these devices can be remotely controlled across the network to improve efficiency, accuracy, automation as well as introducing applications that these devices – the ‘things’ – were previously not capable of (Hanes et al., 2017). The IoT connects people, processes, data, machines and other objects on a hitherto unknown scale.

Whilst 1999 marked the emergence of the term ‘IoT’, its application only started to take off in the latter half of the 2000s with technological advances in high-speed broadband and computational power (Hanes et al., 2017). Although an in-depth discussion of IoT as a multi-faceted ecosystem of physical devices, networks and protocols is outside the scope of this chapter, smart devices beyond the ubiquitous smartphone have entered private household and businesses on a broad scale. Smart speakers, smart lightbulbs, smart fridges or virtual assistants like Amazon’s Alexa or Microsoft’s Cortana have become widely used.

For AIS, the IoT means both opportunities and challenges. The increased amount of data captured can improve data analytics and decision-support systems in real-time, allowing e.g., auditors to test full populations instead of small samples or accountants to gain much more accurate data for cost estimates and decision-support (Romney et al., 2021). Whilst the introduction of a high number of sensors might introduce additional security challenges to the AIS itself (see below), it also facilitates new types of physical controls to monitor movement of staff and visitors across premises when embedded in wearables such as key cards, name tags, or wrist bands (Romney et al. 2021). When sensors are attached to raw materials and goods in various stages of completion, their movements and status can be monitored in real time between warehouses, production areas and shipping points.

As indicated above, the IoT adds considerable challenges for the information security in AIS, as every new internet-enabled and networked device is another endpoint in the system (Romney et al., 2021). Traditionally, the number of input and output devices (computers, servers, printers, etc.) was limited (see section ‘Hardware’ earlier), with information security and access controls focused on them. Many additional devices now add many new access points to the system (Romney et al., 2021). Internal control systems need to address this new layer of risk to the integrity of AIS, adding complexity to their design (Wu et al., 2019). Added challenges may arise from the need for adequate computational power for the AIS to process a much higher amount of data into meaningful information (Sandner et al., 2020).

Artificial Intelligence

Artificial Intelligence (AI) aims to computerize typical human processes such as learning, reasoning and self-improvement (Romney et al., 2021) to simulate the style of human decision-makers (Hall, 2019). As such, they form expert systems (ESs) and decision support systems (DSSs) that can either provide the basis for human decision-making or even automate decisions (Romney et al., 2021). In imitating human decision making, AI can be employed in AIS to deal with complex and ambiguous situations in a fraction of the time (Gelinas et al., 2018), to automate mundane tasks (Marr, 2016) and to improve processes by detecting patterns in data and optimizing outcomes (Sandner et al., 2020). Often used synonymously to 'AI' is the concept of 'machine learning' that involves coding computers to 'think like human beings' (Marr, 2016) and is a current application of AI rather than a synonym to it.

AI has gained traction with the big accounting firms, used to review tens of thousands of documents, to evaluate compliance with accounting standards or to employ machine learning for detection of anomalies and potential fraud (Zhou, 2017). Natural language processing (NLG) is used, for example, by Deloitte to generate 50,000 tax returns annually for their clients, completing work in weeks instead of months.

The link between blockchain, IoT and AI

These three emerging technologies should not necessarily be seen as separate or mutually exclusive. They can act as complements as they converge towards the enablement of new business models (Sandner et al., 2020). In fact, actively interconnecting or even converging them may reduce their individual risks. As discussed earlier, IoT devices attach additional risks to the AIS. The subsequent increase in data volume also increases risks of fraud and theft. Here, blockchain technology may serve as an internal control and alleviate some of the risk when data is sent and received (Wu et al., 2019; Sandner et al., 2020). At the same time, blockchain can improve data transmitted and information quality in terms of standardization, interoperability, and compatibility (Sandner et al. 2020) as well as relevance, timeliness, faithful representation and comparability (Wu et al., 2019).

Further, the IoT devices can act and even make decisions autonomously when AI is leveraged (Salah et al., 2019; Sandner et al., 2020), as algorithms enable IoT devices to learn faster due to the much higher amount of data processed (Yin et al., 2019). Blockchain also benefits from AI being able to detect patterns of illicit activities and fraud in case the blockchain is fully or partially anonymous (Sandner et al., 2020).

Summary

This chapter detailed the technological underpinnings of AIS that are predominantly the same as for general corporate information systems. It detailed and discussed the technological perspective on networks, hardware and software that enable an AIS to record, process and display accounting information for reporting and decision-making. A main emphasis was placed on computer networks that not only enable AIS to record transactions in any part across a company, but also furnish the business with the computing power needed to process large amounts of data. Connected within a network are hardware that provides the physical resources, as well as software that enables the smooth operation of an information system. Common

standards like protocols facilitate the inclusion of various accounting software packages to create an efficient technological environment for running an AIS.

The future of AIS will continue to be inextricably linked to their technological underpinnings. With cloud computing offering processing power hitherto unavailable to many businesses (Strauss et al., 2015), emerging technological developments such as blockchain, IoT and AI have already started to rewrite the story of AIS technology in terms of higher security of and trust in data used in businesses, higher volumes of data captured and intelligent systems to automate mundane tasks and even decision-making. As such, the technological future of AIS seems a promising and bright one.

References

BBC (2016, July 6). US nuclear force still uses floppy disks. *BBC Online*. http://www.bbc.co.uk/news/world-us-canada-36385839.

Boczko, T. (2007). *Corporate Accounting Information Systems*. Harlow: FT Prentice Hall.

Brandas, C., Megan, O., and Didraga, O. (2015). Global perspectives on accounting. information systems: mobile and cloud approach. *Procedia Economics and Finance*, 20, 88-93.

Curtis, G., and Cobham, D. (2005). *Business Information Systems: analysis, design and practice*. 5e. Harlow: FT Prentice Hall.

Dutta, S. (2020). *The Definitive Guide to Blockchain for Accounting and Business*. Bingley: Emerald publishing.

Eurostat (2020). Digital economy and society statistics - enterprises. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_enterprises#Access_and_use_of_the_internet.

Gelinas, U.J., Dull, R.B., Wheeler, P.R., and Hill, M.C. (2018). *Accounting Information Systems*. 11e. Boston: Cengage Learning.

Ghasemi, M., Shafeiepour, V., Aslani, M., and Barvayeh, E. (2011). The impact of Information Technology (IT) on modern accounting systems. *Procedia – Social and Behavioral Sciences*, 28, 112-116.

Granlund, M. (2011). Extending AIS research to management accounting and control issues: A research note. *International Journal of Accounting Information Systems*, 12(1), 3-19.

Hall, J.A. (2019). *Accounting Information Systems*. 10e. Boston: Cengage Learning.

Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., and Henry, J. (2017). *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Indianapolis: Cisco Press.

Hart, L. (2018, May 21). What you should know about smart speakers at work. *CPA Insider*. https://www.journalofaccountancy.com/newsletters/2018/may/smart-speakers-work.html.

Hurt, R.L. (2016). *Accounting Information Systems – Basic Concepts and Current Issues*. 4e. New York: McGraw-Hill Education.

Kranz, M. (2017). *Building the Internet of Things*. Hoboken: Wiley.

Lin, A., and Chen, N.-C. (2012). Cloud computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, 32(6), 533-540.

Magal, S.R., and Word, J. (2012). *Integrated Business Processes with ERP Systems*. Hoboken: John Wiley & Sons.

Marr, B. (2016, Dec 6). What Is The Difference Between Artificial Intelligence and Machine Learning? *Forbes*. https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/?sh=4e23c32e2742.

Mazhelis, O., Luoma, E., and Warma, H. (2012). Defining an Internet-of-Things Ecosystem, 1-14. In: S. Andreev, S. Balandin, and Y. Koucheryavy, eds. (2012). *Internet of Things, Smart Spaces, and Next Generation Networking*. Berlin: Springer.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

O'Donnell, E., & David, J. S. (2000). How information systems influence user decisions: a research framework and literature review. *International Journal of Accounting Information Systems*, 1(3), 178-203.

Quinn, M., and Kristandl, G. (2014). *Business Information Systems for Accounting Students*. London: Pearson.

Ramakrishnan, R. and Gaur, L. (2019). *Internet of Things – Approach and Applicability in Manufacturing*. Boca Raton: CRC Press.
Romney, M.B, Steinbart, P.J., Summers, S.L., and Wood, D.A. (2021). *Accounting Information Systems.* 15e. Harlow: Pearson.
Richardson, V.J., Chang, C.J., and Smith, R. (2014). *Accounting Information Systems*. New York: McGraw-Hill Education.
Salah, K., Rehman, M. H., Nizamuddin, N., and Al-Fuqaha, A. (2019). Blockchain for AI: review and open research challenges. *IEEE Access*, 7, 10127–10149.
Sandner, P., Gross, J., and Richter, R. (2020). Convergence of Blockchain, IoT, and AI. *Frontiers in Blockchain.* 3. https://www.frontiersin.org/article/10.3389/fbloc.2020.522600
Shinder, D.L. (2001). *Computer Networking Essentials*. Indianapolis: Cisco Press Core Series.
Strauss, E., Kristandl, G., and Quinn, M., (2015). The effects of cloud technology on management accounting and decision-making. *CIMA Research executive summary series*, 10(6).
Tanenbaum, A.S., and Wetherall, D.J. (2021). *Computer Networks*. 6e. Boston: Pearson.
Trigo, A., Belfo, F., and Estebanez, R.P. (2014). Accounting Information Systems: The Challenge of the Real-Time Reporting. *Procedia Technology*, 16, 118-127.
Wisna, N. (2013). The Effect of Information Technology on the Quality of Accounting Information system and Its impact on the Quality of Accounting Information. Research *Journal of Finance and Accounting*, 4(15), 69-75.
Wu, J., Xiong, F., and Li, C. (2019). Application of Internet of Things and Blockchain Technologies to Improve Accounting Information Quality. *IEEE Access*, 7, 100090-100098.
Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., and Vatrapu, R. (2019). Regulating cryptocurrencies: a supervised machine learning approach to deanonymizing the bitcoin blockchain. *Journal of Management Information Systems*, 36(1), 37–73.
Zissis, D., and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592.
Zhou, A. (2017, November 14). EY, Deloitte And PwC Embrace Artificial Intelligence For Tax And Accounting. *Forbes.* https://www.forbes.com/sites/adelynzhou/2017/11/14/ey-deloitte-and-pwc-embrace-artificial-intelligence-for-tax-and-accounting/?sh=342ce9b73498.